Okoseszközök

Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára

BÁNYÁSZ PÉTER – BODÓ ATTILA PÁL – KAPITÁNY SÁNDOR – SZABÓ ANDRÁS – ORBÓK ÁKOS – ZÁMBÓ NÓRA

Nemzeti Közszolgálati Egyetem, Budapest

A Nemzeti Közszolgálati Egyetem kiadványa

Szerzők:
Bányász Péter
dr. Bodó Attila Pál
Kapitány Sándor
Orbók Ákos
Szabó András
dr. Zámbó Nóra

Szakmai lektor:
Dr. Krasznay Csaba

A hatályosítást 2022-ben végezte:
Mikula Fanni

A hatályosításért felelős szakmai szakértő:
Legárd Ildikó

A hatályosított kézirat lezásrásának dátuma:
2022. február 25.

Eredeti megjelenés éve:
2016

Kiadja:

Közigazgatási Továbbképzési Intézet

Felelős kiadó:
Prof. Dr. Kis Norbert
rektorhelyettes

TARTALOM

I. DR. BODÓ ATTILA PÁL – DR. ZÁMBÓ NÓRA: OKOSTELEFONOK INFORMÁCIÓBIZTONSÁGI ÉS ADATVÉDELMI KIHÍVÁSAI A SZABÁLYOZÁSI KÖRNYEZET OLDALÁRÓL

1. Információbiztonsági és adatvédelmi alapvetés

1.1. Bevezető gondolatok

Az ezredfordulót követően a mobil eszközök világában ugrásszerűen bekövetkező változások új kihívások elé állították a piac és az állam szereplőit. A rohamosan növekvő értékesítési mutatók, a sorozatban megjelenő fejlesztések és az azokat generáló felhasználói igények nemcsak technológia és biztonsági problémákat és azok megoldását, hanem számos szabályozási kérdést is felvetnek mind az állam, mind a szakmai szervezetek részéről. A mobil eszközök piacán az egyik legelterjedtebb és legkeresettebb termék az okostelefon, amely esetén a felmerülő kockázatokat számba véve több szempontot is szükséges figyelembe venni, így:

a) mely korcsoport (gyermek, felnőtt),
b) milyen célból (magán, üzleti),
c) milyen funkciók (alkalmazások)

tekintetében használja az eszközt, amely használat meghatározza a várható fenyegetettséget és az ezzel összefüggő kockázatokat. Emellett az okostelefonoknál eltérő igényekkel kell szembe nézni a készülék és annak hordozhatóságából adódóan az „útköben” felmerülő biztonsági kihívásokkal kapcsolatban.

A használati szokások kapcsán felmerülő és a mobilitásból adódó kockázatokhoz szükséges igazítani a biztonsági intézkedéseket, a lopás, eltulajdonítás elleni védelemtől kezdve, a hálózati kapcsolatok és a kényelmi funkciók – részleges vagy átmeneti – tiltásán át, egészen az adatok titkosításáig. Mindemellett olyan alapvető felhasználói magatartásokat is szükséges megjegyezni és alkalmazni, mint a PIN-kód rendszeres használata, az IMEI szám feljegyzése, webes felületen a mobilszám megadásának mellőzése, az alkalmazások telepítése előtt azok ellenőrzése, valamint a publikus WiFi hálózatok kerülése. A felelőtlen eszközhasználat komoly problémákat okozhat, amelyek megelőzése érdekében az eszközön meglévő biztonsági beállítások használatával minimális biztonsági intézkedéseket a felhasználó maga is megtehet. Fentiek magatartásokon túl ilyen a helymeghatározó és az adathálózat üzemmód (3G/4G) – átmeneti vagy teljes – kikapcsolása, a QR kódok linkjeinek előzetes ellenőrzése, amellett, hogy tanácsos vírusirtó szoftver feltelepítése okostelefonunkra. Fokozott védelem biztosítható a be- és kimenő adatforgalom szűrésével (WiFi-n és 3G-n) és rendszeres törléssel (mind az internet előzmények, mind az adatok tekintetében).

Ezzel azonban a felhasználó által megtehető – egyszerűbb – intézkedések köre bezárul, a megjelenő kihívások komplex kezelése azonban ezen túlmutat, ezért szükséges a piac és az állam szerepvállalása is. Utóbbi szereplőnek, mint a közhatalom birtokosának legerősebb és legszélesebb körre kiterjedő eszköze a szabályozás. Jelen tananyag célja, hogy mind a nemzeti, mind a nemzetközi jogi környezetet áttekintve kitekintést nyújtson a hatályos jogi normák rendszerére. Az áttekintés azonban nem lehet teljes körű néhány elméleti alapvetés és a fogalmi keretek számbavétele nélkül.

1.2. Alapvetés az adatvédelemhez és az információbiztonsághoz

Az áttekintés első lépése az adatvédelem és az információbiztonság fogalmi alapjainak felvázolása, amely jelentőségét az adja, hogy napról napra nő a társadalom tagjainak – legyen az magán- vagy jogi személy – irányába bekövetkezett biztonsági fenyegetések és események száma. Gondoljunk csak az elmúlt időszakban bekövetkezett adatlopások kiemelkedő számára, amely során mind személyes – esetenként különleges személyes –, mind üzleti adatok jogosulatlan megszerzésére került sor, úgy, hogy eközben az adatokat kezelő elektronikus információs rendszerek is sérültek. Ezen események nem csak az adatvédelem fontosságára, hanem az elektronikus információk sebezhetőségére, valamint az elektronikus információs rendszerek kitettségére is rávilágítottak. Az elektronikus információs rendszerekben akár csak átmenetileg bekövetkező működési zavarok, valamint az ezekben kezelt adatok, információk jogosulatlan megszerzése, időszakos kiesése, megsemmisülése, vagy bizalmasságának sérülése jelentős kihatással van a szervezet, a gazdaság, az állam működésére, a társadalom – minden tagjának – életére. Ennek hatására tehát az adatok védelme mellett az azokat tároló és kezelő elektronikus információs rendszerek védelmét is biztosítani kell. De mi a különbség, és egyáltalán van-e különbség adat és információ, adat- és információvédelem, illetve adatbiztonság és információbiztonság között?

E kérdések megválaszolására számtalan megközelítés létezik, megszámlálhatatlan azoknak a szakkönyveknek, szakcikkeknek, tudományos munkának vagy jegyzeteknek a száma, amelyek rávilágítanak e kettő közötti különbségre. Jelen fejezetnek a célja kizárólag gyakorlati szempontból történő rendszertani alapvetés rögzítése, a részletes kifejtés és ismertetés mind célját, témáját és terjedelmét tekintve túlmutat ezen jegyzeten. Anélkül, hogy a legegyszerűbb forrást választva a magyar értelmező kéziszótár meghatározásait számba vennénk általános megközelítés szempontjából vizsgálva alapvetésként rögzíthetjük, hogy az adat az információ hordozója.

Ezen alapvetést elfogadva különbség abban található, hogy az *adat* közlésre, megjelenítésre vagy további feldolgozásra alkalmas entitás, amely számos megjelenési formát vehet fel (pl.: alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása. Az *információ* valamilyen megfigyelés, tapasztalat vagy ismeret, amely által következtetések vonhatók le és döntések alapjául szolgálhat. Az információ, ha úgy tetszik nem más, mint a jelentéssel felruházott adat, azaz adatból akkor lesz információ, ha valamiről informál.[1]

Az adat és az információ tehát eltérő jelentéstartalommal felruházott fogalmak, amelyek tartalmukat tekintve eltérő védelem és biztonság fogalommal rendelkeznek különösen akkor, ha elfogadjuk azt az alapvetést, hogy védelem az a tevékenység, amely a biztonság állapotának elérésére szolgál. Ezen meghatározásból kiindulva az *adatvédelem* központi eleme az adatkezelés jogszerűségét biztosító – főként szabályozási – tevékenységek, elsősorban a védelmet biztosító szabályok és eljárások, valamint az adatkezelési eszközök és módszerek összessége. Az adatvédelemmel szemben az *adatbiztonság* meghatározása alatt alapvetően az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében.

Az *információvédelem* összetettsége miatt a definíciós meghatározás helyett, azokat a tevékenységeket rögzítjük, amelyekkel maga a védelmi tevékenyég leírható. Ide sorolható az információt hordozó entitások (személyek és eszközök) védelme, azaz az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az irat- és dokumentumvédelem, valamint a személyi védelem is. Az információvédelem célja – hasonlóan az adatvédelemhez – a jogosulatlan hozzáférés,

[1] *Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz* felhasználásával – Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016. április 21. oldal

módosítás vagy megsemmisítés elleni védelem és az információk folyamatos rendelkezésre állásának biztosítása. Az *információbiztonság* – a hatályos nemzeti szabályozás alapvetéseiből kiindulva – olyan követelményrendszerként jellemezhető, amely középpontjában:

a) a bizalmasság (csak az arra jogosult és csak a jogosultság szintje szerint férhet az adathoz és használhatja fel),
b) a sértetlenség (az adat hitelessége és megváltoztatásának elkerülése), és
c) a rendelkezésre állás (az adatok elérhetőek és felhasználhatóak legyenek)

jelenik meg[2], függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (pl.: alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg.

Fenti elméleti alapvetést követően – igazodva a hatályos törvényi rendelkezésekhez – a továbbiakban az okostelefonokhoz kapcsolódó adatvédelemi és információbiztonsági szabályozásról (elektronikus információbiztonságról) szól jelen jegyzet, mivel a védelmi és biztonsági szempontok meghatározásánál az adatok és információk megjelenési formája és hordozója eltérő szabályozást igényel.

Az okostelefonok esetében szabályozási szempontból az adatvédelmi szempontú megközelítés az eszközökön tárolt adatok hozzáférhetőségre és azok felhasználásra vonatkozik, míg az információbiztonsági szempontú megközelítés az okos eszközökkel végzett „műveletekre" és az eszközökön futtatott IT rendszerekre és alkalmazásokra, mint elektronikus információs eszközökre vonatkozik.

2. Rendszertani és szabályozási környezet

Az adatvédelemre és az információbiztonságra vonatkozó szabályozási környezetre megfelelő szintű tagoltság jellemző. A szabályozás a jogforrási hierarchia mentén a törvényi rendelkezésekből és a törvényi felhatalmazás alapján megalkotott végrehajtási rendeletekből kiindulva a közjogi szervezetszabályzó eszközök szintjéig (pl.: központi államigazgatási szerv vagy fővárosi és megyei kormányhivatal vezetője által kiadott Adatvédelmi Szabályzat, Informatikai Biztonsági Szabályzat) tart, figyelemmel Magyarország Alaptörvénye T) cikkének és a jogalkotásról szóló 2010. évi CXXX. törvény rendelkezéseire. Jelen fejezet célja a jogforrási hierarchia mentén a nemzeti főbb szabályzók számbavétele – amelyek részleteit a 3. és 4. fejezetek tartalmazzák – és az európai uniós kapcsolódások bemutatása – utóbbi esetében a gyakorlati adaptációt az 5. fejezet tartalmazza.

2.1. Nemzeti szabályozás

Magyarország Alaptörvénye, mint a jogforrási hierarchia csúcsán álló jogszabály az információs alapjogokat – a személyes adatok védelmét és a közérdekű adatok nyilvánosságát – közös bekezdésben rögzíti. Az Alaptörvény VI. cikk (2) bekezdése szerint *„Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez."*[3]. Az Alaptörvény szövegezése nem szakít a korábbi Alkotmány[4] elveivel, így bár az e tárgykörben hozott 15/1991. (IV. 13.) AB határozat az Alaptörvény 5. pontja alapján hatályát vesztette, a határozat által kifejtett joghatások mellett az értelmezési keretek véleményünk szerint napjainkban is helytállóak.

[2] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján
[3] Magyarország Alaptörvénye, VI. cikk (2) bekezdés
[4] 1949. évi XX. törvény 59. § és 61. §-ai

Az Alkotmánybíróság rögzíti: *„Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is. Az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel az Alkotmány 8. §-ában megkövetelt feltételeknek.”*[5] Az Alkotmánybíróság ezen határozatában az információs önrendelkezési jog gyakorlásának feltételeként és garanciális elemeként rögzítette a célhoz kötöttség, az adattovábbítás és az adatok nyilvánosságra hozása korlátozása elvét és részletesen kifejtette ezen elvek egymáshoz való viszonyát. A célhoz kötöttség elvéhez kapcsolódóan az Alkotmánybíróság azt is kimondta, hogy a meghatározott cél nélküli „készletre”, azaz az előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és adattárolás, az un. „adatkészletezés” alkotmányellenes.[6] Ezen – máig érvényes elveket tartalmazó – döntésével az Alkotmánybíróság már az 1990-es évek elején rámutatott arra, hogy az alapjogok korlátozására alkotmányos keretek között, meghatározott elvek mentén kerülhet sor. Emellett elvi alapvetésként kell rögzíteni, hogy az alapjogok korlátozása nem lehet önkényes.

Az Alaptörvény kimondja, hogy *„Az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható.”*[7] Az alapjogi konfliktusok feloldásának, az alapjogok korlátozásának alkotmányossági megítélésének módszere az alapjogi teszt, az ún. szükségességi-arányossági teszt. A teszt lényege az a kétlépcsős eljárás, amely során először a jogkorlátozás céljának vizsgálatát, azaz a szükségességet kell elvégezni (pl.: más alapjogokkal való összeütközés), majd az alkalmazott jogkorlátozás mértékéről, azaz az arányosságról kell dönteni. A második lépcsőben külön szükséges vizsgálni, hogy ésszerű (alkalmas), elengedhetetlen (szükséges) és arányos (cél és az okozott jogsérelem arányban áll-e egymással) az alkalmazott korlátozás vagy felfüggesztés. Ezen garanciális elvek érvényesítése érdekében az Alaptörvény rendelkezik arról, hogy fenti információs alapjogok érvényesülését sarkalatos törvénnyel létrehozott független hatóság – A Nemzeti Adatvédelmi és Információszabadság Hatóság – ellenőrzi.[8]

2012. január 1-től hatályos az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), amely – megtartva a korábbi szabályozás[9] főbb elveit – az információs alapjogok védelme céljából meghatározza az adatkezelés általános követelményeit és a védelem garanciális elemeit. Az Infotv. a hatálybalépését követően – az Alaptörvényben rögzített és fentebb említett hatóság létrehozása érdekében – újrafogalmazta és átrendezte az adatvédelem felügyeleti rendszerét és annak az államszervezetben elfoglalt helyét. A szabályozást áttekintve érzékelhető, hogy az adatvédelem komplex kérdésköre nem kezelhető egyetlen törvényben, az adatkezelés speciális, ágazati szabályait számos kapcsolódó jogszabály tartalmazza, amely az Infotv.-ben neghatározott általános szabályrendszert egészíti ki. (Az Infotv. kapcsolódó szabályainak ismertetésére a 3. fejezetben kerül sor.)

Az Alaptörvényben rögzített és az Infotv.-ben részletezett alapjogok kiemelt védelméből adódóan a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) XXI. fejezete az emberi méltóság és egyes alapvető jogok elleni bűncselekmények körébe emeli a személyes adattal való visszaélés cselekményét[10]. A törvényi tényállás szerint a személyes adattal való visszaélés vétségét

[5] 15/1991. (IV. 13.) AB határozat Indokolás II. fejezet
[6] 15/1991. (IV. 13.) AB határozat Indokolás II. fejezet
[7] Magyarország Alaptörvénye, I. cikk (3) bekezdés
[8] Magyarország Alaptörvénye, VI. cikk (3) bekezdés
[9] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény
[10] Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 219. §

követi el, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével:

a) haszonszerzési célból vagy jelentős érdeksérelmet okozva:
  aa) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
  ab) az adatok biztonságát szolgáló intézkedést elmulasztja,
b) az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

Az elkövető a vétség elkövetése miatt egy évig terjedő szabadságvesztéssel büntetendő. Ha a cselekményt különleges adatra vagy bűnügyi személyes adatra követik el, a büntetés két évig terjedő szabadságvesztés. Ha a visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el a cselekmény bűntettnek minősül és három évig terjedő szabadságvesztéssel büntetendő.

A Btk. a XXI. fejezetben az Infotv. rendelkezéseivel összhangban a közérdekű adattal visszaélés cselekményét is pönalizálja. A közérdekű adattal visszaélés vétségét követi el és két évig terjedő szabadságvesztéssel büntetendő, aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével:

a) közérdekű adatot az adatigénylő elől eltitkol, vagy azt követően, hogy a bíróság jogerősen a közérdekű adat közlésére kötelezte, tájékoztatási kötelezettségének nem tesz eleget,
b) közérdekű adatot hozzáférhetetlenné tesz vagy meghamisít, illetve
c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz.

Ha a közérdekű adattal visszaélést jogtalan haszonszerzés céljából követik el a cselekmény bűntettnek minősül és három évig terjedő szabadságvesztéssel büntetendő.[11]

Az Infotv. rögzíti, hogy ha a Nemzeti Adatvédelmi és Információszabadság Hatóság az eljárása során:

a) bűncselekmény elkövetésének alapos gyanúját észleli, büntetőeljárást kezdeményez,
b) ha szabálysértés vagy fegyelmi vétség elkövetésének alapos gyanúját észleli, szabálysértési, illetve fegyelmi eljárást kezdeményez

az eljárás lefolytatására jogosult szervnél.[12]

Az adatok védelme terén az Infotv. mellett – bár a társadalom tagjainak körében kevésbé ismert – kiemelt jelentőségű szabályozás a 2010 év végén kihirdetett, a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény, majd az ezt felváltó, a nemzeti adatvagyonról szóló 2021. évi XCI. törvény (a továbbiakban: Adatvagyon tv.), amely nemzeti adatvagyonként a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összességét[13] határozza meg. Az állam felismerve annak jelentőségét, hogy az általa kezelt nemzeti adatvagyon körébe tartozó alapadatok az állam és a közigazgatás működéséhez elengedhetetlenek, kiemelt jelentőséget tulajdonított ezen adatok védelmének a szabályozás megalkotásával.

Az Adatvagyon tv. kimondja[14], hogy a nemzeti adatvagyon részét képező adatállomány tekintetében törvény az adatfeldolgozással megbízható személyek és szervezetek körét korlátozhatja, vagy az adatfeldolgozásnak az adatkezelőtől különböző személy vagy szervezet általi ellátását kizárhatja. Az adatok védelme érdekében az Adatvagyon tv. rendelkezik arról is, hogy nemzeti adatvagyon esetében adatfeldolgozást csak államigazgatási szerv vagy kizárólagos állami tulajdonú gazdálkodó szervezet láthat el. Kiegészítő szabályként rögzíti, hogy az adatkezelő kizárólag a Kormány rendeletében az adott nyilvántartás tekintetében meghatározott szervvel vagy szervezettel köthet adatfeldolgozási

[11] Btk. 220. §
[12] Infotv. 70. §
[13] A nemzeti adatvagyonról szóló 2021. évi XCI.. törvény (a továbbiakban. Adatvagyon tv.) 2. § a) bekezdés
[14] Adatvagyon tv. 12. § (1)–(2) bekezdések

szerződést, és ha ez esetben meghatározott adatfeldolgozó igénybevétele kötelező, az adatkezelő ezen adatfeldolgozót bízhatja csak meg az adatfeldolgozással. Ezen szervek körét a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet melléklete tartalmazza.

Az Adatvagyon tv. kimondja továbbá, hogy ezen nyilvántartásokhoz kapcsolódó adatfeldolgozási műveletet az adatfeldolgozó kizárólag Magyarország területén végezhet.[15]

Amennyiben a fent említett korlátozás valamely adatkezelő esetében a jogszabályban előírt feladatok határidőben történő teljesítését, vagy a rendelkezésre álló erőforrások szűkössége miatt a jogszabályban előírt feladatok teljesítéséhez szükséges fejlesztések határidőben történő megvalósítását veszélyezteti, az adatkezelő szakmai irányítására vagy felügyeletére kijelölt miniszter előterjesztésére a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter a korlátozás alól egyedi felmentést adhat.

Egyedi felmentés adható az időszakosan jelentkező adatfeldolgozási feladatok hatékony ellátásának biztosítása érdekében is, ha azok határidőben való ellátása a rendelkezésre álló erőforrások mellett más módon nem lehetséges. Az egyedi felmentés határozott időre adható meg.[16]

Az Adatvagyon tv. alkalmazásában a nemzeti adatvagyon a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.[17] Tartalmát tekintve ide sorolhatók az állami vagy helyi önkormányzati feladatot, továbbá jogszabályban meghatározott egyéb közfeladatot ellátó szervek vagy személyek kezelésében lévő hatósági nyilvántartási adatok, jogi normákkal és egyéb szervezeti normákkal összefüggő adatok, közművelődési és kulturális gyűjteményi adatok, illetőleg más (pl. levéltári) archívumok adatai, ezen felül statisztikai adatok, topográfiai és más téradatok, meteorológiai adatok, a közfeladat-ellátással és a közszolgáltatás-nyújtással összefüggő egyéb leíró adatok.[18]

Ilyen széles adatkör és kiemelt védelem tekintetében az Adatvagyon tv. célja a nemzeti adatvagyon körébe tartozó nyilvántartások biztonságának megteremtése, ezen nyilvántartások jogszerű felhasználását akadályozó cselekmények bűncselekménnyé nyilvánításával azok megelőzése. A Btk. XXV. fejezete nevesíti a nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekményt.A Btk. szerinti tényállás alapján[19] nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény esetén – ha más, súlyosabb bűncselekmény nem valósul meg – bűntett miatt három évig terjedő szabadságvesztéssel büntetendő, aki a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatot az adatkezelő részére hozzáférhetetlenné tesz, vagy a nemzeti adatvagyon körébe tartozó állami nyilvántartás működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza. Ha a bűncselekmény jelentős érdeksérelmet okoz, vagy a bűncselekményt haszonszerzés végett követik el, a büntetés egy évtől öt évig terjedő szabadságvesztés.

Az információbiztonság szabályozási környezetének kialakításával összefüggő első jogalkotási lépés az Országgyűlés 2013. április 15-ei ülésnapján elfogadott, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.). Az Ibtv. elkészítésével párhuzamosan került 2013 márciusában elfogadásra Magyarország Nemzeti Kiberbiztonsági Stratégiája[20] (a továbbiakban: Kiberstratégia), amely elemezte Magyarország aktuális kiberbiztonsági helyzetét, jövőképét, továbbá megnevezte az aktuálisan elérendő célokat és az alkalmazandó eszközöket. Az Ibtv. az elektronikus információs rendszerekben tárolt, kezelt információk védelmét célozza és olyan szabályozási környezet alapjait teremti meg, amely a prevenciót, a fenyegetéseket számba vevő, az elektronikus információs rendszer minden elemére kiterjedő védelmet, illetve az

[15] Adatvagyon tv. 13. §

[16] Adatvagyon tv. 12. § (5)-(6) bekezdések

[17] Adatvagyon tv. 2. § a) pont

[18] *Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz* – Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016. április, 19. oldal

[19] Btk. 267. § (1) bekezdés

[20] 1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

elektronikus információbiztonság tudatosságnövelését tekinti alapvetésnek. A törvény végrehajtását számos végrehajtási rendelet segíti. Az Ibtv. és végrehajtási rendeleteinek ismertetésére – kitérve a Kiberstratégia főbb rendelkezéseire – a 4. fejezetben kerül sor.

Az eddigiekben leírtak alapján nem szükséges annak részletes kifejtése, hogy az állam – az információs alapjogok és a nemzeti adatvagyon védelme mellett – milyen védelem- és biztonságpolitikai célok érdekében határozta meg azokat az információs rendszerekkel összefüggő magatartásszabályokat, amelyeket büntetni rendel. Ez esetben is kiemelten fontos érdek, hogy az információs rendszerek, az abban kezelt adatok, a felhasználók és az üzemeltetők védelme biztosított legyen.

A Btk. önálló tényállásként szabályozza az információs rendszerekkel kapcsolatos bűncselekményeket, ezzel is kiemelve az információbiztonsághoz és az adatvédelemhez fűződő társadalmi érdek fontosságát. A Btk. alapján információs rendszer alatt az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezést, vagy az egymással kapcsolatban lévő ilyen berendezések összességét kell érteni[21].

A Btk. a vagyon elleni bűncselekmények között szabályozza *az információs rendszer felhasználásával elkövetett csalást*.[22] A bűntettet az valósítja meg, aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz. A kár bekövetkezésére az információs rendszer jogtalan befolyásolása miatt kerül sor. Alapesetben 3 év szabadságvesztéssel rendeli büntetni a jogalkotó a cselekményt, amely az okozott kár mértékétől függően akár 5 évtől 10 évig terjedő szabadságvesztés büntetéssel jár.

A *tiltott adatszerzés*[23] bűntett azáltal valósul meg, hogy az elkövető a személyes adatot, magántitokot, gazdasági titokot vagy üzleti titokot jogosulatlan módon akarja megismerni. Ezen adatok jogosulatlan megszerzése megvalósulhat:

- más lakásának, egyéb helyiségének vagy az azokhoz tartozó bekerített helynek a titokban való átkutatásával,
- az ott történtek technikai eszköz alkalmazásával való megfigyelésével, rögzítésével;
- más postai vagy egyéb zárt küldeményének felbontásával vagy megszerzésével, és tartalmának technikai eszközzel való rögzítésével;
- elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren másnak továbbított vagy azon tárolt adat kifürkészésével, és az észleltek technikai eszközzel való rögzítésével,
- információs rendszerben kezelt adatok titokban történő kifürkészésével, és az észleltek technikai eszközzel való rögzítésével.

A szabályozás szerint bűncselekménynek minősül az is, ha a fentiek szerinti információgyűjtésre a fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából kerül sor. Alapesetben 3 év szabadságvesztéssel rendeli büntetni a jogalkotó a cselekményt, minősített esetben (bűnszövetség, üzletszerűség, jelentős érdeksérelem okozása, hivatalos eljárás színlelése) a büntetési tétel 5 év is lehet.

Az *információs rendszer vagy adat megsértése*[24] bűncselekmény elkövetője olyan személy lehet, akinek a jogosultsága alapvetően kiterjed a szankcionált magatartásra (információs rendszerbe való belépés, adat megváltoztatása, törlése), azonban, ha e személy a jogosultsága kereteit túllépi, akkor már

[21] Btk. 459. § (1) bekezdés 15. pont
[22] Btk. 375. §
[23] Btk 422. §
[24] Btk. 423. §

bűncselekményt követ el. Az információs rendszerbe való jogosulatlan adatbevitel önmagában nem szankcionálandó magatartás, csak abban az esetben, ha az további, nem kívánt következményekhez vezet, így, ha a rendszer működését akadályozza. Az alaptényállás vétség, melyet a Btk. két évig terjedő szabadságvesztéssel rendel büntetni.

Az *információs rendszer védelmét biztosító technikai intézkedés kijátszása* bűncselekmény[25] tényállása akkor valósul meg, ha az elkövető az információs rendszer felhasználásával elkövetett csalás, illetve az információs rendszer vagy adat megsértése bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

- jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve
- jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja.

A tényállással összefüggően büntethetőséget megszüntető oknak minősíti a Btk. az eljáró hatósággal való együttműködést (tevékenység hatóság előtti felfedése, az elkészített dolognak a hatóság részére történő átadása, a készítésben részt vevő más személy kiléte megállapításának lehetővé tétele). Az alaptényállás vétség, melyet a Btk. két évig terjedő szabadságvesztéssel rendel büntetni.

Fentiekben azokat a főbb jogforrásokat vettük sorra, amelyek az adatvédelem és az információbiztonság szempontjából releváns szabályzók és minden egyéb, a jogforrási hierarchia alsóbb szintjén álló jogszabály vagy szabályzó ezek rendelkezéseihez zsinórmértékként viszonyul. Az alapjogi szabályozás érvényesítésétől kezdve egészen azon közhatalom birtokában végezhető, állami kényszerrel kikényszeríthető szabályokig terjedt e kör, melyek végső soron, mint ultima ratio egyes alapjogok korlátozásához is vezethetnek. Az adtvédelem és az információbiztonság témakörét érintően számos további szabályzó (ágazati törvények, végrejhajtási rendeletek) tartalmaz speciális rendelkezéseket vagy részletszabályokat, ezek ismertetése azonban jelen jegyzet kereteit – azok egyedi és specifikus jellegét tekintve – meghaladja.

2.2. Európai uniós kapcsolódások

A következőkben az Európai Unió digitális világot érintő szabályozási keretrendszerét mutatjuk be. A bemutatás a 2010. évet követő dokumentumokra szorítkozik. Ennek oka az, hogy a pénzügyi és gazdasági világválság következményeinek kezelése új gondolkodásmódot követelt meg az Euroóai Unió vezetőitől. A fenntartható fejlődés és a jövő érdekében hosszútávú, tíz éves (jellemzően 2020-ig szóló) stratégiai tervdokumentumok születettek, melyeknek a jelenkor és az eljövendő időszak kihívásaira és dinamikus modernizációjára, valamint az erőteljes globalizációra válaszul szerves részét képezi a tudáson és innováción alapuló gazdaság kialakítása.

Elsőként az elkövetkezendő évek intézkedései alapdokumentumának számító *Europa 2020 foglalkoztatási és növekedési stratégiát*[26] ismertetjük (a továbbiakban: Europa 2020 stratégia).

Az Európai Unió 2010-ben azzal a céllal alkotta meg az Europa 2020 stratégiát, hogy megteremtse az *intelligens* (hatékonyabb oktatási, kutatási és innovációs beruházások, valamint a digitális társadalom fejlesztése), *fenntartható* (erőforrás-hatékonyabb, környezetbarátabb és versenyképesebb gazdaság) és *inkluzív* (a gazdasági, szociális és területi kohéziót előmozdító, magas foglalkoztatási arányt biztosító gazdaság) növekedés feltételeit. Fontos, hogy az Europa 2020 stratégia az európai uniós

[25] Btk. 424. §

[26] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF

intézmények, a tagállamok és a szociális partnerek közös stratégiája, azaz valamennyi címzettnek azonosulnia kell a stratégia célkitűzéseivel, és meg kell tennie az ezen célkitűzések végrehajtását szolgáló ütemezett intézkedéseket[27].

Az Intelligens növekedés prioritásban az Europa 2020 stratégia beavatkozási területként rögzítette a digitális társadalmat. Megállapítja ugyanis, hogy az információs és kommunikációs technológiák iránti globális kereslet 2 000 milliárd EUR értékű piacot jelent, ennek azonban csak negyede származik európai vállalkozásoktól. Európában elmaradás tapasztalható továbbá a nagy sebességű internet használata terén is, ami – főként a vidéki területeken – hátrányos hatással van Európa innovációs képességére, a tudás online terjesztésére, valamint az áruk és szolgáltatások online forgalmazására.

Az Europa 2020 stratégia margóján 7 új kiemelt kezdeményezés indult, melyek esetében az Uniónak és a tagállami hatóságoknak össze kell hangolniuk intézkedéseiket. Az egyik ilyen kiemelt kezdeményezés – a digitális társadalom beavatkozási terület kapcsán felvázoltakra figyelemmel – az Intelligens növekedés célrendszerén belül az *Európai digitális menetrend*.

Az Europa 2020 stratégia célként fogalmazta meg az Európai digitális menetrend kapcsán, hogy:

a) a nagy sebességű és szupergyors internetre és az interoperábilis alkalmazásokra épülő egységes digitális piac révén fenntartható gazdasági és szociális előnyöket teremtsen,
b) 2013-ig mindenkinek szélessávú, 2020-ig pedig mindenki számára ennél is sokkal gyorsabb, legalább 30 Mbps sebességű internet-hozzáférést biztosítson,
c) az európai háztartások legalább fele a 100 Mbps-t meghaladó internetkapcsolatra szóló előfizetéssel rendelkezzen.

Az Európai digitális menetrend keretében tervezett intézkedések:

a) az egységes digitális piac megteremtése (az online tartalmakhoz való jogszerű hozzáférés, valamint az elektronikus fizetés és számlázás megkönnyítése),
b) az uniós adatvédelmi szabályozási keret felülvizsgálata,
c) távközlési szolgáltatások egységesítése,
d) fokozott interoperabilitás és szabványok,
e) készülékek, alkalmazások, adattárolók, szolgáltatások és hálózatok átjárhatóságának növelése,
f) bizalom és az internetes biztonság megerősítése,
g) nagy sebességű és szupergyors internet-hozzáférés mindenki számára,
h) befektetés a kutatásba és az innovációba,
i) digitális jártasság, a digitális készségek és a digitális integráció előmozdítása,
j) technológia intelligens használatából eredő előnyök kiaknázása a társadalom számára.

Jelen tananyag tematikáját érintően kiemelendő, hogy az Európai digitális menetrend problémaként rögzítette, hogy a számítógépes bűnözés terjedése miatt az emberek bizalmatlanok az online alkalmazásokkal és az internettel szemben, ezért nem szívesen használják azokat. Megoldási javaslatként a dokumentumban megfogalmazásra került, hogy meg kell erősíteni az infokommunikációs megoldások használatát számos olyan területen, ahol az uniós polgárok kézzelfoghatóan érzik ezen alkalmazások használatának előnyeit (pl. egészségügyi ellátás, méltóságteljes életvitellel, kultúra, e-közigazgatás fejlesztése, intelligens közlekedési rendszerek). Tovbbi célkitűzés a nagy sebességű és szupergyors internet-hozzáférés biztosítása minél szélesebb körben, ennek keretében a szélessávú lefedettség és az új generációs, szupergyors hálózatok kiépítése, a nyílt és technológia-semleges szolgáltatások elterjesztése.

[27] http://ec.europa.eu/europe2020/who-does-what/index_hu.htm

Az Európai Digitális Menetrend hét beavatkozási területe közül a Bizalom és biztonság intézkedési területen célként kerültek meghatározásra az alábbiak:

a) javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;
b) számítógépes támadások elleni gyorsreagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok (CERT) hálózatának létrehozása, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepének megerősítése;
c) javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról;
d) tudatosságnövelés, így többek között az internetes védelem iskolai oktatása;
e) egyebek mellett a gyermekbántalmazással, a személyazonosság-lopással és számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása;
f) magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten és azon kívül egyaránt.

A hét beavatkozási terület minden eleme kapcsolódik valamilyen mértékben a hatályos szabályozáshoz. A 4. fejezet részletes betekintést nyújt a hazai információbiztonsági szabályokba, az 5. fejezetben pedig bemutatjuk annak hazai stratégiai megalapozását is. Erre figyelemmel nem szabad figyelmen kívül hagynunk az információbiztonságot érintő uniós szabályozókat sem.

A kiberbiztonság kérdéskörét az Európai Unió hosszú időn keresztül csupán büntetőjogi szempontból kezelte, annak széles spektrumú átfogó áttekintését először az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága végezte el *„Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér”* című uniós stratégiáról szóló, 2013-ban közzétett közös közleményében (továbbiakban: uniós stratégia). Az uniós stratégia az alábbi prioritásokat vázolja fel:

a) az információs rendszerek kibertámadásokkal szembeni ellenálló képességének megteremtése;
b) a számítástechnikai bűnözés drasztikus visszaszorítása;
c) kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát érintő képességek fejlesztése;
d) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
e) az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése;
f) a számítógépes bűnözéssel foglalkozó nemzeti kiválósági központok hálózatának kialakítása és finanszírozása.

Az uniós stratégiában foglaltak egyfajta intézkedési tervének tekinthető *a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvjavaslat* (továbbiakban: irányelvjavaslat).

Az irányelvjavaslat előírásai között szerepelnek az alábbiak:

a) a tagállamok a hálózat- és információbiztonság területén illetékes hatóságok létrehozásával, hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-ek) felállításával és nemzeti hálózat- és információbiztonsági stratégiák és együttműködési tervek elfogadásával nemzeti szinten biztosítsák a képességek minimális szintjét;

b) az illetékes nemzeti hatóságoknak hálózatot kell alkotniuk, amelyben együttműködnek az összehangolt információcsere, valamint az uniós szinten történő felderítés és reagálás biztosítása érdekében; a tagállamok e hálózaton keresztül az európai hálózat- és információbiztonsági együttműködési terv alapján bonyolítják a hálózat- és információbiztonsági fenyegetések és események elleni küzdelemhez szükséges információcserét és együttműködést;
c) kialakuljon egy kockázatkezelési kultúra, és gyakorlattá váljon a magán- és a közszféra közötti információ-megosztás a hálózatokat és információs rendszereket komolyan veszélyeztető, valamint a kritikus szolgáltatások folyamatosságát és az áruellátást jelentősen befolyásolni képes biztonsági eseményekről;
d) a tagállamok nemzeti hálózat- és információbiztonsági stratégiát és együttműködési tervet készítsenek, hálózat- és információbiztonságért felelős nemzeti hatóságot jelöljenek ki, illetve ún. számítógépes vészhelyzeteket elhárító csoportot állítsanak fel a biztonsági események és kockázatok kezelésére;
e) az érintett vállalkozások és a közszféra számára bizonyos biztonsági követelmények kerüljenek meghatározásra és ezen szereplők számára esemény bejelentési kötelezettség álljon fenn.

Az Európai Bizottság 2015. április 28-án közzétett, *„Az európai biztonsági stratégia”* című közleménye (a továbbiakban: biztonsági stratégia) az együttműködés fontosságát hangsúlyozza valamennyi szinten: együttműködés az Európai Unió egyes szervei között és a tagállamokkal, azok hatóságaival.[28] A biztonsági stratégia ***a terrorizmus leküzdése és a radikalizálódás megelőzése, valamint a*** szervezett bűnözés felszámolása mellett alappillérként rögzíti a számítástechnikai bűnözés elleni harcot és annak legfőbb eszközeként a kiberbiztonságot határozza meg.

A számítástechnikai bűnözés elleni harc területén szükséges fellépések a biztonsági stratégia szerint:
a) a kiberbiztonsággal kapcsolatos meglévő szakpolitikai eszközrendszer végrehajtásának megerősítése, az információs rendszerek elleni támadások és a gyermekek szexuális kizsákmányolása elleni küzdelem előtérbe helyezése (a tagállami jogszabályok közelítése egymáshoz, továbbá együttműködés a tagállamokkal az irányelvek megfelelő végrehajtása érdekében);
b) a készpénz-helyettesítő fizetési eszközökkel kapcsolatos csalás és hamisítás elleni küzdelemmel foglalkozó jogi aktusok felülvizsgálata és esetleges kiterjesztése a pénzügyi eszközöket érintő bűncselekmények és hamisítás újabb formáinak figyelembevétele érdekében, és az ezzel kapcsolatos javaslatok előterjesztése 2016-ban (a kerethatározat 2001. évi kiadása óta felmerült legújabb technikai kihívásokra reagáló szabályozás megalkotása);
c) a számítástechnikai bűncselekmények ügyében folytatott nyomozások útjában álló, nevezetesen az illetékes joghatósággal és a bizonyítékokhoz és információkhoz való hozzáféréssel kapcsolatos akadályok felszámolása (új technológiák alkalmazása, magánszektorral történő együttműködés, valós idejű elektronikus bizonyítékok beszerzése);
d) a kiberbiztonsági kapacitásépítést célzó fellépések előmozdítása a külső támogatási eszközök keretében (a nemzetközi együttműködés terén hozzáadott értékkel bíró kezdeményezések támogatása, pl. budapesti egyezmény[29]).

[28] *„Az Unió által az elmúlt években létrehozott eszközök sikere mindenekelőtt az összes résztvevő szereplő – az uniós intézmények és ügynökségek, a tagállamok és a nemzeti hatóságok – közötti felelősség-megosztásra, kölcsönös bizalomra és hatékony együttműködésre épül.”* – Az Európai Bizottságnak az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának szóló, *„Az európai biztonsági stratégia”* című közleménye

[29] Az Európa Tanács egyezménye a számítógépes bűnözésről, Budapest, 2001. november 23.

Fentiek alapján érzékelhető, hogy az Európai Unió szabályozásának középpontjában a keretjellegű elvek és intézkedési javaslatok, döntések meghatározása áll, azok végrehajtása és az ehhez szükséges szervezetrendszer kialakítása önálló feladatként jelentkezik minden tagállam számára.

A szakanyag lezárását követően a Tanács 2019. április 9-én elfogadta azt a kiberbiztonsági jogszabályként is ismert rendeletet, amely lehetővé teszi az EU számára, hogy célzott korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést jelentenek az EU vagy annak tagállamai számára. [30]

2020 decemberében az Európai Bizottság és az Európai Külügyi Szolgálat (EKSZ) új uniós kiberbiztonsági stratégiát terjesztett elő (Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér).[31] E stratégia célja, hogy:

- megerősödjön Európa kiberfenyegetésekkel szembeni rezilienciája,
- minden polgár és vállalkozás megbízható szolgáltatásokat és digitális eszközöket vehessen igénybe, és ezek előnyeit teljes mértékben ki tudja használni,
- megőrizze a globális és nyílt internetet, biztosítékot nyújtva ugyanakkor arra, hogy a biztonság mellett az európai értékek és a mindenkit megillető alapvető jogok is védelmet élvezzenek.

2021. november 26-án az Európai Unió Tanácsa elfogadta az EU egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekkel kapcsolatos álláspontját, amely intézkedések célja, hogy tovább javuljon mind az állami, mind a magánszektornak, illetve az Unió egészének kiberrezilienciája és a kiberbiztonsági eseményekre való reagálási képessége. Elfogadását követően az új, „NIS 2” elnevezésű irányelv a hálózati és információs rendszerek biztonságáról szóló jelenlegi irányelv (NIS-irányelv) helyébe lép. [32]

3. Adatvédelem és az Infotv. szabályozási környezete

Az adatvédelmi szabályozás történeti fejlődését bemutató szakirodalmak általánosan rögzítenek olyan szakaszokat, melyek a technológiai fejlődés kihívásaira és a társadalom szerkezeti változásaira is reflektálnak. A magyar szakirodalom egy része három fázist különböztet meg. Az első generációs szabályozás az 1970-es években fejlődött ki és az állami, automatizált nyilvántartásokkal szembeni védelmet alakította ki. A második generációs szabályok az 1980-as, 1990-es években jelentek meg, melyek már a papíralapú nyilvántartásokat is a szabályozás hatálya alá vonták. Az ezredfordulón előtérbe kerülő harmadik generációs szabályok főbb jellemzői közé az európai integráció sajátosságainak figyelembe vételét, és a szektorális szabályok megjelenését soroljuk.[33] Napjainkban egyre több szerző foglalkozik a szabályok kiegészítésével, vagy ha tetszik, egy újabb generációs szabályozás szükségességével és megjelenésével, amelynek középpontjában az információs társadalom, az infokommunikáció térhódításából eredően az Internet és az önszabályozás kérdése áll. Jelen fejezetnek nem célja az adatvédelmi szabályozás történeti áttekintése, az egyes főbb irányok melletti elköteleződés, azonban a főbb mérföldkövek rövid bemutatása szükséges ahhoz, hogy az Infotv. rendelkezéseivel összhangban az újabb – negyedik vagy harmadik (amely attól függ, hogy mely főáram tanait követjük[34]) – generációs szabályozás igényét felismerjük.

[30] AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”)

[31] Lásd: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001

[32] Bővebben lásd: https://www.consilium.europa.eu/hu/press/press-releases/2021/12/03/strengthening-eu-wide-cyber-security-and-resilience-council-agrees-its-position/

[33] Majtényi László: Az információs jogok. In: Halmai Gábor – Tóth Gábor Attila (szerkesztők): *Emberi jogok.* Osiris Kiadó, 2003. 582–583. oldal

[34] *Szerző* megjegyzése.

3.1. Az adatvédelmi szabályozás főbb mérföldkövei

Adatvédelmi szempontból főbb mérföldkövekről szabályozási szinten akkor érdemes beszélni, ha azok olyan átfogó változásokat hoztak vagy hoznak, melyek igazodnak valamely társadalmi, technológiai változáshoz és ezáltal új szabályok megalkotását igénylik.

A szakirodalom egységesen az 1970-es évekre vezeti vissza az ún. *első generációs adatvédelmi szabályozás* kialakulását, amely középpontjában a számítástechnika fejlődéséből eredően az állami nyilvántartások adatainak elektronikus tárolásából, és ezen nyilvántartásokban való keresés lehetőségeiből adódó kérdések és azok jogi reflexiója állt. A technológiai fejlődés lehetővé tette a nagy tömegű automatizált adatfeldolgozást, amely a központi nyilvántartások kialakításának irányába mutatott. Az állam, mint nagy adatkezelő jelent meg, amely egy, egyedi azonosítószám alkalmazásával kívánta kezelni a nyilvántartásokat és az azokban tárol személyes adatokat. Ez vezetett odáig, hogy Európában – főként a jóléti államok körében – sorra jelentek meg az első szabályzók (Svédország, Német Szövetségi Köztársaság, Dánia, Norvégia, Ausztria, Franciaország). A szabályozás elsődleges célja a fentiekben említett nagy állami adatbázisok átláthatóságának megteremtése, amely alapvetően az automatizált adatkezelésekre terjedt ki, és hangsúlyos szerepet kapott benne a konkrét technológia szabályozása. Mindemellett ezen szabályzók az egyén részére nem garantálták az általános rendelkezési jogot a személyes adataik felett. A szabályozás már ekkor is tartalmazta az adatvédelemi rendelkezések felett őrködő felügyeleti szervek feladat- és hatásköreit. [35]

Az 1980-as években a számítástechnika ugrásszerű fejlődése eredményeképpen teret hódított a személyi számítógép (a továbbiakban: PC – Personal Computer) amely mind a gazdasági és üzleti szektorban, mind a lakosság körében is széles körben elterjedt. Ezeket a PC-ket az 1990-es években megjelenő Internet hálózatba kötötte, ahol minden eddiginél gyorsabban, és nagyobb mennyiségben, ámde kontrolálatlanul lehetett az adatokat (pl.: e-mailen) továbbítani. Az üzleti szektor adatbázisai az ügyfelekről számos – esetenként különleges – adatot is kezeltek. [36] Az információ oly mértékben felértékelődött, amely elvezetett az ún. *második generációs adatvédelmi szabályozás* megjelenéséhez. A szabályozás kialakítását sürgette azon álláspont Európai Unión belüli térnyerése, amely szerint az adatok szabad áramlását úgy kell biztosítani, hogy a magánszféra és a személyes adatok védelme garantált legyen. A második generációs szabályozás fő eleme, hogy a technológiai megközelítés helyett az adatkezeléssel érintett személyt – az adatgazdát – széleskörű rendelkezési joggal ruházta fel.[37] A szabályozás az elektronikus adatkezelésekre és a manuális, papír alapú adatkezelésekre egyaránt kiterjedt.

A szabályozásban megjelentek a nemzetközi dokumentumok, melyek közül egy, ugyan nem kötelező érvényű, de számos máig is fontos alapelvet tartalmazó szabályt külön ki kell emelni.

A magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló OECD irányelveket 1980-ban fogadták el[38], amely az adatvédelem alapelveinek az alábbiakat tekinti:

1. Adatgyűjtés korlátozásának elve: személyes adatok gyűjtésére csak törvényes és tisztességes eszközökkel, az adatalany tudtával és beleegyezésével kerülhet sor.
2. Az adatminőség elve: a gyűjtött adatoknak az adatkezelés céljával összhangban pontosnak, teljesnek és aktuálisnak kell lenniük.
3. A célhoz kötöttség elve: személyes adatokat csak előre meghatározott célból, csak a cél megvalósulásához szükséges mértékben és ideig lehet kezelni.
4. A korlátozott felhasználás elve: az adatokat csak az adatalany hozzájárulásával vagy törvényi felhatalmazással lehet felhasználni.

---

[35] Jóri András: *Adatvédelmi kézikönyv.* Osiris Kiadó, Budapest, 2005. 24–25. oldal

[36] Majtényi László: Az információs szabadságok, in.: Halmai Gábor – Tóth Gábor Attila (szerkesztők): *Emberi jogok.* Osiris Kiadó, 2003. 36. oldal

[37] Jóri András: *Adatvédelmi kézikönyv.* Osiris Kiadó, Budapest, 2005. 27. oldal

[38] Jóri András: *Adatvédelmi kézikönyv.* Osiris Kiadó, Budapest, 2005. 28-29. oldal és Majtényi László: Az információs szabadságok, in.: Halmai Gábor – Tóth Gábor Attila (szerkesztők): *Emberi jogok.* Osiris Kiadó, 2003. 95–96. oldal

5. A biztonság elve: az adatokat a technológia mindenkori állásának megfelelő ésszerű intézkedésekkel és eszközökkel kell védeni a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás, sérülés és megsemmisülés ellen.
6. A nyíltság elve: az adatkezelés tényének, helyének és céljának, az adatkezelő személyének, valamint az adatkezelési politikának nyilvánosnak kell lennie.
7. A személyes részvétel elve: az adatalany megismerheti a rá vonatkozó adatokat, azokat szükség esetén helyesbítheti, kiegészítheti vagy töröltetheti.
8. A felelősség elve: az adatkezelő a felelős a fentebb felsorolt elvek betartásáért, s bizonyítani kell tudnia az adatkezelés jogszerűségét.

Ezen OECD elvek már a második generációs szabályozásban is megjelennek, mindemellett fontos szerepet töltöttek be abban a harmonizációs folyamatban, melyek az Európai Unió 1995-ben elfogadott adatvédelmi irányelvéhez[39], majd a harmadik generációs egységes adatvédelmi szabályrendszer kialakításához vezettek.

Az infokommunikációs szolgáltatások térhódítása és az Internet világméretű elterjedése, a fokozódó felhasználó igények (közösségi oldalak elterjedése) miatt vált szükségessé a harmadik generációs adatvédelmi szabályozás kialakítása, amely jelenleg is tart (és vagy kiegészítése, vagy új generációs szabályozás szükséges a kihívások kezelésére). A tartalomszolgáltatás megváltozása mellett ez a térhódítás óriási méretű adatbázisok kialakulását is jelentette, amely együtt jár az adatbányászati tevékenységgel. Komoly kockázatot jelent a mobileszközök elterjedése és ezzel összefüggésben a helymeghatározáson alapuló szolgáltatások elterjedése, amely nem más, mint a személy valósidejű tartózkodási helyének közvetítése „ismeretlen" számú adatkezelő irányába. Ugyanakkor egyre nagyobb igény mutatkozik a felhő alapú szolgáltatások igénybevételére, amely alapjaiban rendezi át az adatok tárolásának módját.

Ezen szabályozási elvek már megjelennek a 2016. május 25-én hatályba lépett, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679 Rendeletében (a továbbiakban: általános adatvédelmi rendelet). Az általános adatvédelmi rendeletet 2018. május 25-től kell kötelezően alkalmazni, amely a hátralévő időszakban számos jogharmonizációs feladatot keletkeztet (többek között az Infotv. módosítását is). A szabályozás – a teljesség igénye nélkül – főbb jellemezője, hogy alapvetően az adatkezelők kötelezettségeit és felelősségét helyezi előtérbe, ezáltal az információs önrendelkezési jog egyéni érvényesítését mellérendelt pozicióba helyezi. Kötelezettségként rögzíti a megfelelő eljárásrendek, szabályzatok elfogadását, adatkezelési dokumentáció vezetését, adatbiztonsági intézkedések megtételét, belső adatvédelmi felelős kijelölését. A szabályozásban ismét megjelenik a technológia szabályozás problematikája, hiszen az közvetlen hatással van az adatvédelemre és az információbiztonságra.[40] Az általános adatvédelmi rendelet hatálybalépésig – jelen kézirat készítésekor – még közel 18 hónap van, azonban már most meg kell kezdeni az ezzel kapcsolatos szabályozási feladatok ellátását.

[39] A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelve

[40] A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679 Rendelet alapján.

3.2. Az Infotv. releváns rendelkezései

3.2.1. A törvény hatálya[41]

Az Infotv. hatálya kiterjed minden olyan adatkezelésre, amely személyes adatra, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik. A törvény területi hatálya Magyarországra terjed ki.

Nem kell alkalmazni az adatvédelmi szabályokra vonatkozó Infotv. rendelkezéseket a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezelései esetében (pl.: magánszemély okostelefonjában szereplő címjegyzék, ha magáncélra használják).

3.2.2. Az értelmező rendelkezések köre[42]

Az egységes jogértelmezés biztosítása érdekében az Infotv. közel harminc pontban rögzíti az értelmező rendelkezéseket, többek között meghatározza:

a) az adatok milyenségére vonatkozó (személyes adat, különleges adat, bűnügyi személyes adat, közérdekű adat, közérdekből nyilvános adat stb.),
b) az adatkezelési tevékenységgel összefüggő (hozzájárulás, adatkezelés, adattovábbítás, nyilvánosságra hozatal, adattörlés, adatmegsemmisítés, adatfeldolgozás stb.), és
c) az adatkezelésben érintett szereplőkre vonatkozó (érintett, adatkezelő, adatfeldolgozó, adatfelelős, adatközlő, harmadik személy stb.)

alapfogalmakat. Az alapfogalmak teljes körű részletes ismertetése jelen jegyzet tárgykörét tekintve nem releváns, ezért a következőkben az adatvédelmi szempontból fontos fogalmakat vesszük sorra.

A *személyes adat* fogalmának meghatározása tág keretek között mozog, személyes adat az érintettre vonatkozó bármely információ. E széles körű megfogalmazásba a személy azonosítására vonatkozó adatok – természetes (pl.: név, születési és lakcím adatok) és mesterséges azonosítók (pl.: TAJ szám, adóazonosító jel, útlevélszám) – is beletartoznak. A személyes adat fogalma együtt értelmezhető az *érintett* fogalmával, amely bármely információ alapján azonosított vagy azonosítható természetes személy.

Kiemelt jelentőséget tulajdonít a jogszabály a személyes adatok speciális körének, a különleges adatoknak, mivel ezek olyan szenzitív jelleggel bírnak, amely adatokkal való visszaélés súlyosabb sérelemmel, jogkövetkezményekkel jár. Az Infotv. szerint *különleges adat* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Annak érdekében, hogy a személyes adatokkal végzett tevékenységek, műveletek jól körbehatárolhatóak legyenek, az Infotv. mintegy gyűjtő fogalomként meghatározza, mi minősül:

*a) adatkezelés*nek (az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a

[41] Infotv. 2. §
[42] Infotv. 3. §

személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése), és

b) *adatfeldolgozás*nak (az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége).

Fentiekhez igazodóan az Infotv. rögzíti az *adatkezelő* (az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja) és az *adatfeldolgozó* (az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel) fogalmát.

2015. október 1-től hatályos az *adatvédelmi incidens* fogalma, amely szerint adatvédelmi incidensnek kell tekinteni az adatbiztonság olyan sérelmét, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Ez a fogalom meghatározás összhangban áll az Ibtv. által alkalmazott biztonsági esemény fogalmával (bővebben a 4. fejezetben), melyek együttes értelmezésével az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosítása – jogi szempontból – könnyebben elvégezhető.

3.2.3. Az adatkezelés elvei és jogalapja

Az Infotv. az előzőekben már említett OECD adatvédelmi alapelvek figyelembevételével főbb garanciális elemként a célhoz kötöttség elvét alkalmazza és rögzíti, hogy:

a) személyes adat kizárólag meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető,

b) az adatkezelés minden szakaszában meg kell felelni az adatkezelési célnak,

c) csak az adatkezelés céljának megvalósulásához elengedhetetlen, és a cél elérésére alkalmas személyes adat kezelésére kerülhet sor,

d) a személyes adat kezelése nem haladhatja meg a cél megvalósulásához szükséges mértéket és időtartamot, azaz, ha az adatkezelés célja megszűnt, akkor a személyes adatot törölni kell.[43]

Az Infotv. a személyes adat kezelésére vonatkozó minőségi követelményeket is meghatározza, és rögzíti, hogy az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. E követelmény alapján az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. A törvény kimondja, hogy a személyes adat az adatkezelés során mindaddig megőrzi az adatok felvételével és kezelésével szemben támasztott tisztesség és törvényesség követelményét, amíg kapcsolata az érintettel helyreállítható, azaz, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

[43] Infotv. 4. § (1)-(2) bekezdés

Már a második generációs szabályozástól kezdve az adatvédelmi szabályok megalkotása során alapvetésként volt kezelve, hogy személyes adatok kezelésére kizárólag jogszabályban felsorolt jogalap alapján kerülhet sor. Ezen jogalapok az Infotv.-ben természetszerűen megjelennek, melyek a következők:

a) *Az érintett hozzájárulása.* Az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez. Személyes adat akkor kezelhető, ha azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli, ennek hiányában az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult, vagy az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.[44] Az előzetes tájékozódáshoz való jog érvényesülése érdekében az adatkezelő az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek megkezdését megelőzően vagy legkésőbb az első adatkezelési művelet megkezdését követően haladéktalanul az érintett rendelkezésére bocsátja az adatkezelő és – ha valamely adatkezelési műveletet adatfeldolgozó végez, az adatfeldolgozó – megnevezését és elérhetőségeit, az adatvédelmi tisztviselő nevét és elérhetőségeit, a tervezett adatkezelés célját és az érintettet e törvény alapján megillető jogok, valamint azok érvényesítése módjának ismertetését. Ezekkel egyidejűleg, azzal azonos módon vagy az érintettnek címzetten az adatkezelő az érintett számára tájékoztatást nyújt az adatkezelés jogalapjáról, a kezelt személyes adatok megőrzésének időtartamáról, ezen időtartam meghatározásának szempontjairól, a kezelt személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek – ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket – köréről, a kezelt személyes adatok gyűjtésének forrásáról és az adatkezelés körülményeivel összefüggő minden további érdemi tényről.[45] Az Infotv. két esetben vélelmezi a hozzájárulást, az érintett közszereplése során általa közölt vagy a nyilvánosságra hozatal céljából általa átadott adatoknál, valamint az érintett kérelmére, kezdeményezésére indult bírósági vagy hatósági eljárásban az eljárás lefolytatásához szükséges, illetve az érintett kérelmére indult más ügyben az általa megadott személyes adatoknál.[46]

b) *Jogszabályon alapuló adatkezelés.* Személyes adat kezelését közérdekből törvény, valamint törvény felhatalmazása alapján kiadott helyi önkormányzati rendelet is előírhatja (kötelező adatkezelés).[47] A kötelező adatkezelés célját és egyéb feltételeit az adatkezelést elrendelő jogszabály határozza meg, de ez esetben is az adatkezelés csak a jogszabályban meghatározott célra, adatkörre és időtartamra terjedhet ki.

c) *Jogi kötelezettség teljesítésén vagy érdekérvényesítésen alapuló adatkezelés.* Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése:
   - az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy
   - az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.[48]

[44] Infotv. 3. § 7. pont és 5. § (1) bekezdés b) pont
[45] Infotv. 16. § (1)–(2) bekezdései
[46] Infotv. 6. § (6)–(7) bekezdései
[47] Infotv. 5. § (1) bekezdés a) pont
[48] Infotv. 6. § (1) bekezdés b) pont

3.2.4. Az adatkezelés korlátai[49]

Az Infotv. rögzíti, hogy törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az adatkezelő személyes adatot úgy vehet át, hogy az adattovábbító adatkezelő vagy adatfeldolgozó az adattovábbítással egyidejűleg jelzi a személyes adat

a) kezelésének lehetséges célját,
b) kezelésének lehetséges időtartamát,
c) továbbításának lehetséges címzettjeit,
d) érintettje e törvényben biztosított jogainak korlátozását, vagy
e) kezelésének egyéb korlátozását.

A személyes adatokat átvevő adatkezelő fenti adatkezelési korlátozásoknak megfelelő terjedelemben és módon köteles a személyes adatot kezelni és az érintett jogait megfelelően biztosítani. A fentiekben felsorolt adatkezelési korlátozásoktól eltérni csak az adatot továbbító adatkezelő előzetes hozzájárulásával lehet, ha az nem ütközik a Magyarország joghatósága alatt álló jogalanyok tekintetében alkalmazandó jogi rendelkezésbe. Az adatkezelőnek a személyes adat továbbításával egyidejűleg a címzettet kötelessége tájékoztatni az alkalmazandó adatkezelési korlátozásról.

3.2.5. Az adatbiztonságra vonatkozó szabályok[50]

Az adatbiztonság követelményeinek törvényi feltételei garantálják az adatkezelés teljesítése során felmerült kockázatok kezelését. Az Infotv. önálló alcímben szabályozza az adatbiztonság követelményét és rögzíti az adatkezelő azon kötelezettségét, amely az adatkezelési műveletek olyan formában történő megtervezésére és végrehajtására vonatkozik, amely az Infotv. és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítja az érintett magánszférájának védelmét. Az adatok biztonságáról az adatkezelő mellett tevékenységi körére vonatkozóan az az adatfeldolgozó is köteles gondoskodni és köteles megtenni azokat a technikai és szervezési intézkedéseket, továbbá kialakítani azokat az eljárási szabályokat, amelyek az Infotv., valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatkezelő és tevékenységi körében az adatfeldolgozó szervezési és műszaki intézkedésekkel biztosítja:

a) az adatkezeléshez használt eszközök (a továbbiakban: adatkezelő rendszer) jogosulatlan személyek általi hozzáférésének megtagadását,
b) az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását,
c) az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását,
d) az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását,
e) azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá,
f) azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére,

[49] Infotv. 9. §
[50] Infotv. 3. §

g) azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban ki vitt be az adatkezelő rendszerbe,
h) a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását,
i) azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen, valamint
j) azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.[51]

A védelmet erősíti az a követelmény is, amely a különböző nyilvántartásokban elektronikusan kezelt adatállományokra vonatkozóan rögzíti, hogy a nyilvántartásokban tárolt adatok esetében megfelelő műszaki megoldással biztosítani kell, hogy azok közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők. Az összekapcsolás és összerendelést kizárólag törvényi előírás teheti lehetővé.[52]

3.2.6. A személyes adatok továbbítása külföldre[53]

Személyes adatot az e törvény hatálya alá tartozó adatkezelő vagy adatfeldolgozó harmadik országban[54], továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére – a közvetett adattovábbítást is ideértve – akkor továbbíthat (a továbbiakban együtt: nemzetközi adattovábbítás), ha

- ehhez az érintett kifejezetten hozzájárult, vagy
- a nemzetközi adattovábbítás az adatkezelés céljának eléréséhez szükséges, valamint
  - annak során az adatkezelés jogalapja és általános feltételei teljesülnek, és
  - a harmadik országban, illetve a nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó tekintetében a továbbított személyes adatok megfelelő szintű védelme biztosított, vagy
- a nemzetközi adattovábbítás a 11. §-ban meghatározott kivételes esetekben szükséges.

A személyes adatok megfelelő szintű védelme akkor biztosított, ha:

a) az Európai Unió kötelező jogi aktusa azt megállapítja,
b) a harmadik ország és Magyarország között az érintetteknek a személyes adatainak kezeléséről szóló tájékoztatásával, az adatok helyesbítésével, törlésével és zárolsával összefüggő jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat biztosító nemzetközi szerződés van hatályban, vagy
c) az adatkezelés, illetve az adatfeldolgozás kötelező szervezeti szabályozásnak megfelelően történik.

A személyes adatok a nemzetközi jogsegélyről, az adóügyi információcseréről, valamint a kettős adóztatás elkerüléséről szóló nemzetközi szerződés végrehajtása érdekében, a nemzetközi szerződésben meghatározott célból, feltételekkel és adatkörben a személyes adatok megfelelő szintű védelmét biztosító – és fentiekben részletezett – feltételek hiányában is továbbíthatók harmadik országba.

---

[51] Infotv. 25/I. § (3) bekezdés
[52] Infotv. 25/I.§ (4)
[53] Infotv. 8. §
[54] *Harmadik ország:* minden olyan állam, amely nem EGT-állam (Infotv. 3. § 24. pont)

Kiegészítő szabály, hogy az EGT-államba[55], valamint az Európai Unió működéséről szóló szerződés V. címének 4. és 5. fejezete szerint létrehozott ügynökségek, hivatalok és szervek részére irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor, azaz a fentiekben részletezett harmadik országba irányuló szabályok az Európai Unión belüli adattovábbításra, továbbá az EGT tagság miatt Izlandra, Lichtensteinre és Norvégiára nem vonatkoznak.

3.2.7. Az adatok feldolgozására vonatkozó szabályok

Az adatfeldolgozó az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel. [56]

A személyes adatok feldolgozására vonatkozó jogokat és kötelezettségeket az Infotv. önálló alcím alatt, generális jelleggel tartalmazza, kiegészítő szabályként felhívva a külön ágazati törvényeket, azzal, hogy főszabályként rögzíti, az adatkezelő az általa adott utasítások jogszerűségéért felel. Korlátozó szabály az adatfeldolgozó irányába, hogy:

a) Adatfeldolgozóként kizárólag olyan személy vagy szervezet járhat el, aki megfelelő garanciákat nyújt az adatkezelés jogszerűségének és az érintettek jogai védelmének biztosítására alkalmas műszaki és szervezési intézkedések végrehajtására, amely garanciákat az adatkezelés megkezdését megelőzően igazolja az adatkezelő számára.

b) Az adatfeldolgozó további adatfeldolgozót kizárólag abban az esetben vehet igénybe, ha azt jogszabály nem zárja ki, továbbá ha az adatkezelő további adatfeldolgozó igénybevételéhez előzetesen a meghatározott módon felhatalmazást adott.

c) Ha az adatfeldolgozó a további adatfeldolgozót az adatkezelő általános felhatalmazása alapján veszi igénybe, az adatfeldolgozó a további adatfeldolgozó igénybevételét megelőzően tájékoztatja az adatkezelőt a további adatfeldolgozó személyéről, valamint a további adatfeldolgozó által végzendő tervezett feladatokról. Ha az adatkezelő ezen tájékoztatás alapján a további adatfeldolgozó igénybevételével szemben kifogást emel, a további adatfeldolgozó igénybevételére az adatfeldolgozó kizárólag a kifogásban megjelölt feltételek teljesítése esetén jogosult.[57]

Az adatfeldolgozás főszabályai mellett az Infotv. több ponton kiegészítő rendelkezéseket rögzít:

a) *Automatizált adatkezelésen*[58] – így különösen profilalkotáson – alapuló, az érintett személyére vagy jogos érdekeire hátrányos vagy az érintettet jelentős mértékben érintő jogkövetkezményekkel járó döntés meghozatalára kizárólag akkor kerülhet sor, ha azt törvény vagy az Európai Unió kötelező jogi aktusa kifejezetten lehetővé teszi és az nem sérti az egyenlő bánásmód követelményét, az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó az érintettet – kérelmére – tájékoztatja a döntéshozatali mechanizmus során alkalmazott módszerről és szempontokról, érintett kérelmére a döntés eredményét emberi közreműködés alkalmazásával felülvizsgálja, valamint arra – törvény vagy az Európai Unió kötelező jogi aktusának eltérő rendelkezése hiányában – nem különleges adatok felhasználásával kerül sor.

---

[55] *EGT-állam:* az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez. (Infotv. 3. § 23. pont)

[56] Infotv. 3. § 18. pont

[57] Infotv. 25/C. §

[58] Infotv. 6. §

b) Személyes adatok tudományos kutatás során történő kezelése[59] esetében az Infotv. rögzíti, hogy a tudományos kutatást végző szerv vagy személy személyes adatot nyilvánosságra hozhat, ha az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges.

3.2.8. Az érintett jogai az adatkezeléssel kapcsolatban és azok érvényesítése

Az információs önrendelkezési jog alapjogi jellegéből adódóan az Infotv. rögzíti, hogy az érintett jogait kizárólag törvény korlátozhatja, az Infotv.-ben tételesen meghatározott esetekben.[60] Az érintett részére a személyes adataik kezelésével összefüggésben biztosított jogok az adatkezelési folyamat összes elemére kiterjednek, melyek szabályai az alábbiak szerint összegezhetők:

Az érintett jogosult arra, hogy az adatkezelő és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában:

a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (előzetes tájékozódáshoz való jog),
b) kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa (hozzáféréshez való jog),
c) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő helyesbítse, illetve kiegészítse (helyesbítéshez való jog),
d) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatai kezelését az adatkezelő korlátozza (az adatkezelés korlátozásához való jog),
e) kérelmére, valamint meghatározott további esetekben személyes adatait az adatkezelő törölje (törléshez való jog).[61]

Az érintett az adatkezelő, illetve – az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli. Ha a bíróság a keresetnek helyt ad, a jogsértés tényét megállapítja és az adatkezelőt, illetve az adatfeldolgozót a jogellenes adatkezelési művelet megszüntetésére, az adatkezelés jogszerűségének helyreállítására, illetve az érintett jogai érvényesülésének biztosítására pontosan meghatározott magatartás tanúsítására kötelezi, és szükség esetén egyúttal határoz a kártérítés, sérelemdíj iránti igényről is.

A bíróság elrendelheti ítéletének – az adatkezelő, illetve adatfeldolgozó azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha az ítélet személyek széles körét érinti, ha az alperes adatkezelő, illetve adatfeldolgozó közfeladatot ellátó szerv, vagy ha a bekövetkezett jogsérelem súlya a nyilvánosságra hozatalt indokolja.[62]

---

[59] Infotv. 5. § (8) bekezdés

[60] Infotv. 16. § (3) bekezdés: A (2) bekezdésben foglaltak szerinti tájékoztatás teljesítését az elérni kívánt céllal arányosan az adatkezelő késleltetheti, a tájékoztatás tartalmát korlátozhatja vagy a tájékoztatást mellőzheti, ha ezen intézkedése elengedhetetlenül szükséges
a) az általa vagy részvételével végzett vizsgálatok vagy eljárások – így különösen a büntetőeljárás – hatékony és eredményes lefolytatásának,
b) a bűncselekmények hatékony és eredményes megelőzésének és felderítésének,
c) a bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának,
d) a közbiztonság hatékony és eredményes védelmének,
e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen a honvédelem és a nemzetbiztonság vagy
f) harmadik személyek alapvető jogai védelmének biztosításához.

[61] Infotv. 14.§

[62] Infotv. 23. § (1), (5)-(6) bekezdés

3.2.9. Adatkezelő kötelezettségei

Az adatkezelő köteles[63]:

a) az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzésére,

b) az érintett tájékoztatása céljából nyilvántartás vezetésére[64], amely tartalmazza:

a. az adatkezelő, ideértve minden egyes közös adatkezelőt is, valamint az adatvédelmi tisztviselő nevét és elérhetőségeit,
b. az adatkezelés célját vagy céljait,
c. személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek – ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket – körét,
d. az érintettek, valamint a kezelt adatok körét,
e. profilalkotás alkalmazása esetén annak tényét,
f. nemzetközi adattovábbítás esetén a továbbított adatok körét,
g. az adatkezelési műveletek – ideértve az adattovábbítást is – jogalapjait,
h. ha az ismert, a kezelt személyes adatok törlésének időpontját,
i. az e törvény szerint végrehajtott műszaki és szervezési biztonsági intézkedések általános leírását,
j. az általa kezelt adatokkal összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és a kezelésükre tett intézkedéseket,
k. az érintett hozzáférési jogának érvényesítését e törvény szerint korlátozó vagy megtagadó intézkedésének jogi és ténybeli indokait.

3.2.10. Kártérítési felelősség és sérelemdíj

Az Infotv. szigorú szabályokat telepít az adatvédelmi követelmények megszegésével okozott károk iránti felelősséghez. Az adatkezelő kötelezettsége az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt megtérítése.

Az érintett az adatkezelő, illetve – az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli.

Azt, hogy az adatkezelés a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásoknak megfelel, az adatkezelő, illetve az adatfeldolgozó köteles bizonyítani. Ha a bíróság a keresetnek helyt ad, a jogsértés tényét megállapítja, és az adatkezelőt, illetve az adatfeldolgozót:

a) a jogellenes adatkezelési művelet megszüntetésére,

b) az adatkezelés jogszerűségének helyreállítására, illetve

c) az érintett jogai érvényesülésének biztosítására pontosan meghatározott magatartás tanúsítására

kötelezi, és szükség esetén egyúttal határoz a kártérítés, sérelemdíj iránti igényről is.

A bíróság elrendelheti ítéletének – az adatkezelő, illetve adatfeldolgozó azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha az ítélet személyek széles körét érinti, ha az alperes adatkezelő, illetve adatfeldolgozó közfeladatot ellátó szerv, vagy ha a bekövetkezett jogsérelem súlya a nyilvánosságra hozatalt indokolja.[65]

[63] Infotv. 15. § (1a) bekezdés és (2)-(3) bekezdések

[64] Infotv. 25/E. § (1) bekezdés

[65] Infotv. 23.§

Ha az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásokat megsérti és ezzel másnak kárt okoz, köteles azt megtéríteni. Ha az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásokat megsérti és ezzel más személyiségi jogát megsérti, az, akinek személyiségi joga sérelmet szenvedett, az adatkezelőtől, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozótól sérelemdíjat követelhet. Az adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy a személyiségi jog megsértésével okozott jogsérelmet az adatkezelés körén kívül eső elháríthatatlan ok idézte elő, továbbá, ha bizonyítja, hogy az általa végzett adatkezelési műveletek során a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségek, valamint az adatkezelő jogszerű utasításainak betartásával járt el.

Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj annyiban, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem a személyiségi jogi jogsérelmet szenvedő személy szándékos vagy súlyosan gondatlan magatartásából származott.[66]

3.2.11. A Nemzeti Adatvédelmi és Információszabadság Hatóság feladat- és hatásköre

Ha hatósági eljárás megindítása az Infotv. szerint nem kötelező, a Hatóság hivatalból vizsgálatot indíthat.[67] A Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll. A bejelentés miatt senkit sem érhet hátrány, a bejelentő kilétét a Hatóság csak akkor fedheti fel, ha ennek hiányában a vizsgálat nem lenne lefolytatható. Ha a bejelentő kéri, kilétét a Hatóság akkor sem fedheti fel, ha ennek hiányában a vizsgálat nem folytatható le – erről a következményről a Hatóság a bejelentőt köteles tájékoztatni.[68] A Hatóság a bejelentést köteles érdemben megvizsgálni, kivéve az Infotv.-ben előírt eseteket.[69]

A Hatóság a vizsgálat során

a) a vizsgált adatkezelő kezelésében levő, a vizsgált üggyel összefüggésbe hozható összes iratba betekinthet, illetve azokról másolatot kérhet,

b) a vizsgált üggyel összefüggésbe hozható adatkezelést megismerheti, az adatkezelés helyszínéül szolgáló helyiségbe beléphet, az adatkezelési műveletek végzéséhez használt eszközökhöz hozzáférhet,

---

[66] Infotv. 24.§

[67] Infotv. 51/A. §

[68] Infotv. 52. § (3) bekezdés

[69] Infotv. 53. § (2)–(3) bekezdések

A Hatóság a bejelentést érdemi vizsgálat nélkül elutasíthatja, ha

a) a bejelentésben megjelölt jogsérelem csekély jelentőségű, vagy

b) a bejelentés névtelen.

A Hatóság a bejelentést érdemi vizsgálat nélkül elutasítja, ha

a) az adott ügyben bírósági eljárás van folyamatban, vagy az ügyben korábban jogerős bírósági határozat született,

b) ha a Hatóság vizsgálat le nem folytathatóságára vonatkozó tájékoztatás ellenére a bejelentő továbbra is kéri, hogy a kilétét ne fedjék fel,

c) a bejelentés nyilvánvalóan alaptalan,

d) az ismételten előterjesztett bejelentés érdemben új tényt, adatot nem tartalmaz,

e) a bejelentést határidőn túl nyújtották be.

c) a vizsgált adatkezelőtől, illetve az adatkezelő bármely munkatársától írásbeli és szóbeli felvilágosítást kérhet,
d) a vizsgált üggyel összefüggésbe hozható bármely szervezettől vagy személytől írásbeli felvilágosítást, illetve a vizsgált üggyel összefüggésbe hozható iratról másolatot kérhet, és
e) az adatkezelő hatóság felügyeleti szervének vezetőjét vizsgálat lefolytatására kérheti fel.[70]

A vizsgálat végeztével – a bejelentés érkezésétől számított 2 hónapon belül – a Hatóság:
a) ha a bejelentést megalapozottnak tartja:
   a. felszólítja az adatkezelőt a jogsérelem orvoslására, illetve annak közvetlen veszélye megszüntetésére, amelynek megtételéről, vagy arról, hogy az abban foglaltakkal nem ért egyet, az adatkezelő 30 napon belül köteles a Hatóságot tájékoztatni, és ha a felszólítás nem jár eredménnyel a Hatóság ajánlást tehet a szerv felügyeleti szervének;
   b. nyilvános jelentést készíthet az ügyről;
   c. adatvédelmi hatósági eljárást, vagy
   d. titokfelügyeleti hatósági eljárást indít.
b) ha a bejelentésben foglaltakat nem tartja megalapozottnak, a vizsgálatot lezárja.[71]

A Hatóság a vizsgálat eredményeként ajánlást tehet jogszabályalkotásra, illetve a közjogi szervezetszabályozó eszköz kiadására jogosult szervnek, illetve a jogszabály előkészítőjének a jogszabály, illetve a közjogi szervezetszabályozó eszköz módosítására, hatályon kívül helyezésére vagy megalkotására, ha a jogsérelem, illetve annak közvetlen veszélye valamely jogszabály vagy közjogi szervezetszabályozó eszköz fölösleges, nem egyértelmű vagy nem megfelelő rendelkezésére, illetve az adatkezeléssel összefüggő kérdések jogi szabályozásának hiányára vagy hiányosságára vezethető vissza.[72]

Az adatvédelmi hatósági eljárás megindításának feltétele, hogy valószínűsíthető az, hogy a személyes adatok jogellenes kezelése, és a jogellenes adatkezelés személyek széles körét érinti vagy nagy érdeksérelmet vagy kárveszélyt idézhet elő.[73]

Az adatvédelmi hatósági eljárás jogkövetkezménye lehet[74]:
a) a személyes adatok jogellenes kezelésének megállapítása,
b) a valóságnak nem megfelelő személyes adat helyesbítésének elrendelése,
c) a jogellenesen kezelt vagy feldolgozott személyes adatok zárolásának, törlésének vagy megsemmisítésének elrendelése,
d) a személyes adatok jogellenes kezelésének vagy feldolgozásának megtiltása,
e) a személyes adatok külföldre történő továbbításának vagy átadásának megtiltása,
f) az érintett tájékoztatásának elrendelése, ha azt az adatkezelő jogellenesen tagadta meg vagy mellőzte,
g) bírság kiszabása, valamint
h) határozat – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalának elrendelése, ha azt az adatvédelem érdekeinek, illetve nagyobb számú érintett jogainak védelme ezt megköveteli.

Az Infotv. rövid bemutatását követően is jól látható, hogy az adatvédelmi célkitűzésekhez általános jogi kereteket ad, a védelem formáját és ezzel összefüggésben a technológia kiválasztását az adatkezelőre bízza, még akkor is, ha a személyes adatok vonatkozásában az adatkezelő által telje-

[70] Infotv. 54. § (1) bekezdés
[71] Infotv. 55. §, 56. §, 58. §.
[72] Infotv. 57. §
[73] Infotv. 60. § (1)–(4) bekezdései
[74] Infotv. 61. § (1)–(4) bekezdései

sítendő egyes biztonsági elvárásokat rögzíti. Az adatkezelő ebből adódóan köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az az Infotv. és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Az elektronikus információbiztonság szabályozása az általános kereteken túlmutat, ezen esetekben a speciális szabályokat az elektronikus információs rendszer biztonságára és ezekben a rendszerekben kezelt adatok védelmére vonatkozóan az Ibtv. és végrehajtási rendeletei tartalmazzák, melyek hozzájárulnak az adatbiztonság szintjének növeléséhez, különös tekintettel az elektronikus információs rendszerekben tárolt személyes adatok kezelése esetén.

4. Az Ibtv. és a vhr-ek rendelkezései

A 2. fejezetben már említett Kiberstratégia célja, hogy *„…meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is,”*[75] melynek szabad, demokratikus jogállami és biztonságos működését Magyarország alapvető értéknek és érdeknek tekinti. A magyar kibertér fogalmát az Ibtv. határozza meg, e szerint a magyar kibertér a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne.[76]

A Kiberstratégia előírja, hogy a magyar kibertérnek biztonságos és megbízható környezetet kell biztosítania:

a) az egyének és közösségek számára a szabad, félelemmentes, a személyes adatok védelmét garantáló kommunikáción keresztül a társadalmi fejlődéshez és integrációhoz,
b) a gazdasági szereplők számára a hatékony, innovatív üzleti megoldások kialakításához,
c) a jövő generációi számára az értékelven alapuló tanuláshoz és az egészséges lelki fejlődést eredményező, sérülésmentes tapasztalatszerzéshez,
d) az elektronikus közigazgatás számára az állami szolgáltatások innovatív és előremutató fejlesztéséhez hozzájárulva.[77]

Mindezen feladat nemzeti szinten a kormányzat, a tudományos, a gazdasági és a civil szféra szereplőinek hatékony együttműködését feltételezi.

A Kiberstratégia kilenc cselekvési területet, azaz intézkedési vagy beavatkozási irányt azonosít, amelyek kezelése a kiberbiztonság megfelelő szinten tartásához, folyamatos fejlesztéséhez és a kitűzött célok eléréséhez szükséges. Ezen cselekvési területek között szerepel a tudatosság[78], az oktatás, kutatás-fejlesztés[79] és a gyermekvédelem[80].

---

[75] Kiberstratégia 1. pont.

[76] Ibtv. 1. § (1) bekezdés 35. pont

[77] Kiberstratégia 8. pont

[78] A kiberbiztonsággal összefüggő hazai és nemzetközi szakmai fórumok szervezése; a kibertér biztonságos használatát célzó és figyelemfelhívó tevékenységek, a kiberbiztonsági gyakorlati tudást elősegítő kezdeményezések, valamint a civil és gazdasági szféra tudatosságnövelésének támogatása.

[79] A kiberbiztonság szakterület beépítése az általános, a közép- és felsőoktatás, továbbá a kormányzati tisztviselők képzésének és a szakmai továbbképzések informatikai oktatásába; stratégiai együttműködési megállapodások kidolgozása az állam és azon egyetemi és tudományos kutatóhelyek között, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását.

[80] A gyermekeknek és fiataloknak szóló minőségi online tartalmak előállításának ösztönzésére, a tudatosságnövelő és felkészítő intézkedések támogatására, a gyermekek zaklatása és kizsákmányolása elleni küzdelemre és a biztonságos online környezet megteremtésére irányuló intézkedések bevezetése, együttműködve az online gyermekvédelem terén eredményeket elért magyar civil szervezetekkel.

4.1. Az Ibtv. alapelvei és fogalmi rendszere

A megelőzés, a biztonság, a védelem és a tudatosságnövelés fontosságát jelzi, hogy ezen alapelvek már az Ibtv. preambulumában is helyet kapnak: *„A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések[81] miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága."*A preambulum kimondja továbbá, hogy *„Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."*

Fenti alapelvek az értelmező rendelkezések között is helyet kapnak, mivel az Ibtv.-ben önálló fogalomként jelenik meg – többek között – a *bizalmasság,*[82] a *sértetlenség,*[83] a *rendelkezésre állás*[84] és a védelem különböző formáinak a meghatározása. Az Ibtv. fogalom meghatározása szerint:

a) Bizalmasságnak az elektronikus információs rendszer azon tulajdonságát kell érteni, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.

b) Sértetlenség az adat azon tulajdonsága, amely szerint az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

c) Rendelkezésre állás annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak.

Az Ibtv. – a PreDeCo (Preventive-Detective-Corrective) elvet alapul véve – a védelmi feladatok közé a *megelőzést*, a *korai figyelmeztetést*, az *észlelést*, a *reagálást*, és az *eseménykezelést* sorolja:

a) megelőzés a fenyegetés által okozható hatás bekövetkezésének elkerülése [Ibtv. 1. § (1) bekezdés 36. pont];

b) korai figyelmeztetés olyan aktív szervezeti cselekvés, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni [Ibtv. 1. § (1) bekezdés 32. pont];

c) észlelés a biztonsági esemény bekövetkezésének felismerése [Ibtv. 1. § (1) bekezdés 17. pont];

d) reagálás a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés [Ibtv. 1. § (1) bekezdés 37. pont].

A *kockázatokkal arányos védelem* [a védelmi intézkedésekre fordított költségeknek arányosnak kell lenni a fenyegetések által okozható károk értékével – Ibtv. 1. § (1) bekezdés 31. pont] alábbi formáit különbözteti meg az Ibtv:

a) adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás [Ibtv. 1. § (1) bekezdés 6. pont];

---

[81] Ibtv. 1. § (1) bekezdés 19. pont, fenyegetés: olyan lehetséges művelet, esemény vagy mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát.

[82] Ibtv. 1. § (1) bekezdés 8. pont

[83] Ibtv. 1. § (1) bekezdés 39. pont

[84] Ibtv. 1. § (1) bekezdés 38. pont

b) fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem [Ibtv. 1. § (1) bekezdés 20. pont];
c) logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem [Ibtv. 1. § (1) bekezdés 34. pont];
d) folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem [Ibtv. 1. § (1) bekezdés 21. pont];
e) teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem [Ibtv. 1. § (1) bekezdés 44. pont];
f) zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem [Ibtv. 1. § (1) bekezdés 48. pont].

Az elektronikus információs rendszerek teljes életciklusában meg kell valósítani azt, hogy az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása, a poszt-kvantumtitkosítás alkalmazásra kötelezett szervezetek esetén a fizikailag elkülönített helyszíneik közötti kormányzati célú hálózaton, továbbá a publikus internetfelületen zajló, az elektronikus hírközlési törvény szerinti szolgáltató igénybevételével vagy egyéb információs társadalommal összefüggő szolgáltatásaik igénybevétele során a hagyományos kriptográfiai alkalmazáson felüli biztonságot nyújtó poszt-kvantum titkosítási alkalmazással történő zárt, teljes körű, folytonos és kockázatokkal arányos védelmére kerüljön sor.[85]

A gyakorlatban fontos szerepe van annak, hogy a felsorolt védelmi intézkedések által lehetőleg elkerülhető legyen a biztonsági események bekövetkezése. Biztonsági eseménynek azt a nem kívánt vagy nem várt egyedi eseményt vagy eseménysorozatot tekintjük, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.[86] Az Ibtv. szerinti biztonsági esemény fogalma – ahogy arra a 2.2 pontban már utaltunk – az Infotv. szerinti adatvédelmi incidens fogalmával együttesen az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosításához megfelelő jogi alapokat adnnak.

Ha sor kerül bármely biztonsági esemény bekövetkezésére, azonnal intézkedni kell annak hatékony kezelése iránt.[87] A védelmi intézkedések kiegészítésével vagy megerősítésével, a szabályozás javításával és az érintettek oktatásával kell gondoskodni arról, hogy a biztonsági események bekövetkezésének a valószínűsége és az ezáltal okozott kár minimalizálható legyen.

Az elektronikus információs rendszerek védelmének körében az Ibtv. hatálya alá tartozó szervezeteknek a külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatározniuk, úgy, hogy az intézkedéseknek támogatniuk kell a *megelőzés*t és a *korai figyelmeztetés*t, az *észlelés*t, a *reagálás*t és a *biztonsági események kezelését*.[88]

Biztonság alatt az elektronikus információs rendszer olyan állapotát kell tehát érteni, amely során az összes számításba vehető fenyegetést figyelembe kell venni, és amely az elektronikus információs rendszer valamennyi elemére kiterjed, folyamatában megvalósul, illetve költségei arányosak a fenyegetések által okozható károkkal.

[85] Ibtv. 5. § és Ibtv. 1. § (1) bekezdés 15. pont
[86] Ibtv. 1. § (1) bekezdés 9. pont
[87] *Biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység (Ibtv. 1. § (1) bekezdés 10. pont)
[88] Ibtv. 6. §

4.2. Az Ibtv. hatálya

Az Ibtv. hatálya igen összetett és értelmezése mind a személyi, mind a tárgyi és területi hatály tekintetében részletekbe menően szabályzott, mivel tárgyi hatályát tekintve rögzíti magának az elektronikus információs rendszernek, mint védett jogi tárgynak a fogalamát. Az Ibtv. értelmében elektronikus információs rendszernek[89] kell tekinteni:

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

1. Az Ibtv. *személyi hatály*a alá az alkotmányos rend és a közigazgatás hatékony működésének fenntartása szempontjából kiemelt jelentőséggel rendelkező, valamint a nemzeti adatvagyon kezelését ellátó szervezetek tartoznak[90]:

a) *a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvényben* rögzítettek figyelembevételével kiterjed a központi államigazgatási szervekre[91], ezen belül:
   – a minisztériumokra,
   – az autonóm államigazgatási szervekre (Közbeszerzési Hatóság, a Gazdasági Versenyhivatal, Nemzeti Adatvédelmi és Információszabadság Hatóság, Nemzeti Választási Iroda),
   – a kormányhivatalra, mint törvény által létrehozott, a Kormány irányítása alatt működő szervre (Központi Statisztikai Hivatal, Országos Atomenergia Hivatal, Szellemi Tulajdon Nemzeti Hivatala, Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal),
   – a központi hivatalokra, mint a kormányrendelet által létrehozott, miniszter irányítása alatt működő szervekre (pl.: Magyar Államkincstár, Országos Meteorológiai Szolgálat, Oktatási Hivatal, Klebelsberg Intézményfenntartó Központ, Szociális és Gyermekvédelmi Főigazgatóság),
   – a rendvédelmi szervekre (rendőrség, büntetés-végrehajtási szervezet, hivatásos katasztrófavédelmi szerv, polgári nemzetbiztonsági szolgálatok[92] – Információs Hivatal, Alkotmányvédelmi Hivatal, Nemzetbiztonsági Szakszolgálat, Terrorelhárítási Információs és Bűnügyi Elemző Központ) és a Katonai Nemzetbiztonsági Szolgálatra,
   – az önálló szabályozó szervekre (Nemzeti Média- és Hírközlési Hatóság, Magyar Energetikai és Közmű-szabályozási Hivatal, Szabályozott Tevékenységek Felügyeleti Hatósága, Országos Atomenergia Hivatal).

   A jogszabály szerint a Kormány és a kormánybizottságok is központi államigazgatási szerveknek minősülnek, azonban az Ibtv. hatálya nem terjed ki ezekre a szervekre, mivel önálló szervezetrendszerrel nem rendelkező testületként gyakorolják feladataikat és önálló elektronikus információs rendszerekkel nem rendelkeznek.
b) kiterjed a Köztársasági Elnöki Hivatalra,[93] az Országgyűlés Hivatalára;[94]

[89] Ibtv.1. § (1) bekezdés 14b. pont és (3) bekezdés
[90] Ibtv. 2. §
[91] A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (2)-(6) bekezdései.
[92] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 2. §-a.
[93] A köztársasági elnök jogállásáról és javadalmazásáról szóló 2011. évi CX. törvény 15. §-a.
[94] Az Országgyűlésről szóló 2012. évi XXXVI. törvény 123. §-a.

c) kiterjed az Alkotmánybíróság Hivatalára;[95]
d) *a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény* rendelkezései figyelembevételével kiterjed az Országos Bírósági Hivatalra és a bíróságokra (Kúria, ítélőtábla, törvényszék, járásbíróság és a kerületi bíróság, közigazgatási és munkaügyi bíróság[96]);
e) *az ügyészségről szóló 2011. évi CLXIII. törvény* figyelembevételével kiterjed az ügyészségekre (Legfőbb Ügyészség, fellebbviteli főügyészségek, főügyészségek, járási ügyészségek[97]);
f) az Alapvető Jogok Biztosának Hivatalára;[98]
g) az Állami Számvevőszékre;[99]
h) a Magyar Nemzeti Bankra;[100]
i) *a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról szóló 2010. évi CXXVI. törvény* figyelembevételével kiterjed a fővárosi és megyei kormányhivatalokra (ideértve a fővárosi és megyei kormányhivatal szervezeti egységeit a járási és fővárosi kerületi hivatalokat[101]);
j) a helyi önkormányzatok képviselő-testületének hivatalaira (polgármesteri hivatal, megyei önkormányzati hivatal, közös önkormányzati hivatal[102]), a hatósági igazgatási társulásokra;[103]

Az Ibtv. hatálya nem terjed ki az önkormányzatok képviselő-testületeire, azok bizottságaira, és a közgyűlésre.

k) a Magyar Honvédségre[104].

Az Ibtv. hatálya kiterjed továbbá az a)-k) pontokban felsorolt szervek és a számukra adatkezelést végző szervek[105] elektronikus információs rendszereinek védelmére.

2. Az Ibtv. *szervi hatály*a kiterjed:[106]

a) a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói elektronikus információs rendszereinek védelmére,[107] így többek között:
- a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala esetében:
  - a Foglalkoztatási és Közfoglalkoztatási Adatbázisra;
  - az állami foglalkoztatási szerv feladatainak ellátásához szükséges adatbázisra (pl.: a közfoglalkoztatásért felelős miniszter, mint első fokon eljáró állami foglalkoztatási szerv a kormányhivatalok bevonásával működteti a munkavédelmi és a munkaügyi feladatok ellátásához, az adatok nyilvántartásához szükséges egységes informatikai rendszert[108]);
  - az egységes szociális nyilvántartásra;
  - a polgárok személyi adatainak és lakcímének nyilvántartására;

---

95 Az Alkotmánybíróságról szóló 2011. évi CLI. törvény 22. §-a.
96 A bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény 16. §-a.
97 Az ügyészségről szóló 2011. évi CLXIII. törvény 8. §-a.
98 Az alapvető jogok biztosáról szóló 2011. évi CXI. törvény 41. §-a.
99 Az Állami Számvevőszékről szóló 2011. évi LXVI. törvény 1-2. §-ai.
100 A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 5. §-a.
101 A fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról szóló 2010. évi CXXVI. törvény 3. §-a.
102 Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 85. §-a.
103 Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 87. §-a.
104 A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 35. §-a és 38. §-a.
105 Ibtv. 1. § (1) bekezdés 4. és 5. pontja.
106 Ibtv. 2. §
107 A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III.22.) Korm. rendelet melléklete alapján.
108 Az állami foglalkoztatási szerv, a munkavédelmi és munkaügyi hatóság kijelöléséről, valamint e szervek hatósági és más feladatainak ellátásáról szóló 320/2014. (XII. 13.) Korm. rendelet 5. § f) pontja.

    - elektronikus anyakönyvi nyilvántartásra;
    - a központi idegenrendészeti nyilvántartására (a Bünügyi Szakértői és Kutató Intézettel együttesen);
    - a kötvénynyilvántartásra;
    - az egyéni vállalkozók nyilvántartására;
    - a központi útiokmány-nyilvántartásra;
    - a közúti közlekedési nyilvántartásra;
    - a Magyar igazolvány és a Magyar hozzátartozói igazolvány tulajdonosainak nyilvántartására;
    - a szabálysértési nyilvántartási rendszerre;
    - a bűnügyi nyilvántartási rendszerre;
  - a Nemzeti Rehabilitációs és Szociális Hivatalnak az egységes szociális nyilvántartására és az egységes örökbefogadási nyilvántartásra;
  - a Földmérési és Távérzékelési Intézetre és a járási hivatalokra, mint az ingatlan-nyilvántartás, a földhasználati nyilvántartás és egyéb földmérési és térképészeti, a rendeletben meghatározott nyilvántartás adatfeldolgozóira;
  - az Országos Nyugdíjbiztosítási Főigazgatóságra,[109], mint a nyugdíjbiztosítási nyilvántartás adatkezelőjére;
  - az Országos Egészségbiztosítási Pénztárra,[110] mint az egészségbiztosítási nyilvántartás adatkezelőjére;
  - az MH Geoinformációs Szolgálat és HM Térképészeti Közhasznú Nonprofit Kft.-re, a közepes és kisméretarányú állami topográfiai térképek adatfeldolgozása tekintetében;
  - a Pillér Pénzügyi és Számítástechnikai Kft.-re, a Nemzeti Adó- és Vámhivatal által kezelt adó- és vámhatósági adatok nyilvántartásának adatfeldolgozása tekintetében;
  - a Mezőgazdasági és Vidékfejlesztési Hivatal a mezőgazdasági és vidékfejlesztési támogatási szerv által kezelt nyilvántartási rendszerek adatfeldolgozása tekintetében;
  - a Cégnyilvántartás, a természetes személyek közhiteles országos adósságrendezési nyilvántartása, az adósságrendezési eljárással összefüggő hirdetményi rendszer tekintetében a Magyar Közlöny Lap- és Könyvkiadó Kft;
  - a természetes személyek adósságrendezési eljárásával összefüggő nyomtatványellenőrzési és nyomtatványkitöltő informatikai rendszer, valamint az európai uniós források felhasználásához kötődő adatfeldolgozói feladatok tekintetében a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

b) az európai létfontosságú rendszerelemmé vagy nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemeknek a létfontosságú tevékenységben közreműködő elektronikus információs rendszereinek védelmére (pl.: pénzintézetek, erőművek, távközlési rendszerek, egészségbiztosítás informatikai rendszerei);

c) az alapvető szolgáltatást nyújtó szereplőknek az alapvető szolgáltatás nyújtásában közreműködő elektronikus információs rendszereinek védelmére;

d) az elektronikus információs rendszert működtető, a központi államigazgatási és kormányzati tevékenység szempontjából fontos, nemzetbiztonsági védelem alá eső szervek elektronikus információs rendszereinek védelmére.

[109] A társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény 40. § a) pont.

[110] A társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény 40. § b) pont.

Ezen széles körű személyi és szervi hatály által a szabályozás minden, az állam működése szempontjából lényeges elektronikus információs rendszer védelmére kitérjed. Bizonyos védelmi szempontok – kül- és belbiztonság, adat- és információvédelem – alapján szükséges azonban, hogy az Ibtv. rendelkezései korlátok között érvényesüljenek. Ennek érdekében az Ibtv. rendelkezéseit:

a) a minősített adatokat kezelő elektronikus információs rendszereket érintően *a minősített adat védelméről szóló 2009. évi CLV. törvényben* (a továbbiakban: Mavtv.),

b) a médiaszolgáltatási és elektronikus hírközlési tevékenység esetén az elektronikus hírközlésről szóló 2003. évi C. törvényben, továbbá a médiaszolgáltatásokról és tömegkommunikációról szóló 2010. évi CLXXXV. törvényben

meghatározott eltérésekkel kell alkalmazni.[111] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény rendelkezései alapján a különleges jogrend ideje alatt nemzeti létfontosságú rendszerelemmé kijelölt rendszerelem tekintetében e törvény rendelkezéseit kizárólag akkor kell alkalmazni, ha a különleges jogrend megszűnését követő felülvizsgálat eredményeként a kijelölését fenntartották.[112]

Az Ibtv.-ben a *tárgyi hatály* kapcsán rögzítésre került, hogy a hatósági feladatokat és a biztonsági felügyeletet egyes ún. zárt célú elektronikus információs rendszerek, a honvédelmi célú elektornikus információs rendszerek esetében a Kormány rendeletében kijelölt szerv kormányrendeletben meghatározottak szerint látja el.[113]

Az Ibtv. az elektronikus információs rendszerekben kezelt adatok esetében korlátozza a Magyarország területén kívüli kezelést és előírja, hogy egyes személyi hatály alá tartozó szervek – lásd 2. § (1) bekezdés a)–h) és j)–l) pontjai és, a monetáris politika végrehajtásával és a devizatartalék kezelésével kapcsolatos kockázatértékelési és portfóliókezelési tevékenység keretében kezelt adatok kivételével, a 2. § (1) bekezdés i) pontjában megjelölt szerv által kezelt adatok és a 2. § (2) bekezdés a), b) és e) pontjai – esetében az általuk kezelt, a nemzeti adatvagyon részét képező adatok csak Magyarország területén üzemeltetett és tárolt elektronikus információs rendszerekben, valamint diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetőek.[114]

Az Ibtv. a személyi hatálya alá tartozó egyes szervek (lásd 2. § (1) bekezdés a)–h) és j)–k) pontjai, a monetáris politika végrehajtásával és a devizatartalék kezelésével kapcsolatos kockázatértékelési és portfóliókezelési tevékenység keretében kezelt adatok kivételével) által kezelt adatok esetében biztosítja az EGT tagállamok területén belül üzemeltetett elektronikus információs rendszerekben történő adatkezelést is, amennyiben erre az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság engedélye vagy nemzetközi szerződésben előírt kötelezettség alapján kerül sor.[115]

4.3. Az elektronikus információs rendszerek biztonsági osztályba sorolása és a szervezetek biztonsági szintjének meghatározása

Az Ibtv. hatálya alá tartozó elektronikus információs rendszer és az ezekben kezelt adatok biztonsági kockázatának meghatározása és értékelése, a kockázatokkal arányos védelem kialakítása és biztosítása érdekében a szervezetnek el kell végezni az elektronikus információs rendszer biztonsági osztályba sorolását.[116] Ennek elvégzése a szervezet vezetőjének a felelőssége. A biztonsági osztályba

[111] Ibtv. 2. § (7) bekezdés
[112] Ibtv. 2. § (4) bekezdés
[113] Ibtv. 2. § (3)–(5) bekezdései
[114] Ibtv. 3. § (1) bekezdés
[115] Ibtv. 3. § (3) bekezdés
[116] Ibtv. 1. § (1) bekezdés 11. pont és 7. § (1) bekezdés

sorolás[117] célja, hogy meghatározásra kerüljön a felmért kockázatok[118] alapján az elektronikus információs rendszer védelmének elvárt erőssége.

A besorolás alapján meghatározott biztonsági osztály alapján kell megvalósítani az elektronikus információs rendszer teljes életciklusában a zárt, teljes körű, folytonos és kockázatokkal arányos védelmet úgy, hogy a szervezetnek meg kell határoznia azokat a külön jogszabályban előírt védelmi intézkedéseket, melyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást és a biztonsági események kezelését.[119]

Az Ibtv. hatálya alá tartozó szervezetnek a biztonsági osztályba sorolást minden egyes elektronikus információs rendszer esetében önbesorolás útján, 1-től 5-ig terjedő számozással ellátott skálán kell legalább háromévente elvégezni akként, hogy a számozás emelkedésével fokozatosan szigorúbb védelmi előírások kerültek megfogalmazásra.[120] Az Ibtv. rendelkezései alapján lehetőség van arra, hogy az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb vagy hatósági engedély birtokában alacsonyabb biztonsági osztály kerüljön megállapításra. Az ilyen egyedi esetek megalapozottságát a hatóság minden alkalommal ellenőrzi.

Az elektronikus információs rendszerek biztonsági osztályba sorolásával párhuzamosan, annak szabályrendszeréhez igazodva a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében kell elvégezni a szervezet vagy a szervezeti egység biztonsági szintjének[121] a meghatározását is, amely ugyancsak a szervezet vezetőjének a felelőssége. Az Ibtv. a szervezeti struktúra, az elektronikus információs rendszerek és a biztonsági követelmények eltéréseinek kezelése érdekében előírja, hogy az elektronikus információs rendszer

a) a) fejlesztését végző,
b) b) üzemeltetését végző,
c) c) üzemeltetéséért felelős vagy
d) d) információbiztonságáért felelős

szervezeti egységeket – az elektronikus információs rendszerek védelmére való felkészültségük alapján – a szervezettől elvárt, eltérő biztonsági szintekbe sorolhatók a külön jogszabályban meghatározott szempontok szerint.[122]

Fő szabály szerint a biztonsági szint meghatározását a korábban meghatározott biztonsági szint elérését követően legalább háromévenként kell elvégezni, azonban az elektronikus információs rendszer biztonságát érintő változás esetén vagy új elektronikus információs rendszer bevezetésekor, soron kívüli felülvizsgálatot kell elvégezni.[123]

A biztonsági osztályba sorolást és a biztonsági szint meghatározását dokumentált módon kell elvégezni. A dokumentációt a szervezet vezetője hagyja jóvá, eredménye – azaz azt, hogy az elektronikus információs rendszernek melyik biztonsági osztályba kell tartoznia és a szervezetnek milyen biztonsági szintet kell elérnie – a szervezet informatikai biztonsági szabályzatában kerül rögzítésre.[124]

A biztonsági osztályba sorolás értéke és az ezzel járó kötelezettségek a hatálya alá tartozó szervezetek esetében azokra az elektronikus információs rendszerekre is érvényesek, melyek az okoseszközökön IT alkalmazásként futtatásra kerülnek, vagy mint szolgáltatást a felhasználó igénybe veszi.

---

117 Ibtv. 1. § (1) bekezdés 12. pont

118 Ibtv. 1. § (1) bekezdés 28. pont, kockázat: a fenyegetettség mérte, amely mérték egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye

119 Ibtv. 7. § (4) bekezdés

120 Ibtv. 7. § (2) bekezdés

121 Ibtv. 1. § (1) bekezdés 13. pont, biztonsági szint: a szervezet felkészültségi szintje az Ibtv.-ben és végrehajtási rendeleteiben meghatározott biztonsági feladatok kezelésére

122 Ibtv. 9. § (2) bekezdés

123 Ibtv. 10. § (5) és (6) bekezdés

124 Ibtv. 7. § (3) bekezdés

Az Ibtv. alapelveinek figyelembevételével, az ún. kockázatokkal arányos védelem megvalósítása érdekében a szervezetnek az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: technológiai rendelet) 4. melléklete szerinti adminisztratív, fizikai és logikai védelmi intézkedéseket kell megtennie.

A technológiai rendelet rögzíti, hogy mely eljárásokat tekint helyettesítő biztonsági intézkedéseknek és a szervezet milyen feltételek teljesülése esetén alkalmazhat ilyen intézkedést.[125]

1. Az adminisztratív védelmi intézkedések között kerültek meghatározásra:
   a) a szervezeti szintű alapfeladatok,
   b) a kockázatelemzés,
   c) a rendszer és szolgáltatás beszerzés,
   d) üzletmenet- (ügymenet-) folytonosság elemzés
   e) a biztonsági események kezelése,
   f) az emberi tényezőket figyelembe vevő (személy)biztonság,
   g) a tudatosság és a képzés
   körében végrehajtásra kerülő védelmi intézkedési típusok.

2. A fizikai védelmi intézkedésekhez tartozó, a fizikai és környezeti védelem egyes elemeit felsoroló intézkedéseket (pl. élőerős védelem, tűzvédelem, áramellátás, klímatechnológia, stb.) a technológiai rendelet 4. mellékletének 3.2. pontja tartalmazza.

3. Az elektronikus információs rendszerek védelmét szolgáló intézkedések legnagyobb csoportját a logikai védelmi intézkedések alkotják, amelyek az adminisztratív és fizikai védelmet kiegészítve lehetővé teszik a teljes körű védelem kialakítását. Ezek az intézkedések kiterjednek az alábbi területekre:
   a) általános intézkedések,
   b) tervezés,
   c) rendszer és szolgáltatás beszerzés,
   d) biztonsági elemzés,
   e) tesztelés, képzés és felügyelet,
   f) konfigurációkezelés,
   g) karbantartás,
   h) adathordozók védelme,
   i) azonosítás és hitelesítés,
   j) hozzáférés ellenőrzése,
   k) rendszer- és információsértetlenség,
   l) naplózás és az elszámoltathatóság,
   m) rendszer- és kommunikációvédelem.

A védelmi intézkedések magvalósítása során a szervezet sajátosságaihoz igazodóan egyedi eltéréseket állapíthat meg
   a) a működtetéssel, környezettel,
   b) a fizikai infrastruktúrával,
   c) a nyilvános hozzáféréssel,
   d) a technológiával,

[125] Technológiai rendelet 4. melléklet 2. pont.

e) a biztonsági szabályozással,
f) a biztonsági intézkedések bevezetésének fokozatosságával,
g) a biztonsági célokkal
kapcsolatban.

A védelmi intézkedéseket a szervezet sajátosságaihoz, a kezelt adatokhoz és az elektronikus információs rendszerekhez igazodva egyedileg kell meghatározni.

4.4. Az elektronikus információbiztonság szervezetrendszere

A Kiberstratégia és az Ibtv. rendelkezései alapján a Kormány javaslattevő, véleményező szerveként az e-közigazgatásért felelős miniszter vezetésével létrehozásra került a *Nemzeti Kiberbiztonsági Koordinációs Tanács,* amely gondoskodik az Ibtv. hatálya alá tartozó szervezetek jogszabályokban meghatározott információbiztonsági tevékenységeinek koordinációjáról, és amelynek tevékenységét munkacsoportok segítik.

Az Ibtv. a hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét a Kormány által kijelölt hatóság (továbbiakban: *Hatóság*) látja el. A Hatóság feladata[126]:

a) a biztonsági osztályba és a biztonsági szintbe sorolás megalapozottságának vizsgálata és a vizsgálat eredménye alapján döntés meghozatala,
b) az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése,
c) az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése,
d) a hozzá érkező biztonsági eseményekről az eseménykezelő központ értesítése, hatósági eljárás megindítása,
e) javaslattétel a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, az Lrtv. szerinti ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére;
f) együttműködés az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvényben meghatározott elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,
g) kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal;
h) kapcsolattartás az eseménykezelő központokkal.

Az elektronikus információs rendszer ellenőrzésére irányuló eljárás eredményétől függően a Hatóság különböző jogkövetkezményeket[127] alkalmazhat:

a) Köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére, [128]
b) A felügyeleti szerv közreműködésre történő felkérése: csak költségvetési szerv esetében alkalmazható, abban az esetben alkalmazható, ha a szervezet az írásbeli felszólításnak nem tesz eleget.[129]

[126] Ibtv. 14.§
[127] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet (a továbbiakban: Korm. rendelet) 13. §
[128] Ibtv. 16. § (2) bekezdés a) pont, (3) bekezdés a) pont, Korm. rendelet 13. § (1) bekezdés
[129] Ibtv. 16. § (3) bekezdés b) pont

c) Az azonnali intézkedés megtételére való kötelezés: abban az esetben, ha az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelmény súlyos biztonsági esemény bekövetkeztével fenyeget.[130]
d) Bírságolás: 50 ezer forinttól 5 millió forintig terjedő bírság kiszabása, amely jogkövetkezmény költségvetési szerv esetében külön kormányrendeletben meghatározottak szerint alkalmazható.[131]
e) Információbiztonsági felügyelő kirendelése: csak költségvetési szerv esetében kerülhet sor, ha a szerv a jogszabályokban foglalt biztonsági követelményeket és az ezekhez kapcsolódó eljárási szabályokat nem teljesíti.[132]

Az állami és önkormányzati elektronikus információs rendszerek működését biztosító infokommunikációs infrastruktúrát, illetve az Ibtv. hatálya alá tartozó szervek nyílt elektronikus információs rendszereit – kivéve egyes meghatározott elektronikus információs rendszereket – érintő biztonsági események és fenyegetések kezelése érdekében kormányzati eseménykezelő központ működik a belügyminiszter irányítása alá tartozó Nemzetbiztonsági Szakszolgálat keretén belül működő *eseménykezelő központ* [Számítógépes Vészhelyzeti Reagáló Egység – Computer Emergency Response Team, (a továbbiakban: GovCert)].

A nemzeti szabályozás igazodik az Európai Unió Digitális menetrendjében megfogalmazott célokhoz, melyek között szerepel az európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok (CERT) hálózatának létrehozása. Ezen intézkedés végrehajtását szolgálja az Európai Parlament és a Tanács 2013. augusztus 12-i, 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Az irányelv – mely hatályon kívül helyezte a 2005/222/IB tanácsi kerethatározatot – meghatározza azokat a minimumszabályokat, amelyek mentén a tagállamoknak 2015. szeptember 4-ig harmonizálniuk kellett a vonatkozó nemzeti büntetőjogi szabályaikat.

5. Nemzetközi kitekintés, jó gyakorlatok itthon és más országokban

Az Európai Unió tagállamaként Magyarország is hozzájárul azon célok megvalósulásához, melyek a 2. fejezet Európai Uniós kapcsolódások részében említésre kerültek. Ezen célok olyan uniós dokumentumokban kerültek megfogalmazásra, melyek tagállami implementációt igényelnek, amely adminisztratív szinten magában foglalja nemzeti stratégiák megalkotását, intézkedési tervek kidolgozását és a kodifikációs munkát. A hosszútávú uniós célkitűzések eléréséhez (melyekhez az aktuális, 2014–2020 közötti uniós költségvetési időszak dedikált pályázati forrásokat allokál) a tagállami sajátosságokból adódóan minden országnak meg kell alkotnia saját cél- és eszközrendszerét annak érdekében, hogy valamennyi tagállam közel azonos fejlettségi és szabályozottsági szintet mutasson az uniós stratégiákban jelölt céldátumok elérésekor.

5.1. Nemzeti Infokommunikációs Stratégia

Az Európai digitális menetrendben foglaltakra is figyelemmel jelent meg 2014-ben a hazai IKT szektor fejlesztésének stratégiai irányait, fejlesztési prioritásait meghatározó *Nemzeti Infokommunikációs Stratégia* és Zöld Könyv.[133] A stratégia megvalósításának akciótervét a „Digitális Nemzet Fejlesztési

[130] Korm. rendelet 13. § (2) bekezdés
[131] Ibtv. 16. § (2) bekezdés b) pont, Korm. rendelet 13. § (5) bekezdés
[132] Ibtv. 16. § (3) bekezdés c) pont
[133] http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf

Program" megvalósításáról szóló 1631/2014. (XI. 6.) Korm. határozat tartalmazza. A Nemzeti Infokommunikációs Stratégia 2020-ig elérni kívánt célja a *Digitális Magyarország* létrehozása a kormányzat, az intézményi és a piaci szereplők együttműködésével. A Digitális Magyarország tehát kiterjed valamennyi hazai költségvetési és uniós forrásból megvalósítani kívánt IKT fejlesztésre és a nem kormányzati szektor részéről vállalt fejlesztésekre.

A Digitális Magyarország főbb céljai:

a) szupergyors internet elérhetővé tétele;
b) a helyi közösségek, valamint a teljes magyar közösség összetartozásának erősítése a digitális technológia révén;
c) az állam által nyújtott szolgáltatások fejlődése;
d) az ország versenyképességének növelése a digitális szolgáltatások, valamint a digitális készségek terjedésének elősegítése által;
e) digitális infokommunikációs alkalmazások, szolgáltatások elterjesztésének támogatásán keresztül az életminőség javítása minden élethelyzetben.

A következőkben röviden bemutatjuk a Digitális Magyarország program 4 pillérét és a Nemzeti infokommunikációs Stratégia jelenleg zajló felülvizsgálatának eddigi főbb megállapításait a 2013-2015. között felmért adatok tükrében.[134]

1. pillér: Szupergyors Internet

A Digitális Menetrendben megfogalmazott elvárás, hogy 2020-ra a háztartások legalább 30 Mbps-os sebességgel csatlakozhassanak a világhálóra. Hazánk a Digitális Magyarország program keretében vállalja, hogy ezt a célt 2018-ig teljesíti és biztosítja az egész országot lefedő, nagy sávszélességet (legalább 30 Mbps) biztosító infrastruktúra megépítését.

A Nemzeti Infokommunikációs Stratégia 2015-ben kezdődött monitoringja során végzett felmérések alapján Magyarországon 2015-ben a háztartások 78,5%-a ért el újgenerációs, vagyis legalább 30 Mbps sebességű internetkapcsolatra alkalmas hálózatot, ami meghaladja az uniós átlagot. A 100 Mbps feletti letöltési sebességre is képes negyedik generációs mobil szélessávú lefedettség 2015-ben a magyar háztartások 95%-a (uniós átlag 85,9%) számára vált elérhetővé, ami jelentős változást mutat a 2013. évi adatokhoz képest, amikor ez arány 39,1% volt.

2013 és 2015 között a mobil internet penetráció nagy mértékben növekedett, 34,5 előfizetés jut 100 lakosra, ez azonban nagy lemaradást mutat az uniós átlagtól (75,3). Magyarországon 2013. végén 2,62 millió mobil szélessáv előfizetést regisztráltak, 2015-ben már 3,39 millió aktív előfizetés volt. Az adatforgalmat bonyolító előfizetések aránya 2013-ban 78,9% volt, míg 2016-ben 90%, ami majdnem 50%-os bővülést jelent. Növekedett az adatforgalom mennyisége is, összesítve csaknem megháromszorozódott, az egy előfizető által éves szinten forgalmazott átlagos adatmennyiség pedig több mint kétszeresével nőtt.

A szolgáltatás minőségével kapcsolatos ügyfélelégedettségi adatokról a Nemzeti Média és Hírközlési Hatóság (a továbbiakban: NMHH) 2015-ben végzett kutatásából szerezhetünk információkat, melyek szerint a magyar internet felhasználók alapvetően elgédettek az igénybe vett internet szolgáltatással, a vezetékes szolgáltatásoknál nagyobb elégedettség tapasztalható, mint a mobilinternet szolgáltatások esetén. Mindkét esetben a kapcsolat megszakadása, illetve lelassulása az elsődlegesen jelzett probléma[135].

[134] A most ismertetett mutatók hazai és uniós szervek által elvégzett felmérések, hatásvizsgálatok értékelésén alapulnak.

[135] Forrás: NMHH számára készített kutatási jelentés, Lakossági internethasználat, Online piackutatás 2015, Ariosz Kft., NRC Kft.(http://nmhh.hu/dokumentum/170534/lakossagi_internethasznalat_2015_teljes.pdf)

A kormányzati hálózatok alapinfrastruktúráját vizsgálva megállapítható, hogy a Nemzeti Távközlési Gerinchálózat (NTG) vonatkozásában nagy mértékű infrastruktúrális bővítésre nem került sor, ugyanakkor a hálózatba bekötött intézményi végpontok száma 4500-ról 5500-ra nőtt.

Összességében elmondható, hogy bár kiemelkedő mértékű fejlesztés ment végbe az elmúlt három évben, 2015-ben még mindig kb. 1 millió háztartás számára nem állt fenn annak lehetősége, hogy a Digitális Menetrendben meghatározott legalább 30 Mbps sebességű internethálózathoz hozzáférjen. A Digitális Magyarország keretében megkezdődött nagyarányú hálózatfejlesztések és az NMHH frekvencia értékesítési folyamata nagyban hozzájárul a 2018-as végcél teljesítéséhez.

2. pillér: Digitális közösség és gazdaság

Az elektronikus szolgáltatások igénybe vételének lehetőségét kívánja megteremteni

a) eszközbeszerzések;
b) intelligens városi szolgáltatások bevezetése;
c) a térségi gazdaságfejlesztési programok lebonyolítása és
d) a helyi kis és középvállalkozások informatikai fejlesztése

által.

A Nemzeti Infokommunikációs Stratégia pillérei közül itt tapasztalható a legnagyobb elmaradás az uniós átlaghoz képest. Fontos megemlíteni, hogy az IKT export dinamikus mértékben növekszik, hazai felvevőpiaca vállalati oldalon azonban kétségeket ébreszthet (pl. a hazai kis- és középvállalkozások 10%-a vesz igénybe felhőszolgáltatást, honlappal csak 63% rendelkezik, e-kereskedelemből származó árbevételük 7,22%), mivel a negyedik ipari forradalom küszöbén sem rendelkeznek a magyarországi vállalkozások olyan digitális képességekkel, amelyek az itthoni IKT keresletet aktívabbá tehetnék.

3. pillér: E-közszolgáltatások

Ezen pilléren belül Magyarország célul tűzte ki, hogy a vállalkozások számára valamennyi, az állampolgárok számára pedig minél szélesebb körben elérhetővé tegye elektronikus úton a közszolgáltatásokat.

A 2007-2013-as programozási időszakban lezajlott fejlesztések okán az infrastrukturális feltételek adottak, ugyanakkor azok összetétele jelentősen heterogén képet mutat. A 2014–2020-as programozási időszakban – az uniós célkitűzésekre is figyelemmel – az e-közigazgatási szolgáltatások minél szélesebb körben történő elérhetővé tétele a prioritás. Elsőként a szolgáltatások határon túli átjárhatóságának uniós mutatóit vizsgálva megállapítható, hogy Magyarország jelentős elmaradásban van ezen a téren.

Szükséges azonban kiemelni, hogy 2016. július 1-jén hatályba lépett a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló az Európai Parlamenti és Tanácsi 910/2014/EU rendelet (a továbbiakban: eIDAS rendelet), annak hazai részletszabályait megteremtő jogforrások (az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény és annak végrehajtási rendeletei) várhatóan javítani fogják a szolgáltatás igénybe vételével kapcsolatos mutatókat. (A 2016 januárjában bevezetett új elektronikus személyazonosító kártya már megfelel az eIDAS rendeletben foglaltaknak).

A hazai e-közigazgatási szolgáltatások ügyfélelégedettségi mutatói kapcsán az Európai Bizottság a felmérései során azt a megállapítást tette, hogy 2012 és 2015 között lényegesen nem növekedett az e-közigazgatási szolgáltatások igénybevétele Magyarországon, bizonyos mutatók tekintetében még visszaesés is megfigyelhető. A e-kormányzati tájékoztatás 2013-as Eurostat vizsgálata szerint a magyar polgárok 44%-a szerint könnyű megtalálni az online keresett információt, és a kormányzat által elérhetővé tett információk hasznosnak tekinthetők. Az ügyfélkapun keresztül online intézhető

közigazgatási ügyek (így pl. születési anyakönyvi kivonat beszerzése, jogosítvány és műszaki engedély meghosszabbítása, adóbevallás online benyújtása) könnyen használhatóak. Kiemelendő, hogy Magyarországon az e-közigazgatási ügyek és információk mobil applikáción történő elérhetősége jelentősen elmarad az uniós átlagtól.

4. pillér: Digitális készségek

A digitális írástudás készségének elterjesztése, továbbá a magas szintű közép- és felsőoktatási IT-képzés megvalósítása teszi lehetővé, hogy a fenti három pillér eredményei hasznosuljanak.

A 2013-2014. évi használati szokásokat vizsgáló kutatások adatai azt mutatják, hogy a magyarországi internet használók jelentős részben kizárólag alapszintű online szolgáltatásokat (pl. információ keresése, közösségi médiahasználat, online hírportál/magazin olvasása, film, zene, játék letöltése, oktatással kapcsolatos böngészés) vesznek igénybe, értéknövelt, online kereskedelmi vagy fizetési tranzakciót is magába foglaló tevékenységekkel (pl. online bankolás, e-közigazgatási szolgáltatások igénybevétele, hazai és határon túli online vásárlás) szemben – az enyhe növekedés ellenére is – távolságtartás figyelhető meg. A legtöbb vizsgálat szerint ez két okra vezethető vissza: egyrészt megjelennek a digitális írástudatlanokra jellemző jegyek („nem tudom használni", „túl bonyolult", „nincs rá szükségem" stb.), másrészt egy tudatos magatartás tapasztalható, ami abból fakad, hogy a felhasználók a személyes adatokkal való visszaéléstől tartva bizalmatlanok az ilyen jellegű szolgáltatásokkal szemben.

Figyelemre méltó adat a Bell Research 2012. és 2014. évi Magyar Infokommunikációs Jelentésében az, hogy bár az internetet nem használók száma az elmúlt három évben 6%-kal mérséklődött, Magyarországon 3,5 millió ember még mindig nem rendelkezik digitális kompetenciával.

A Nemzeti Infokommunikációs Stratégiához kapcsolódó Zöld Könyvben (mely a stratégia végrehajtását szolgáló legfontosabb beavatkozási területeket és akciókat részletezi) megfogalmazott több intézkedés is kapcsolódik a lakosság, a közigazgatásban dolgozók és a vállalkozások digitális kompetenciájának fejlesztéséhez.

A Zöld Könyv egyebek mellett célul tűzi ki a köznevelésben és felsőoktatásban dolgozók (tanárok, oktatók) körében az alap-, közép- és felső szintű digitális kompetenciák elsajátításának támogatását, hogy ezáltal motiválhassák a diákokat ilyen irányú ismereteik bővítésére, az IKT eszközök tudatos és biztonságos használatára. Közvetlenül a diákok digitális tudatosságát célzó intézkedés a Zöld Könyvben, hogy az internetes bűnözés elleni védekezés a pedagógus továbbképzés, illetve az iskolai tananyag részévé váljon azáltal, hogy a tudatos médiahasználat beépítésre kerül a pedagógus továbbképzések programjába és az iskolai tananyagokba, és olyan alapfogalmakat, kérdésköröket ismertet meg és tudatosít a diákokban mint a biztonság vs. szabadság, számítógépes és internetes bűncselekmények, csalás, visszaélés, szerzői jogi jogsértés, torrentoldalak, digitális adatvédelem).

5.2. Magyarország Digitális Oktatási Stratégiája

A Kormány a köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és *Magyarország Digitális Oktatási Stratégiájáról* szóló 1536/2016. (X. 13.) Korm. határozatával elfogadta a teljes magyar oktatási-képzési rendszerre (köznevelés, szakképzés, felsőoktatás, felnőttkori tanulás) kiterjedő átfogó Digitális Oktatási Stratégiát (a továbbiakban: DOS) azzal a céllal, hogy *„az ágazati stratégiákkal és szakmai célkitűzésekkel összhangban az oktatási rendszer minden szintjén megteremtse a digitális írástudás tényleges elterjesztésének lehetőségét, hozzájárulva Magyarország versenyképességének növeléséhez."*[136] A DOS és annak előkészítés alatt álló intézkedési terve a Digitális Magyarország 4. pillérének megvalósítását szolgálja.

[136] Magyarország Digitális Oktatási Stratégiája, Vezetői összefoglaló 7. oldal https://2015-2019.kormany.hu/download/a/59/d0000/Magyarorsza%CC%81g%20Digita%CC%81lis%20Oktata%CC%81si%20Strate%CC%81gia%CC%81ja.pdf

A továbbiakban a DOS azon megállapításait és céljait vesszük sorra, melyek jelen tananyagunk szempontjából relevánsak, ezáltal betekintést nyújtva a hazai oktatási-képzési rendszer hatályos infrastrukturális viszonyaiba, adatvédelmi és információbiztonsági helyzetébe, továbbá a pedagógusok és a tanulók digitális kompetenciájának jelenlegi színvonalába és az ezen tényezők javítását célzó intézkedésekbe.

A DOS előkészítése során elvégzett helyzetelemzés megállapította, hogy:

1. a köznevelés esetében:
   - *a)* bár a digitális készségek átadása kimeneti célként szerepel a Nemzeti Alaptantervben, de a horizontális elvárásként megfogalmazott absztrakt követelmények teljesítéséhez (tanulási életút nyomon követése, oktatás akadálymentesítése, biztonságtudatosságra nevelés) a pedagógusoknak nem állnak rendelkezésre egységes irányelvek, tananyagok, útmutatások és legfőképpen egységes, megbízhatóan működő infrastruktúra;
   - *b)* az eszközállomány elavult,
   - *c)* a pedagógusok kevéssé használják az IKT-eszközöket és a modern technológiát;
   - *d)* a tanulók jelentős része digitális írástudatlanként hagyja el a köznevelést;
   - *e)* az informatikaoktatást támogató számítástechnika termek eszközfelszereltségét jogszabály határozza meg[137], azonban általánosságban véve az oktatást támogató infrastruktúrára vonatkozó szabályozás nem került megalkotásra;
   - *f)* szinte valamennyi iskolában van IKT-terem;
   - *g)* 5500 iskolai végpontot érhető el az internet, 1700 köznevelési intézményben van WiFi-szolgáltatás;

2. a szakképzés esetében:
   - *a)* a szakképző intézményekben továbbtanuló diákok körében magasabb a digitális írástudatlanok aránya, mint a gimnáziumi tanulók esetében;
   - *b)* az iskolák sok esetben nem rendelkeznek az adott szakmák legújabb technológiáinak bemutatásához szükséges feltételekkel;
   - *c)* az oktatók nem rendelkeznek megfelelő digitális tudással és pedagógiai-módszertani ismerettel ahhoz, hogy a tanítási-tanulási folyamatot digitális környezetbe helyezzék;
   - *d)* az elavuló eszközrendszer soha nem volt alkalmas a digitális pedagógia kiszolgálására.

3. a felsőoktatás esetében:
   - *a)* az IKT alapinfrastruktúra egyes területeken kimagasló, világszínvonalú (HBONE+ rendszer), egyes területeken azonban az EU-átlag alatti;
   - *b)* a felsőoktatásba belépő hallgatók közel 100%-a rendelkezik megfelelő digitális munkaeszközökkel (laptop, okostelefon, asztali számítógép), ezeknek az oktatási folyamatba történő aktív bevonása azonban nem megoldott;
   - *c)* a számítástechnikai infrastruktúra cseréje, illetve a jogtiszta szoftverek beszerzése ajánlott;
   - *d)* alacsony szintű a digitális támogatás a kurzusok elvégzése alatt;
   - *e)* a hazai szakok leírásai nagyon csekély mértékben tartalmaznak a hagyományostól (előadás, szeminárium, gyakorlat) eltérő munkaformákat;
   - *f)* az e-közszolgáltatások területén a felsőoktatás kimagasló eredményt mutat, a célcsoport egésze lefedett e szolgáltatásokkal.

[137] A nevelési-oktatási intézmények működéséről és a köznevelési intézmények névhasználatáról szóló 20/2012. EMMI rendelet

4. a felnőttkori képzés esetében:
   a) kevesen jutnak el a digitális írástudás magasabb szintjeire, illetve jelentkeznek és fejezik be sikeresen az IKT szakmai képzéseket;
   b) a leginkább digitális készségfejlesztésre szorulók nem rendelkeznek otthoni eszközökkel és internet-hozzáféréssel;
   c) a felnőttek digitális kompetenciái hiányoznak ahhoz, hogy bekapcsolódjanak a digitális tanulásba;
   d) a felnőttkori tanulás szereplői nem használják ki az IKT-ban rejlő lehetőségeket;
   e) a rendelkezésre álló digitális tananyagok köre nehezen átlátható és kereshető.

A DOS egyebek mellett az alábbi eszközcsoportokat és akciókat rögzíti:
1. a köznevelés tekintetében:
   a) a digitális kompetencia követelmények megállapítása a pedagógusok, oktatók, szakoktatók és a tanulók számára;
   b) a tanulási feladatok közé az információkeresés, feldolgozás, kollaboráció IKT-val támogatott megoldásainak beépítése, valmint a médiatudatosság fejlesztése;
   c) az IKT gyakorlati alkalmazásának beépítése a természettudományos tantárgyak elsajátításába;
   d) a diákok életkori sajátosságainak, igényeinek megfelelő elektronikus tananyagok elérhetővé tétele;
   e) a tantermi és szaktantermi digitális eszközök kötelező tantermi felszereltséggé tétele;
   f) internet-tudatosság és biztonságtudatos magatartás beépítése a köznevelés rendszerébe a pedagógusok továbbképzésén keresztül (már az óvodai nevelésben meg kell találni a helyét a kisgyermekkori informatikai nevelésnek);
   g) legalább 100 Mbps az 500 fő alatti, és legalább 1 Gbps sávszélesség biztosítása az 500 fő feletti gyermek-, illetve tanulói létszámú köznevelési intézményekben (idővel a tantermek internet ellátottságát biztosító Gb/s helyi hálózat kialakítása);
   h) WiFi-lefedettség biztosítása minden tanteremben és iskolai könyvtárban;
   i) tanterem menedzsment szolgáltatás biztosítása a tanteremben lévő számítógépek és mobil eszközök kezelésére (képernyőmegosztás, internetelérés letiltása, felhasználó kezelés);
   j) a tanulók saját eszközeinek bevonása a tanítási folyamatba;
   k) a pedagógusok számára mobil informatikai eszközkészlet biztosítása a tantermen kívüli foglalkozásokhoz is.

2. szakképzés tekintetében:
   a) szakma-specifikus informatikai követelmények és digitális tartalmak meghatározása;
   b) oktatók képzése, speciális továbbképzések biztosítása;
   c) digitális infrastruktúrafejlesztés a szaktantermekben és a tanműhelyekben;
   d) a helyi adatforgalom biztosításához szükséges Gb/s hálózat kialakítása és WiFi-lefedettség biztosítása minden tanteremben és gyakorlati képzőhelyen.

3. a felsőoktatás vonatkozásában:
   a) digitális tankönyvtár továbbfejlesztése;
   b) tiszta-szoftver program kiterjesztése és megújítása;
   c) digitális taneszköz, eszköz és tananyag fejlesztése;
   d) az egyetemi honlapok többnyelvűsítése és akadálymentesítése.

4. felnőttkori tanulás vonatkozásában:
   a) digitális tanulást népszerűsítő promóciók;
   b) elektronikus közszolgáltatások széles körben történő elterjesztése;
   c) informatikai szakmai képzéseken való részvétel ösztönzése;
   d) digitális tartalmak és nyitott oktatási segédanyagok biztosítása.

Információbiztonsági és adatvédelmi szempontból kiemelendő, hogy a DOS horizontális pilléreinek egyike a Biztonság, melynek eszközrendszerét a dokumentum az alábbiak szerint határozza meg:
   a) biztonságtudatosság növelése a gyermekek, szülők és hozzátartozók esetében;
   b) jogi lehetőségek széleskörű ismertetése és tudatosítása;
   c) szankcióalkalmazás és kommunikáció erősítése;
   d) segítségnyújtás és áldozatsegítés erősítése és kiterjesztése;
   e) rendszergazdák információbiztonsággal kapcsolatos kompetenciáinak erősítése;
   f) kríziscenter kialakítása;
   g) központi ajánlás és támogató rendszer;
   h) biztonságos információmenedzsment technikák tanítása;
   i) a pedagógusok információbiztonsági képzése;
   j) rendszeres információbiztonsági oktatás és képzés;
   k) cyber-bullying segélyvonal.[138]

Különösen fontos, hogy ezzel a témakörrel kiemelten foglalkozik a DOS, mivel a nemzetközi és hazai felmérések is azt mutatják, hogy a köznevelési és szakképzési intézményekben tanulók rendszeresen használnak IKT-eszközöket, gyakori internet használók, ezáltal szinte kivétel nélkül találkoztak már káros tartalmakkal, kockázatos tevékenységekkel a világhálón. A felmérésekből azonban az is látható, hogy a megkérdezett gyermekek többsége nincsen tisztában azzal, hogy miként kezelje, előzze meg a számára veszélyt jelentő tartalmakat.

Nem szabad figyelmen kívül hagyni a DOS első horizontális pillérét, a Tanulási életút nyomon követését sem. Oktatási területen jelenleg öt nagy adatbázis létezik (Köznevelési Információs Rendszer; Felsőoktatási Információs Rendszer; Komplex szakmai vizsgán kiadott bizonyítványok központi elektronikus nyilvántartása; Felnőttképzési Információs Rendszer; Felnőttképzési statisztikai adatbázis), melyek párhuzamosan működnek. A DOS a Tanulási életút nyomon követése horizontális pilléren belül a meglévő adatbázisok, nyilvántartások összekapcsolását tűzte ki célul, hogy egy átfogó, komplex módon hasznosítható ágazati oktatási információs rendszer jöjjön létre. Ez pedig csak a korábban felvázolt adatvédelmi és személyiségi jogi jogszabályi keretek között történhet meg.

5.3. Magyarország Digitális Gyermekvédelmi Stratégiája

A DOS-hoz szorosan kapcsolódik a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és *Magyarország Digitális Gyermekvédelmi Stratégiájáról* szóló 1488/2016. (IX. 2.) Korm. határozattal elfogadott Digitális Gyermekvédelmi Stratégia (a továbbiakban: DGYS), mely ugyancsak a Digitális Magyarország 4. pillérének végrehajtását támogatja.

A DGYS három egymásra épülő pilléren nyugszik, ezen pillérek mentén kerültek meghatározásra a digitális gyermekvédelem terén elérendő célok és az azok megvalósítását szolgáló eszközök.

[138] Magyarország Digitális Oktatási Stratégiája, 25. oldal https://2015-2019.kormany.hu/download/a/59/d0000/Magyarorsza%CC%81g%20Digita%CC%81lis%20Oktata%CC%81si%20Strate%CC%81gia%CC%81ja.pdf

1. Tudatosítás és médiaműveltség

Az első pillér megelőző célt szolgál azáltal, hogy a tudatosság növelésében részt vevők (köznevelés, állami szféra szereplői, civil szervezetek, piaci szereplők, szakmai, érdekképviseleti szervek, szülők) aktívan közreműködnek abban, hogy rendszeres és célzott kommunikációval a gyermekek és fiatalkorúak egészséges fejlődését káros hatások ne érjék, illetve annak szintje csökkenthető legyen.[139]

A DGYS-ben az első pillérhez megfogalmazott stratégia célok az alábbiak:

a) a gyermekek internethasználatát vizsgáló monitoring rendszer felállítása és rendszeres mérések, kutatások elvégzése,
b) a gyermekek médiaműveltség oktatása,
c) tanárképzés és tananyagfejlesztés (a DOS célkitűzéseiben is megjelenik),
d) egyéb érdekeltek (igazságszolgáltatás, rendvédelem képviselői, iskolapszichológusok, szociális munkások) képzése,
e) gyűjtőhonlap az internetes gyermekvédelemhez kapcsolódó információkról és azok hitelesítése.

2. Védelem és biztonság

Ugyancsak preventív célú a DGYS második pillére. Az itt megjelenő intézkedések elsődleges letéteményese az állam a vonatkozó jogszabályi keretek és az azt érvényesítő szervezetrendszer kialakításával. Mindez azonban mit sem ér, ha a gyermek nem rendelkezik mindazon alapvető ismeretekkel, amelynek birtokában képes a veszélyt felismerni és arra felkészülten reagálni. A védelmet tehát elsőként a tudatosítással lehet és kell biztosítani, erre építkezve lehet egyéb olyan lehetőségeket a védelem szolgálatába helyezni, mint például az oldalakon elhelyezett figyelemfelhívó tájékoztatás a káros tartalomhoz való hozzáférést megelőzően vagy szűrőszoftverek alkalmazása.

A gyermekek jogainak védelmére irányuló hatályos magyar jogi szabályozás alapját az Alaptörvény XVI. cikk (1) bekezdése képezi, mely szerint minden gyermeknek joga van a megfelelő testi, szellemi és erkölcsi fejlődéséhez szükséges védelemhez és gondoskodáshoz.

Az Alaptörvény mellett a Polgári Törvénykönyvről szóló 2013. évi V. törvény személyiségi jogok védelmének alapvető rendelkezéseit határozza meg, míg a Büntető Törvénykönyvről szóló 2012. évi C. törvény számos büntetőjogi tényállás megfogalmazásával értékeli a gyermekek sérelmére elkövetett cselekményeket (pl. személyes adattal visszaélés, zaklatás, magántitok megsértése, rágalmazás, becsületsértés, tiltott adatszerzés, információs rendszer vagy adat megsértése). Az adatvédelemmel és információbiztonsággal összefüggő bűncselekmények körét a 2. fejezetben már ismertettük.

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) – összhangban az Európai Parlament és a Tanács 2000. június 8-i 2000/31/EK irányelvével a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól – fontos szabályokat rögzít a kiskorúak védelme érdekében (figyelemfelhívó tájékoztatás elhelyezése az internetes oldalon arról, hogy az aloldalon a kiskorúra nézve káros tartalom található). Hasonló jellegű szabályt tartalmaz a fogyasztóvédelemről szóló 1997. évi CLV. törvény a játékszoftverek csomagolásán elhelyezendő tájékoztatóról és a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény a felelős játékszervezés érdekében.

[139] Nagyon fontos szerepet tölt be a tudatosításban a Nemzeti Média- és Hírközlési Hatóság Bűvösvölgy Médiaértés-oktató Központja. A civil szervezetek közül kiemelendő a Nemzetközi Gyermekmentő Szolgálat, mely konzorciumi partnere az Európai Unió Safer Internet programjának (www.saferinternet.hu), a Digitális Tudás Akadémia önkéntes oktató hálózata, valamint az UNICEF Magyar Bizottság Alapítvány és a Telenor Magyarország Ébresztő-óra Programja.

Manapság számos jó hazai és nemzetközi gyakorlat alakult ki az online gyermekvédelem kapcsán, melyek a tudatos médiahasználatot és a gyermekek káros tartalmakra való reagálását segíti elő.[140]

A DGYS második pilléréhez kapcsolódó stratégiai célkitűzések:

a) megfelelős szűrőszoftver-megoldások folyamatos biztosítása,
b) káros tartalmak szűrésére vonatkozó alternatív megoldások összegyűjtése nemzetközi példák alapján,
c) hatékony műszaki megoldások alkalmazása,
d) veszélyes és javasolt tartalmakról lista összeállítása,
e) a biztonságos és hasznos tartalmak körének bővítése a gyermekek számára,
f) iparági társszabályozás erősítése a média- és hírközlési piacon működő szervezetek számára,
g) büntetőjog ultima ratio jellege.

3. Szankcióalkalmazás és segítségnyújtás

A DGYS harmadik pillére arra esetre vonatkozó hatékony intézkedéseket hangsúlyozza, amikor a tudatosítás és a védelmi intézkedések ellenére a gyermeket negatív hatás éri a digitális eszköz használata során. A káros következmény feltárása esetén egyrészt segítséget kell nyújtani a gyermek számára, másrészt a sérelmet meg kell szüntetni és szankcionálni kell azt.[141]

A szankcionálásnak[142] jelen esetben van egy speciális formája, a jogsértő tartalmak elérhetetlenné tétele, melynek részletes szabályait az Ekertv. tartalmazza (13. §). Ezen részletesen szabályozott eljárásrend alkalmazására még az előtt lehetőség van, hogy a sérelmes ügyben polgári peres vagy büntetőeljárás indulna.

A DGYS harmadik pilléréhez kapcsolódó stratégiai célkitűzések:

a) információgyűjtés a sérelmes magatartások számáról, jellegéről, típusáról,
b) alternatív sérelemkezelési eljárások annak érdekében, hogy az érintett gyermek kezelése minél kíméletesebb módon történjen,
c) online megfélemlítés (cyberbulling) kezelése,
d) a jogorvoslati lehetőség széles körben történő ismertté tétele.

A DOS és a DGYS tehát olyan intézkedések és programok összefoglalója a magyar állampolgárok számára, melyek elősegítik, hogy tudatos használóivá, fogyasztóivá váljanak a digitális világ nyújtotta a lehetőségeknek, eszközöknek.

5.4. Okos Város (Smart City)

Röviden bemutatnánk az okos város (smart city) projekttel kapcsolatos legfontosabb információkat, az ezzel összefüggésben felmerülő adatvédelmi és egyéb kihívások, hazai és nemzetközi példák és jó gyakorlatok tekintetében. Jelen fejezetben a Smart City jogi vetületét kívánjuk ismertetni, áttekintve az Európai Unió és hazánk által a tárgyhoz kapcsolódóan meglévő (és leginkább hiányzó) szabályozókat és egyéb dokumentumokat, szabályozási kérdéseket.

[140] Ilyen pl. az Egyesült Királyságban 2013. óta tartó gyakorlat, melynek értelmében a szolgáltatók önként korlátozzák a pornográf tartalmak elérését a WiFi-szolgáltatások és valamennyi eszköz esetén is, tehát az új előfizetőknek már egy a Gyermekek Számára Biztonságos Internetszolgáltatást nyújtanak a szolgáltatók.

[141] A Nemzeti Infokommunikációs Stratégia Zöld Könyvében külön intézkedés vonatkozik a számítógépes bűnözés (gyermekekkel szembeni bűncselekmények, digitális kalózkodás digitális adat- és információlopás, stb.) elleni hatékony hatósági fellépés jogszabályi hátterének megteremtésére. Kapcsolódó feladatként került meghatározásra a gyermekvédelmi és kiberbűnözés elleni forródrót széles körben történő ismertté tétele.

[142] A gyermekvédelmi jogszabályi előírásokat lásd korábban.

Az Okos Város programok sajátossága, hogy számos részelemből tevődnek össze. A Lechner Tudásközpont által elkészített Smart City Tudásplatform Metodikai Javaslat[143] definíciója szerint az *„okos város egy komplex stratégiát, az ebben foglalt célkitűzések és a meglévő eszközök, fejlesztések és infrastruktúrák összehangolását és egymást szolgáló tervezését jelenti a fenntarthatóság és hatékonyság jegyében”*. A fogalomból is érzékelhető, hogy nincs egységes, szabványosított tartalma, stratégiája az okos város programnak, annak egyes részelemei országonként, sőt városonként változhatnak. Ebből következően sem Magyarországon, sem az Európai Unióban nem találunk átfogó, egységes okos város szabályozást. A vonatkozó szabályozás vizsgálatakor tehát az egyes részelemekre irányadó rendelkezéseket és jogi kötőerővel nem bíró dokumentumokat tudjuk figyelemben venni.

Az Európai Unió, így kiemelten annak Regionális Bizottsága állandó napirendjén szerepel a városfejlesztés kérdése, amely szorosan kapcsolódik az *Európa 2020 növekedési stratégia* és a *Digitális Menetrend* fent bemutatott célkitűzéseihez. Ennek megvalósítását szolgálja a Regionális Bizottság 2011-ben készült *„Jövő városai”* elnevezésű tanulmánya[144], amely szerint az európai városokat érintő kihívásoknak egy új típusú irányítási rendszer kidolgozásával lehet megfelelni, melyben a *„társadalmi-gazdasági, kulturális, generációs és etnikai sokféleségben rejlő lehetőségeket az innováció szolgálatába kell állítani”*.

Ezen tanulmány képezi alapját a 2016 nyarán elfogadott *uniós városfejlesztési menetrend*nek[145], mely 12 kiemelt témát ölel fel és ezek megoldására 12 partnerséget hoz létre, amelyek egyenként 15–20, azonos alapon együttműködő érdekelt felet fognak össze. A kiemelt témák között szerepel a digitális átállás is, melynek fókuszában az adatgyűjtés (beleértve az adatgazda kérdéskörét), a nyilvános adatok felhasználása, az adatkezelés, valamint a digitális szolgáltatások, valamint az idős és fogyatékos személyek számára biztosított digitális közszolgáltatásokhoz történő hozzáférés áll. Az uniós városfejlesztési menetrend nem titkolt célja, hogy az annak megvalósítása során szerzett tapasztalatok egyfajta indikátorként szolgáljanak az uniós döntéshozók számára az európai szintű szabályozók megalkotásához.

Az Európai Unió régiói és települései közötti együttműködést, információcserét hivatott szolgálni az Európai Innovációs Térség (EIP) *Okos Városok és Közösségek programja*[146], mely jelenleg 13 kategóriában nevez meg kutatás-fejlesztés-innovációt támogató programot (pl. adatkezelés, állampolgár központúság, integrált infrastruktúrák az IKT területen, standardizáció) a részt vevők számára.

Fontos megemlíteni még két további együttműködési formát. Az *URBACT*[147] abban segít a részt vevő településeknek, hogy olyan új és fenntartható gyakorlati megoldásokat találjanak, melyek összekapcsolják a városok gazdasági, szociális és környezeti megoldásait. Az 1986-ban alapított több mint 130 tagú *EUROCITIES*[148] (melynek Budapest is tagja) a stratégiaalkotás és a kutatás-fejlesztés területén segíti a partner városokat hat tematikus témakörben (kultúra, gazdaság, környezet, tudásalapú társadalom, mobilitás, társadalmi ügyek, együttműködés) történő információ átadással.

Magyarországon a 2010–2014. közötti időszakra szóló *Digitális Megújulás Cselekvési Terv* a célok között nevesítette a Smart City – „Élhető és intelligens város” elnevezésű pilot projektet, hogy *„legyen legalább egy olyan város(rész) Magyarországon, amelyben a leginnovatívabb magyar IKT megoldások élhetőbbé és intelligensebbé tesznek egy város(rész)t”*. A cselekvési tervben megfogalmazottak alapján az IKT szektor több piacvezető vállalkozása is kínált a közigazgatás szereplői számára eszközöket, tartalmakat, melyekhez a hagyományos jogszabályi keretek között, az általános közbeszerzési szabályok alkalmazása mellett lehetett hozzáférni, mely sok esetben időigényes,

143 http://lechnerkozpont.hu/doc/okos-varos/smart-city-tudasplatform-metodikai-javaslat.pdf

144 http://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/citiesoftomorrow/citiesoftomorrow_summary_hu.pdf

145 http://ec.europa.eu/regional_policy/sources/policy/themes/urban-development/agenda/pact-of-amsterdam.pdf

146 https://eu-smartcities.eu/

147 www.urbact.eu

148 www.eurocities.eu

bonyolult folyamatot jelentett nem szolgálva ezzel az állampolgárokkal történő kapcsolattartás gördülékenyebbé tételét.

A fenti cselekvési tervet váltotta fel 2014-ben az Európai Unió Digitális Menetrendjéhez kapcsolódó Nemzeti Infokommunikációs Stratégia és az annak végrehajtását szolgáló Digitális Nemzet Fejlesztési Program (a továbbiakban: DNFP; a stratégia és a DNFP együtt: Digitális Magyarország program, részletesebben ld. 5.1. pont). A Digitális Magyarország Program négy pillére közül a Digitális Közösség és Gazdaság pillérhez tartozik az intelligens városi szolgáltatások bevezetése.

A „Digitális Nemzet Fejlesztési Program" megvalósításáról szóló 1631/2014. (XI. 6.) Korm. határozat 7. a) alpontja feladatként rögzítette az intelligens városi szolgáltatások elterjesztéséhez kapcsolódó koncepciót, melyet a Lechner Tudásközpont készített el. A koncepció megalapozását szolgálja a „Digitális Nemzet Fejlesztési Program" település-központú kísérleti alprogramjának megvalósításához szükséges források biztosításáról szóló 1854/2014. (XII. 30.) Korm. határozat 3. b) alpontja alapján Nyíregyházán elindult intelligens városi szolgáltatási modellprogram, amely példaértékű megoldásokat mutathat be az adatvédelmi és információbiztonsági kihívások kezelése során.

A Digitális Nemzet Fejlesztési Program megvalósításával kapcsolatos aktuális feladatokról, valamint egyes kapcsolódó kormányhatározatok módosításáról szóló 1486/2015. (VII. 21.) Korm. határozat 9. pontja 2018. december 31-i határidővel előírja a Digitális Magyarország program megvalósítását elősegítő, annak gazdasági, társadalmi és versenyképességi hatásait bemutató monitoring rendszer kiépítését, valamint működtetését. Ezen folyamat keretében megkezdődött az ún. jogi akadálymentesítés, elfogadás, illetve hatályba lépés előtt áll több az adózási terheket, az informatikai eszközök és kapcsolódó szolgáltatások beszerzését könnyítő jogszabályi rendelkezés. Ugyanezen kormányhatározat a Lechner Tudásközpont feladatává tette az intelligens városi szolgáltatások összehangolt bevezetését és működtetését támogató szervezeti- és tudásplatform létrehozását és működtetését, valamint a teljes rendszer működésének monitoringját.

A nemzetközi példák azt mutatják, hogy a városértékelések számos eltérő alrendszert vizsgáltak egy-egy város smart city szempontú áttekintése során, azonban jellemzően hat főcsoportra lehet tematizálni a vizsgált szempontokat:

a) Okos mobilitás (közlekedés),
b) Okos környezet (környezetvédelem, környezeti fenntarthatóság, levegővédelem, zöld épületek),
c) Okos emberek (tudásmenedzsment, oktatás képzés, továbbképzés),
d) Okos életkörülmények, életminőség (szociális háló, kultúra, településfejlesztés),
e) Okos kormányzás (információbiztoság, adatvédelem, közbeszerzés, e-aláírás),
f) Okos, fenntartható gazdaság (kereskedelem, szakképzés, kutatás-fejlesztés-innováció)[149].

Valamennyi szempont tekintetében elmondható, hogy sem uniós szinten, sem Magyarországon nem valósult meg az adott területet átfogó jogi szabályozás. A fenti főcsoportokat magukba foglaló szakterületek szakmai szintű szabályozása megtörtént, smart city szempontú összehangolásukra azonban ezidáig a legtöbb esetben nem került sor.

Az egyes dokumentumok és együttműködési platformok részletes tanulmányozása alapján elmondható, hogy hosszú távon nem lehet megoldás az okos város programba tartozó részelemek szigetszerű fejlesztése, kidolgozása, hanem biztosítani kell ezen folyamatok átjárhatóságát, az adatok és a fejlesztés során alkalmazott technológiák összeegyeztethetőségét, és szükségszerűen a vonatkozó jogi szabályozó eszközök megalkotását, különös tekintettel az adatvédelmi kérdések rendezésére.

Az okos város projektek jelentős része IKT fejlesztésre, az adatok cseréjének biztosítására alapoz, ezért az ilyen fejlesztések révén létrejövő informatikai rendszerek védelme és adatok biztonsága kiemelt fontosságú. Ennek is köszönhető az, hogy az okos város fent ismertetett hat területe közül az

[149] A Lechner Tudásközpont magyar városokra kidolgozott Településértékelés és Monitoring módszertani javaslata is ezen alrendszereket javasolja vizsgálni: http://lechnerkozpont.hu/doc/okos-varos/telepulesertekeles-es-monitornig-modszertani-javaslat.pdf

Okos Kormányzás területén születettek meg hazai és uniós szinten is azok a szabályozó eszközök és ajánlások, melyek biztosítják az átjárhatóságot és a tagállami szabályozók egymáshoz közelítését (lásd: Infotv., Ibtv.). 2018-ban fogadták el az okos város központi platformszolgáltatás létrehozásáról és működtetéséről szóló 252/2018. (XII. 17.) Korm. rendeletet, 2021-ben pedig a településtervek tartalmáról, elkészítésének és elfogadásának rendjéről, valamint egyes településrendezési sajátos jogintézményekről szóló 419/2021. (VII. 15.) Korm. rendeletet.

5.5. Bizalmi szolgáltatások

Végezetül szükséges kitérni arra a körülményre, hogy a papír alapú dokumentumok helyett egyre szélesebb körben terjed az elektronikus okirat és a hagyományos, papír alapú szerződéskötés vagy hatósági eljárás helyett az elektronikus szerződéskötés és ügyintézés alkalmazása. 2014 júliusában jelent meg az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (a továbbiakban: eIDAS rendelet). Az eIDAS rendelet az uniós szintű elektronikus tranzakciókkal kapcsolatos bizalom, az online köz- és magánszolgáltatások, valamint az e-kereskedelem hatékonyságának növelése érdekében közvetlenül alkalmazandó általános hatállyal bíró rendelkezéseket tartalmaz a tagállamok számára.

Az eIDAS rendelet egyrészt felszámolja az elektronikus azonosítás használatát akadályozó korlátokat az EU-ban, amely azt jelenti, hogy a biztonságos elektronikus tranzakciók megkönnyítése érdekében a rendeletben meghatározott feltételek teljesülése esetén valamely uniós országban kiadott elektronikus azonosítót az összes többi uniós országban is el kell ismerni 2018 őszétől. Az elektronikus azonosítási rendszereknek a három **biztonsági** (alacsony, jelentős, magas) **szint** egyikét meg kell jelölniük az adott rendszer szerint kiadott elektronikus azonosítási eszközhöz. A kölcsönös elismerés kizárólag akkor kötelező, amikor az illetékes közigazgatási szerv a „jelentős" vagy a „magas" szintet használja az adott online szolgáltatás eléréséhez. **A kölcsönös elismerés és az átjárhatóság biztosítása okán az elektronikus azonosítási rendszerrel szemben alapvető követelmény a technológia semlegesség.**

Az eIDAS **rendelet másrészt létrehozza a bizalmi szolgáltatások általános jogi keretét. Bizalmi szolgáltatásnak minősülnek a rendelet szerint:**

a) elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

b) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy;

c) elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése.

Az eIDAS rendelet hazai részletszabályait az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény tartalmazza, amely törvény részletes ismertetése nem tárgya jelen jegyzetnek. Témánk és a biztonsági kihívások kezelése szempontjából az e-aláírás mint bizalmi szolgáltatás okos telefonon történő felhasználása lehet irányadó a jövőre nézve azzal, hogy annak megjelenési formája vizsgálat tárgyát képezze. Az elektronikus aláírásnak most is számos formája ismert Magyarországon, az élet számos területén találkozhatunk vele, az eIDAS rendelet és a hazai szabályok teljes körű hatályba lépésével azonban még szélesebb körben megjelennek az elektronikus aláírások létrehozására használt technikai megoldások és az ezeket alkalmazó szolgáltatók köre. Az eIDAS rendelet és ezáltal a hazai szabályozás például lehetővé teszi a biometrikus aláírás hiteles aláírásként történő elismerését és az ennek használatával készített okiratot hiteles okiratnak ismeri el (ezen az elven alapuló megoldást alkalmaznak napjainkban pl a csomagküldő szolgálatok a csomag átadásakor).

6. Jövőbeni kihívások és lehetőségek

Az okostelefonok (mobileszközök) adatvédelmi és információbiztonsági kockázata – ahogy azt a bevezetőben már említettük – alapvetően két tényezőre vezethető vissza: az egyik, hogy hogyan és mire használjuk az eszközt, a másik, hogy milyen szolgáltatásokat szeretnénk elérni azzal. A hogyan és mire használjuk az eszközt felhasználói magatartásra és biztonságtudatosságra vezethető alapvetően vissza, amely elsődlegesen nem a szabályozás oldaláról, hanem a tudatosítás és a képzés oldaláról igényel törekvéseket (bár kétségtelen, hogy szabályozási alapok nélkül nem megy). Alapvető probléma, hogy a felhasználók nincsenek felkészítve a technológiai fejlődésből eredő biztonsági kockázatokra. Már egy 2011-es felmérés során is kimutatták, hogy bár a felhasználók aggódnak az okostelefonon tárolt adataik biztonságáért, a védelmi intézkedések körével és a lehetőségekkel azonban nincsenek tisztában.[150] A szolgáltatások igénybevételével járó veszélyek túlmutatnak a biztonságtudatosságon, a külső és belső intézményi információk, továbbá az új és újabb alkalmazások igénye a véletlen adatvesztéstől kezdve egészen a szándékos adatszivárgásig biztonsági kockázatot jelent. A mobil alkalmazások fejlesztésénél ezért előtérbe kell helyezni a felhasználók azonosítását és a jogosultságkezelését. Meg kell valósítani a magán és üzleti adatok elkülönítését és védelmét, az eszközök, alkalmazások, felhasználók központi adminisztrációját és támogatását, az intraneten futó alkalmazások biztonságos elérését és használatát. Mindezt hogyan támogatja a – fentiekben bemutatott – szabályozási környezet?

A szabályozási környezetből jól érzékelhető, hogy a stratégiai szintű, hosszú távú tervezés mind a nemzeti, mind a nemzetközi szinten kiemelkedő eredményeket mutat. Ez a hosszú távú tervezés a 2014-2020 közötti fejlesztési időszakban megjelenő források lehívásával váltható „aprópénzre". A „beváltás" feltétele a törvényi szintű szabályozás jelenleg meglévő keretszabályainak specializálása, az ágazati szabályzók kiegészítése. Mindezt úgy szükséges kodifikálni, hogy a jelenlegi szabályozással elért eredmények mind az adatvédelem – különös tekintettel a nemzeti adatvagyon védelmére – mind az információbiztonság tekintetében továbbra is érvénybe maradjanak és az újonnan megjelenő technológiai kihívásokhoz, valamint a biztonsági kockázatokhoz igazodjanak.

Fontos, hogy:

a) az okotelefonunkon tárolt és felhasznált adatokat minősítsük és szűrjük,
b) személyes és különleges adatot csak az Infotv. szabályrendszere alapján, megfelelő, az Ibtv. által biztonsági osztályba sorolt elektronikus információs rendszeren kezeljük,
c) a meglévő és védett adatvagyon tekintetében ne használjunk olyan alkalmazásokat, amelyek sérülékenyek.

Releváns változást az általános adatvédelmi rendelet 2018. május 25-től kötelező alkalmazása hozhat, amely az adatkezelők kötelezettségeként írja elő és felelősségi körükbe helyezi a megfelelő eljárásrendek, szabályzatok elfogadását és a biztonság garantáláshoz szükséges adatbiztonsági intézkedések megtételét. Emellett szükséges továbbá a technológiai szabályok ismételt megjelenése is (vö. a 3. fejezetben az első generációs adatvédelmi szabályozásnál leírtakkal), mivel a biztonsági kockázatok csökkenthetők azáltal, ha megfelelően van szabályozva – mind jogi, mind műszaki megvalósítás szempontjából – az, hogy a mobil alkalmazás:

a) csak a szükséges és engedélyezett adatot tölti (töltheti) le – vö. célhoz kötöttség elve és információbiztonsági szempontok,
b) minimalizálja az adatforgalmat, ezáltal csökkenti a várakozási időt,
c) minél nagyobb mennyiségű személyes adatot kezel és magasabb a biztonsági osztályba sorolt értéke jelszó alapú hitelesítést követeljen meg.

[150] www.fudzilla.com Smartphone users fear data loss – 2011. 06. 09.

Nem szabad figyelmen kívül hagyni, hogy személyes adatot felvenni és felhasználni alapesetben csak az érintett beleegyezésével szabad, úgy, hogy az adatfeldolgozás útját az érintett részére követhetővé és ellenőrizhetővé kell tenni. Alapvetés, hogy mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel a személyes adatát. Ezen elvek a mobileszközök, különös tekintettel az okostelefonok világában fokozottan kell, hogy érvényesüljenek, hiszen az okostelefonokon rengeteg személyes adatot és információt tárolunk. Gondoljunk csak arra, hogy hogyan és mennyire biztosítható a magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten. Hogyan tud érvényesülni a szolgáltatóknál az, hogy az érintett jogai védelme érdekében a személyes adatainak helyesbítését, azok törlését vagy zárolását kérje, feltételezve, hogy a személyes adat kezelésének jogalapja biztosított. Mindez anélkül, hogy a felhasználók tudatosítása ne kapjon kiemelt figyelmet nem biztosít megfelelő sikereket.

A jogi keretek adottak, azonban a jelenlegi szabályozások mentén sok tényező határozza meg azt, hogy a jogérvényesítésre mikor és mely személy vagy szerv által, és szükség esetén a megfelelő szankciók alkalmazásával kerülhet sor.

7. Felhasznált irodalom

- Halmai Gábor – Tóth Gábor Attila (Szerkesztők): Emberi jogok. Osiris Kiadó, 2003.
- Jóri András: Adatvédelmi kézikönyv Osiris Kiadó, Budapest, 2005.
- Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz – Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016. április

8. Jogszabályok jegyzéke

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- A nemzeti adatvagyonról szóló 2021. évi XCI. törvény
- A minősített adat védelméről szóló 2009. évi CLV. törvény
- A szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény
- A Büntető Törvénykönyvről szóló 2012. évi C. törvény
- A Polgári Törvénykönyvről szóló 2013. évi V. törvény
- Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény
- Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény
- Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat
- Digitális Nemzet Fejlesztési Program" megvalósításáról szóló 1631/2014. (XI. 6.) Korm. határozat
- „Digitális Nemzet Fejlesztési Program" település-központú kísérleti alprogramjának megvalósításához szükséges források biztosításáról szóló 1854/2014. (XII. 30.) Korm. határozat
- Az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" című közös közleménye

- Az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

9. Felhasznált internetes források jegyzéke

- http://lechnerkozpont.hu/doc/okos-varos/smart-city-tudasplatform-metodikai-javaslat.pdf
- http://lechnerkozpont.hu/doc/okos-varos/telepulesertekeles-es-monitornig-modszertani-javaslat.pdf
- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF
- http://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/citiesoftomorrow/citiesoftomorrow_summary_hu.pdf
- https://eu-smartcities.eu/
- www.urbact.eu
- www.eurocities.eu
- http://ec.europa.eu/regional_policy/sources/policy/themes/urban-development/agenda/pact-of-amsterdam.pdf
- http://ec.europa.eu/europe2020/who-does-what/index_hu.htm
- http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=URISERV:si0016&from=HU
- http://digitalismagyarorszag.kormany.hu/digitalis-magyarorszag
- https://2015-2019.kormany.hu/download/a/59/d0000/Magyarorsza%CC%81g%20Digita%CC%81lis%20Oktata%CC%81si%20Strate%CC%81gia%CC%81ja.pdf
- https://2015-2019.kormany.hu/download/a/59/d0000/Magyarorsza%CC%81g%20Digita%CC%81lis%20Oktata%CC%81si%20Strate%CC%81gia%CC%81ja.pdf
- http://nmhh.hu/dokumentum/170534/lakossagi_internethasznalat_2015_teljes.pdf)

II. BÁNYÁSZ PÉTER: AZ OKOS MOBIL ESZKÖZÖK JELENTETTE KIBERBIZTONSÁGI KIHÍVÁSOK

1. Bevezető

Napjainkban az okos mobil eszközök használata majdhogynem evidensnek tekinthető. A Gartner által készített, okostelefonok eladást és piaci részesedést taglaló legfrissebb jelentéséből kiderül, hogy 2016. második negyedévében összesen 344 millió okostelefont értékesítettek globálisan, ami 4,3 százalékos növekedést jelent a 2015-ös év azonos időszakához képest (bővebben lásd 1. táblázat).[151] Az okostelefon piac meghatározó szereplője az Android, amely 86,2 százalékos piaci részesedést tudhat magának. Az Android mögött messze lemaradva található az iOS, amely a piac 12,9 százalékát adja.

Gyártó	2016 Q2 (millió eladott telefon darab)	2016 Q2 (piaci részesdés %-ban)	2015 Q2 (millió eladott telefon darab)	2015 Q2 (piaci részesdés %-ban)
Samsung	76. 743,5	22,3	72. 072,5	21,8
Apple	44. 395,0	12,9	48. 085,5	14,6
Huawei	30. 670,7	8,9	26. 454,4	8,0
Oppo	18. 489,6	5,4	8. 073,8	2,4
Xiaomi	15. 530,7	4,5	15. 464,5	4,7
Egyéb	158. 530,3	46,0	160. 162,1	48,5
Összesen	**344. 359,7**	**100,0**	**330. 312,9**	**100,0**

1. táblázat Okostelefonok eladási mutatója 2016. második negyedévében
Forrás: Saját szerkesztés, Gartner alapján

A fenti számok kizárólag okostelefonokra vonatkoznak, nem tartalmazzák a tabletek és más okos eszközök eladási mutatóit. Az okostelefonok ilyen fokú elterjedéséhez nagyban hozzájárult – az új technológiák térhódítása mellett- az alkalmazások használatában levő kényelem, egyszerű kezelhetőség. Az okos mobil eszközökre írt alkalmazások számos olyan funkcióval rendelkeznek, amelyek nagyban megkönnyítik mindennapjainkat, hatékonyabb életvezetést biztosítanak számunkra. Az Ericsson 2013 októberében publikált[152] egy közvélemény kutatást, amely 7500 nagyvárosi okostelefon használó 15-69 év közti személyt szólított meg. A kutatás egyik jelentős megállapítása, hogy a felhasználók a felmerülő problémák megoldását a technikától várják, egy okostelefonra készített alkalmazás segítségével. Legyen szó idősgondozásról, vásárlásról, közösségi közlekedésről, hivatali ügyintézésről, a megkérdezettek többsége ezeket az ügyeket egy direkt ilyen célra optimalizált alkalmazással kívánja elvégezni.

[151] Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016, In. Press Release, 2016. augusztus 19., http://www.gartner.com/newsroom/id/3415117 (2016. szeptember 5.)

[152] Ericsson Consumerlab: Smarthphones Change Citys, Ericsson Consumer Insight Summary Report, 2013. október, http://www.ericsson.com/res/docs/2013/consumerlab/smartphones-change-cities.pdf (2016. szeptember 5.)

Az új technológia azonban egyúttal számos új típusú kihívást is magával hozott, amelyekre a felhasználók jelentős része nem készült fel, így igen komoly veszélyeknek teszi ki magát. Azáltal, hogy az okostelefonjaink szinte eggyé váltak velünk, a használókkal, az eszközök fenyegetettsége egyúttal a mi veszélyezettségünket is fokozatosan növeli.

Jelen tananyag célja, hogy növelje a felhasználók okos mobil eszközökre vonatkozó adat- és információérzékenységét, tudatosabb felhasználókat neveljen, hiszen ahogy a későbbiekben látni fogjuk, igen komoly kockázatai lehetnek az óvatlan eszközhasználatnak. Okos mobil eszköz alatt e tanulmány alapvetően az okostelefonokat és tableteket érti.

2. Az okos mobil eszközök evolúciója

Az okos mobil eszközök megjelenését a közvélemény általában az Apple által először piacra dobott iPhonehoz tulajdonítja, ez azonban nem helytálló. Bár az Apple számos olyan újítást vezetett be, aminek hatására elterjedtek az okostelefonok, később a tabletek, már a 90-es évek elején megjelentek olyan eszközök, amiket az „okos" jelzővel lehetett leírni. Az okos mobil eszközök evolúciója így korántsem tekinthető irrelevánsnak abban a tekintetben, hogyan alakul ezen eszközök védelme. A fejezet azt a fejlődést mutatja be, amely napjainkig meghatározta az okos mobil eszközök piacát, illetve bepillantást enged a jövőbe.

Az okostelefon az angol smartphone szó tükörfordításából ered. A smartphone kifejezést első ízben az Ericsson a GS88 „Penelope" nevet viselő készülékre alkalmazták 1997-ben. Akkoriban a smartphone tehát egy leíró szó volt, ami jellemezte a GEOS operációs rendszerrel szerelt, E-mail, WAP[153] és IrDA[154]-képes telefont. Összehasonlítva a napjainkban elterjedt okostelefonokkal, rendkívül kezdetleges technológiának tűnik mindez, azonban abban az időben csúcstechnológiának számított, s csupán egy évtizedre volt szükség, hogy egy olyan rendkívül gyorsan fejlődő iparág alakuljon ki, amely a mai okos mobil eszközöket takarja. A fejezetben a fontosabb mérföldköveket vesszük górcső alá, amelyek a napjainkban elterjedt okos mobil eszközök megszületéséhez vezettek. Az okostelefonok fejlődéstörténetéről a LogOut nevű portál szerzője, HuMarc készített egy rendkívül széleskörű áttekintést, amelyből az általunk jelentősebb mérföldköveket vesszük alapul.[155]

Az okostelefonok első generációja 1994 és 2002 közé datálható, ami inkább egy elő-elő okostelefon korszakként lehetne jellemezni, de ekkor még nem volt olyan komolyabb technológiai robbanás, ami segítette volna az elterjedésüket. A készülékek technikai leírását a 2. számú táblázat tartalmazza.

Az első telefon, ami már „okos"-ként nevezhető az IBM által 1994-ben megalkotott Simon nevet viselő készülék. Az IBM Simon után a Nokia próbálkozott újra betörni az okostelefon piacra 1996-ban a 9000 Communicator nevű készülékével. A telefon újítását az jelentette, hogy kinyitható volt, így kétféleképpen is használhattuk.

Két évvel később ismét a Nokia újítása jelent meg, a Nokia 9110 legnagyobb újdonsága az MMC-kártyával való bővíthetőség jelentette.

2000-ben az Ericsson is piacra dobott egy okostelefont, az R380-at, ami a Symbianos mobilok ősének tekinthető, ugyanis az EPOC 6. verziója, ami közvetlen utódja az EPOC 5.1-nek, már Symbian Operating System néven jelent meg. Ez év novemberébenben a Nokia is új készüléket jelentett meg, Nokia 9210 néven, ami a Nokia 9110 utódjaként tartható számon. Az elődhöz képest nagyon jelentős fejlődésen ment keresztül.

---

153 A Wireless Application Protocol (WAP) a vezeték nélküli adatátvitel egy nyílt nemzetközi szabványa. Hordozható eszközökhöz (mobiltelefonok, PDA-k) fejlesztették ki. A protokollcsalád célja a webböngészés lehetővé tétele csökkentett funkciókkal és néhány mobilspecifikus kiegészítéssel. Ezt a protokollt használja a legtöbb mobiltelefonra írt internetes oldal (wap site).

154 Infravörös port

155 HuMarc: Okostelefon-evolúció, In. LogOut, 2013. május 15., https://logout.hu/cikk/okostelefon-evolucio/bevezeto.html (2016. szeptember 15.)

2001 februárjában a Palm is megjelentetett egy telefonálásra alkalmas szoftvert a PalmOS-t futtató PDA-k számára.[156] A Palm már 2001-ben is (talán az egyetlen, a HP mellett) nagy név volt a PDA-piacon, így kézenfekvő lehetett, hogy egy telefonálásra is alkalmas szoftvert adjanak ki. A szoftver adott volt, ám a Palm Inc. egyelőre nem adott ki hardvert is a szoftverhez, így az első PalmOS-szel hajtott okostelefon a Kyocera nevű cég 6035 nevű/kódszámú készüléke volt. El volt látva webböngészővel, így korlátozott módon ugyan, de képes volt fellépni a világhálóra. Tartalmazta a PalmOS-szel megtámogatott PDA-k (vagy éppen palmtopok) érdekességét, a Palm OS Graffiti technológiáját. A Kyocera 6035 volt az első, széles körben elterjedt okostelefon.

Az első Series 60-nal megjelent mobiltelefon/okostelefon a 2001 novemberében megjelent Nokia 7650 volt, ami bár egy régi Nokia telefonra emlékeztetett, ám belül egy okostelefon hardverét tartalmazta, és számos változáson ment keresztül. A legnagyobb újítása mégis a beépített kamera volt. Bár eddig is voltak fényképezésre képes telefonok, hiszen az első kamerás mobil valójában a Kyocera VP-210 volt, ám ez nem terjedt el széles körben, mivel csak Japánban forgalmazták.

Telefon	Processzor	Memória	Operációs Rendszer	Kamera	Kijelző	Egyéb
IBM Simon	16 MHz-s 16 bites, x86	1 MB	Dos	–	monokróm	Harmadik féltől származó alkalmazások futtatása
Nokia 9000 Communicator	Intel 24 MHz i386	8 MB	GEOS	–	monokróm 200*640	QWERTY billentyűzet
Nokia 9110	AMD 486	8 MB	GEOSTM	–	monokróm 200*640	bővíthető MMC-kártyával
Ericson R380	nincs adat	2 MB	EPOC 5.1	–	monokróm	
Nokia 9210	52 MHz ARM 9	14 MB	Symbian 6,0	–	200*640(12 bit)	WAP, E-mail
Nokia 7650	104 MHz ARM 9	4 MB	Symbian 6,1	VGA	176*208 (12 bit)	WAP, E-mail, MMS, Bluetooth, Infra, JAVA alkalmazások

2. táblázat Okostelefonok 1994-2002. között
Forrás: Saját szerkesztés Logout, TelefonGuru alapján

Ahogy korábban megjegyeztük, az 1994-2002 közé datált időszak egyfajta elő-elő okostelefon korszak volt. 2002-ben azonban beindul egy olyan technológiai robbanás, egy gyorsabb fejlődés, aminek hatására nagyobb ütemben terjednek az okostelefonok, míg el nem érünk az Apple nevével fémjelzett korszakig. A 2001 után kezdődő időszakban az okostelefonok gyorsabb ütemben kezdtek el fejlődni, mint addig, de 2002-ben valószínűleg kevesen gondolták volna, hogy 2016-ban év múlva többmagos, 216 GB RAM-mal és Full HD kijelzővel szerelt telefonok kerülnek a piacra, hiszen akkoriban az ilyen hardver még asztali számítógépek szintjén sem tűnt általánosnak. Mindenesetre 2002-ben a Nokia elkezdi uralni az eddig igen kicsiny, ám egyre nagyobbá duzzadó okostelefon-piacot, és

[156] Fontos megjegyezni, hogy a Kyocera 6035 nem a Handsprings – későbbi nevén Palm Inc. – terméke volt, hanem a Kyoceráé, tehát tulajdonképpen nem a Palm jelentette meg ezt a készüléket, ám mégis fontos lépés, hiszen a Palm végre beleteszi a szoftverébe a PalmOS-be a GSM-támogatást. A Palm csak 2002-ben jelent meg a piacon okostelefonnal. Ez volt a Palm Treo 180, ami azonban nem hordozott semmiféle technikai újdonságot, nem is terjedt el különösen nagymértékben.

ez így marad talán egészen 2008-ig, amikor már mind az iOS, mind az Android piacvezetővé válik. A Blackberry is gyorsabb ütemű fejlődésbe kezd és egyre több telefonálásra alkalmas Microsoft Pocket PC jelenik meg. A készülékek leírását a 3. számú táblázat tartalmazza.

2002. január elsején jelent meg az első, Blackberry néven forgalmazott készüléke, amelynek érdekessége, hogy telefonálni csak headseten keresztül lehetett vele, ami annyit jelent, hogy nem volt beépített mikrofonja és hangszórója.

Az első Androidos operációs rendszerrel működő telefon a HTC G1 „Dream" (és G2 „Magic") volt. Amit sokan nem tudnak az az, hogy a HTC-t 1997-ben alapították és eleinte az volt a cég fő profilja, hogy legyártott egy készüléket, amit aztán több cég vagy szolgáltató is brandelt. 2002-ben megjelenik az első HTC „okostelefon" Wallaby néven. Ezt a készüléket 6 cég is brandelte (Qtek, i-mate, Dopod, O2, T-mobile és Siemens), ami azt jelenti, hogy 2002-ben összesen 6 cég kínálatában jelent meg ugyanaz a telefon, más márkajelzéssel.

A következő években alapvetően különböző hibridekkel próbálkoztak a gyártók, amelyek mind alakjukban, mind funkciójukban jelentették inkább újdonságot. 2003 megjelent az első "igazi" Blackberry, a 6210-es, amely bár hasonló volt az 5810-hez, ám ez már képes volt headset, vagy bármilyen egyéb kiegészítő nélkül hívást indítani és fogadni. Eltért viszont a 5810-től abban, hogy míg annak egy négyzet alakú, 160×160 pixeles kijelzője volt, ez egy 160×100 pixeles kijelzővel rendelkezett, ami természetesen azt jelenti, hogy egy teljesen más képarányú kijelzőt kapott.

2003-ban a Nokia egy nagyon merész ötlettel állt a világ elé, amikor bemutatta a Nokia N-Gage nevű okostelefon-marokkonzol hibridet. Kialakítását tekintve nem nevezhető éppen közönségesnek. A Nintendo Gameboy Advance ellenfelének szánták, azonban az eladások tekintetében messze elmaradt riválisától. Okostelefon mivolta csak a rendszer szempontjából tűnik fel, ami egy Symbian Series 60. Az N-Gage inkább mint játékkonzol jelentős, hiszen ha maga az N-Gage mint brand később meg is bukott, maga az első N-Gage akár sikeresnek is nevezhető, hisz 56 játék jelent meg rá. A készülékben már megtalálható az MMC-kártyával való bővítés lehetősége, ami tulajdonképpen megfelelhet a GameBoy cartridge-nek vagy éppen az akkor még nem létező PSP-k UMD-jének, amiről beolvassa a játékot, viszont akár hagyományos módon, memóriakártyaként képek, zenék tárolására is alkalmas volt.

Ugyanebben az évben a Blackberry új telefonnal, a 72×× széria első darabját jelentő 7210-el lépett a piacra, az újítás a 6210-hez képest az volt, hogy ez színes kijelzővel, jóval nagyobb, 240×160 pixeles felbontással került piacra. További eltérést jelentett az, hogy a RIM ugyanazzal a hardverrel többféle telefont gyártott (7210, 7220, 7230, 7250, 7270, 7280. 7290), azonban az eltérő típusszámok eltérő hálózatot kezeltek. Példának okáért a 7210 900 és 1900 MHz-s GSM-hálózatokra képes fellépni, míg a 7250 a 800 és az 1900 MHz-s CDMA2000-re. Ebből az okból egy-egy sorozatnak (58××, Quark, 72××) elég csak az első modelljét bemutatni. Mindazonáltal vannak típusok, amelyek mellett nem mehetünk el szó nélkül, mert nem csak a hálózati módban különböznek az alapverziótól. Ilyen például a 7270 is, ami az első WiFi-s Blackberry és egyike az első WiFi-s telefonoknak.

A 2003 4. negyedévében megjelent Nokia 6600 és a Symbian 7.0, azaz a Series 60 2nd Edition nem rendelkezett sok újdonsággal a 7650-hez képest, viszont egy népszerű modellről van szó, így meg kell említenünk. A telefon képes videót felvenni, illetve témákat is lehetett rá tölteni. Tojásdad formája nem nevezhető éppen megszokottnak, de ennek ellenére a maga korában sikeres és népszerű volt. A Nokia 6600-zal egy időben jelent meg a PalmOne Treo 600 is. Egy nagyon sikeres modellről beszélünk, ami a Blackberryk tényleges felvirágzása és elterjedése előtt kicsivel az egyik legsikeresebb üzleti mobil volt, hisz tökéletesen ötvözte a telefont, a PDA-t és a kamerát.

2005-ben jelent meg a Nokia 6680, ami az első 3G-s mobilok egyike volt, illetve két kamerával rendelkezett. Az elsődleges, hátoldali kamera egy 1,3 megapixeles egység LED-villanóval, a másodlagos, előlapi kamera pedig videóhívások lebonyolítására tette alkalmassá.

Telefon	Processzor	Memória	Operációs Rendszer	Kamera	Kijelző	Egyéb
Blackberry 5810	ARM 7EJ-S	8 MB	BlackBerry OS 3.6	-	monokróm 160*160	WAP, GPRS, POP3
HTC Wallaby	206 MHz-s StrongARM	32/64 MB	Microsoft Pocket PC	-	240 * 320	
Blackberry 6210	nincs adat	16 MB	BlackBerry OS	-	160 * 100	USB
Nokia N-Gage	104 MHz ARM 920T	-	Symbian 6,0	-	176*208 (12 bit)	GPRS, WAP, Bluetooth, E-mail
Blackberry 7210	nincs adat	16 MB	BlackBerry OS	-	240 * 160	USB, GPRS, WAP, 7270 WIFI képes
Nokia 6600	104 MHz ARM 9	6 MB	Symbian 7,0	VGA	176*208 (16 bit)	videó rögzítés, támák letöltése, GPRS, WAP, Bluetooth, E-mail, Infra
PalmOne Treo 600	Intel PXA270 312 MHz	23 MB	5,x Garnet Palm Os	VGA	320*320 (16 bit)	GPRS, EDGE, WAP, Bluetooth, E-mail, Infra
Nokia 6680	TI OMAP 1710, 220 MHz AR-M926EJ-S	10 MB	Symbian 8,0	1,x Mpi-xel két ka-mera	176*208 (18 bit)	GPRS, EDGE, WAP, Bluetooth, E-mail,

3. táblázat Okostelefonok 2002-2007. között
Forrás: Saját szerkesztés, Logout, TelefonGuru alapján

Az iPhone 2007 júniusában mindent megváltoztatott. Letisztultsága, kezelhetősége elért egy olyan szintre, amit azelőtt egyetlen más rendszer sem volt képes elérni. Forradalmasította az okostelefonokat, hiszen most már nemcsak informatikusok és hozzáértők kiváltsága volt az okostelefon, ugyanis egy iPhone-t bárki tud kezelni. Természetesen nem egyedül az iPhone-nak köszönhető az, hogy napjainkban ilyen okostelefonok vannak, ám ha az Apple 2007-ben inkább egy új iPodot ad ki, ma nem így néznének ki az okostelefonok. Az iPhone nélkül vélhetően az Android is teljesen más fejlődési utat jár be. Az iPhone-t közel sem lehet tökéletesnek nevezni, azonban egy olyan paradigmaváltást indított be, amely alapvetően alakította át az okos mobil eszközökkel kapcsolatos viszonyunkat, megteremtette az igényt a könnyen kezelhető okostelefonok iránt.

A tabletek esetében hasonló folyamat írható le, mint a mobiltelefonok esetében. Az első kereskedelmi forgalomba kerülő készülékek közül az 1989-ben piacra dobott Grid Systems GRiDPAD-ja volt az, ami legjobban egyesítette mindazt formában, amit alapvetően a táblagépekben ma is meghatározónak tartunk, de a 10 hüvelykes kijelző itt még monokróm, és beépített toll segítségével volt lehetőség az adatbevitelre. Képességei korlátozottak voltak mai szemmel és természetesen a technikai fejlettség azon időszakában még szó sem lehetett médiakezelésről, de abban az időben jóval meghaladta korát. Az első mai értelemben vett táblagépet a Microsoft cég jelentette be 2001-ben, ami 2002-ben került forgalomba, de magas ára miatt nem lett sikere és gazdasági bukás volt. Az igazi sikert és áttörést itt is az Apple iPad megjelenése hozta 2010-ben. Az Apple már a Microsoft

készülékének 2002 forgalomba hozása után fejleszteni kezdte a maga táblagépét, de a munkákat felfüggesztették, amikor az iPhone ötlete felmerült, és az erőforrásokat és az addigi fejlesztéseket a telefongyártásnál használták fel. Az iPhone sikere után aztán újraindult az új termékszegmens fejlesztése, ami – köszönhetően a tudatos tervezésnek és marketingnek – páratlan áttörést hozott. A 2002 és 2010 közötti időszakban csak szórványosan jelent meg egy-egy új modell, de az iPad sikere után 2010-ben a főbb hardvergyártók piacra dobták a maguk modelljét. Többségük már az iPad felépítése alapján fejlesztett, ami több szabadalmi perhez is vezetett később. Az erős konkurencia hatására az árak esni kezdtek. 2011-ben a korábban e-könyv olvasók piacán vezető szerepet betöltő Amazon is belépett a táblagépek piacára a Kindle Fire táblagépével. Az Amazon piacszerzési módszerének alapja a rendkívül nyomott alacsony ár tartása a hardvereladásoknál így a Kindle Fire megjelenésével alámént a korábban lélektaninak számító 200 dollárnak új irányt mutatva a piacnak.

3. Az okos mobil eszközök csoportosítása

A csoportosítás alapját jelen fejezetben a három legjobban elterjedt operációs rendszer képezi, illetve ismerteti azokat a kockázatokat, amelyeket magukban hordoznak, továbbá javaslatot fogalmaz meg az ellenük történő védekezésre. Az operációs rendszerek egy nagy csoportjának Linux rendszer az alapja. Bár maga a Linux is készített operációs rendszert okos telefonokra, de a későbbiekben már csak mint kiindulópont volt a szoftver fejlesztés folyamatában. A Linuxon alapuló operációs rendszerek közül a legismertebb és elterjedtebb az Android OS, amelyet a Google fejlesztett ki és használ a saját márkás (NEXUS) okos eszközein. A Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve Android 1.0 platform néven került kiadásra Apache licenc alatt. Elég nagy számban készültek változatai a különböző gyártók saját verziókat fejlesztettek a saját készülékükre optimalizálva azt. Az Android előnye, hogy mindenféle árkategóriában vannak készülékek, fájlból is lehet telepíteni programokat, maximálisan testre szabható, rengeteg Google szolgáltatás, melyet alapból ismer. A hátrányait tekintve meg kell említenünk a fragmentációt. A készülékek eltérő képességei miatt az Android sok modell változata működik egy időben. ezek összehangolása a különböző alkalmazásokkal nagyon nehezen megy így előfordul, hogy egyes alkalmazások nem indulnak el bizonyos eszközökön. Egy másik hátránya, hogy bizonyos alkalmazások csak egy meghatározott konfiguráció esetén működik. Hátrányként említhető még az, hogy nehezebb optimalizálni az operációs rendszert a sokfajta hardverre. Mivel az Android operációs rendszer a legelterjedtebb a világon így a legnagyobb számban ezt is támadják. Ehhez az is hozzájárul, hogy az alkalmazásokat csak felületesen elemzik biztonsági szempontból. Így a hivatalos Play webáruházból letöltött alkalmazás is lehet rosszindulatú.

Az iOS az iPhone és az iPad operációs rendszere, amit az OS X-ből készítettek. Kezdetben csak saját alkalmazásai futottak rajta, később váltak elérhetővé más gyártók által készített alkalmazások iOS-kompatibilis verziói. Ma már előnyei között említhetjük az alkalmazások nagy választékát. A biztonsági szempontot szintén az előnyökhöz sorolhatjuk ugyanis az minden App store-ba kerülő alkalmazást ellenőriznek. További előnye hogy a jól optimalizált szoftver hatására az eszközök nagy hatékonysággal képesek működni. A sok kiegészítő, amely érhető hozzájuk tovább növeli a használhatóságukat.

Azonban hátrányokkal is rendelkeznek az Apple termékek. Elsősorban a drága készülékek jelentik az első korlátot az eszközök terjedésében. Ehhez kapcsolódik a korlátozott testreszabhatóság is, amellyel szintén szűköl a felhasználó mozgástere. szinte csak az iTunes szolgáltatásait lehet használni, a bluetooth használhatósága korlátozott Meg kell említeni, hogy a biztonságos alkalmazások csak akkor azok ha a hivatalos forrásból szerezzük be. Több gyártó is kínál olyan programokat amellyel feloldhatjuk (jailbreak) az iOS korlátozásait és nem hivatalos helyről is letölthetjük az alkalmazásokat vagy hozzáférhetünk az operációs rendszerhez. Ezek az eljárások több kockázatot is magukkal vonnak.

A Windows operációs rendszere nem csak okos mobil eszközökre készült, ezt az előnyei közé sorolhatjuk. Az erős integráció Microsoft környezetbe, sok előnnyél jár, úgy mint a Microsoft szolgáltatások (Skydrive, Bing, Bingmaps, Web Office, Skype, OneDrive, e-mail) Microsoft fejlesztői eszközök (c#, .Net, Silverlight) és a szintén ellenőrzött alkalmazások, mindezt azzal fokozva hogy az alkalmazások bármelyik készüléken működnek. Ezzel kompatibilitás szempontjából a többi versenytársa előtt jár. Azonban itt is találkozunk a hátrányokkal. A drága készülékek mellett, ugyan azt a felületet találjuk mindegyik telefonon és tableten. Korlátozott testreszabhatósága, a programok nem tudnak a rendszerbe beleépülni, valamint kevés program érhető el. Emellett a rosszindulatú programok ugyanúgy veszélyeztetik, mint az asztali gépeket hiszen ugyanaz a Windows program fut rajtuk.

4. A kiberfenyegetettségek osztályozása

A *„Bevezető az okos mobil eszközök világába”* címet viselő tananyagban az Olvasó már szembesült az okostelefon definíciós nehézségeivel, ebben a fejezetben egy közös jellemzőt azonban ki kell ragadnunk. Nevezetesen, bár internetkapcsolat nélkül is használhatóak az okos mobil eszközök, akárcsak elődjeik, de az igazán hatékony működés megköveteli mobil- vagy vezeték nélküli internet használatát. Azáltal, hogy csatlakozunk a kibertérhez, számos támadási felületet nyújtunk.

A kibertér kifejezést William Gibson sci-fi író használta először az 1982-ben megjelent Izzó króm című novellájában, majd az 1984-es Neurománc című regényében, és innen szivárgott át a köztudatba. Gibson a kibertér fogalma alatt hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális teret értett.[157] A kibertér kifejezés a görög kyber (hajózni) szóból származik, és hajózásra alkalmas teret jelent. A Neurománc óta különböző fogalmi meghatározások születtek a kibertérre, de földrajzi értelemben az infokommunikációs technológiákban megnyilvánuló térfogalmat jelent, nem pedig a technológiára utal.

A kibertér térszerkezetének leírására számos kísérlet született geometriai, formai, szerkezeti jellemzőinek meghatározásával. A térgeometriai jellemzők feltárása azonban nem egyszerű, hiszen a kibertér számos különböző, eltérő funkciójú tartományból tevődik össze, illetve mindegyike mesterségesen konstruált. A különböző térfelfogásokat az alapján alkották meg, hogy a fogalom használói a kibertér mely csoportjával foglalkoztak.[158]

A kibertér definiálására a magyar stratégiai gondolkodásban is születtek kísérletek. A Magyarország Nemzeti Kiberbiztonsági Stratégiája a következő megfogalmazást tartalmazza: *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”*[159]

Resperger István megfogalmazása szerint *„A biztonsági kockázatot az általános meghatározásból következően, a biztonsági dimenziók vonatkozásában értelmezhetjük. A fenyegetés a veszély konkrét, cselekvési szándékot is megjelenítő formája.”*[160] A fenyegetések az általánosan értelmezett biztonság egyes összetevőire ható helyzetek és állapotok összessége a lehetséges veszélyek legmagasabb megnyilvánulási szintjét tekintve.

A szakirodalom napjainkban a kiberfenyegetettségek négy típusát különbözteti meg, amelyek nem csak az elkövetés módja, de motivációja szerint is eltérnek.

---

157 Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése, In. *Magyar Tudomány*, 2001/7., pp. 769-779., 2001.

158 Jakobi Ákos: A virtuális világ terei – Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése” című tanulmányához, In. *Magyar Tudomány*, 2002/11., pp. 1482–1491., 2002.

159 1139/2013, (III. 21.) Korm. határozat Magyarország Nemzet Kiberbiztonsági stratégiájáról, In. *Magyar Közlöny*, 2013/47.

160 Resperger István: Kockázatok, kihívások, fenyegetések a XXI. században. Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest, 2002.

Az első kategóriába a kiberbűnözés, amelynek a célja, hogy informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket. Az EUROPOL minden évben közzéteszi jelentését az internetes szervezett bűnözés általi fenyegetettségről. Ez alapján 2015-ben az alábbi területeket azonosították:[161]

1. Malwarekkel[162] (pl. CryptoLocker, CTB-LOCKER stb.) való visszaélés.
2. Gyerekek szexuális kizsákmányolása;
3. Fizetőeszközzel elkövetett csalás;
4. Social engineering;
5. Adatok megszerzése, hálózatok támadása;
6. Létfontosságú rendszerelemek ellen elkövetett támadások;
7. Különböző pénzügyi tevékenységek (criminal-to-criminal payments, payment for legitimate services, victim payments);
8. Online kommunikáció;
9. Darknet;
10. Internet of Things, Big Data, Clouds

A kiberbűnözés esetében évek óta megjelent a Crime as a Service, vagyis a szolgáltatásszerű bűnözés, ami összekapcsolta a szervezett bűnözői köröket a feketekalapos hackerekkel.[163] Ez esetben a megrendelő számos szolgáltatást vehet igénybe, legyen szó betörést elősegítő eszköz vásárlásáról, egy adott informatikai bűncselekmény végrehajtásáról, vagy mindezek technológiai támogatásáról az üzleti szférából jól ismert „tech support" mintájára.

A kiberfenyegetettségek második típusa alatt a hacktivizmust és a kiberterrorizmust értjük, amelyek bár fogalmilag eltérőek ugyan, mégis több közös pont határozható meg esetükben. Ilyen közös pont, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport.

A harmadik típust a kiberkémkedés jelenti, amely alatt az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést értünk. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület.

A kiberfenyegetettségek negyedik csoportjába a kiberhadviselés sorolható. A kiberhadviselés az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására (ahogy történt a 2008-as orosz-grúz háború esetében), azonban ahogy a 2007-es észtországi

---

161 The 2015 Internet Organised Crime Threat Assessment (IOCTA), Europol, Hága, 2015., https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (2016. szeptember 20.)

162 Az angol *malware* kifejezés az angol *malicious software* (rosszindulatú szoftver, káros szoftver, kártékony szoftver) összevonásából kialakított mozaikszó. Ide tartoznak a vírusok, férgek (*worm*), kémprogramok (*spyware*), agresszív reklámprogramok (*adware*), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (*rootkit*). Az informatikai eszközökre írt kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el.

163 Feketekalapos (black-hat) hackernek nevezzük azokat a hackereket, akik tudásukkal visszaélve, jogosulatlanul számítógépbe illetve számítógép-hálózatokba törnek be haszonszerzés vagy károkozás céljából. Black-hat hackerek csoportjába tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba. Sok black-hat válik később white-hat hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon white-hat hackerként, hogy előtte soha nem próbált betörni egy számítógépbe sem. Így a határ inkább etikus és etikátlan hackerre osztható.

események is igazolták, önmagában is képes egy államot térdre kényszeríteni.[164] Amellett, hogy igen komoly károkozást lehet véghez vinni kibertámadással, bonyolítja a problémát, hogy szinte lehetetlen bizonyítani, ki is áll valójában a támadás mögött. támadásként értelmezte a történteket. Napjainkra egyre többen hangoztatják, hogy a kibertámadások háborús cselekmények, amelyek kiváltják az önvédelemhez való jogot. Ezek közé tartozik többek között Harold Koh, az amerikai Külügyminisztérium jogtanácsosa vagy Tony Blair korábbi nemzetbiztonsági főtanácsadója, Sir Richard Mottram, de az úgynevezett tallinni jegyzőkönyv, ami a NATO kérésére nemzetközi szakértők által összeállított ajánlás arra nézve, hogy a kiberhadviselés milyen nemzetközi jogi elvek szerint legyen szabályozva. A kézikönyv az online háborút próbálja értelmezni a klasszikus hadviselés elvei alapján, követve a genfi és hágai konvenciókat követve, deklaráltan a civilek védelmére. Ebből adódóan tiltja a kórházak, vízi- és nukleáris erőművek ellen intézett támadásokat. A halálos áldozatokkal, illetve különösen nagy anyagi kárral járó támadásokat háborús cselekménynek minősíti, ami kiváltja a konvencionális eszközökkel való válaszcsapás jogát is, valamint a támadást végrehajtó hackereket nem civilekként, hanem katonákként értelmezni. Fontos azonban látni, elképesztően nehéz bizonyítani, hogy ki állt a támadások mögött. Ahogy az említett Észtországot ért kibertámadás is mutatta, hiába lehetett tudni, hogy kikhez köthető a támadás, nem voltak lehetett egyértelmű bizonyítékokkal alátámasztani az orosz érdekeltséget. Már pedig, ha a tallinni jegyzőkönyv háborús cselekményként aposztrofált kitételeit nézzük, különösen nagy anyagi kárral járó támadás kiváltja az önvédelemhez való jogot.

Napóleontól származtatják a „legjobb védekezés a támadás" elvét, természetesen ez a kibertámadásokra is megfeleltethető. Egyre több állam ismeri fel ennek szükségességét és hozza létre. Ebbe a körbe tartozik az Egyesül Államok, Kínához, Oroszország, Izrael, Irán, de nem lebecsülendő Észak-Korea 3000 főre tehető kiberserege sem, amely egy kiszámíthatatlan, irracionális döntések meghozatalára hajlamos rezsim kezében növeli a veszély mértékét.

Ahogy látni fogjuk, az okos mobil eszközök közvetetten vagy közvetlenül mind a négy kiberfenyegetettség esetében kockázatot jelenthetnek.

5. Új típusú kihívások az okos mobil eszközök tekintetében

Függőségünk az infokommunikációs eszközöktől, beleértve az okos mobil eszközöket is nem elhanyagolható. Mielőtt minden infokommunikációs eszközünket az internetre kötöttük volna, a kockázatok megmaradtak bizonyos fizikai korlátok között. A klasszikus mobiltelefonok esetében korábban a legnagyobb kockázatot az jelentette, ha megtámadták a használóját, ami természetesen a támadástól függően komolyabb sérüléssel is járhatott. Az okos mobil eszközök, az által, hogy az internetre csatlakoznak, új típusú kihívásokat eredményeztek. Ezek az új típusú kihívások egyáltalán nem követelik meg, hogy a támadó és a megtámadott fizikailag egy helyen legyenek egy időben, egy támadás adott esetben több ezer kilométeres távolságból is elkövethető.

Értelemszerűen nem szűnt meg a klasszikus kockázat, amely az okos mobil eszközök eltulajdonításából fakad, hiszen egy-egy készülék több százezer Ft-os értéket is képviselhet, ez pedig meglehetősen motiváló lehet egyeseknek, hogy megszerezzék válogatott eszközökkel a telefonunk. Fontos azonban látni, olyan mértékű fenyegetéseket okozhatnak ezek az eszközök, amelyek mellett már nem tűnhet olyan jelentősnek, ha ellopják a telefonunkat.

Figyelembe véve a kiberfenyegetettségek négy típusát, mielőtt konkrét példákon keresztül mutatnánk be az okos mobil eszközök használatából fakadó kockázatokat, vizsgáljuk meg általánosan, milyen területeken vagyunk veszélynek kitéve.

[164] 2007-ben, miután a kormányzat megpróbált eltávolítani egy szovjet köztéri emlékművet, Észtország kormányzati és pénzügyi rendszereit közel egy hónapon keresztül érte kibertámadás, amely óriási anyagi károkat szenvedett el. Ahogy az egyik észt politikus fogalmazta, országukat „a digitális kőkorszakba bombázták vissza".

Az előző fejezetben említett Europol jelentésből kitűnik, hogy a legnépszerűbb bűnelkövetési forma a malwarekkel való visszaélés. Az okos mobil eszközök esetében is igen gyakoriak az úgynevezett zsaroló vírusok, amelyek a megfertőzött telefonok/tabletek tartalmát titkosítják, a feloldásért cserébe pedig pénzt követelnek – többnyire bitcoinban[165]. Az esetek nagy részében természetesen a követelés teljesítése után sem kapjuk vissza filejainkat, így nem érdemes fizetni a zsarolóknak. Az okos mobil eszközök vírusfenyegettségével a „Bevezető az okos mobil eszközök világába" címet viselő tananyag részletesen foglalkozik, így itt külön nem ismételnénk meg, azonban szükséges minden esetben hangsúlyozni, hogy a nem biztonságtudatos eszközhasználat nagymértékben növeli kitettségünket a rosszindulatú támadással szemben.

Megítélésünk szerint rendkívül fontos, hogy odafigyeljünk a fiatalok, gyermekek sérelmére elkövetett bűncselekményekre, illetve ezek lehetőség szerinti megelőzésére, ezek közül is kiemelten a gyermekek szexuális zaklatására, kizsákmányolására. A közösségi oldalak és az okos mobileszközök elterjedésével egyfajta paradigmaváltás figyelhető meg az internethasználat tekintetében, amelynek egy sarkalatos pontja a magánszféra egyre nagyobb mértékben történő visszaszorulása. Minden cselekedetünket, életünk minden apró mozzanatát megosztjuk ismerőseinkkel és ismeretlenekkel egyaránt. Az okos mobileszközök technikai fejlődése egyre jobb és jobb minőségű képek, videók elkészítését teszi lehetővé, az állandó internetkapcsolat pedig nem csupán az azonnali megosztásukat segíti elő, de élőben sugározhatjuk a nagyvilágnak, hogy éppen milyen tevékenységet végzünk. A fiatalok körében különösen népszerűek a képmegosztó és képküldő alkalmazások, mint az Instagram vagy a Snapchat. Ezeken kívül számos üzenetküldő alkalmazás biztosít névtelenséget és titkosított üzenetküldést is, ami megkönnyíti pl. a pedofil tevékenységek végzését. Az interneten számos olyan fórum fellelhető, ahol nem csak pedofilok, de a kiskorúak is cserélgetik egymás között a magukról, társaikról készített erotikus képeket, videókat. Nem szabad elfelejteni, hogy míg ezek megragadnak „amatőr" szinten, elképesztően nagy üzletet jelent egyes köröknek a képek, videók terjesztése, de különösen a különböző szexuális tevékenységeket élőben közvetítő stream-szolgáltatások üzemeltetése. De nem szükséges, hogy valaki szándékosan, üzleti céllal tegye nyilvánossá privát képeinket, videóinkat. Óriási károkat okozhat az embernek, ha akarata ellenére akár pár ember, akár szélesebb tömegek ismerik meg ezeket a tartalmakat rólunk. A tananyag készítésének idején foglalkoztak a hírek a 31 éves olasz nő, Tiziana Cantone esetével, aki öngyilkos lett a róla kikerült házi pornó miatt. A videóból meme lett, pólókat nyomtattak belőle és azokat forgalmazták. Cantone otthagyta a munkáját, Toszkánába költözött, még a nevét is megpróbálta megváltoztatni. Végül hosszú pereskedés után sikerült elérnie, hogy levegyék a róla készült videót az internetről, még a Facebooknak is törölnie kellett. A bíróság végül Cantonet kötelezte arra, hogy fizesse meg a 20 ezer eurós jogi költséget. Korábban kétszer próbált meg öngyilkosságot elkövetni.[166]

Az okos mobileszközök elterjedése utat nyitott a fizetési eljárások kiszélesítésének is. Számos alkalmazás használatáért cserébe fizetnünk szükséges, amiért a telefonunk egyben pénztálcaként is szolgálhat. De nem csak alkalmazásokért fizethetünk mobilunkon keresztül, szolgáltatásokat is vehetünk így igénybe, gondoljunk csak a parkolásra, vagy autópálya-matrica vásárlásra. Ezek mellett ugyanúgy intézhetjük az online bankolást is mobil eszközökről. Mivel pénzügyi tranzakciók végzéséről van szó, kiemelten fontos, hogy az eszköz, amiről fizetünk, illetve az eljárás, amit követünk, biztonságos legyen. Sajnálatos módon a felhasználók jelentős része igen csak óvatlan az eszközei védelmét illetően. A mobilitással együtt jár az, hogy pénzügyi tranzakciót bárhonnan indíthatunk. A bárhonnan egyben azt is jelenti, hogy nem biztonságos kapcsolaton keresztül használjuk telefonunkat. Ha nem otthonról, saját, védett wi-fi hálózatról kapcsolódunk az internethez, a legbiztonságosabb, ha

[165] A bitcoin egy virtuális fizetőeszköz, amely titkosított csatornán keresztül teszi lehetővé a fizetést. Ennél fogva különösen népszerű az illegális cselekmények finanszírozásában, legyen szó kábítószer- vagy fegyverkereskedelemről, vagy akár terrorizmus finanszírozásról.

[166] Index: Öngyilkos lett egy nő, mert kikerült a netre a szexvideója, In. Index, 2016. szeptember 15., http://index.hu/kulfold/2016/09/15/ongyilkos_lett_egy_no_mert_nem_nem_toroltek_le_a_szexvideojat/ (2016. szeptember 15.)

saját mobil internetünket használjuk. Ennek természetesen anyagi vonzata van, egy olcsóbb előfizetés kisebb adatforgalommal, lassabb letöltési sebességgel jár együtt, ezért sokan igyekeznek valamilyen nyilvános wi-fi hálózatra csatlakozni. Ez azonban igen komoly biztonsági kockázatot jelent, hiszen az adatforgalmunkat a hálózat üzemeltetője is látja, és megfelelő eszközök segítségével képes lehet hozzáférni jelszavainkhoz, beszélgetéseinkhez.

Az Europol jelentése is kiemeli a social engineeringet, ami alatt egy olyan eljárást értünk, amelynek során az emberi hiszékenységet kihasználva próbálnak meg a támadók hozzáférést szerezni egy védett rendszerhez. Maga a social engineering megítélésünk szerint mind a négy kiberfenyegetettség esetében alkalmazható eljárás, éppen ezért e tanulmányban külön fejezetet szenteltünk a bemutatására.

Az okos mobileszközök elterjedése sok esetben összemossa a munkaidőt a szabadidővel. Utazás közben a telefonunkról elérjük a munkahelyi e-mailjeinket, munka közben tudunk ismerőseinkkel csetelni, képeket megosztani stb. Mindez megnöveli a támadások lehetőségét, hiszen ha mobiltelefonunkról egy kevésbé vagy egyáltalán nem biztonságos kapcsolatról jelentkezünk be munkahelyi levelezésünkhöz, hiába van egyébként a munkahelyünkön jól védett, biztonságos rendszer, a támadók megkerülhetik rajtunk keresztül azt, és könnyedén hozzáférhetnek védett adatokhoz, hálózatokhoz. A social engineeringhez hasonlóan ez sem kizárólag a kiberbűnözök által alkalmazott eljárás.

2013 óta, amikor Edward Snowden a nyilvánosságra hozta az amerikai Nemzetbiztonsági Ügynökség megfigyeléssel kapcsolatos eljárásait, a laikusok számára is világossá vált, mennyire könnyen hozzáférhető „kíváncsi fülek" számára a mindennapos kommunikációnk. Természetesen ez nem csak egyes nemzetbiztonsági szolgálatok kiváltsága, rosszindulatú támadók ugyanúgy megfigyelhetik online kommunikációnkat. A Snowden-iratok egyik következménye, hogy megnőtt az igény a titkosított online kommunikációra. Ezzel egy időben a valóban illegális tevékenységet elkövetni szándékozók óvatosabbak lettek az online kommunikációjukat illetően- gondoljunk csak a 2015 év végén elkövetett párizsi merényletek elkövetőire, akik a lebukást elkerülendő tudatosan régi, eldobható mobil eszközöket használtak. Másrészt egyre több olyan alkalmazás került piacra, ami titkosítást ígér a felhasználóknak.[167] Az egyik ilyen alkalmazás a Telegram Messenger nevű alkalmazás, amelyet nemzetbiztonsági jelentések szerint újabban az Iszlám Állam nevű terrorszervezet is előszeretettel használ kapcsolattartásra, propagandára.

A hacktivizmus, kiberterrorizmus esetében elsősorban a már említett social engineeringet, valamint az adatokhoz, védett rendszerekhez hozzáférést kell értenünk, ami értelemszerűen a kiberkémkedésre is vonatkozik.

Az okos mobil eszközök jelentette új típusú kihívások a korábbiak esetében elsősorban közvetlenül jelentkeztek, a kibertámadás esetében azonban inkább közvetett hatásról beszélhetünk, amely alapvetően az okos mobil eszközök rosszindulatú programok elterjesztésében írhatóak le.

6. Az alkalmazások használatából fakadó biztonsági kockázatok

Az előző fejezet egyfajta általános leírását adta az új típusú kihívásoknak, amelyek az okos mobil eszközök használatából erednek, a továbbiakban, kapcsolódva a tananyag mellett elkészített esettanulmányokhoz, egy-egy kockázatot kiemelve részletesebben is megvizsgáljuk a ránk leselkedő fenyegetéseket.

Az okos mobil eszközök kockázatait alapvetően az alkalmazások biztonságán keresztül foghatjuk meg. Ahhoz, hogy egy alkalmazást használhassunk, valahonnan le kell töltenünk. Ez történhet biztonságos, illetve nem biztonságos forrásból. Ez természetesen nem jelenti azt, hogy biztonságos forrásból letöltött alkalmazás biztonságos, csupán nagyobb esélyünk van arra, hogy megvédjük

[167] Ezt azonban érdemes fenntartásokkal kezelnünk.

adataink, eszközünk biztonságát. A telefonok, tabletek alapbeállítása általában tiltja, hogy nem biztonságos forrásból tölthessünk le alkalmazásokat, ezt azonban a beállítások között a felhasználható kikapcsolhatja. Létezhetnek alkalmak, amikor indokolt lehet nem biztonságos forrásból letölteni egy-egy alkalmazást, de alapesetben célszerű csak megbízható forrásból származó alkalmazásokat telepíteni. A megbízható forrás esetünkben az okos mobil eszköz (pl. Samsung készülékek esetében Galaxy App) vagy az általa használt operációs rendszerének hivatalos alkalmazás áruháza (Android esetében Google Play Áruház, iOS esetében Apple Store, Windows Phone esetében Microsoft Áruház stb.). Az egyes áruházak eltérő biztonsági előírásokat fogalmaznak meg az alkalmazások gyártóival kapcsolatban, így androidos alkalmazások esetében jelentősen nagyobb számban találkozhatunk rosszindulatú kódokat is tartalmazó vagy adathalász alkalmazásokkal.[168] Egyes népszerű alkalmazások nem érhetőek el globálisan mindenhol. A 2016 nyarán megjelent Pokémon Go alkalmazás szinte egyből óriási érdeklődésre tett szert, azonban a világ sok országában később vált letölthetővé, és akkor sem minden platformra. A játékra kíváncsi tömegek mindent megpróbáltak, hogy idő előtt hozzájussanak a várva várt alkalmazáshoz, így nagyon sokan nem megbízható forrásból töltötték. Ezt az eljárást követve azonban nem lehetett tudni, kiknek szolgáltatják ki adataikat. A lehetőségek tárháza széles.

Ha letöltünk és telepítünk egy alkalmazást, a használatáért cserébe különböző engedélyeket követel meg. Egy alkalmazás letöltése lehet ingyenes, de a használatért cserébe az adatainkat kéri. Alkalmazástól függ, hogy mennyihez akar hozzáférést szerezni. Ne legyenek illúzióink, ha valami ingyenes, ott minden esetben mi vagyunk a termék. Minden esetben, mielőtt egy alkalmazás telepítése mellett döntenénk, olvassuk el figyelmesen, milyen engedélyeket kér a használatért cserébe, és ha túlzónak ítéljük meg, szakítsuk meg a telepítési folyamatot. Célszerű telepítés előtt ellenőrizni az egyes alkalmazásokat különböző adatbiztonsággal foglalkozó honlapokon. Ilyen weboldal pl. a Privacy Grade (http://privacygrade.org/home), ami biztonsági kategóriába sorolja az alkalmazásokat annak függvényében, hogy milyen engedélyeket kér a használatáért cserébe, és ez mennyire reális az alkalmazás alapvető funkciójához képest. Egy „zseblámpa” alkalmazás esetében például több mint indokolatlan az üzenetek tartalmához, geolokációs adatainkhoz való hozzáférés kérdése. Amennyiben ilyennel találkozunk, ne telepítsük az alkalmazást, mert vélhetően adathalász programmal van dolgunk. Egy alkalmazás adatkezelési gyakorlatánál mindig komoly kockázatot jelent, hogy nem tudjuk, a rólunk gyűjtött adatokat ki kezeli, és milyen módon. Nem egy esetben volt már rá precedens, hogy az alkalmazásfejlesztők harmadik félnek adták el az adatokat. Rendkívül jól jövedelmező üzletág az adatok forgalmazása.

Egy alkalmazás a legkülönfélébb adatainkhoz kérhet hozzáférést. A legnépszerűbb alkalmazások, mint a Facebook vagy a Google alkalmazásai többek között az alábbi adatokhoz férnek hozzá: személyes adatok (névjegyadatok), tartózkodási hely (hálózatalapú és GPS alapú helymeghatározás), hálózati kommunikáció (teljes internet hozzáférés), fiókok adatai (üzenetek olvasása), tárhely (lehetőség az USB-tároló tartalmának módosítására vagy törlésére), telefonhívások, hardver vezérlők (fénykép és videókészítés, hangrögzítés), rendszereszközök (szinkronizálás). A Facebook közel 30 hozzáférés engedélyt kér cserébe, hogy használhassuk. Nem nehéz belátni, rossz kezekben milyen hatalmat jelenthetnek azok az adatok, amiket kiárusítunk magunkról. Az okos mobil eszközökhöz való függőségünk azzal is jár, hogy mindenhová magunkkal visszük őket. Amennyiben feltelepítettünk egy olyan nem megbízható alkalmazást, amelynek a kamerához is hozzáférést biztosítottunk, a fejlesztők adott esetben bármikor átvehetik az irányítást a kameránk fölött, kompromittáló képeket is megszerezve az által. Elég, ha arra gondolunk, milyen sokan viszik magukkal a telefonjukat a mosdóba, hogy gyorsabban teljen az idő a használatával.

[168] Fontos látni, készülékünkre csak a saját operációs rendszerére megírt alkalmazást telepíthetünk, eltérő platformét nem. Ha például csak iOS-ra írt alkalmazást kínálnak számunkra Android rendszerre, ne foglalkozzunk vele, ugyanis egyértelműen csalásról van szó.

A Pokémon Go megjelenése után pár nappal elterjedt, hogy az alkalmazás valójában a CIA kémprogramja. Emögött az állt, hogy az alkalmazás a használatért cserébe a teljesen Google fiókhoz hozzáférést kért. A felhasználói felháborodás hatására a fejlesztők kiadtak egy frissítést, ami korlátozta a hozzáférést, arra hivatkozva, hogy tévedésből kértek teljes hozzáférést, természetesen nem az amerikai nemzetbiztonsági szolgálatok állnak a játék mögött.

Vannak esetek, amikor azonban nem dönthetünk egyes alkalmazások telepítéséről, ugyanis a szolgáltató előre telepítette őket, és törölni sem tudjuk. A Google-t ezen gyakorlata miatt számos támadás éri, ugyanis ezáltal aránytalan előnyt élvez más, hasonló szolgáltatást nyújtó alkalmazásokkal szemben. Az sem mellékes, hogy a telefon memóriájának bizonyos százalékát is leköti, ami olcsóbb eszközök esetében igen csak komoly erőforrás pazarlást jelenthet. A nagy tech cégek és az amerikai Nemzetbiztonsági Ügynökség közti kapcsolatot a már említett Snowden-iratokból ismerjük, ez alapján tudjuk, hogy az NSA elérte, ezeknek a cégeknek a felhasználókról gyűjtött adatbázisához hozzáférjenek (amiket aztán továbbadhattak a partnerszolgálataiknak), vagyis nem tehetünk az ellen semmit alapesetben, hogy ezek az alkalmazások ne továbbítsák igény esetében az adatainkat az NSA-nek. Természetesen van rá mód, hogy töröljük ezeket az előre telepített alkalmazásokat, ehhez azonban rendszergazda hozzáférésre van szüksége a telefon tulajdonosának, ami azonban alapesetben nem jár a telefonhoz. Ennek megszerzése különböző eljárásokkal elérhető, ezek azonban olyan informatikai tudást követelnek meg, ami az átlag felhasználó számára nem ismertek. Persze felismerték ezt többen, így szolgáltatásszerűen megvásárolható nem hivatalos úton, hogy a telefonhoz rendszergazda hozzáférést biztosítsanak. Ezzel az eljárással azonban nem csak a készülék garanciáját kockáztatjuk, hanem szabad utat engedünk a rosszindulatú programok elharapódzásának.

Az előre telepített programoknak van egy másik aspektusa, amelyről a felhasználó nem tud. Több esetben bebizonyosodott, hogy egyes kínai telefongyártók már a gyártósoron – vagy később a forgalmazók – olyan kémprogramokat telepítenek az eszközre, amelyeknél nem lehet tudni, kihez kerülnek a rólunk gyűjtött adatok. 2015-ben a Lenovo laptopok[169] esetében fedezték fel, hogy a gyártó olyan hirdetéskezelő rendszert és gyökérszintű tanúsítványt telepített a számítógépeire, amely akár a webes forgalom monitorozására, de akár támadások lebonyolítására is alkalmas lehet.[170] A Superfish nevű programot felhasználói panaszok hatására eltávolították. Az eset során olyan képernyőmentések is készültek, amelyben egy tanúsítvány úgy tett, mintha a kibocsátója a Bank of America lenne. A Superfish gyárilag rajta volt a rendszereken, és alapvetően nem is ártó szándékú, csupán arra akarták használni, hogy a Google keresési eredményei közt másoktól származó hirdetések is megjelenjenek. A laptopgyártó azzal védte meg a szoftvert, hogy az képekkel segíti a termékek megtalálását. Emellett a vevők a laptop beüzemelése során elutasíthatják a használati feltételeket, hogy ne települjön a szoftver. Figyelembe véve, hogy az átlag felhasználó telepítéskor mindent elfogad anélkül, hogy elolvasná, nem nevezhető a legkorrektebb eljárásnak. A Superfish úgynevezett közbeékelődéses (man-in-the-middle) támadást használt, amivel belenyúlt a felhasználó webes adatforgalmába. Ilyenkor mindkét fél azt hiszi, hogy közvetlenül egymással kommunikálnak, pedig mindketten csak a csatornát irányító rejtett szereplővel állnak kapcsolatban. Nem véletlen, hogy a Superfish szoftverét a vírusirtók veszélyes alkalmazásként azonosítják, és az eltávolítását javasolják. A Lenovót képviselő PR-ügynökség reakciójában azt írta, hogy az október és december között szállított notebookokon rajta volt a Superfish. Hozzátették, hogy alaposan megvizsgálták a technológiát, és nem találtak arra bizonyítékot, ami egyértelműen alátámasztaná a biztonsági problémát, de a felhasználói aggályok miatt léptek. Azóta teljes mértékben eltávolították a szerveroldali interakciókat minden Lenovo termékről, így az minden terméken le van tiltva, illetve nem telepítik előre a szoftvert a notebookokon, és ezt a jövőben sem tervezik.

[169] Az eljárás természetesen érvényes lehet az okos mobil eszközökre is.

[170] Williams, Owen: Lenovo caught installing adware on new computers, In. The Next Web, 2015. február 19., http://thenextweb.com/insider/2015/02/19/lenovo-caught-installing-adware-new-computers/ (2016. szeptember 7.)

Szintén 2015-ben több mint húsz különböző típusú kínai okostelefonon találtak előre telepített kémprogramokat.[171] Ezek közé tartoztak többek között Lenovo, a Xiaomi és a Huawei készülékei, de kémprogramokat felfedező, G Data vírusvédelmi cég szakértői szerint nem a gyártók, hanem valószínűleg a kereskedők telepítették a kártevőket a Németországban forgalomba kerülő készülékekre. A kémprogramok jellemzően a Facebook vagy a Google Drive alkalmazások egyikébe voltak elrejtve. A manipulált alkalmazások teljesen úgy működnek, mint az eredetiek. A kártevőt tartalmazó Facebook-alkalmazásnál például minden funkció elérhető, a felhasználó nem vesz észre semmit abból, hogy az alkalmazásban elrejtett kémprogram hátsó ajtót nyitott a mobilján a támadók számára, akik így hozzáférhetnek az összes adatához. Az alkalmazás pedig nem kér engedélyeket, mivel már minden szükséges engedélyt megkapott a telepítésekor. A felhasználó így kizárólag akkor veszi észre, hogy a telefonja fertőzött, ha telepít valamilyen biztonsági alkalmazást, amelynek során a biztonsági program jelzi a fertőzött állományt. A megtisztítás azonban gyakran nem lehetséges, mivel a kártevő bele van égetve a telefon gyári meghajtóprogramjába (firmware-jébe). Ilyen esetben a vásárlónak fel kell vennie a kapcsolatot a mobilkészülék gyártójával. A kártevőt tartalmazó hamis Facebook-alkalmazás rendkívül sok funkcióhoz szerezhet hozzáférést. A korábban ismertetett hozzáférési engedélyek mellett a támadók belehallgathatnak a telefonhívásokba és rögzíthetik azokat, vásárlásokat indíthatnak vagy emelt díjas számokat hívhatnak.

A Kínában gyártott informatikai eszközök, beleértve az okos mobil eszközöket is, komoly aggodalmakat szülnek a nemzetbiztonsági területen dolgozók számára. 2012-ben az Egyesült Államok két kínai telekommunikációs cég, a Huawei és a ZTE kitiltását tervezte az amerikai piacról, ugyanis megítélésük szerint nemzetbiztonsági kockázatot jelentenek az által, hogy az érintett cégeknél túlságosan nagy a kínai állam befolyása. Az amerikai Védelmi Minisztériumnak a kínai haderőről a Kongresszus számára készített éves jelentése szerint a Huawei technológiája olyan „hátsó kapukat" tartalmaz, amely a kínai hadsereg számára lehallgatási lehetőséget biztosít az amerikai telekommunikációs hálózaton belül.

Részben kapcsolódik a megbízhatatlan gyártókhoz a soron következő kockázat, ami a telefonok üzemidejéből ered. Az okos mobil eszközök akkumulátorának az üzemideje nagyban függ a használattól. Az okostelefonok jelenleg nagyon ritkán bírják egy feltöltéssel akár több napig is, mint a „butatelefonok". Eltérő módon terheli az akkumulátort, ha mobil internetet vagy wifit használunk. Egyes alkalmazások olyan mértékben veszik igénybe az akkumulátort, hogy akár órák alatt is lemerülhet a telefonunk. Ilyen alkalmazás a már említett Pokémon Go is, aminek az a célja, hogy kiterjesztett valóságot felhasználva a városban mászkálva Pokémonokat gyűjtsünk a telefonunkkal. Az okos mobil eszközöket nem csak hálózatról, de USB portról is feltölthetjük. Léteznek városszerte olyan USB portok, amikről a lemerült vagy éppen a teljes lemerülés szélén álló eszközeinket feltölthetjük, ezek azonban igen komoly kockázatot jelentenek, ugyanis az ismeretlen forráshoz való csatlakozás megteremti annak a lehetőségét, hogy rosszindulatú programmal fertőzzük meg az eszközeinket. Ennél fogva kerüljük az ismeretlen forrásból történő töltés lehetőségeit USB portról, igyekezzünk csak hálózatról tölteni telefonunkat.

A gyenge üzemidő egyúttal újabb támadási felületeket is jelent. Rengeteg olyan alkalmazást készítenek, amelyek azt ígérik, megnövelik a készülék üzemidejét, optimalizálják az alkalmazások energiafogyasztását. Egyes alkalmazások a klasszikus árukapcsolás elvét követve folyamatosan ajánlják a jobbnál jobb alkalmazások további letöltését, nem egy esetben eltúlozva a telefonra leselkedő veszélyeket. Természetesen ez nem azt jelenti, hogy minden alkalmazás, ami hasonló módon jár el, veszélyt jelent, de a felhasználónak rendkívül óvatosnak kell lennie. Mindig értelmezzük, amit az alkalmazás kiír, ugyanis gyakran az emberi hiszékenységre alapoznak, kétértelmű megfogalmazással. Például „Telefonja veszélynek van kitéve, akár 17 vírusos alkalmazás is lehet rajta". Nem állítja, hogy a telefon fertőzött lenne, az az állítás, pedig hogy veszélynek van kitéve, a tananyag ezen pont-

[171] Khandelwal, Swati: 26 Android Phone Models Shipped with Pre-Installed Spyware, In. The Hacker News, 2015. szeptember 3., http://thehackernews.com/2015/09/android-smartphone-malware.html (2016. szeptember 7.)

ján pedig egyértelműen igaz. Az a felhasználó pedig, aki kevésbé jártas az informatikában vagy nem igazán jellemezhető biztonságtudatosnak, nagyobb eséllyel tölti le a rosszindulatú alkalmazást.

Nem csak alkalmazások letöltésével fertőzhetjük meg telefonunkat, tabletünket, ugyanúgy kattinthatunk egy fertőzött honlapra böngészés közben, mint ahogy számítógépen lehetséges. De mit tehetünk akkor, ha akár óvatlanságból, akár egyéb okból kifolyólag megfertőződött az általunk használt eszköz? Először is, nem mindegy, milyen platformot használ a telefonunk, ugyanis iOS esetében nagyon ritkán beszélhetünk vírusokról, a rosszindulatú alkalmazások elsősorban az adathalászat tekintetében jelentkeznek. Az Apple sokáig kifejezetten büszkén hirdethette, hogy alkalmazásboltjába nem kerülhetnek károkozó kódokat tartalmazó alkalmazások, mivel mindegyiket heteken, akár hónapokon keresztül vizsgálják, mielőtt engedélyezik őket. Most azonban egy trükkös megoldással kerülték meg ezt a folyamatot, valószínűleg kínai hackerek. A vírust ugyanis nem az alkalmazásokba próbálták utólag beerőszakolni, hanem már az Xcode nevű fejlesztőkörnyezetet támadták meg. Ez az a programozási környezet, amelyet az alkalmazások készítői használnak az alkalmazások megírása során. A károkozók azt használták ki, hogy egy csomó fejlesztő az Xcode-nak sem hivatalos verzióját használta (ugyanúgy, ahogy mezei felhasználók tört Windows-t futtatnak a gépükön, vagy filmeket torrenteznek). A hackerek az Xcode egyik kalózváltozatába rejtették a kártevő kódokat, majd feltöltötték a fejlesztőcsomagokat kínai warez szerverekre. Így a fejlesztők észre sem vették, hogy vírus kerül az általuk készített mobilos alkalmazásokba a már eleve fertőzött eszközből. Amennyiben olyan alkalmazást töltöttünk le, amit hasonló eljárással megfertőztek, azonnal töröljük, vagy frissítsük még újabb verzióra. Ezen felül pedig érdemes egy másik eszközről megváltoztatni a jelszavainkat a webes szolgáltatásokhoz (például levelezéshez), de akár a netbankhoz és egyéb fontos helyekhez is érdemes új belépési adatokat megadni.

Az Androidot használó készülékek tulajdonosai nagyobb számban vannak veszélynek kitéve, ugyanis nincs olyan szigorú ellenőrzés az alkalmazásboltba való bekerüléshez. A biztonsági szakértők információi szerint a legtöbb vírus fizetés alapú, ami azt jelenti, hogy megpróbálnak hozzájutni a bankkártya-adatokhoz, a felhasználónevekhez, a jelszavakhoz és más személyes beazonosításra is alkalmas adatokhoz. Emellett persze több száz olyan mobilvírus is létezik, amelyek „kevésbé ártalmas” célokra készültek. Ezek közé tartozik például a névjegyzék, az e-mail címek és más adatok harmadik feleknek való továbbítása, „prémium” szolgáltatások megjelenítése, a beszélgetések rögzítése, további malware-ek letöltése, felugró ablakok megjelenítése és kétes weboldalakat célzó átirányítások indítása. A szokásos vírusokhoz hasonlóan először az androidos fertőzések esetében is nehéz észrevenni a problémát, mert a fájlok a rendszer mélyében rejtőznek. A rendszer lassulása, a gyanús értesítések, az átirányítások és a valamivel magasabb telefonszámla azonban mind gyanúra ad okot. Ilyen esetekben mindig ellenőrizze a készüléket egy elismert antivírus programmal. Az esetek többségében a felhasználók valamilyen nemhivatalos forrásból származó alkalmazás mellékleteként töltik le a fertőzést.

Miből ismerhetjük fel, ha az eszközünk megfertőződött? Ha az alábbi problémák jelentkezhetnek, akkor vírusos a telefonunk:

- *Érzékeny adatok elvesztése*. A rosszindulatú alkalmazások számos információhoz férhetnek hozzá, például a névjegyzékhez, a bejelentkezési adatokhoz és az e-mail címekhez.
- *Anyagi kár*. Az androidos malware-ek akár emeltdíjas számokra is küldhetnek üzeneteket, és feliratkozhatnak fizetős szolgáltatásokra. Mindezt természetesen az áldozat fizeti.
- *További malware-ek bejutása*. Az Android vírus további fertőzéseket juttathat a rendszerbe. Emellett hirdetéseket, felugró ablakokat és megtévesztő értesítéseket is megjeleníthet.
- *A teljesítmény romlása*. A fertőzött rendszer lassabbá, instabilabbá válik.

Ha úgy sejti, hogy készülékébe bejutott az Android vírus, mielőbb vizsgálja át a rendszert a valamilyen antivírus-programmal, amely képes észlelni a kártékony fájlokat és más víruskomponenseket. Előfordul, hogy a vírus letiltja a biztonsági szoftvereket. Ebben az esetben indítsa a készüléket csökkentett módban, és úgy futtassa az antivírus-alkalmazást.

Csökkentett mód indítása kétféleképpen lehetséges. Az egyik, hogy kikapcsoláskor választhatjuk azt a lehetőséget, hogy a készülék csökkentett módban induljon újra. Ha ezt nem ajánlja fel a rendszer, akkor kapcsoljuk ki a telefont, majd indítsuk újra. Amint a készülék bekapcsol, tartsuk lenyomva a Menü, Hangerő le vagy Hangerő fel gombokat, esetleg a Hangerő le és Hangerő fel gombokat egyszerre, így csökkentett módban indíthatjuk el a rendszert. Megpróbálhatunk kézzel is megszabadulni az Android vírustól, az alkalmazás szokásos módú eltávolításával. Legyünk óvatosak ezzel a módszerrel, véletlenül akár hasznos alkalmazásokat is törölhetünk. A kézi eltávolítás lépései a következők:

1. A fenti lépések segítségével indítsuk a készüléket csökkentett módban.
2. Csökkentett módban nyissuk meg a *Beállítások* menüt. Válasszuk ki az Alkalmazások vagy Alkalmazáskezelő menüpontot (a pontos név készülékenként eltérő lehet).
3. Keressük ki a kártékony alkalmazást és távolítsuk el.

Megjelentek azonban olyan trójai vírusként működő hirdetőprogramok, amelyek népszerű alkalmazásként álcázzák magukat (Candy Crush, Facebook, GoogleNow, Twitter, SnapChat, WhatsApp és sok más), és telepítésükkor automatikusan, a felhasználó tudta nélkül rootolják[172] a mobil eszközt, rendszer alkalmazásként ágyazva be magukat, amelyet aztán szinte lehetetlen eltávolítani. Ugyanis az egyszerű letelepítés (uninstall) esetükben nem használható, így a pórul járt felhasználónak nincs más választása, mint a telefon gyártójával töröltetni a tárolót (a mobil alaphelyzetbe állítása nem segít a gondon) vagy egy új okostelefont vásárolni. A dolog érdekessége, hogy az álcázásként használt alkalmazások jó része rendeltetésszerűen működik, miközben rosszindulatú tevékenységet is végez.

Korábban volt szó a zsarolóvírusokról, más néven ransomwarekről, amik olyan rosszindulatú programok, amelyek valamilyen fenyegetéssel próbálnak meg pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszik az eszközt vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, aminek a hatására visszaállítják az eredeti állapotot. Ha a felhasználó kártékony alkalmazást telepít és futtat, értesítést kap a képernyőn, amely szokványos rendszerüzenetnek tűnik, és arról tájékoztat, hogy bizonyos beállításokat módosítania kell, vagy további alkalmazást kell (vagy ajánlott) telepítenie. Ha a felhasználó rákattint az ablakra vagy máshogy beleegyezik a folytatásba, rendszergazdai hozzáférést ad a vírusnak. Pontosan erre van szüksége a ransomware-nek. A felhasználó beleegyezésének ezt a közvetett megszerzését clickjacking néven szokás említeni – ezzel az áldozat rákényszerül, hogy olyan dolgot telepítsen, amit nem is szeretett volna. Amikor a fenyegetés (amely az Android vírushoz kapcsolódik) adminisztrátorként fér a telefonhoz, minden tárolt filet megkeres, majd titkosítja őket. Az eredmény, hogy ezek a fileok hozzáférhetetlenné válnak. Ezt követően a mobilvírus fenyegető üzenetet jelenít meg, azt állítva, hogy az áldozat illegális tartalmakhoz fért hozzá. Figyelmeztet továbbá, hogy a személyes adatokat – beleértve a böngészési előzményeket is – minden névjegynek elküldte. A vírus mindemellett képes megváltoztatni a telefon feloldókódját és PIN-kódját is. A fenyegető üzenet váltságdíjat követel a személyes adatok visszaállításáért cserébe. Ne fizessen! A vírus titkosítja a fileokat, de állítólag végleg törölni is képes őket. Nincs tehát értelme fizetni. Rendkívül valószínűtlen, hogy visszakapja a fileokat, az egyetlen dolog, amit tehet, hogy eltávolítja az Android ransomware-t és megvédi a készüléket a hasonló vírustámadásoktól. A vírus eltávolítását bár a felhasználó is elvégezheti, de ha csupán felhasználói szintű kompetenciával rendelkezik, célszerű szakemberhez fordulni vele.

Egy alkalmazás nem csak akkor jelenthet veszélyt ránk nézve, ha valamilyen rosszindulatú programmal fertőzött. A már többször említett Pokémon Go nem egy esetben emberéletet követelt, ugyanis a játékos nem figyelt a környezetére, és magánterületre tévedt, ahol lelőtték.[173] A szarajevói magyar

[172] A rootolás folyamán a felhaszáló root user-ré/superuser-ré válik, vagyis egy olyan felhasználóvá, akinek teljes hozzáférése van minden utasításhoz és filehoz az operációs rendszerben.

[173] Az első eset Guatemalában történt, két héttel az alkalmazás megjelenését követően. Bővebben lásd: Origo: Meghalt egy tinédzser pokémonozás közben, In. Origo, 2016. július 20., http://www.origo.hu/techbazis/20160720-pokemon-go-halal-baleset.html (2016. szeptember 16.)

nagykövetség közleményt adott ki,[174] amelyben arra figyelmeztetik a Bosznia-Hercegovinába látogató magyar állampolgárokat, hogy „*a Pokémon Go játék nem veszi figyelembe az aknamezőket*”, és kéri az embereket, hogy figyeljenek oda az aknamezőket jelző táblákra, emellett arra is figyelmeztetnek, hogy a gyakori esőzések miatt a jelzőtáblák és szalagok mozoghatnak, így egyáltalán nem javasolják, hogy lakatlan területen játsszák a játékot. Ha nem is mindennapi, hogy aknamezőre tévedjünk, de figyelmetlenségünkből kifolyólag bármikor nagyon könnyen szenvedhetünk balesetet, akár úgy, hogy a telefonunkat nyomkodva nekimegyünk valaminek, valakinek, lelépünk az útról és úgy szenvedünk balesetet. Ezek elkerülése érdekében lehetőleg ne használjuk a telefonunkat gyaloglás, különösen autóvezetés közben. Amennyiben mégis rákényszerülünk, legyünk tekintettel környezetünkre.

Maradva a Pokémon Go-nál, a játék lehetőséget biztosít úgynevezett PokéStopokat is, amelyek előfizetés eredményeképpen egy adott pontra lokalizál különböző gyűjthető dolgokat. Amellett, hogy ennek akár bizonyos gazdaságélénkítő hatása is lehet,[175] komoly biztonsági kockázata is van egyben. Nem sokkal az alkalmazás megjelenését követően a new yorki Central Parkban okozott kisebb csődületet egy ritka Pokémon feltűnése,[176] amit megpróbáltak sokan befogni egyszerre. Tekintsünk most el attól, hogy megfelelő körülmények között akár egy ilyen eset is elmérgesedhet, sokkal fontosabb számunkra az, hogy bárki szándékosan előállíthat egy ilyen helyzetet, amit saját céljaira használhat ki. Történhet ez véletlenszerűen kiválasztott célpontokkal, de akár célzottan is, hogy egy adott időben adott helyre csaljunk valakit. Nem csak rablók, pedofilok, de akár terroristák is könnyű szerrel hozhatnak létre ilyen pontokat, hogy aztán az odatévedő tömeg ellen merényletet hajtsanak végre. A terrorizmus lételeme a médiafelhajtás, egy ilyen óriási hypeal járó alkalmazás esetében, mint a Pokémon Go is, minden bizonnyal, ha sikertelen merényletet is követnének el, garantáltan hosszú ideig vezető hír lenne.

Fontos leszögezni, a Pokémon Go-val kapcsolatban leírtak kockázatok, példák nem magából az alkalmazásból fakadnak, ellenkezőleg![177] Az alkalmazás népszerűsége újszerűségéből, eredetiségéből ered, amit kihasználhatnak rosszindulatú támadók. Minél népszerűbb, minél elterjedtebb egy alkalmazás, szolgáltatás, annál nagyobb eséllyel fogják valakik megtalálni a módját, hogy saját céljukra használják fel. A következő fejezet a közösségi média és az okos mobil eszközök kapcsolatában alaposabban körbejárja ezt az állítást.

7. A közösségi média és az okos mobil eszközök

Az okos mobil eszközök jelentette biztonsági kockázatoknak van egy teljesen más aspektusa, mint amiket már tárgyaltunk, hiszen míg az eddigiek közvetlen következményeivel szembesültünk, addig vannak területek, amelyek közvetetten fenyegetik biztonságunkat. A modernkori terrorizmus megítélésünk szerint több paradigmaváltáson is átesett. A 2001. szeptember 11-én elkövetett terrortámadások az egész világ biztonságfelfogására voltak jelentős hatással, míg az Iszlám Állam nevű terrorszervezet megjelenése számos területen forradalmi változásokat jelentett. Az Iszlám Állam legnagyobb

[174] Konzuli tájékoztatás, In. Konzuli Szolgálat, http://konzuliszolgalat.kormany.hu/europa-utazasi-tanacsok?bosznia-hercegovina (2016. szeptember 16.).

[175] Gondoljunk csak arra az esetre, amikor egy pizzázó tulajdonosa az üzletébe csábította így a játékosokat, akiknek jó része végül vásárolt is egy-egy szelet pizzát. Bővebben lásd: Mosendz, Polly- Kawa, Luke: Pokémon Go Brings Real Money to Random Bars and Pizzerias- Brick-and-mortar shops find themselves in the middle of an invisible game craze, In. Bloomberg, 2016. július 12., http://www.bloomberg.com/news/articles/2016-07-11/pok-mon-go-brings-real-money-to-random-bars-and-pizzerias (2016. szeptember 16.)

[176] Hooton, Christopher: This video of Pokémon GO players in Central Park is proof that The Matrix is coming, In. Independent, 2016. július 12., http://www.independent.co.uk/arts-entertainment/pokemon-go-central-park-pokestop-gym-nyc-new-york-the-matrix-is-coming-a7132391.html (2016. szeptember 16.)

[177] Maga a Pokemon Go természetesen csak a megjelenést követő hype hatására döntött meg rengeteg rekordot, ahogy elmúlt az újdonság hatása, mind a letöltések, mind a felhasználók száma csökkent. Ettől függetlenül bármikor jöhet egy újabb sikeres alkalmazás.

hatása abban fogható meg, ahogyan a propagandát átalakította. A szervezet vezetői ismerik és professzionálisan, készség szinten használják az új technikai eszközöket, illetve rendkívül adaptívak az eszközhasználatot illetően.

Terrorszervezetek viszonylag korán, már az első csecsen háború idején felismerték az általuk végrehajtott terrortámadásokról készült felvételek propaganda célra történő felhasználásának jelentőségét. Ibn al-Hatták szaúdi gerillavezért tekintjük az első dzsihádistának, aki 1996-ban e céllal rögzítette videóra az általa végrehajtott támadásokat. Napjainkban, a közösségi média korában, rendkívüli mértékben megnövekedett azoknak az eszközöknek a száma, amelyeket a terroristák felhasználnak pánikkeltésre, új tagok toborzására, támogatók megnyerésére, propaganda célokra, hírszerzés végzésére, illetve informatikai támadások kivitelezésére. Az Iszlám Állam egyik paradigmaváltása a közösségi média használatban valósult meg, ugyanis előtte egyik terrorszervezet sem használta ilyen tudatosan, ilyen professzionális jelleggel a különböző közösségi oldalakat. Azáltal, hogy ennyire aktívan használják ezeket az eszközöket, könnyű azonosulási pontot adnak az identitásválságon áteső nyugati fiataloknak, akik így nagy számban csatlakoztak a szervezethez. A toborzást sok esetben párkereső oldalakon, Facebookon, chaten, tematikus fórumokon végzik.

Egyes feltételezések szerint az Iszlám Állam profi közösségi média jelenlétéért egy informatikus végzettségű, egykoron telekommunikációs cégeknél dolgozó amerikai-szír kettős állampolgár, Ahmad Abousamra felel.[178] Szemben az elődök homályos, VHS-en továbbított, modernnek nem igen mondható kommunikációs stratégiáival, az IS nagy felbontású, profin szerkesztett videókkal, hashtaggel[179] ellátott Twitter-kampányokkal megragadta a fiatalok figyelmét, és sokkal könnyebb azonosulási pontot jelentett számukra. Nem véletlen tehát, hogy az Iszlám Állam toborzásában gyakran a fiatalok szempontjából könnyű azonosulási pontokat hangsúlyozzák, amellyel a szervezetet egy fiatalos, menő csoportként percepcionálják. Erre talán az egyik legjobb példa, amikor az IS-t a Grand Theft Auto nevű, a fiatalok körében rendkívül népszerű számítógépes játékhoz hasonlítják, mondván, ők a való életben ugyanazt csinálják, mint a nyugati fiatalok mindennapos játékaik közben.[180] A gyerekekre egyébként is különösen nagy hangsúlyt fektet a szervezet, ahogy ez Medyan Dairieh Vice News részére készített riportjából kiderül.[181] Ahmad Abousamra technológiai felkészültségét mi sem mutatja jobban, mintsem a nagy közösségi oldalakról az IS profiljainak kitiltására adott válasz: saját alkalmazást fejlesztettek The Dawn of Glad Tidings néven, amelyet a Google Play áruházból bárki letölthetett, [182] amíg a Google el nem távolította.[183] Az alkalmazás telepítésével a felhasználók engedélyt adnak a programnak, hogy a saját nevükben a Twitter profiljukon az IS helyett posztolja a legfrissebb tartalmakat. Ez által lényegében lehetetlenné válik a szervezetet törölni a Twitterről, továbbá sokkal nagyobb mértékű elérést tesz lehetővé.

James Foley, amerikai újságíró 2014. augusztusi lefejezéséig az IS-nek több ezer Twitter profilja volt, amelyeken propagandát fejtett ki. A videó publikálást követően a szervezethez köthető profilokat letiltották a nagyobb közösségi oldalakról, amelynek hatását az Iszlám Állam is megérezte. Nem sokkal Foley kivégzését követően véletlenül felkerült az Internetre egy másik elrabolt amerikai újságíró, Steven Sotloff meggyilkolásáról szóló videó is, amely azonban nem képezte részét az IS propagandájának, ugyanis idő előtt került nyilvánosságra, amiért követőitől hivatalosan elnézést kértek.[184]

---

178 McPhee, Michele – Ross, Brian: Official: American May Be Key in ISIS Social Media Blitz. http://abcnews.go.com/blogs/headlines/2014/09/official-american-may-be-key-in-isis-social-media-blitz/ (2016. szeptember 25.)

179 A hashtaget először a Twitter vezette be és terjesztette el más platformokra. Egy olyan egyszerű címke rendszert takar, amin keresztül az eltérő forrásokat szűrni és kategorizálni lehet, és ami könnyed átjárást jelent egy téma mentén a különböző bejegyzésekben. Hashtaget a # szimbólummal kezdődően lehet elhelyezni.

180 Tassi, Paul: ISIS Uses ‚GTA 5' In New Teen Recruitment Video. http://www.forbes.com/sites/insertcoin/2014/09/20/isis-uses-gta-5-in-new-teen-recruitment-video/ (2016. szeptember 25.)

181 Dairieh, Medyan: The Islamic State (Part 2). https://news.vice.com/video/the-islamic-state-part-2 (2016. szeptember 25.)

182 Berger, J.M.: How Iraqi militants are gaming Twitter. http://qz.com/221981/a-rebel-army-in-iraq-is-putting-corporate-social-media-mavens-to-shame/ (2016. szeptember 25.)

183 Az alkalmazást 2014 júniusában tette elérhetetlenné a Google az áruházából.

184 Price, Rob: ISIS apologizes for leaking the Sotloff video ‚by accident'. http://www.dailydot.com/politics/sotloff-isis-accident-video/ (2016. szeptember 25.)

A média előszeretettel erősíti fel az Iszlám Állam propagandáját, igaz, Foley és Sotloff kivégzése után némi önmérsékletet tanúsít. A közösségi média átalakította a hírközlést is, hiszen míg korábban egy-egy hírt több forrásból megerősítettek, ellenőriztek, addig a hírverseny miatt sok esetben a közösségi oldalakról vesznek át egy az egyben tartalmakat, mi több, az is jellemző gyakorlat lett, hogy egy bejegyzés alatti kommentből születik egy új hír a mainstream médiában. Pédául egy Twitter bejegyzés, amelyben egy ausztrál dzsihádista, Khaled Sharrouf hét éves fiát fényképezte le, miközben ő a hajánál fogva tartja magasba egy lemészárolt szír kormánykatona fejét, „Ez az én fiam!" aláírással.[185] Az ilyen tartalmak egyáltalán nem egyedi esetek, az Iszlám Állam rendszeresen publikálja a közösségi médiában az általa elkövetett barbár cselekedeteket: keresztre feszítéseket, tömeges kivégzéseket, lefejezéseket stb., hiszen ahogy célpontválasztásakor, úgy minden egyes megnyilvánulásnál kiemelt jelentőséggel bír, hogy a végrehajtott támadás a lehető legnagyobb publicitást kapja.[186]

Médiafogyasztásunk egyre jobban a közösségi oldalakra helyeződik át, amihez leginkább okos mobil eszközökről csatlakozunk. 2016. harmadik negyedévében a Facebookot világszerte 1,3 milliárd ember használja napi szinten, amiből 1 milliárdan mobiltelefonról/tabletről csatlakoznak.

A terrorizmus sajátosságaiból fakadóan a csoportok működését magas fokú konspirációs attitűd kell jellemezze. A konspiratív kapcsolattartásnak jelentik egy új eszközrendszerét a különböző közösségi oldalak és alkalmazások. Ennek módszerei eltérőek lehetnek, attól függően, hogy a kapcsolattartás valós időben zajlik vagy sem. Utóbbi esetben lehet szó valamilyen üzenet elhelyezéséről egy blog posztnak álcázva; egy legendával alátámasztott, videó megosztóra feltöltött videó, ami egy laikusnak a legendának megfelelő tartalmat jelent, de a beavatottaknak dekódolják az üzenetet. A valós időben folytatott kapcsolattartásnak eszközei a különböző chatszobák, illetve közösségi játékok[187] nem nyilvános chatszobái. Az Edward Snowden által nyilvánosságra került információk alapján feltételezhetjük, hogy a terroristák rendszeresen élnek ezekkel a módszerekkel, ugyanis az NSA külön osztályt tartott fenn az online játékokba beépült ügynökök koordinálására. Napjainkban számos mobilalkalmazás biztosít titkosított kommunikációt (Viber, What's up, Telegraph Messenger). A Telegraph esetében az alkalmazással titkosított csatornán lehet chatelni, de indítható vele nyilvános csatorna is, így az Iszlám Állam előszeretettel használja toborzásra és propagandaterjesztésre. Teljesen ingyenes, reklámok sincsenek benne, ellenben azt is kijelzi, amikor a beszélgetőpartner lefényképezi a készülék kijelzőjét.

Egy terrortámadás megszervezésében nem csak a titkosított kommunikáció segítheti a támadókat, de a hírszerzésben, információgyűjtésben is fontos szerepe lehet az okos mobil eszközöknek. Az okos mobil eszközök nem megfelelő használata a social engineering alkalmazásának széles tárházát biztosítja. Elég ha arra gondolunk, hogy egy nem megbízható alkalmazás feltelepítésével számos információt szolgáltatunk ki magunkról. Természetesen ez esetben célzott támadásról van szó, de egy hiszékeny felhasználót könnyű megfelelő irányba terelni, hogy egy adott alkalmazást telepítsen – igaz, ehhez előzetesen fel kell mérni az érdeklődési körét, személyiségének jellemzőit. Ez ismét csak nem jelenthet problémát egy adat- és információbiztonságra kevésbé érzékeny személy esetében, hiszen ha rendszeresen publikál a nyilvánosság számára képeket, rendszeresen bejelentkezik különböző helyszínekről stb., nagyban megkönnyíti a nyílt forrású információgyűjtést.

Képzeljünk el egy személyt, aki rendszeresen csalja a házastársát, szeretőjével pedig valamilyen közösségi oldalon szervezi a találkozóit, míg a házastársának közben azt írja, túlóráznia kell. Ha egy nem biztonságos alkalmazással, egy előre feltelepített rosszindulatú programmal hozzáférnek a telefonja tartalmához a fentebb ismertetett eljárásokkal, akkor a célszemély könnyen zsarolhatóvá válik, hogy megtegye azt, amire a támadóknak szüksége van, például hozzáférni egy védett rendszerhez.

---

185 Owens, Jared: Barbaric image of Khaled Sharrouf's son a warning to the world: Tony Abbott. http://www.theaustralian.com.au/national-affairs/barbaric-image-of-khaled-sharroufs-son-a-warning-to-the-world-tony-abbott/story-fn59niix-1227020303828?nk=401238c785be93cd8954b2c15b326168 (2016. szeptember 25.)

186 Horváth L. Attila: *A terrorizmus csapdájában.* Budapest, Zrínyi Kiadó, 2014.

187 Pl. World of Warcraft, Second Life.

***

Le kell számolni a biztonság illúziójával, hogy mi, felhasználók nem vagyunk érdekesek, eléggé fontosak, hogy ilyen támadások áldozataivá váljunk. Ahhoz, hogy minimalizáljuk a veszélyeket, elengedhetetlen, hogy nagyfokú érzékenységet tulajdonítsunk adataink védelméhez. Ez persze nem azt jelenti, hogy ha például csaljuk a párunkat, akkor elővigyázatosabban járjunk el, hogy ne válhassunk támadás célpontjává; törekedni kell olyan életvitelre, ami nem tesz minket zsarolhatóvá, ugyanis ha egy célpont különösen értékes, akkor bizony valakinek meg fogja érni az erőforrások megfelelő allokációja, hogy felfedje titkainkat. A közszférában dolgozók számára ez különösen érvényes. A biztonságtudatosság megteremtésében fontos szerep jut a Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet által kínált továbbképzéseknek, amelynek keretében ez a tananyag is elkészült; de ezek mellett a munkahelyeknek önálló biztonságtudatossági tréningeket célszerű szervezni, figyelmet fordítva az integritás programokra egyaránt.

8. Felhasznált irodalom

- 1139/2013, (III. 21.) Korm. határozat Magyarország Nemzet Kiberbiztonsági stratégiájáról, In. Magyar Közlöny, 2013/47.
- Berger, J.M.: How Iraqi militants are gaming Twitter. http://qz.com/221981/a-rebel-army-in-iraq-is-putting-corporate-social-media-mavens-to-shame/ (2016. szeptember 25.)
- Dairieh, Medyan: The Islamic State (Part 2). https://news.vice.com/video/the-islamic-state-part-2 (2016. szeptember 25.)
- Ericsson Consumerlab: Smarthphones Change Citys, Ericsson Consumer Insight Summary Report, 2013. október, http://www.ericsson.com/res/docs/2013/consumerlab/smartphones-change-cities.pdf (2016. szeptember 5.)
- Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016, In. Press Release, 2016. augusztus 19., http://www.gartner.com/newsroom/id/3415117 (2016. szeptember 5.)
- Hooton, Christopher: This video of Pokémon GO players in Central Park is proof that The Matrix is coming, In. Independent, 2016. július 12., http://www.independent.co.uk/arts-entertainment/pokemon-go-central-park-pokestop-gym-nyc-new-york-the-matrix-is-coming-a7132391.html (2016. szeptember 16.)
- Horváth L. Attila: *A terrorizmus csapdájában*. Budapest, Zrínyi Kiadó, 2014.
- Index: Öngyilkos lett egy nő, mert kikerült a netre a szexvideója, In. Index, 2016. szeptember 15., http://index.hu/kulfold/2016/09/15/ongyilkos_lett_egy_no_mert_nem_nem_toroltek_le_a_szexvideojat/ (2016. szeptember 15.)
- Jakobi Ákos: A virtuális világ terei – Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése" című tanulmányához, In. *Magyar Tudomány*, 2002/11., pp. 1482-1491., 2002.
- Khandelwal, Swati: 26 Android Phone Models Shipped with Pre-Installed Spyware, In. The Hacker News, 2015. szeptember 3., http://thehackernews.com/2015/09/android-smartphone-malware.html (2016. szeptember 7.)
- Konzuli tájékoztatás, In Konzuli Szolgálat, http://konzuliszolgalat.kormany.hu/europa-utazasi-tanacsok?bosznia-hercegovina (2016. szeptember 16.).
- McPhee, Michele – Ross, Brian: Official: American May Be Key in ISIS Social Media Blitz. http://abcnews.go.com/blogs/headlines/2014/09/official-american-may-be-key-in-isis-social-media-blitz/ (2016. szeptember 25.)
- Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése, In. *Magyar Tudomány*, 2001/7., pp. 769-779., 2001.

- Mosendz, Polly – Kawa, Luke: Pokémon Go Brings Real Money to Random Bars and Pizzerias – Brick-and-mortar shops find themselves in the middle of an invisible game craze, In. Bloomberg, 2016. július 12., http://www.bloomberg.com/news/articles/2016-07-11/pokmon-go-brings-real-money-to-random-bars-and-pizzerias (2016. szeptember 16.)
- Origo: Meghalt egy tinédzser pokémonozás közben, In. Origo, 2016. július 20., http://www.origo.hu/techbazis/20160720-pokemon-go-halal-baleset.html (2016. szeptember 16.)
- Owens, Jared: Barbaric image of Khaled Sharrouf's son a warning to the world: Tony Abbott. http://www.theaustralian.com.au/national-affairs/barbaric-image-of-khaled-sharroufs-son-a-warning-to-the-world-tony-abbott/story-fn59niix-1227020303828?nk=401238c785be93cd-8954b2c15b326168 (2016. szeptember 25.)
- Price, Rob: ISIS apologizes for leaking the Sotloff video ‚by accident'. http://www.dailydot.com/politics/sotloff-isis-accident-video/ (2016. szeptember 25.)
- Tassi, Paul: ISIS Uses ‚GTA 5' In New Teen Recruitment Video. http://www.forbes.com/sites/insertcoin/2014/09/20/isis-uses-gta-5-in-new-teen-recruitment-video/ (2016. szeptember 25.)
- The 2015 Internet Organised Crime Threat Assessment (IOCTA), Europol, Hága, 2015., https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (2016. szeptember 20.)
- Williams, Owen: Lenovo caught installing adware on new computers, In. The Next Web, 2015. február 19., http://thenextweb.com/insider/2015/02/19/lenovo-caught-installing-adware-new-computers/ (2016. szeptember 7.)

III. KAPITÁNY SÁNDOR: OKOSESZKÖZÖK ÉS KOCKÁZATELEMZÉS

1. A kockázat fogalma, értelmezése, kockázat mint döntéstámogatás

Egy szervezet működésének értékelésére, a döntések meghozatalának támogatására manapság temérdek eszköz áll a vezetők rendelkezésére. A különböző – akár technikai eszközökkel támogatott – monitoring rendszerek, a működésből származó adatok statisztikai értékelése, a piaci viszonyok elemzése stb. mind arra hivatott, hogy a meglévő információk megfelelő feldolgozásával képet alkossanak egy aktuális folyamatról, működésről, és ez alapján – különböző pontosságú – becslést adjanak a döntéshozó számára az elkövetkező időszak változásaira, illetve ennek a becslésnek az elvégzését támogassák. Ha kellően távolról közelítjük meg, a kockázatok felmérése, értékelése szintén (lehet) ilyen döntéstámogató módszer, hiszen a vezetői döntések egy jelentős részében a kockázatok elkerülése vagy csökkentése – ha nem is mindig kimondva, de – jelentős szerepet kap.

A kockázat, a mai társadalmi működés szerves részévé vált és megjelenik a legegyszerűbb napi döntéseinktől a legbonyolultabb műszaki vagy tudományos kérdések megválaszolásáig az élet szinte minden területén. Irányt mutathat akár egy lakóhely kiválasztásában, pénzügyi döntéseinkben, egy nyaralás részleteinek megtervezésében vagy éppen egy műszaki probléma megoldásában épp úgy, mint környezetünk megóvásában. Ennek köszönhetően a kockázatok felmérésének, értékelésének tudományos és technikai megoldási lehetőségei egyre nagyobb számban állnak rendelkezésünkre a legkülönbözőbb módszertanok formájában.

Mindenekelőtt azonban jó lenne tisztázni, hogy mit is értünk a kockázat fogalma alatt. Bármilyen egyszerűen is hangzik a kérdés, a már említett sokrétűsége miatt, a különböző megközelítésekben megjelenő más-más hangsúlyok részben eltérő definíciókat adhatnak. Alapvetően azonban abban megegyeznek, hogy kockázatként valamilyen esemény bekövetkezési valószínűségének és az ebből származó következmény mértékének együttesét definiálják, mint a kockázat értéke. Fontos megjegyezni, hogy a kockázat hagyományos értelmezésben valamilyen „negatív” eseményhez kapcsolódik. manapság azonban elterjedőben van az úgynevezett pozitív kockázat értelmezése is, amikor a vizsgált esemény következménye nem valamilyen veszteség, hanem valamilyen „pozitív” hatás. Bár ma még ez a gondolat nem mondható általánosan bevettnek, de egyre több területen jelenik meg.

Mint azt a későbbiekben látni fogjuk a kockázatokkal kapcsolatos fogalmak terén – éppen a szerteágazó megjelenési területnek köszönhetően – egyes fogalomdefiníciók nem egységesen használtak. Ez azt jelenti, hogy egy-egy módszertan, szabvány vagy éppen jogszabály olykor a kockázat – illetve annak elemzése, kezelése alatt – részben mást ért. Fontos tehát, hogyha valamely keretrendszer alkalmazása mellett döntünk, akkor annak a definícióit rögzítsük, és következetesen alkalmazzuk.

1.1. Biztonsági kockázat

Ha a biztonság szempontjából közelítjük meg, akkor a kockázat egyértelműen valamilyen nem kívánt esemény bekövetkezési valószínűsége, és az ebből származó veszteség együttese. A jelen jegyzet szempontjából leginkább releváns jogszabály megfogalmazásában ez az alábbiak szerint hangzik:

„kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;”[188]

Amennyiben a kockázatelemzés, illetve -kezelés célját nagyon röviden szeretnénk meghatározni, azt mondhatjuk, hogy az nem más, mint megismerni a kockázatot, és lehetőség szerint változtatni rajta a szervezet szempontjából előnyös módon. [31k]

1.2. Kockázatkezelési lehetőségek kiválasztása

A kockázat megismerése több lehetséges célt is szolgálhat. Lehetséges olyan döntési szituáció, amikor a kockázatok felmérése az adott körülmények között releváns kockázatkezelési vagy kockázatcsökkentési alternatívák közötti megfelelő választást támasztja alá. Ilyenkor a kockázat mértékén túl nyilvánvalóan szerepet játszik a döntésben az alternatívák egyéb szempontú értékelése is, mint például az egyes lehetőségekhez szükséges erőforrások nagysága, elérhetősége. Ezekben a helyzetekben a biztonság egyik alapelvét, a kockázattal arányos biztonságot kell szem előtt tartani. Ez az elv azt mondja ki, hogy -mivel teljes biztonság soha nem valósítható meg – a biztonságot olyan mértékűre kell választani, amely az adott kockázat nagyságának megfelelő. Magasabb biztonsági szint csak magasabb ráfordítással érhető el, és ad abszurdum egy kockázatcsökkentő intézkedés ráfordítása akár meg is haladhatja a lehetséges veszteség mértékét, ami nem lenne túl logikus megoldás.

1.3. Kritikus (folyamat)elemek azonosítása

Inkább az ipari gyakorlatban elterjedt, de iránya lehet a kockázatok megismerésének az, amikor egy folyamat (vagy éppen termék) kritikus elemeinek azonosítására használunk valamilyen kockázati módszertant. Nyilvánvaló, hogy elsődleges szempont itt is, hogy a kockázatokat elfogadható szintre csökkentsük, azonban ekkor mindezt azzal a megközelítéssel tesszük, hogy a rendelkezésre álló erőforrásokat azokra az elemekre koncentráljuk, ahol a „legnagyobb a baj”. Ezeknél a módszertanoknál gyakori elem, hogy kockázati alapon sorrendet állítunk fel, hogy a beavatkozások prioritását meg lehessen határozni. Ebben a megközelítésben tipikus kockázatcsökkentő intézkedés lehet, hogy a kritikus elemet kiváltjuk, és olyan helyettesítő megoldás alkalmazunk, melynek a kockázati szintje alacsonyabb.

1.4. Rendszerek, technológiák összehasonlítása

Rendszerek, technológiák kockázati alapú összehasonlítása egy beszerzés, fejlesztés során kerülhet előtérbe. Ilyenkor kellően átgondolt módszertanok alkalmazásával a kockázati szempontból legjobb alternatíva kiválasztása lehet a cél, hogy ezzel csökkentsük minimálisra egy későbbi lehetségesen bekövetkező veszteség valószínűségének, illetve nagyságának mértékét.

2. A kockázatok menedzselése

Az eddig leírt kockázatelemzési és kezelési gondolatok látszólag egy egyszeri tevékenységet jelentenek a szervezet számára, ez azonban csak akkor van így, ha egy konkrét döntést készítenek elő. Egy szervezet, ahhoz, hogy a kockázatait – legyenek azok biztonsági vagy más vonatkozásúak – csak akkor képes folyamatosan kézben tartani, ha azok kezelése, értékelése rendszeres tevékenységként

[188] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

részévé válik a működésnek. A legstabilabbnak gondolt folyamatokban is időről időre jelennek meg változások. Ezek a változások pedig befolyásolják a korábban kialakított kockázati értékeléseket. Ha ezekkel nem törődünk, az újonnan megjelenő tényezőket nem vesszük számításba egy hamis biztonságtudat alakul ki, amely jelentős veszélyeket hordoz magában.

Ennek megfelelően a kockázatok kezelése hosszú távon akkor megfelelő egy szervezetnél, ha az – az imént leírtak szerint – rendszeresen felülvizsgált értékelésen alapul, részévé válik a szervezeti működésnek, a hozzá kapcsolható felelősségek, hatáskörök tisztázottak, a szükséges erőforrások biztosítva vannak, és a szervezetben elfogadott mértékben és részletezettséggel szabályozottak a tevékenységei.

2.1. A kockázat információbiztonsági értelmezése

Mint az látszik, a kockázatmenedzsment kialakítása több tényezőtől függ. Például attól, hogy milyen típusú kockázatokat kell kezelnünk, mi a célunk a kockázat értékelésével, kezelésével, de jelentősen befolyásolja a módszertant, hogy milyen szakmaterületen végezzük az elemzést. Az információbiztonság területén az elvárásrendek (jogszabályok, szabványok, jó gyakorlat) alapján nagyjából egységes szemlélet alakult ki a kockázatok elemzésére, kezelésére. Ennek alapja, hogy a kockázatok felmérést vagyonleltár alapon végzik, a kockázatokat a sebezhetőség, fenyegetettség, hatás hármasságában értékelik. Ezek természetesen nem kötelező szabályok, de a gyakorlatban ez terjedt el a leginkább, és mint az látható volt az Ibtv. is ezt definiálja. A cél azonban mindig az, hogy kockázatkezelési intézkedéseket tudjunk meghatározni a szervezet számára.

2.2. Vonatkozó követelményrendszerek

Az információbiztonsági kockázatok elemzésének általános szempontjait, követelményeit több elvárásrendszerben, különböző szempontok szerint is megfogalmazzák. Ezekről egységesen ki lehet jelenteni, hogy alkalmazásuk jellemzően önkéntes, így az alkalmazott módszertan saját döntésünkön, illetve adott esetben a vállalásunkon múlik. Az Ibtv. és a kapcsolódó jogszabályi kör szintén nem határoz meg módszertant a kockázatok elemzésére, pusztán annak a követelményét állítja fel, hogy az intézkedések a kockázatoknak megfelelőek legyenek. Ebben a formában tehát a szervezeteknek teljes a szabadsága a megvalósítás terén.

2.2.1. ISO 31000-es szabványok

A kockázatelemzés elvégzéséhez az egyik legelterjedtebb módszertani segítséget nyújtó szabvány(család) az ISO 31000-es. Történetét tekintve nem egy réges-régen kialakult családtól beszélünk. Kiadásában- és sikerében – a különböző ISO szabvány alapú irányítási/menedzsment rendszerek (minőségirányítás, környezetközpontú irányítás, információbiztonsági irányítás), elterjedése, és kockázati alapokra helyezése játszotta a legnagyobb szerepet

Mint általában az ilyen menedzsment jellegű szabványok, ez sem konkrét megoldást, illetve egyszerűen, lépésről lépésre alkalmazandó technikát definiál, hanem azt a folyamatot, amit egy kockázatelemzés során végig kell vinni. Megadja, hogy milyen szempontokat kell figyelembe venni, amikor kiválasztjuk, illetve kialakítjuk a saját működésünknek leginkább megfelelő kockázatelemzést. Definiálja a kockázatelemzés-értékelés folyamatát, és a 31010 szabvány különböző eszközöket mutat be, értékelve azokat abból a szempontból, hogy melyiket mikor érdemes használni a kockázatfelmérés során. Ezt a szabványt haszonnal forgathatja mindenki, aki segítséget szeretne kapni a saját eljárásainak kialakításában.

2.2.2. ISO 2700x szabványcsalád

Az információbiztonsági menedzsment rendszerek mára alapvetővé vált szabványcsaládja. Története (elődszabványaival együtt) a 90-es évek közepéig nyúlik vissza, és mára meghatározó szerepet tölt be a szervezetek információbiztonsági rendszereinek kialakításában, tanúsításában. A jelenlegi törekvések szerint ebbe a szabványcsaládba rendezi az ISO minden olyan szabványát, mely többé-kevésbé szorosan kapcsolódik az információbiztonsághoz. Ennek megfelelően igen népes a 2700x szabványcsalád, több tíz szabványból áll.

Alapja az ISO/IEC 27001, amely alapvetően nem technikai, hanem egy menedzsment szabvány, még akkor is, ha tartalmaz technikai vonatkozású elvárásokat. Felépítését tekintve két részből áll. A szabvány törzse tartalmazza a menedzsment rendszerekre vonatkozó elvárásokat, az A melléklet pedig az információbiztonsági kontrolkövetelményeket. Ez utóbbiak kiterjedésükben és jellegükben hasonlóak a 41/2015. (VII. 15.) BM rendelet mellékleteiben megtalálható követelményekhez.

Kockázatmenedzsment szempontból érdemes kiemelni ebből a családból ISO/IEC 27005 szabványt, amely az információbiztonsági kockázatmenedzsmenttel foglalkozik. Logikája és felépítése hasonló a már korábban említett ISO 31000-hez, ugyanakkor több a kifejezetten információbiztonsági vonatkozása, és a mellékletei sok segítséget jelentenek egy kockázatkezelési eljárás kialakításához, illetve tartalommal való feltöltéséhez.

2.3. Kockázatmenedzsment-lépések

A kockázatok kézbentartását többféle módon megközelíthetjük. Mint azt láttuk, nincs egységes, minden szervezetre egyaránt jól alkalmazható módszertan, van ugyanakkor kellő átgondolással alkalmazható közel egységes logika. A következőkben bemutatott kockázatmenedzsment logika az ISO 31000 szabványcsalád értelmezését követi. Fontos megjegyezni, hogy időnként szóhasználatában eltér például az Ibtv. és rendeletei által használt definícióktól, azonban ez nem jelet logikai ellentmondást, pusztán azt, hogy a jogszabály, illetve szabvány ugyanarra a feladatra más-más magyar megfelelőt alkalmaztak. Ahol csak lehet, kitérünk erre a különbségre, de szem előtt kell azt is tartani, hogy a jogszabályi követelményeknek való megfelelés nem a szóhasználatból, hanem a megfelelően kialakított működésből származik.

Szögezzük le az elején, hogy elsődleges célunk minden kockázatkezelés során megismerni a kockázatot, és lehetőség szerint változtatni rajta a szervezet szempontjából előnyös módon. Az nyilvánvaló, hogy mind a megismerése, mind a változtatás elég összetett folyamat, Azt se hagyjuk figyelmen kívül, hogy a változtatás mellett a kockázat elfogadása, vagy átruházása is lehetséges megoldás, de ezekhez is az első lépés egy kellően alapos kockázatfelmérés. Könnyen belátható, hogy a kockázatok kezelésének megvalósítása (vagy elfogadása, áthárítása) elsősorban a szervezet erőforrásainak függvénye, és nagyban befolyásolják a külső követelményeknek való megfelelés kényszerei, olyanok mint jogszabályi vagy szerződéses kötelezettsége, esetleg piaci elvárások. A kockázatok felmérése azonban a szervezet – és nem utolsó sorban a vezetés – szempontjából bír nagy jelentőséggel. Megfelelő megvalósítása esetén elkerülhető a hamis biztonságtudat. Egy ismert – és bevállalt – kockázatra könnyebb hosszabb távon fejlesztést kezdeményezni, vagy „vészhelyzeti forgatókönyvet” kigondolni, mint egy nem is azonosított kockázatra. Ezért a kockázat felmérésének kiemelt jelentősége van.

2.3.1. Kockázatfelmérés

Ha a működési logika szabályait követjük, akkor a felmérés előtt magának a módszertannak a kidolgozása, az ehhez szükséges erőforrások biztosítása megelőzi a felmérést. Mivel azonban a jelen dokumentum célja pont ennek az előkészítő munkának a segítése, erre külön nem térünk ki.

„A kockázatfelmérés a kockázatok egy olyan növelt megértését nyújtja a döntéshozóknak és felelős résztvevőknek, amely befolyásolhatja a célok elérését, és az irányítás megfelelőségét és hatékonyságát a szóban forgó helyen. Ez alapot ad a döntéshez, hogy a leginkább megfelelő megközelítést használják a kockázatok kezeléséhez."[189]

A kockázatok felmérése során összességében az alábbi kérdésekre keressük a válaszokat:

- Mi történhet (és miért)?
- Mi a valószínűsége?
- Mi a következménye?
- Van-e bármi, ami csökkenti a valószínűséget, illetve a következményt?
- A kockázati szint elfogadható-e?

2.3.2. Kockázatazonosítás

A kockázatazonosítás célja, azon helyzetek, lehetőségek, események felismerése, melyek a kitűzött céloknak való megfelelést befolyásolhatják. Az azonosítás, a lehetőségek felmérésén túl magában kell foglalja mindazokat a tényezőket, melyek a kockázat kialakulásának környezetét jelentik. Ebben ki kell térni azokra a folyamatokra, szabályozókra, technikai eszközökre, emberekre, rendszerekre, hardver és szoftver tényezőkre stb. melyek relevánsak a kockázat és környezet megértésének szempontjából.

A kockázatazonosítási folyamatnak része annak a felmérése, hogy az adott kockázati tényező milyen esemény, helyzet vagy körülmény okozza illetve ez milyen forrásra vezethető vissza. Egyszerűbben megfogalmazva a kockázatazonosítás során magukat a lehetséges kockázatokat, az azok bekövetkezéséhez vezető fenyegetési forrásokat, és saját szervezetünkben értelmezhető sebezhetőségeket gyűjtjük össze. Ennek a feladatnak az elvégzése komoly felkészültséget és célszerűen megfelelő rutint kíván, azonban a megvalósítást gyakran támogathatjuk meglévő tudásbázisok felhasználásával.

Ha egy meglévő rendszert korábbi adatok elemzésével, általános, vagy az adott kockázatelemzés céljaira kialakított ellenőrzőlisták segítségével vizsgáljuk át, azt evidencián alapuló kockázatazonosításnak szokták nevezni. A megvalósítás terén ennek a módszernek az alkalmazása a legkönnyebb, hiszen csak egy lista alapján kell „igent vagy nemet" mondani, hogy az adott szervezet és cél vonatkozásában felmerül(het)-e az a kockázat. Ugyanakkor, ha nem rendelkezünk kellően alapos, az adott célra kialakított adatbázissal, vagy ellenőrzőlistával, akkor fennáll a veszélye, hogy azonosítatlan kockázatok maradnak a rendszerben.

Nagyobb erőforrásráfordítást és több szakértelmet igényelnek azok a módszerek, melyek nem ellenőrzőlistákra, hanem a felmérési folyamatot meghatározó tervekre épülnek. Ilyenkor nem a konkrét kockázatok, illetve forrásaik szerepelnek egy tervben, hanem az a lépéssor, amelyet a csoportnak követni kell, hogy lehetőleg mindenre kiterjedően tudják azonosítani a kockázatokat és forrásaikat. Ilyen módszert akkor érdemes választani, ha nem áll rendelkezésre megfelelő háttér az evidenciákra alapozott módszerhez, de a felmérendő terület generálisan már jól leírt, azaz a felmérés folyamata általánosítható, és kellő részletességet biztosít.

Ha a tervszerű megközelítéshez sincs elegendő előzetes információ, mindenképpen szükséges, hogy kellő háttérismerettel rendelkező csoportot alkossunk a feladat elvégzésére. Ilyenkor ugyanis nincs más lehetőség, mint néhány általános csoporttechnikát alkalmazva, intuitív módon keressük és azonosítjuk a kockázatokat, forrásaikat, és a sebezhetőségeket.

[189] MSZ EN 31010:2010 Kockázatkezelés. Kockázatfelmérési eljárások

2.3.3. Kockázatelemzés

Ha szigorúan vesszük a kockázatfelmérés szakaszainak elkülönítését, akkor az előzőekben bemutatott azonosítás kizárólag a „kockázati lehetőségek listáját” hozta létre, vagyis még nem ismerjük az összefüggéseket, illetve nem tudunk nagyságokat rendelni sem az előfordulásokhoz, sem a következményekhez. A kockázatelemzés ilyen módon a kockázatok „megértésének” a lépése. A vizsgálódások során fel kell tárjuk az okok, források, következmények összefüggéseit, és meg kell határozzuk mindazon tényezőket, melyek a kockázatok kialakulását befolyásolják.

A kockázatelemzés során két fő célt kell megvalósítanunk. Egyrészt az okozati láncokat kell felderítenünk, azaz azt, hogy egy fenyegetési forrásból milyen események következhetnek be, és azoknak milyen a hatása. Másrészt ezeket a fenyegetéseket, hatásokat összemérhetővé kell tennünk úgy, hogy a későbbiek során alkalmasak legyenek a kockázatkezelő intézkedések meghatározására. Fontos kiemelni, hogy egy eseménynek több következménye lehet, és ugyanez az esemény adott esetben több okra is visszavezethető lehet. Így a kockázatelemzés feladata egyáltalán nem egyszerű. Az ilyen oksági láncokat a különböző kockázatelemző technikák különböző módon próbálják meg leírni, modellezni, attól függően, hogy egy fenyegetést felmérve, az abból származó összes eseményt és azoknak minden hatását vizsgálják, vagy éppen az események jól azonosíthatósága miatt innen közelítenek, és a vizsgált esemény okainak, és következményeinek láncait derítik fel. Illetve létezhet olyan megközelítés is, amely a következményekre koncentrál, és azokat az eseményeket, illetve az egyes eseményeknek a forrását igyekszik felderíteni, amelyek a definiált következményhez vezettek.

A kockázatelemzés feladata az összefüggések megállapításán túl, hogy jól értékelhetővé tegye a kockázatokat, azaz valamilyen egységes értékeléssel lássa el a már felmért kockázati láncolatokat. Egyszerűen – bár mint látni fogjuk nem kifejezetten pontosan – megfogalmazva, számszerűsítse a kockázatokat.

A számszerűsítés kifejezés azért nem helytálló teljesen, mert a módszerek egy része valójában nem rendel számokat vagy számítást a kockázatok nagyságának meghatározásához. Az ilyen módszerek, az úgynevezett kvalitatív módszerek. Az ilyen megoldások a valószínűségeket, illetve a következményeket olyan besorolások szerint értékelik, mint az „elhanyagolható”, „kicsi”, „közepes”, „nagy”, „katasztrofális” stb. Nagy előnye az ilyen elemzésekhez, hogy nincs szükség komolyabb matematikai apparátusra, se előzetes „mérési” adatokra. Megköveteli ugyanakkor ez a megoldás, hogy az egyes besorolási szinteket kellő alapossággal definiálják, ami olykor nehézséget okoz. Buktatója lehet a kvalitatív értékelésnek, ha több, egymástól valamennyire független értékelés során nem egységesek a besorolás alkalmazásában, így az összehasonlítás alapja nem lesz egyenszilárdságú.

A félkvalitatív módszerek már tartalmaznak számszerűsítést, így azok összegzésének szabályai a valószínűségek és hatások tekintetében matematikailag megadhatók, ugyanakkor az egyes tényezők számértékének megadásakor nem egzakt adatokra támaszkodnak, hanem valamilyen korábbi tapasztalatok, esetleges leírások alapján sorolják be. Ezzel a módszerrel csökkenthető ugyan a szubjektivitás a kvalitatív módszerhez képest, de a definíciós nehézségek itt is fennállnak. Tovább nehezítheti az elemzést végzők munkáját, hogy a félkvantitatív megoldások alkalmazásakor gyakran 5-ös, vagy 10-es skálát definiálnak, ami jó érzékenységet biztosít, de – különösen a közepes értékek esetén – még nehezebbé teszi a különbségtételt két érték között.

Amennyiben a szervezet megfelelő mennyiségű – és minőségű – információ birtokában van, a kockázatainak értékelésére alkalmazhatja a kvantitatív elemzést. Ennek lényege, hogy előre meghatározott matematikai összefüggésekkel összesíti a bekövetkezési valószínűség statisztikai vagy más elemzésekből számított számszerű értékét, a következmény szintén számításokkal alátámasztható értékével. Ebben az esetben egyértelmű, hogy valóban egzakt, és teljeskörűen alátámasztott értékeket kaphatunk, azonban az olyan adatbázisok megléte, és hozzáférhetősége, melyek alkalmasak ilyen elemzésekre, igen szűkkörű. Bizonyos – magas kockázatú – iparágak azonban rendelkeznek ilyenekkel. Gyakran ezekben az iparágakban a vonatkozó szabályozók csak az ilyen, kellően megalapozott elemzéseket fogadják el.

2.3.4. Kockázatértékelés

A kockázatfelmérés előkészítése során figyelembe vettük a szervezet és a működés sajátosságait, és ezek alapján határoztuk meg – többek között – az alkalmazott módszertanokat. Mindezzel párhuzamosan azt is definiálni kellett, hogy a szervezet szempontjából milyen kockázati szinteket tekintenek elfogadhatónak. Ezek a kvantitatív, illetve félkvantitatív elemzések esetében számszerűen meghatározhatók, kvalitatív esetben pedig definiálni lehet azokat az együttállásokat, melyek elfogadhatók. A kockázatértékelés során „csak" annyi a feladatunk, hogy az egyes elemzések során kapott értékeket összevetjük az elfogadhatósági kritériumokkal. Vagyis arra használjuk fel a kapott kockázati értékeket, hogy valamilyen döntést készítsen elő, vagy megoldási prioritásokat jelöljön ki. Választ kaphatunk olyan kérdésekre mint: Kell-e kezelni egy kockázatot? Ha igen, milyen sorrendben? Megkezdhető-e egy adott beruházás, folyamat a jelenlegi paraméterekkel? A különböző lehetséges megoldások közül melyiket kell választani?

A különböző besorolások, értékelése értelmezésére a legtöbb esetben nem két (elfogadható, nem elfogadható) hanem három, (elfogadható, feltételekkel elfogadható, nem elfogadható) kategóriát célszerű létrehozni.

A kockázatértékelés részévé tehetünk olyan metódusokat is, melyek a tapasztalatok függvényébe módosítják a korábban rögzített kockázati követelmények szintjét. Ilyen esetekben azonban gondosan ki kell dolgozni ezt a lehetőséget, hogy csak a valóban szükséges helyzetekben és mértékig módosuljanak a kritériumok, és ne végződjön a kockázatfelmérés egy állandó célmódosításban.

Az eddig leírt kockázatfelmérés folyamatát szakmai szempontból jól elválasztva tárgyaltuk, a valóságban ezek a lépések (azonosítás, elemzés, értékelés) nem kell, hogy elkülönüljenek egymástól sőt, sokszor célszerű ezeket legalább részben együtt kezelni. Vannak olyan módszertanok, melyekben az azonosítás és elemzés nem is választható szét érdemben. Ettől függetlenül látnunk kell, hogy melyik lépésnek mi az elsődleges célja, hiszen csak akkor tudunk alkalmas technikát választani, ha átlátjuk alkalmazásuk célját és az elvárt kimenetet.

2.3.5. Kockázatkezelés

A kockázatok felmérésnek nem szabad „öncélúnak" maradni. Az egész folyamatot azért hoztuk létre, és végeztük el lépésről-lépésre, hogy a felderített kockázatokra válaszokat tudjunk adni. A válaszok sokfélék lehetnek megvalósításuk szerint, azonban négy fő irányt határozhatunk meg a kockázatok kezelésére.

Amennyiben úgy ítéljük meg, hogy a kockázat nagysága, vagy a csökkentésének erőforrásigénye azt indokolja, megszüntethetjük a kockázatos tevékenységet. Ez a lehetőség ritkán adott, de semmiképpen nem elvetendő, hiszen lehetnek olyan – a szervezet fő profiljától távol eső – tevékenységek, melyeket komolyabb értékveszteség nélkül meg lehet szüntetni. Az is előfordulhat, hogy olyan működések maradtak meg, vagy alakultak ki, melyek a szervezet kényelmét szolgálták, de kockázatosságuk miatt inkább érdemes megszüntetni, mint a kellően biztonságos megvalósítást kialakítani. Ilyenre lehet példa, ha egy szervezet hagyományosan elfogadta az otthonról történő munkavégzést. A kockázatfelmérés után azonban ennek a biztonságos megvalósításához a technikai feltételek megteremtése olyan költségekkel járna, hogy inkább megszüntetik ezt a lehetőséget.

A szervezetre vonatkozó kockázatok csökkentésének másik módja, hogy a kockázatokat áthárítják harmadik félre. Ennek leghagyományosabb megvalósulási formája a különböző biztosítások megkötése volt. Manapság az áthárítás fogalmát azonban már tágabban kell értelmezünk. Ide sorolhatunk minden olyan intézkedést, amely olyan megállapodások létrejöttét szolgálja, amelynek következtében a szervezet a kockázatos tevékenységeket nem maga végzi, vagy a megállapodás részeként garanciákat köt ki, például a beszállítóival szemben, hogy azok garantálnak valamilyen szolgáltatási szintet, selejtmentességet stb., és ezek nemteljesülése esetén megfelelő kárcsökkentő/elhárító intézkedéseket tesznek.

Az egyik legkézenfekvőbb megoldás a kockázatok kezelésére a kockázatok csökkentése valamilyen bevezetett (kontrol) intézkedés hatására. Nyilvánvaló, hogy ha se megszüntetni, se „kiszervezni" nem tudjuk az elfogadhatónál nagyobb kockázatot, akkor a csökkentésre kell intézkedéseket tennünk. Egy szervezet életében ez a kockázatkezelés a leginkább elterjedt, mivel ez az a terület, amelyre a leginkább hatással tudunk lenni. Tudjuk a rendelkezésre álló erőforrásaink szerint ütemezni, és az elérhető kockázatcsökkenés mértéke szerint priorizálni az elvégzendő tevékenységeket, valamint közvetlen, vagy közvetett módon mérhetjük a hatásukat. Az intézkedések tárháza szinte végtelen, a legegyszerűbb szervezési, szabályozási megoldásoktól a rendkívül összetett technikai rendszerek alkalmazásáig bármit elvégezhetünk, ami az erőforrásainkból kitelik. Az információbiztonsági kockázatok kezelésére vonatkozó intézkedések lehetséges kontroljait tartalmazza az ISO 27001 szabvány A melléklete, de a kockázatcsökkentő intézkedések jól átgondolt struktúráját találjuk az Ibtv. végrehajtási rendeleteiben is.

A felmért kockázatokkal kapcsolatban végső lehetőségként dönthetünk úgy, hogy elfogadjuk azokat érdemi kockázatkezelő intézkedés nélkül. A kockázat elfogadásnak mindig jól átgondolt, megalapozott és indokolt döntésnek kell lennie, ezért a legtöbb szabvány vagy jogi szabályozás ezt egyértelműen az elsőszámú vezető hatáskörébe utalja, mivel az ebből következő esetleges károkért végső soron ő vállalja a felelősséget. Az elfogadható szintet meghaladó kockázat elfogadása csak akkor helyénvaló, ha az előző három kockázatkezelési lehetőség nem valósítható meg a kockázatokkal arányos módon.

Fontos kitérni egy fogalomra, amely a kockázatkezelés sikerességének fokmérője lehet. Ez az úgynevezett maradványkockázat. Mivel 100%-os biztonság nem teremthető meg, a szervezet működésében mindig lesznek kockázatok. Minden végrehajtott kockázatkezelő intézkedés után marad fent valamilyen nagyságú kockázat. Ezt a fennmaradó kockázatot nevezzük maradványkockázatnak. Ennek mértéke függ az „eredeti" kockázat nagyságától és a végrehajtott csökkentő intézkedéstől. A maradványkockázat értékelése része kell, legyen a kockázatkezelésnek, mint ahogy az is, hogy ennek – mármint a maradványkockázatnak – az elfogadásáról döntést kell hozni.

A kockázatkezelési terv

Minden nem elfogadható szintű kockázatról a fentieknek megfelelően döntést kell hozni. Ez a döntés fogja meghatározni, hogy mely kockázatokat milyen módon kezelünk, és ez fogja az alapját jelenteni a kockázatkezelési tervnek. A kockázatkezelési terv összefoglalja a szervezet által elvégzendő mindazon intézkedéseket, melyeket a különböző kockázatok megszüntetésére, átruházására, csökkentésére alkalmazni kíván. A kockázatkezelési terv tartalmazza az intézkedéseket, azok részletes bemutatásával együtt, az összerendeléseket, hogy egy intézkedés melyik azonosított kockázatra van hatással, a kockázatcsökkenés mértékét, illetve ebből következően a maradványkockázat értékelését, valamint az egyes maradványkockázatok elfogadását.

Fontos kiemelni, hogy az egyes intézkedések során figyelemmel kell lenni azok más kockázatokra gyakorolt hatására.

Az intézkedések meghatározásához számba kell venni a lehetséges intézkedési alternatívákat, és külön-külön vizsgálni kell ezek egyszeri, illetve folyamatosan megjelenő költségeit. Fel kell mérni az intézkedések hatására elérhető kockázat változását, amelyet a ráfordítások függvényében értékelni kell. A kockázatcsökkentő intézkedések meghozatalára a megfelelő szervezeti szinten kell definiálni a felelősséget és hatáskört. Ez a szint gyakran a felső vezetés szintje, úgy ahogy a maradványkockázat elfogadása is ezen a szinten történik meg.

Az, hogy a kockázatazonosításra, elemzésre, értékelésre milyen módszert alkalmazunk, teljesen a szervezet döntésére van bízva. Érdemes azonban néhány szempontot figyelembe venni, mielőtt kialakítjuk a saját folyamatainkat erre a tevékenységre. Először is a kockázatfelmérés, kezelés céljának megfelelően válasszunk. Egyszerű, rövid, esetleg gyakran elvégzendő döntéselőkészítéshez más

módszertan fog illeszkedni, mint egy teljes szervezetre kiterjedő, egyszeri átfogó felmérésre. Vegyük figyelembe a meglévő erőforrásaink mennyiségét és minőségét. Itt éppúgy törődnünk kell a felmérést végző munkatársak kapacitásával, tudásával, mint a támogató eszközök rendelkezésre állásával, de a ráfordítható anyagi erőforrásokkal is, továbbá fontos tényező lehet az idő, amely a munka elvégzésére adott. A kiválasztás szempontjai között szerepel még a folyamataink, illetve a felmérendő kockázataink bizonytalansága, vagy állandósága. Az, hogy egy adott pillanatban mennyire megismerhető egy folyamat vagy külső hatás, illetve hogy mennyire marad állandó, ez a megismert állapot, fontos szempont. Mint ahogy az is, hogy milyen bonyolultságú, ha úgy tetszik mennyire összetett a kockázatelemzés alá vont terület. Ezeket együtt értékelve célszerű meghatároznunk, hogy milyen módszertant alkalmazunk a kockázatok felmérése, illetve kezelése során

Megjegyzés: Az eddigiekben a kockázatfelmérést használtuk együttes definícióként a kockázatok összegyűjtésére, számszerű, vagy minősítéses alapú meghatározására, illetve ezek összevetésére az elfogadható szinttel. Az Ibtv. megfogalmazásában ez a kockázatelemzés. Mint azt korábban már jeleztük, a gyakorlati munka során a megnevezések használata csak abból a szempontból bír jelentőséggel, hogy azokat következetesen, egységes rendszerben alkalmazzuk, azonban a jogszabály értelmezésénél erre a különbségre érdemes figyelemmel lenni.

3. Az okoseszközök specialitásai

Az úgynevezett okoseszközök kapcsán az első probléma, amibe ütközünk, hogy mik is ezek az eszközök, azaz elég komoly definíciós nehézségek adódnak, ha ilyenekről beszélünk. Az okostelefon már szinte mindenki zsebében ott lapul, és egyre többen birtokolnak okos órát, vagy okos TV-t, de ha a reklámokat nézzük, szinte alig találunk olyan eszközt, amiből ne lenne – legalább prototípus szinten – okosnak kikiáltott változat, a kávéfőzőtől a mosógépen át egészen a biztonsági kameráig. De – ha a reklámok szintjétől elvonatkoztatunk – mitől is okos az eszköz? A leginkább elfogadott gondolat szerint azokat az eszközöket tekintjük okoseszköznek, melyek az internethez, más készülékhez (vagy mindkettőhöz) képesek önállóan kapcsolódni és adatkommunikációt folytatnak velük. Ehhez tegyük még hozzá, hogy ezek az eszközök szinte kivétel nélkül rendelkeznek valamilyen érzékelő, illetve beavatkozó egységgel, melyek a felépített kapcsolataikon keresztül lekérdezhetők, vagy vezérelhetők.

Különböző kutatások láttak napvilágot arról, hogy az okoseszközök milyen mértékben terjedhetnek el az elkövetkező években. A számok bár jelentős szórást mutatnak, de 2020-ra 26 és 100 milliárd közé teszik forgalomban lévő olyan eszközök számát, melyek egymással összeköttetésben lesznek. Ha ezt a számot nézzük, egyértelmű, hogy a szervezetek életében sem elkerülhető, hogy megfelelően felkészültek legyenek az okoseszközök adta kihívásokra.

Manapság még kijelenthető, hogy egy szervezet szempontjából a személyhez köthető eszközök, azon belül is leginkább az okostelefonok vannak jelen, de nem szabad megfeledkeznünk az okosórák térhódításáról sem. Az egyéb okoseszközök, például televízió, kávéfőző, épületautomatizálás, vagy biztonsági eszközök szervezeti célok megvalósítása szempontjából – presztízsükön túl – még kevés felismert hozzáadott értékkel bírnak. Beszerzési költségük magas, és a legtöbb esetben elsősorban háztartási felhasználásra tervezték működésüket, illetve kapacitásukat, így nem általános az elterjedtségük céges környezetben.

Mint az ilyen jellegű eszközök közül a legrégebben piacon lévők, – tulajdonképpen a kategóriát megteremtő – az okostelefonok hordoznak szinte minden olyan tulajdonságot és megoldást magukban, melyek jellemzik az okoseszközöket. Azt is bátran kijelenthetjük, hogy az okostelefonok rendelkeznek a legnagyobb funkcionalitással, abban az értelemben, hogy az ezekben fellelhető megoldások kerültek, kerülnek át a más eszköztípusokba. Ennek megfelelően, ha az okostelefonok működését kellő alapossággal körül járjuk, a legtöbb okoseszköz le tudjuk fedni.

3.1. Folyamatos adatkapcsolat

A fent megfogalmazott definícióból is következik, hogy az egyik legjellemzőbb tulajdonság, amelynek létezését kezelni kell egy szervezet működésében, amivel az okoseszközök – és kiemelten az okostelefonok – rendelkeznek, az állandó adatkapcsolat létezése, amely az eszköz folyamatos bekapcsolt, illetve készenléti állapotából következően jellemzően napi 24 órás elérhetőséget jelent az interneten. Az eddig megszokott – informatikai alapokra épülő – eszközök esetében egy kapcsolat mindig szándékosan, egy adott cél érdekében épült fel, és maximum az eszköz bekapcsolt (azaz használatra tervezett) állapotának idejéig volt élő. Minden olyan rendszerelem számára, amely normál működésben igényelte a folyamatos kapcsolat lehetőségét, logikailag lehatárolt hálózatokkal – tűzfalak mögött – teremtettünk biztonságos környezetet. A különböző fenyegetettségeknek kitettség szempontjából ez egy igen jelentős változás.

3.2. Nem kontrollált hálózatok

A folyamatos adatkapcsolat szükségéből adódóan a mobil eszközök esetén komoly kihívást jelent, hogy az adott eszköz milyen hálózatra csatlakozik fel. Az okostelefonok ebből a szempontból speciálisak, hiszen a legtöbb esetben az adatkapcsolatuk egy szolgáltató által biztosított GSM hálózaton keresztül valósul meg. Ez gyakran akkor is igaz, ha amúgy rendelkezésre áll kontrollált hálózat. Ugyanakkor az eszközök mobilitásából adódó kockázat, hogy képesek, és a megfelelő működéshez igénylik is a folyamatos adatkommunikáció érdekében, hogy valamilyen adathálózathoz legyen hozzáférésük, melyet adott esetben ismeretlen, de legalábbis a szervezet által nem kontrollált vezetéknélküli hálózatokon keresztül valósítanak meg. Ilyenkor sem a hálózat összetevőire, sem az adatforgalom biztonságára, sem szolgáltatások megbízhatóságára nincs befolyásunk, de még információnk is csak korlátozottan van.

Szintén fontos kérdés, hogy a megszokott hálózati csatlakozásokon túl az eszközök egy – mára jelentős – része képes ad hoc hálózat kialakítására is, amely egy szervezeten belül többféle anomáliához is vezethet. Fontos továbbá az is, hogy ezek a készülékek jellemzően többféle vezeték nélküli kommunikációs szabványt támogatnak, így képesek olyan kommunikációt folytatni, melyek eddig – alig értelmezhető számosságuk miatt – nem kerültek a szervezeti működés középpontjába.

3.3. Magán- és szervezeti célú felhasználás

Az okoseszközök előnyeinek kiaknázásához a szervezetén túl, az egyes munkatársaknak is érdeke fűződik, különösen, ha az eszközök által nyújtott kényelmi szolgáltatásokra gondolunk. Ezért a legtöbb esteben a kétféle – „céges” és magán – felhasználás keveredik. Ez azonban jelentős mennyiségű megoldandó kérdést vet fel a szervezet részéről. Ezek egy része már ismert más, főleg hordozható eszközök például laptopok esetében. Ilyen kérdés például a céges és magán tevékenység elkülönítése, a szervezeti adatokhoz való hozzáférés, de felmerülnek adatvédelmi és más jogi (például szoftvere licencére vonatkozó) kérdések is.

3.4. Fokozott mobilitás

Az okostelefonok használatának egyik leginkább jellemző vonása, hogy gyakorlatilag a nap 24 órájában a felhasználónál van, folyamatos a használata, és ezt szinte szó szerint kell érteni. Míg bármely más informatikai eszköz méretéből, funkciójából adódóan, ha mobil is, nincs folyamatos használatban és gyakran értelmezhető olyan szituáció, amikor nincs kéznél. Az okostelefonok azonban utazás

alatt, a munkaidő közben tartott szünetekben, étkezések során, de a munkaidő utáni szabadidős tevékenységek alatt is rendszeres használatban vannak. Ez az eszközök biztonsága szempontjából kiemelt jelentőségű. Mindehhez társul az eszközök viszonylagosan kis mérete, mely az elvesztés vagy eltulajdonítás esetén annak felfedezését nehezítik.

3.5. Felhő alapú működés

Az okostelefonok sajátosságai közé tartozik, hogy minden esetben valamilyen felhő alapú szolgáltatás igénybevételéhez kötött a megfelelő működésük. Azaz ahhoz, hogy az eszköz egyáltalán képes legyen érdemben ellátni az „okos" funkcióját, minimum az operációs rendszere által preferált felhőszolgálta-tásban regisztrálni szükséges. Egyes készülékek ezen túl lehetőséget kínálnak további – a gyártó által preferált – felhő alapú szolgáltatásokat igénybe venni, azaz egy készülékről ugyanaz az információ akár több – kevéssé ellenőrizhető – helyre is felkerül. A beállítások módosításával, és kellően tudatos eszközkezeléssel ugyan csökkenthető a készülékek ilyen irányú kitettsége, azonban teljesen nem szüntethető meg.

4. Okoseszközök biztonsági kihívásai

A következőkben bemutatandó biztonsági kihívások általános trendeket, az okoseszközökhöz kapcsolódó szituációkat mutatnak be. Ezekkel olyan területekre akarjuk felhívni a figyelmet, melyek a hagyományosan értelmezett kockázatkezelés módszereivel nehezen kezelhetők, és nem tartoznak egyértelműen a technikai vagy logikai szabályozókkal csökkenthető kockázatok közé. Ezek bemutatásával leginkább a biztonságért felelős személyek figyelmét szeretnénk felhívni olyan folyamatokra, melyeket jó, ha szem előtt tudnak tartani egy-egy döntés előkészítése, vagy meghozatala során. A legtöbb felvetett problémára persze lehet – jellemzően részleges – kockázatcsökkentő megoldást találni, de a mostani bemutatásnak nem ezek felsorolása a célja, hanem annak a felvázolása, hogy milyen potenciális biztonsági problémákat rejt az okoseszközök megkerülhetetlen jelenléte, illetve, hogy ezek milyen összefüggésekkel rendelkeznek.

4.1. A tudásolló nyílása

Hagyományosan a biztonsági kihívások között mindig előre soroljuk az emberi tényezőt. A legtöbb technikai rendszer esetében igaz, hogy a felhasználók magatartása, a területre – és a biztonságra– vonatkozó ismeretek hiánya még az amúgy biztonságosnak mondott, és megfelelően biztonságtudatosan létrehozott rendszerek esetében is jelentős kockázati tényezőt rejt magában. Ez a probléma fokozottan jelenik meg az okoseszközök használata során. Ezek az eszközök felépítésükben, működésükben olyan összetettséget valósítanak meg, amelyet nem csak az „átlag" felhasználó, de még az informatikai területen jártas szakemberek sem mindig látnak át teljességében. Ez persze nem is feltétlenül lenne elvárás, de az okos eszközöket – akár a szervezet keretei között – alkalmazó felhasználók nagyon gyakran a legalapvetőbb biztonsági ismeretekkel sem rendelkeznek az eszközeikre vonatkozóan. Sőt, ha a kérdést tovább vizsgáljuk, hamar arra is fény derül, hogy nem csak az eszközeik (biztonsági) alapfunkcióit nem ismerik, de az általuk telepített applikációk, alkalmazások lehetőségeivel, illetve beállításaival is csak igen korlátozott mértékben vannak tisztában. Ez persze nem róható fel csak a felhasználóknak, hiszen olyan mennyiségű funkciót, választási, illetve beállítási lehetőséget tartalmaznak az eszközök, melyeket követni szinte lehetetlenség.

Ehhez a gondolathoz tartozik még az a folyamatosan bővülő és fejlődő alkalmazáshalmaz, amely a felhasználók rendelkezésére áll. Az egyre nagyobb kínálatban nem csak a tömegesen megjelenő

rossz szándékkal megírt alkalmazások jelentik a veszélyt, hanem a fölösleges, kihasználatlan és a maga voltában potenciális sérülékenységet rejtő többletfunkciók. Bátran kijelenthetjük, hogy egy „átlagos" felhasználó az okos készülékére telepített alkalmazások felét-kétharmadát alig használja és a rendszeresen használt appok funkciói közül is van jónéhány olyan, melynek még csak létezéséről sem nagyon tud. Ilyen módon az információbiztonság egyik alapelve, a szükséges minimumra való törekvés, biztosan nem tud megvalósulni.

4.2. Adatintegráció

Az elmúlt időszak trendjeit figyelve látható, hogy az okoseszközökön (és nem csak ott) futó alkalmazások mind nagyobb integrációra törekednek egymással, a kapcsolódó felhőszolgáltatásokkal, az eszközök más funkcióival, de akár a közösségi médiával is. Ezek az integrációs törekvések mára odáig jutottak, hogy egyes appok telepítése során alapértelmezetten „kérik le" az adatokat az eszköz kontaktlistájából, az elérhető közösségi médiából, vagy más kommunikációra (is) használt alkalmazásból. Ezek a kapcsolódások, adatintegrációk ma még sok esetben kellően tudatos felhasználói magatartással csökkenthetők, de sokszor az ilyen korlátozások az alkalmazások funkcionalitásának korlátait is jelentik. Céges környezetben használt okoseszközök esetén persze elvárás lenne az ilyen összekapcsolások korlátozása, illetve megtiltása, de az imént említett funkcióvesztés ennek az egyik legfőbb akadályozó tényezője. Azt is meg kell említeni, hogy lehetnek olyan esetek, amikor az adatok átadása, szinkronizálása – ha ellenőrzött körülmények között zajlik – a biztonság fokozását szolgálhatja. Ilyen eset lehet például, ha egy lokális címjegyzék nem csak lokálisan, hanem – egy megfelelően védett környezetben – máshol letárolódik.

4.3. Rövidülő életciklus

A legtöbb használati cikkünknél igaz, hogy a tervezett felhasználási ideje rövidül, mind technikailag mind erkölcsileg sokkal hamarabb avulnak el. Terméktípustól függően 1-3 évente a gyártók újabb típusokkal, fejlettebb tudású eszközökkel rukkolnak elő, ezzel téve elavulttá az egy esetleg két generációval korábban kiadott készülékeiket. Ez az okoseszközök piacán különösen igaz. Mivel a technikai fejlődés ezen a területen igen gyors, és a gyártók rendkívül kiélezett harcot folytatnak a piaci részesedésért, gyakorlatilag egy év alatt válnak a piacvezető típusok, eszközök a középkategória képviselőivé. Ez a gyors változás több biztonsági kérdést is felvet. Mivel – ahogy korábban már kitértünk rá – az okoseszközök egy részének használatát elsősorban azok presztízse indokolja, a gyorsan csökkenő presztízs gyakori eszközcserét von maga után. Bármilyen „hagyományos" eszköz cseréjét is biztonsági szempontból jól át kell gondolni, de egy okoseszköznél ez kiemelten fontos. Egyrészt gondoskodni kell a korábbi funkcionalitások új eszközön történő megvalósításáról, másrészt a régi eszközön tárolt adatok átviteléről és a „kivont" készüléken megfelelő törléséről. Meg kell vizsgálni a régi készülék további felhasználásának lehetőségeit is. Nem elhanyagolható kérdés, hogy egy okoseszköz cseréje gyakran jár azzal, hogy újabb verziójú operációs rendszer vagy firmware van az eszközön, ami kompatibilitási problémákhoz vezethet, mind alkalmazás, mind adatstruktúra szinten. Fontos tehát, hogy ezekre a változáskezelés kellően felkészült legyen.

A rövidülő életciklus, és a folyamatos újítási kényszer azonban nem csak az eszközök gyártóit terheli, hanem a szoftverek készítőit is. Ez pedig együtt jár azzal, hogy újabb és újabb szolgáltatásokkal bővítik az alkalmazásokat, illetve egyre újabb appokkal jelennek meg a piacon. Ezen funkcionális fejlesztés mellett azonban általában jóval kevesebb erőforrás – és idő – jut az alkalmazások biztonságának megteremtésére. Bár a legtöbb jelentős fejlesztő cég folyamatosan frissíti az alkalmazásait, és ilyenkor gyakran a biztonsági réseket is foltozzák, ez a feszített tempójú fejlesztés semmiképpen nem tesz jót a biztonságnak. Azt se hagyjuk ki a számításból, hogy az okostelefonokat leszámítva – ahol a

frissítések jellemzően automatikusan érkeznek – más okoseszközöknél ez már nem annyira egyértelmű. Gondoljunk csak bele, hogy például egy okos TV firmware-ét milyen gyakorisággal frissíti egy felhasználó.

4.4. Nagy változatosság

Az okoseszközök gyártói között ugyan van néhány, amelyek viszonylagosan nagyobb piaci részesedéssel bírnak, de jellemző erre a környezetre, hogy sok gyártó, sokféle terméke érhető el bárki számára. A készülékek és a hozzájuk kapcsolt szoftverek sajátossága, hogy sokszor az azonos alapokra épülő eszközök is más-más szoftver, vagy szoftver verziót futtatnak, illetve az egyes gyártók különböző mértékben szabják saját eszközükre az alap operációs rendszereket. Ez már önmagában is lehetőséget jelent arra, hogy kompatibilitási problémák adódjanak, azonban, ha mindezt szervezeti oldalról közelítjük meg, ez azt okozza számunkra, hogy már egy közepes létszámú szervezet esetén is nehezen kezelhetővé válik az egységes menedzsmentje az ilyen eszközöknek. Nem is beszélve a telepíthető alkalmazások hatalmas mennyiségéről. A változatosságot tovább fokozza a – már látott okokra is visszavezethető – nagy gyakoriságú frissítések kérdése. Ez az operációs rendszerek szintjén is eltérhet gyártónként, de az alkalmazások frissítési gyakorisága végképp követhetetlenné teszi az állapotokat. Mindezt egy szervezet részéről úgy kezelni, hogy közben az okoseszközök egyik lényegi tulajdonságát, a személyre szabhatóságot, illetve a felhasználói élményt ne csökkentenénk jelentősen, szinte lehetetlen feladatnak látszik

4.5. Felület egy támadás előkészítésére

Amennyiben általánosan beszélünk a biztonságról, feltételezhetjük, hogy nem csak maga az okoseszköz lehet egy támadás célpontja. Pontosabban a valódi cél nem az eszköz, vagy az azon tárolt információ, hanem egy átfogóbb, más célokat megvalósító támadás előkészítése érdekében veszik célba az eszközünket. Egy sikeres támadás egyik legfőbb, tényezője a megfelelő előkészítés. Erre viszont kiválóan alkalmas lehet egy olyan eszköz, amely folyamatos adatkapcsolattal rendelkezik, többféle szervezeti adatot kezelő rendszerhez van hozzáférése, esetleg megtalálhatók rajta a szervezeti hálózathoz való hozzáférés autentikációs adatai, munkatársak, partnerek elérhetőségei, vagy kinyerhetők belőle az informatikai architektúrára vonatkozó részleges adatok. Az eddig felsoroltak olyan információs aranybányát jelentenek egy támadónak, amely ha már részlegesen is a rendelkezésére áll, komoly segítség a támadás előkészítésében. Ha ez nem volna elég, akkor maga az okoseszköz arra is lehetőséget ad, hogy – megfelelő szaktudással – olyan kódokat juttassanak be rajta a szervezeten belülre, amelyek további információkat szolgáltatnak, vagy éppen kárt okoznak.

4.6. Felhasználói tudatosság (hiánya)

Az okoseszközök használata jelentős kényelmi funkciókkal bővíti a napi működést a felhasználók számára. Ezek a többletszolgáltatások, legyen szó akár csak a mobilitásról, vagy távoli vezérelhetőségről, ellenőrizhetőségről, sokszor szolgálják a szervezet működési céljait is. Ezzel együtt azonban, pont a kényelmi szempontok könnyen felülírják a biztonsági célokat. Általánosságban kijelenthető, hogy a biztonsági megoldások az élet szinte minden területén a kényelmi funkciókkal szembe mennek. Ennek az az eredménye, hogy ahol nincs megfelelő biztonságtudatosság az eszközök használatában, ott a kockázatok fokozottan jelennek meg. A már korábban említett tudásolló egyre tágabbra nyílása miatt azonban sokszor a felhasználó nincs is tisztában az okoseszköz használatából adódó veszélyekkel, illetve, ha mégis, a saját kényelmi szempontjait előrébb sorolja ezeknél.

Mivel az okoseszközök alkalmazása leginkább a privát szférából terjedt át a szervezeti működésbe, még mindig a legtöbben úgy gondolják, hogy ami az otthoni használatban megfelelő, az jó a szervezet számára is. Nagyon gyakran előfordul, hogy az okoseszközök nem a szervezet, hanem a munkavállaló tulajdonában vannak, és ez a kérdést tovább bonyolítja. Mindezek együtt azt adják, hogy egy „átlagos" felhasználó az okoseszközén azokat a biztonsági intézkedéseket sem alkalmazza, amit egyébként már az otthoni számítógépén is természetesnek tart. Sokak számára egy okostelefon még mindig „csak egy telefon", holott sokszor minden paraméterében fejlettebb informatikai eszközről beszélünk, mint egy néhány éves asztali számítógép, más okoseszközeiről pedig fel sem tételezi, hogy biztonsági vonatkozásai is vannak a használatuknak.

5. Kockázatfelmérés okoseszközökre

5.1. Módszertan kiválasztása

Mielőtt megkezdjük a kockázatelemzést a szervezetnél, a legfontosabb, hogy olyan módszert válasszunk, amely mind a céljainknak, mind a lehetőségeinknek megfelel. ez egyrészt vonatkozik az egyes kockázati tényezők azonosítására, másrészt a kockázatok mértékének megítélésére. A cél, a legtöbb esetben egy jól kontrollált kockázati modell felállítása, és a kockázatok folyamatos – vagy legalább rendszeres – értékelése kell, hogy legyen. Ebből adódóan a módszertant hosszabb távra alakítjuk ki. A gyakran változó feltételek vagy értelmezések nem teszik lehetővé, hogy idősoron értékeljük a kockázati szintek alakulását, illetve, ha változtatunk a módszereken, vagy nem lesznek összevethetők az eredmények, vagy minden egyes alkalommal újra el kell(ene) végezzük a teljes kockázatkezelést, ami nyilván nem járható út.

Mivel az okoseszközök piacán napjainkban folyamatos és rendkívül gyors a fejlődés (illetve a változás), ezért számolni kell azzal, hogy a felmért kockázatok gyakran egészülnek ki újabbakkal, illetve a korábbi értékeléseinket felül kell vizsgálni, például egy technológia kifutása miatt, vagy azért mert az adott eszköz – mondjuk új alkalmazások révén – többletfunkcióra tesz szert. Mindez azt jelenti, hogy az alkalmazott módszertan olyan alapokra kell épüljön, amely alkalmas a változások befogadására, követésére is.

Gyakran alkalmaznak a kockázatok felméréséhez olyan listákat, amely valamilyen szempontrendszer alapján segít azonosítani a fenyegetéseket, vagy azok forrását. Az ilyen ellenőrzőlisták alkalmazása kifejezetten előnyös, hiszen sok energiát spórolhatunk vele a saját munkánk során, mert nem magunknak kell kitalálni a helyzetünkben releváns fenyegetéseket, illetve segíti a szisztematikus gondolkodást. További lényeges előny, hogy a – megfelelő forrásból választott – listák egy szakmai jó gyakorlatot tükröznek, amivel biztosítható, hogy a tényleg reális fenyegetések kerüljenek elemzésre, és az aktuális technikai szinten értelmezhető minden fenyegetés felmérése megtörténjen. Ilyen listára mutatunk példát a *Fenyegetési források* fejezetben.

Nem szabad azonban elfeledkezni arról, hogy egy ilyen lista csak egy adott időszakban felismert fenyegetéseket, kockázati tényezőket tartalmazzák, ebből következően időről időre szükséges ellenőrizni, hogy nem jelentek-e meg újabb fenyegetések, amelyeket például a frissebb listák már tartalmaznak.

Az ilyen evidencián alapuló felmérést akkor célszerű alkalmazni, ha viszonylag szűk a rendelkezésre álló erőforrás. Bár a listák megfelelő értelmezése olykor igényel érdemi szakmai tudást, a legtöbb esetben átlagos ismertekkel rendelkezők is sikerrel használhatják. Természetesen ebben az esetben az átlagos ismeret alatt nem a felhasználói ismereteket, hanem a biztonsági, illetve informatikai ismereteket kell érteni.

Röviden összefoglalva, ha kevés idő alatt, néhány munkatárs bevonásával kell elvégezni a kockázatok azonosítását, akkor célszerű egy – kellő alapossággal kiválasztott – listát segítségül hívni. Mindez persze feltételezi, hogy a kockázatkezelés részévé tesszük a listák rendszeres időközönkénti felülvizsgálatát, és a korábbi eredmények szükség szerinti átvizsgálását.

5.2. A vagyonelemek leltára

Ahhoz, hogy megfelelő képet alkothassunk egy szervezetet fenyegető kockázatokról, első körben azt kell tisztáznunk, hogy mi is károsodhat, illetve milyen elemek léteznek a rendszerben, amelyek egy támadással elérhetők. Fontos megjegyezni, hogy a támadást jelen esetben nem csak a szándékos tevékenységekre értjük, hanem minden olyan eseményre, melyekkel az információ biztonsága sérülhet, legyen szó akár az információ sértetlenségéről, bizalmasságáról, vagy rendelkezésre állásáról.

Első lépésként tehát fel kell mérnünk a szervezet információs vagyonát. Tesszük mindezt azért, hogy tudjuk, hogy mit szeretnénk megvédeni, és azért, hogy megismerjünk minden olyan elemet, mely egy incidens bekövetkezésében szerepet játszhat. Bár elsőre furcsának tűnhet, de gyakran előfordul, hogy egy szervezet nem ismeri pontosan azon információk körét, melyet ténylegesen meg kell védjen. Amikor személyes adatokról, vagy minősített adatokról beszélünk, mindenkinek egyértelmű, hogy ezek védelem kiemelt jelentőségű, és külön jogszabály szolgál az ezek védelmével kapcsolatos elvárások leírására. Amikor azonban egy szervezet működéséhez tartozó adatokról beszélünk, gyakran nem ennyire egyértelmű a kép. Vajon foglalkoznunk kell-e egy véleményezésre megküldött anyag, vagy éppen az adott vélemény munkaverziójának biztonságával. Szükséges-e egy vezetői értekezlet jegyzőkönyvének útját követni? És mi a helyzet azokkal a jegyzetekkel, elyet az egyes résztvevők a „saját jegyzetfüzetükbe" írtak fel.

Egy jól felmért vagyonleltár azon túl tehát, hogy segíti az ismert védendő információk védelmi intézkedéseinek a bevezetésében, adott esetben jelentős mennyiségben képes feltárni „újabb" védendő információkat is.

A vagyonelemek felmérésére alapvetően három utat választhatunk. Mindegyik megoldásnak van előnye és hátránya, és a megfelelő vagyonleltár elkészítéséhez mindegyiket célszerű alkalmazni, azonban nem mindegy, hogy melyik lesz a fő irány, és melyek a kiegészítő elemek.

Az első felmérési módszertan a leltár szóból kiindulva az eszköznyilvántartások oldaláról közelít. Ennek komoly előnye, hogy egy (elméletileg) biztos adatbázisra épít, hiszen a szervezet minden eszköze, így az információfeldolgozásban, -tárolásban, -továbbításban résztvevő eszközök is. Ebből adódóan ez a gondolat nem hagyható ki egy alapos vagyonleltár elkészítéséből. Azt azonban fontos szem előtt tartani, hogy az eszközök – amelyek egy ilyen leltár jellegű nyilvántartásban szerepelnek – nagyon sok dolgot biztosan nem tartalmaznak. Például nem tartalmazzák azokat az információkat, melyeket tárolnak, közvetítenek stb. az eszközök. Sőt, adott esetben maga ez a leltár is lehet védendő információ. Vagyis az leltár alapú megközelítés önmagában nem adhat elegendő adatot egy valós információs vagyonelem felméréshez.

Érdemes kitérni a nyilvántartásokon alapló megközelítés kapcsán arra, hogy egyes szervezetek rendelkeznek külön szoftvernyilvántartással. Amely a szervezet tulajdonában – illetve adott esetben használatában – lévő szoftvertermékeket tartalmazzák. Bár ezzel kiegészítve már javul a helyzet, önmagában ez a „többlet" is kevés ahhoz, hogy egy kellő alaposságú információs vagyonleltárat tudjunk elkészíteni.

Még egy vetület, ami miatt nem tanácsos ez a megközelítés. Ez pedig nem más, mint az, hogy egy szervezet által használt eszközök bizonyos része, nem feltétlenül az ő tulajdonában van. Ez különösen igaz az informatikai eszközök esetén. Gyakori, hogy egy külső szolgáltató eszközeit használják a szervezet működésének biztosítására, pl. hálózati eszközök szintjén, de az is elfogadott gyakorlat, hogy még a munkaállomást is jogilag más szervezet biztosítja. Ebben az esetben végképp könnyen elbukik a kísérlet, hogy a vagyonelemeinket teljeskörűen fel tudjuk mérni.

Az okoseszközök szempontjából nézve azért kell különösen óvatosnak lenni a leltár alapú megközelítéssel, mert igen gyakran ezek az eszközök nincsenek is a szervezet tulajdonában – hiszen a munkavállalok zsebében, kezén, stb találhatók, és az ő tulajdonukat képezik. Így nem is szerepelnek egy leltárban. Ugyanakkor a szervezet információ könnyedén elérhetők rajtuk, így az eszköz hibás működése, vagy illetéktelen hozzáférése lényeges a szervezet információbiztonsága szempontjából. Szükséges tehát, hogy az eszköznyilvántartásokból – ha vannak – az okoseszközökre vonatkozó tételeket kiemeljük, de ez az irány önmagában semmiképpen nem ad elégséges forrást az információs vagyonelemleltárhoz.

A vagyonelemek felmérésének egy másik megközelítése, amikor a szervezetben megjelenő információkat veszik a leltár alapjául, és bemenő, illetve kijövő információk (vissza)követésével igyekeznek feltárni a szervezet információs vagyonát. Ez a megközelítés, kellő alapossággal alkalmazva igen hatékony és eredményes tud lenni, hiszen pont a felmérni kívánt elemeket követi. A legtöbb helyen, ahol a szervezet működése állandó keretek között zajlik, és kevéssé kitett külső hatásoknak, ezzel a megközelítéssel jó eredményre juthatunk. Amire ennél a szemléletnél külön figyelmet kell szánni, az egyrészt az információt feldolgozó/tároló/továbbító eszközök felmérése, illetve az, hogy ne csak azokat a lépéseket kövessük az információ áramlásában, amely a szándék szerint történik, hanem az „információs hulladékokat” is mérjük fel. Azaz vegyük figyelembe, hogy addig, míg mondjuk egy határozat kiadmányozásra kerül, több munkaváltozatban is elkészülhet, lehet, hogy több munkatárs végez vele tevékenységet, esetleg különböző állapotaiban ki is nyomtatják, és az élete nem ér véget azzal, hogy az ügyintéző lezárta, hiszen irattárba kerülhet, postázhatják, elektronikusan közzé is tehetik stb.

Az információáramlás követésével a vagyonleltár akkor alkotható meg kellő alapossággal, ha közben a technikai részletek is feldolgozásra kerülnek. Értve ezalatt azokat a berendezéseket, techológiákat, melyek az információ környezetét adják.

Okoseszközök esetében, ha jól tudjuk követni az információáramlást, akkor hamar eljutunk az eszközeinkhez, így a módszer – a fent jelzett kitétellel – működőképesen alkalmazható. Fontos megjegyezni, hogy egy részletes felmérés során az okoseszközök minden környezeti/technikai paraméterét célszerű rögzíteni, hiszen a már előzőekben említett változékonyság és sokrétűség miatt ezek külön-külön kockázati tényezőt jelenthetnek. Az egyszerűsítés érdekében persze dönthetünk úgy, hogy kihagyjuk a részletezést, de ebben az esetben a kockázatok értékelésénél úgy kell eljárnunk, mintha a releváns kockázatok mindegyike megjelenhetne a rendszerünkben. Ez azt jelenti, hogy ha nem mérjük fel például, hogy az okoseszköz milyen operációs rendszert futtat, akkor az összes operációs rendszer összes sérülékenységével számolnunk kell a kockázatelemzés során.

A harmadik megoldás, ahogyan a vagyonelemeket összesíthetjük, ha a szervezet folyamatait követjük, azaz azt, ahogy a munkájukat végzik a munkatársaink. Ezekhez a folyamatokhoz jól kapcsolhatók maguk az információk, melyek alapján dolgoznak, vagy amelyek létrejönnek a tevékenységek során. Az ilyen megközelítés esetén jellemzően könnyű megtalálni mindazokat az eszközöket melyek a munkában – és így az információfeldolgozásban – részt vesznek. Ha nem ragadunk le csak a fő folyamatok felmérésénél, hanem kiterjesztjük a vizsgálódásunkat minden tevékenységre a szervezetnél, akkor tényleg átfogó és közel teljes képet kaphatunk az információs vagyonelemekről, hiszen ilyenkor akár a karbantartási, vagy informatikai folyamatok felmérésével elérjük, hogy azok a tevékenységek – és a hozzájuk kapcsolt elemek is felmérésre kerüljenek, melyek a másik két módszer esetén csak kis valószínűséggel kerültek volna látókörünkbe. Ilyen módon az okoseszközök is könnyebben kerülnek a látókörünkbe, hiszen akár az informatikai folyamatos során, akár egy vezető folyamatait felmérve hamar szembe találhatjuk magunkat azzal az esettel, amikor egy ilyen eszköz beállítását, végezték, vagy amikor ilyen eszközről érkező információk jelennek meg egy tevékenységben.

5.3. Rendszerek elemei

Kérdésként merülhet fel, hogy mi is tartozhat egy információs vagyonleltár elemei közé. Erre a különböző szakirodalmakban sokféle felsorolást találhatunk. Vannak, amelyek megpróbálják egészen leegyszerűsíteni a felmérést, és vannak, melyek hosszú listákat közölnek. Az egyszerűség kedvéért a következőkben felsoroljuk azokat a kategóriákat, amelyre érdemes gondolni, mint az információs rendszerek elemei, illetve, hogy az okoseszközök vonatkozásában mire érdemes külön figyelni

5.3.1. Környezeti infrastruktúra

Sok esteben nem is gondolnánk, hogy mennyi kockázatot hordoz magában az a környezet, amelyben az információ, vagy hordozója megjelenik, vagy éppen tárolásra kerül. Gondoljunk bele, hogy egy monitor és az ablak viszonya hogyan akadályozhatja meg, hogy a munkavégző lássa, amit csinál, illetve, hogy illetéktelenek könnyedén kileshessék a megjelenített információt. De ugyanígy igaz ez a szóbeli közlések esetén a „fal vastagságára", vagy az irattár esetleg a szerverszoba falában futó vízvezetékre, amelynek meghibásodása komoly következményekkel járhat. Az okoseszközök esetében a legtöbb problémát pont az jelentheti, hogy ezek a paraméterek nem határozhatók meg egyértelműen, azaz nincs egy jól körül határolható környezeti infrastruktúra.

5.3.2. Hardver

Az információs rendszerek (talán) legegyértelműbb eleme, mely magában foglal minden olyan eszközt, vagy részelemet, mely az információ feldolgozásában, továbbításában, tárolásában részt vesz. Az okos eszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, melyek ideiglenesen, vagy állandó módon csatlakoztathatok az eszközhöz.

5.3.3. Szoftver

Az információs rendszerek másik egyértelmű eleme, amely alatt a legszűkebb értelemben az információtechnológiai berendezéseket működtető programokat értjük. A jelen technikai szinten hétköznapi körülmények között a legtöbb esetben az azonos hardverkiépítésű eszközök a szoftvereknek köszönhetően a legkülönbözőbb feladatokra válnak alkalmassá, kijelenthető, hogy a szoftverek sokfélesége biztosítja eszközeink feladatra való alkalmasságát. Az okoseszközök esetén szintén ilyen módon működnek. Azaz a különféle szoftverek a legkülönbözőbb tulajdonságokat biztosítanak nekik. Ebből adódóan fontos, hogy kellő alapossággal mérjük fel mind a szoftvereket, mind azok verzióit.

5.3.4. Kommunikáció, hálózatok

Az információ továbbítása nélkül elképzelhetetlen egy megfelelően működő szervezet. Minden olyan eleme, amely ebben a folyamatban részt vesz része az információs rendszerünknek. Egy információ kompromittálódása könnyen megtörténhet ott, ahol az két egység között „szabadon" mozog. Azonban fontos megjegyezni, hogy itt nem kizárólag az informatikai hálózatokra kell gondolni, hiszen ugyanígy ide tartozik egy szóbeli kommunikáció továbbítása is. Okoseszközök esetén definíció szerint az egyik legjellemzőbb tulajdonság az állandó kommunikáció, ezért itt erre külön is célszerű kitérni. Milyen módon, milyen csatornákon, milyen megoldásokkal kommunikál az eszköz.

5.3.5. Adathordozók

Sok esetben elég nehéz elválasztani az adathordozókat a hardverelemektől. Ami a fő különbséget jelenti, az az, hogy ezeket az elemeket arra tervezték, hogy hosszabb-rövidebb ideig megőrizzék, tárolják az információt. Ilyen módon az adatok jelentősen koncentrálódnak az információs rendszer ezen elemein. A koncentrálódás pedig érzékennyé teheti ezeket az információ sértetlensége és bizalmasága szempontjából egyarán. Az okoseszközök többnyire beépítetten és csatlakoztatható módon is tartalmaznak adathordozókat, amelyeknek a kontrolja egyértelmű elvárás az információbiztonság szemszögéből.

5.3.6. Dokumentumok, dokumentáció

Az adattárolás és megőrzés hagyományos formája a (papíralapú) dokumentumok létrehozatala. Ha ezt a rendszerelemet ilyenformán értelmezzük, akkor az információbiztonsági vonatkozások – elvárás szintjén – nagyban megegyeznek az adathordozókéval. Ha azonban ezt a rendszerelemet úgy értjük, mint a dokumentumokban megjelenő információt, akkor valójában magával a védelem tárgyával állunk szemben, azaz ezeket kell megvédenünk. Az okoseszközök kapcsán általában nem igazán jelenik meg a papíralapú dokumentumok kérdésköre, azonban a tárolt, feldolgozott adatok annál inkább. Ilyen módon fontos felmérnünk, hogy mihez férhet hozzá az eszköz, illetve mit lehet rajta tárolni.

5.3.7. Személyek

Az információs rendszer – jellemzően – leginkább sebezhető része az azt használó, működtető ember. Az ember az, aki a szabályokat betartja vagy sem, és ő kezeli és értékeli igazán az információt. Az információs vagyonleltár szempontjából ritka, hogy valaki külön felkerül, de funkciók, feladatok, illetve azok elvégzése már része lehet a leltárnak. Ami pedig elvárás egy vagyonleltár készítésénél, hogy az egyes vagyonelemekhez legyen hozzárendelve annak tulajdonosa, illetve felelőse. Amennyiben olyan okoseszközről van szó, amelyhez közvetlen felhasználó rendelhető, az mindenképpen itt is meg kell jelenjen.

5.4. Fenyegetési források

Az információbiztonsági kockázatmenedzsment logikája szerint a fenyegetések mindig valamilyen vagyonelemen keresztül lehetnek képesek hatni a szervezetre, illetve az információs rendszerre. Ezt a logikát követve a vagyonelemleltár felvételét követően képesekké válunk a fenyegetési források, illetve maguknak a fenyegetéseknek a felmérésére. A korábban leírtaknak megfelelően célszerű lehet olyan megoldást keresnünk, amely a fenyegetéseket egy lista, vagy legalábbis egységes logika alapján méri fel. Ezt a munkát az okos eszközök vonatkozásában a következőkben bemutatandó logikával, illetve fenyegetési listával kívánja segíteni jegyzetünk.

Ahogy azt az első fejezetekben láthattuk, az okos eszközök sokféle kockázatot hordozhatnak magukban. Ezek egyik legjelentősebb forrása, hogy a napjainkban elterjedt okoseszközök egyszerre szolgálnak magán és szervezeti célokat, vagyis sokszor nem elválasztható a két működés rajtuk. Nézzük, milyen fenyegetési forrásokat is rejt ez magában.

Elsőként essék szó *az eszközön tárolt adatokra vonatkozó fenyegetések*ről. Egy okoseszközön a legkülönbözőbb adatok kerülnek tárolásra. Ha a szervezet szempontjából nézzük, akkor kapcsolati adatok (nevek, e-mail-címek, telefonszámok, stb) fellelhetők az eszközön, ami azt jelenti, hogy ezek az adatok elveszhetnek például egy hibás működés, vagy téves művelet eredményeként, de akár egy

eszközcsere során is. Az eszközön tárolt adatok könnyen kerülhetnek illetéktelen kezekbe az eszköz eltulajdonítása, elvesztése során. A kockázat akkor is fennál, ha csak átmenetileg kerül ki a tulajdonos/használó kontrollja alól az eszköz. Mindezen fenyegetések, illetve forrásaik különösen jelentőssé válhatnak, ha az eszköz a kontaktokon kívül – mint ahogy az jellemző – egyéb állományokat is tartalmaz, mint például levelezés, letöltött adatok, vagy hozzáférési adatok (pl. jelszavak, felhasználónevek) Egy alapos kockázatértékelés során mindenképpen ki kell térni a tárol állományok, illetve az eszközön meglévő szenzitív információk kérdéskörére.

Szintén a tárolt adatok problémájához tartozik annak a kérdése, hogy miként oldható meg egy ilyen okoseszközön az egyéb rendszereinkben teljesen természetes alapintézkedések, mint a *vírusvédelem*, vagy a *mentések, visszaállítások* technikai megvalósítása, netán kikényszerítése. Ezek hiánya, illetve az ilyen okokra visszavezethető incidensek részét kell képezzék a fenyegetések, fenyegetési források azonosításának.

A legtöbb szervezet a saját információs eszközeire alkalmaz olyan *szabályozási intézkedések*et, melyek a használatukból eredő kockázatok csökkentésére szolgál. Az okoseszközök esetében – és különösen a magántulajdonban lévő eszközöknél – azonban az ilyen szabályozások érvényesítése, vagy kikényszerítése sokkal nehezebben megvalósítható. Ilyenkor tehát maga a szabályozás megvalósulásának hiánya teremt sebezhetőséget az összes olyan fenyegetéssel szemben, melyek kivédésére azokat megalkották.

Az okoseszközök világában a változások gyakorisága a „hagyományos" informatikai rendszerekéhez képest jóval nagyobb. Ennek ellenére ezek követése, menedzselése, és az egyes változásokból eredő kockázatok azonosítása szinte megoldatlan feladat. Sem az egyes *változások tesztelése*, sem a rendszerekre, alkalmazásokra megjelenő *frissítések ellenőrzése* nem jellemző ebben a környezetben, ami jelentős fenyegetést okozhat.

Mivel az *alkalmazások* felhasználása az okoseszközök lényegi tulajdonságai közé tartozik, külön figyelmet kell(ene) szentelni ezen alkalmazások kérdéseinek. A legtöbb alkalmazás igényel különböző *jogosultságok*at, melyek kockázatokat rejthetnek magukban. Egy hibás működés akár a *stabilitás* rovására is mehet, amely szintén fenyegeti a szervezet információbiztonságát, ha mindez olyan eszközön történik, amely része információs rendszerének.

Az okoseszközök már taglalt sajátossága, hogy a legtöbb esetben szükséges valamilyen *felhő alapú szolgáltatás igénybevétele* ahhoz, hogy funkcionalitásukat teljesmértékben ki tudjuk használni. Az egyes felhőszolgáltatásokhoz való kapcsolódás is többféle fenyegetésnek ad teret.

Kiemelt kérdés a *felhőben tárolt adatok* köre. A szervezet, ha meg kívánja védeni az információit, szükséges, hogy folyamatosan kontroll alatt tudja tartani azokat. Egy felhőszolgáltatáshoz kapcsolódó okoseszköz kontrolja azonban komoly kihívásokat jelent. Gyakran ismeretlen mennyiségű, minőségű adatok kerülnek fel a felhőbe, melyek sorsa – ilyen formában – a szervezet által nehezen ellenőrizhető, amely sokféle fenyegetést hordozhat magában.

Manapság egyre gyakoribb, hogy egy eszköz funkcionalitásának teljes kihasználáshoz regisztrálni szükséges azt a gyártónál, vagy valamilyen szolgáltatónál. Ez a *regisztráció* az okoseszközök kapcsán különösen igaz. A regisztráció során megadott adatok, illetve a szolgáltató/gyártó által a regisztrációhoz kapcsolt szolgáltatások azonban problémásak lehetnek egy szervezet szemszögéből nézve, ilyen módon fenyegetést jelenthetnek.

Egyes okoseszközök tulajdonságai között fellehetjük a *helymeghatározás* képességét is. Ez – megfelelő alkalmazás és felügyelet esetén – akár kockázatok csökkentésére is igénybe vehető, de ha nem kezeljük ezt a lehetőséget, fenyegetést is jelenthet, hiszen az eszköz használójának elhelyezkedéséről, vagy hosszabb távon szokásairól adhat információt, amely egyes szervezetek esetében önagában is érzékeny információt jelenthet.

Az *okoseszközök közötti kommunikáció*, mint azt láttuk korábban, hozzátartozik alapvető funkciójukhoz. Ennek a kommunikációnak – mint minden más kommunikációnak – azonban ellenőrizetlensége fenyegetést jelent. Mivel azonban az ilyen jellegű felügyelet gyakran nehezen valósítható meg, ezzel a területtel feltétlenül célszerű foglalkozni egy fenyegetéselemzés során.

*Távolról történő elérés*t a legtöbb okoseszköz biztosít. Ennek – éppúgy, mint a helymeghatározásnak – lehetnek kockázatcsökkentő hatásai, azonban pontosan ugyanúgy fenyegetést is jelenthet, ha nem tartjuk felügyelet alatt.

Az okoseszközök méretüknél, funkciójuknál fogva sokkal inkább kitettek olyan „támadásoknak", melyek a készülékekhez való fizikai hozzáférésre vezethetők vissza. Ezeket a fenyegetéseket részben már korábban felvetettük, úgy, mint például az eszközön tárolt adatokhoz való hozzáférés. Érdemes azonban további aspektusokból megnézni a mobilitás kérdését.

Egy könnyen mozgatható *eszköz*, amely funkcióinak ellátása érdekében folyamatos kommunikációt igényel, *könnyen csatlakozhat* – „magától", vagy a használója szándékai szerint – *olyan hálózathoz, amely nem kellően biztonságos*. Az ilyen csatlakozások mindenképpen fenyegetéseket rejtenek magukban az információbiztonság szempontjából.

Az információ rendelkezésre állása szempontjából egy *okoseszköz megrongálódása, elvesztése* vagy *eltulajdonítása* akkor is fenyegetés, ha az egyéb kockázatokat (pl. jogosulatlan hozzáférés) elfogadható szintre csökkentettük. Ezzel a fenyegetéssel tehát ilyen értelemben is szükséges foglalkoznunk.

Összefoglalva az okoseszközök fenyegetéseinek felmérése során az eszközök funkciójából, használatából adódó fenyegetések esetén az alábbiakra mindenképpen gondoljunk:

1. Az eszközök magán és hivatali használatának együttese
   - Az eszközön tárolt adatok (kontaktok, levelezés, állományok)
   - Mentés, visszaállítás, vírusvédelem kérdései
   - A szervezeti szabályozások alkalmazása
   - Változások kezelése (tesztelés, frissítés)
   - Appok, alkalmazások kérdése (jogosultságok, appon belüli adatok, stabilitás)

2. A felhőszolgáltatások
   - Felhőben tárolt adatok
   - „Kötelező regisztráció"
   - Helymeghatározás
   - Eszközök közötti kommunikáció
   - Távoli elérés

3. Eszközök fizikai hozzáférés
   - Eszközön tárolt adatok
   - Nem megbízható hálózathoz csatlakozás
   - Megrongálódás, eltulajdonítás

5.5. Speciális mobil fenyegetések

A következő táblázat összefoglal néhány jellemző, a mobileszközök által megjelenített lehetséges fenyegetési forrást, melyet a kockázatok azonosítása során célszerű áttekinteni, hogy az adott szervezet esetében relevánsak-e.

Fenyegetések		
Fenyegetési kategória	**Fenyegetés**	**Fenyegetés leírása**
Eszköz alapú	Illetéktelen hozzáférés üzleti adatokhoz	Illetéktelenek – megfelelő azonosítás hiányában – megnyithatják a telefont, és így hozzáférhetnek a telefonon tárolt vállalati adatokhoz, alkalmazásokhoz, vagy akár a vállalati hálózathoz is hozzáférhetnek a telefonon keresztül.
	adatok illetéktelen módosítása vagy törlése	Szoftversérülékenységek, amelyek lehetővé teszik a „jailbreak-et” vagy „rooting-ot” az eszközökön, kompromittálva ezzel az adatokat.
	lopás	Az eszközök könnyű hordozhatósága növeli az ilyen esetek veszélyét.
	elvesztés	Az eszközök könnyű hordozhatósága növeli az ilyen esetek veszélyét.
Hálózat alapú	megbízhatatlan hozzáférési pont	Vezeték nélküli hozzáférési pont („free wifi”), amelyet egy biztonságos hálózaton hoztak létre (hozzáértő munkavállaló vagy rosszindulatú támadó) engedély nélkül.
	wifi „sniffing” eszköz	A nyílt vagy gyenge titkosítású protokollokból a „lehallgató” eszközzel megszerezhetők a felhasználói nevek, jelszavak.
	kifinomult Man-in-the-Middle támadás	
Felhasználó alapú	megosztás vagy szinkronizálás megbízhatatlan felhő alapú alkalmazáson keresztül	Nem engedélyezett (megbízhatatlan) felhő alapú alkalmazások használata adatok megosztására és szinkronizálására.
	megbízhatatlan teljesítmény-javító alkalmazások	Engedély nélküli hatékonyságnövelő (productivity) alkalmazások használata, amelyek vállalati adatok másolatát tartalmazzák.
	„jailbreaking” / „rooting”	„jailbreak” (telefon feltörése szoftveresen – Apple) vagy „rooting” (Linux „root” jog szerzése – Android) a biztonsági kontrollok megkerülése érdekében.
	rosszindulatú alkalmazások / tartalmak	Nem engedélyezett „áruházakból” származó rosszindulatú alkalmazások használata
	üzleti adatok közzététele	Vállalati adatok közzététele rossz szándékkal.

6. Az okoseszközök kockázatainak csökkentése

Az eddig összegyűjtött, az okoseszközök alkalmazásából származó kockázatokat egy szervezetnek szükséges kezelnie, amelyre több elkülönülten, vagy rendszerben alkalmazott módot választhat. A lényeg, hogy minden estben a kockázattal arányos biztonság megteremtése. Ennek érdekében pedig a legfőbb szempont, hogy a kockázatkezelés folyamatába beépüljön az okoseszközökkel kapcsolatos felmérés és folyamatos értékelés. Ennek első lépése, hogy a szervezet felméri a működésében ténylegesen megjelenő eszközöket. A felmérés eredményeként kialakítható olyan szabályozás, mely gondoskodik, hogy csak a tényleg szükséges és célszerű mértékben épüljenek be az ilyen eszközök a napi tevékenységekbe

A nem közvetlenül a szervezeti működéshez tartozó eszközök csatlakozásának, illetve felhasználásának a korlátozásával jelentős kockázatcsökkentés hajtható végre, és elkerülhető a már korábban kifejtett helyzet, hogy a szervezeti és magánjellegű információk, illetve felhasználás keveredik. Mindezen túl a technikai jellegű fenyegetések egy jelentős része is kizárható.

Bár az eddig leírtakból következik, de érdemes külön kiemelni, hogy az okoseszközökön megjelenő adatokat is fel kell venni a szervezet információs vagyonleltárba, ki kell rá terjeszteni az értékelési módszertanokat, be kell vonni az adatosztályozásba, és az információk érzékenységének megfelelő intézkedéseket kell bevezetni rájuk.

MDM rendszerek

A legjellemzőbb okoseszközök – az okostelefonok – már évek óta jelen vannak a szervezetek életében, és okoznak fejtörést az információbiztonsággal foglalkozó szakemberek számára. Éppen ezért a piacon egyre több eszköz, megoldás jelenik meg az okostelefonok technikai oldalról működtetett kontrolljának megvalósítására. Ezeket összefoglaló néven MDM, azaz mobile device management rendszereknek nevezik. A különböző gyártók különböző megoldásokat kínálnak, a szervezet méretének, céljainak, eszközparkjának függvényében. Mivel ezek a megoldások is folyamatosan fejlődnek, változnak, a következőkben csak néhány jellemző gondolatot összegzünk, hogy mire is alkalmasak ezek a rendszerek. Egy szervezet saját megoldásának keresése során mindenképpen célszerű, ha tájékozódik a piacon aktuálisan fellehető megoldásokról, hiszen ezekben jelentős eltérések lehetnek, mind a technikai megoldást mind pedig az árakat illetően.

Az MDM rendszerek általában alkalmasak a mobil eszközök és a rajtuk tárolt információk, alkalmazások, illetve a kommunikációs folyamatok központi, távoli védelmére, flottában történő menedzselésére, amely így nem csak egységesen, de viszonylag könnyen meg is valósítható.

Az MDM fő funkciói között megtalálható az üzembe helyezés, amely alkalmassá teszi a készülék beszerzését követően, annak üzembe helyezésére, cégprofil kialakítására, a device management rendszerhez csatlakoztatására távolról.

Távoli eszközmenedzsment napi szinten képes ellátni az alkalmazás-menedzsment, távsegítség, hibaelhárítás, eszközvédelem, törlés, zárolás, biztonsági előírások betartatása funkciókat. Kezeli az adatbiztonság kérdéseit, úgy mint biztonsági mentések, telepített szoftverek nyilvántartása, készülék-beállítások követhetősége, készüléktartalom – tárolt adatok és beállítások – gyors visszaállítása. Illetve akár készíthetők jelentések az üzemeltetésről, felhasználásról.

Az MDM rendszerek alkalmazása a felhasználók számára is jelenthet előnyöket, így például a munkatársaknak az esetek nagy részében nem kell a vállalat IT helpdeskjét személyesen felkeresniük az eszközeik regisztrációjához, beállításához. Továbbá nem kell időt tölteniük például a készülék karbantartásával.

Az MDM előnyei egy szervezet és az üzemeltetés számára a következők lehetnek:

- Nagyobb hatékonyság a mobilalkalmazások, illetve a naprakész információk rendelkezésre állásával.
- A szervezet mobilkészülékei központilag menedzselhetők.
- A támogatásra fordított idő csökkenthető.
- Hatékonyabb eszköz- és alkalmazásmenedzsment (pl. alkalmazások tömeges implementálása).
- A készülékeken futó alkalmazások kontrollja.
- Gyors problémamegoldás, hibaelhárítás.

7. Irodalomjegyzék

- [1] Peter Mell, Timothy Grance The NIST Definition of Cloud Computing U.S. Department of Commerce September 2011
- [2] ISO 31000:2009 Risk management -- Principles and guidelines
- [3] MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények
- [4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- [5] Zala Mihály: Mobil biztonság. Mobileszközök biztonsági kockázatai konferencia 2014. június 12.
- [6] Előházi János: Mobil eszközök biztonsági problémái. ROBOTHADVISELÉS 7. Tudományos szakmai konferencia a Zrínyi Miklós Nemzetvédelmi Egyetemen 2007. november 27.
- [7] Mobil eszközök védelme http://www.kurt.hu/megoldasaink/mobil-eszkozok-vedelme (2016. szeptember 17.)
- [8] Sipos Krisztina: Mindent az okos készülékekről. (2014. 05. 28.) http://spiritcode.hu/blog/mindent-az-okos-keszulekekrol/
- [9] Christopher Crowley: A titkosításról. OUCH! (2014. augusztus) https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201408_hu.pdf
- [10] James Tarala, Kelli Tarala: A felhő biztonságos használata. OUCH! (2014. szeptember) https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201409_hu.pdf
- [11] James Lyne: A tárgyak internete. OUCH! (2016. május) https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201605_hu.pdf
- [12] http://www.infobex.hu/hirek/mdm!-de-mi-is-ez/hu (2016. 09. 12.)

IV. ORBÓK ÁKOS: AZ OKOSVÁROS KONCEPCIÓJA ÉS AZ „INTERNET OF THINGS JELENTETTE KIHÍVÁSOK

1. Bevezetés

A civilizációk fejlődésének nagy része párhuzamba állítható a városok fejlődésével. Az emberiség történetében az egyik legnagyobb találmány a város, ahol koncentrálódnak az emberi társadalom előnyei és hátrányai is. Ezeken a helyeken fejlődött a kultúra, a tudomány, és az állam is. A modern civilizáció több kihívással szembesült fejlődése során. A jelenlegi keretek között nincs lehetőség ezeket mind sorra venni, ezért ki kell emelnünk azokat a problémaköröket, amelyek valószínűleg leginkább befolyásolhatják a jövőt. A városok többsége folyamatosan különböző problémákkal és kihívásokkal szembesül működése során. A városi túlnépesedés, az éghajlatváltozás, a vízellátás nehézségei, a szennyezés és a hulladékkezelés, mind olyan megoldásra váró kihívások, amelyek jelenleg nem megoldottak. A hagyományos megoldások ezekre a problémákra nem nyújtanak hosszú távú megoldást, vagy csak részben kezelhetőek. *Ezekre a kihívásokra adott válaszokban van egy közös jellemző, a fenntartható fejlődés igénye. Az ipari társadalom által nyújtott megoldások nem tartották szem előtt a fenntarthatóságot, csak a fejlődés és a gyarapodás állt célként a társadalmak előtt. Ennek a szemléletmódnak az eredményei a mai kihívások.* A technológia fejlődése azonban biztosítja a lehetőséget arra, hogy hatékonyabban lehessen a városok működtetését megoldani és a városi polgárok életminőségén javítani. Azonban a technológia nyújtotta lehetőségek sok olyan kérdést is felvetnek, amelyekre jelenleg nem tudunk megnyugtató válaszokat adni.

2. A modern városok kihívásai

2.1. Demográfiai kihívások

A városok egyik legnagyobb kihívása napjainkban a demográfiai változások és a lakosság városokba vándorlása. Míg a XX. század végén csak néhány 10 milliós lakosságú város létezett, jelenleg több város lakosságszáma a 20 milliót is meghaladja. Az Egyesült Nemzetek Szervezete által 2012-ben készített felmérés alapján a föld lakosságának több mint a fele, a fejlett országok lakosságnak 78%-a városokban élt.[190]

A túlnépesedés és a gyors urbanizáció globális jelenség, és a trendek azt mutatják, hogy ez folytatódni fog. Az ENSZ előrejelzése szerint jelentős változás várható a városi lakosság tekintetében a következő 30-35 évben. A városlakók száma 2007 óta már meghaladja a vidéki területeken élőkét, és ez a tendencia oda fog vezetni, hogy a lakosság több mint 70%-a városban fog élni 2050-re. A változások hatását nem lehet figyelmen kívül hagyni. A városok a demográfiai változások mellet más, de azokkal összefüggő kihívásokkal is szembesülnek. A lakásigények száma meghaladja az ingatlanfejlesztés ütemét. Egyes városokban (Tokió, Mexikóváros) az urbanizáció a működőképesség határait feszegeti. A több mint 100 km átmérőjű Mexikóvárosban a közlekedés, vagy a közösségi

[190] UN Department of Economic and Social Affairs Population Division World Population 2012 http://www.un.org/en/development/desa/population/publications/pdf/trends/WPP2012_Wallchart.pdf 2016. 10. 10.

közlekedés hatékony működtetése rendkívül nehezen megoldható. A várostervezők megoldása a túl nagy területű városokra az volt, hogy felfelé kezdtek el terjeszkedni. Ezzel azonban újabb problémákat generáltak. A városi népsűrűség ezeken a területeken rendkívüli mértékben megnőtt. Dhaka, Banglades fővárosa, jelenleg a világ legsűrűbben lakott települése, itt a népsűrűség meghaladja a 44 100 fő/km^2-t.[191] Összehasonlításképpen Magyarország legsűrűbben lakott települése Budapest, népsűrűsége 3246 fő/km^2.[192]

Az urbanizáció a világon nem egyforma mértékű. Számos város van, amelynek lakossága meghaladja a 10 milliót, de még mindig vannak olyan területek, ahol néhány százezres városokból áll egy ország városhálózata. Azokat a városokat, amelyeknek 10 milliót meghaladó a lakosságszáma, megavárosoknak nevezik. A világ urbanizációs trendjeire jellemző, hogy egyes régiókban több megaváros is kialakult.

Az urbanizáció ütemének gyorsulásával és a lakosságszám növekedésével kapcsolatos kihívásokra a városok egy része nem képes felelni. Az új városi polgárok mennyiségéhez és igényeihez a régi struktúrák nem képesek alkalmazkodni. Kialakulhatnak olyan városrészek, ahol a városi szolgáltatások nem, vagy kevésbé hozzáférhetőek a polgárok számára, ilyenek a dél-amerikai nagyvárosok nyomornegyedei, például a Rio de Janeiró-i favelák. Ezekben a városrészekben nem csak a szolgáltatások hiányosak, de az életkörülmények és a közbiztonság is rosszabb, mint bárhol máshol a városban. Részben ezért is népszerűek az okosváros megoldások a dél-amerikai városokban.

2.2. Városi mobilitás

A városok lakosságának és méretének növekedésével egyre fontosabbá vált a mobilitási lehetőségek fenntartása és fejlesztése. A közlekedési lehetőségek minden városban változóak, de mindenhol vannak fizikai korlátai. A városokat nagyrészt nem a mai járműforgalomra tervezték (ha volt tervezés). Léteznek olyan városok, amelyek alkalmazkodni próbáltak a megnövekedett jármű forgalomhoz, de fel kellett ismerjék, hogy az autópályák fejlesztése-bővítése nem feloldja a forgalmi torlódásokat, hanem járműhasználatra ösztönzi a polgárokat, ezzel növelve a forgalmat. De van olyan közlekedési újítás is, amelynek sikerült elérni a tervezési célját. A már említett riói favelák egy része annyira zsúfolt, hogy csak gyalogosan lehetett közlekedni az épületek között. A riói városvezetés egy olyan eszközt építtetett a favela és az egyik kisebb városközpont közé, amellyel akár egy óra gyaloglást is meg lehet spórolni a közlekedőknek. Az érzékeny terület megbolygatása nélkül kellett megoldást találniuk, ezért egy cablecabin rendszert drótkötélpályán mozgó kabinrendszert építettek a házak fölé.[193]

A fizikai dilemmákon kívül a környezetszennyezés jelenti a legnagyobb kihívást. A szennyezés hatására a 2000-es évektől kezdve[194] az elektromos és hibrid meghajtású autók fejlesztése és használata megnövekedett, de még elhanyagolható az arányuk a többi jármű számához viszonyítva.[195] Az alacsony számuk annak köszönhető, hogy magas az áruk és korlátozott a használhatóságuk (300-500km hatótáv, min. 45 perc töltés). Ezek mellett több alternatív megoldás is született (kerékpár, e-roller, carsharing), amellyel csökkenteni lehetne a szennyezés mértékét, de minden lehetőség kompromisszumokat követel a használójától.

[191] http://www.demographia.com/db-worldua.pdf 2016. 10. 10.
[192] https://www.teir.hu/idosoros-elemzo/ 2016. 10. 10.
[193] http://www.bbc.com/news/world-latin-america-30727877 2016. 10. 29.
[194] Worldwide Prius sales top 3-million mark; Prius family sales at 3.4 million url: http://www.greencarcongress.com/2013/07/prius-20130703.html
[195] 1.2 Billion Vehicles On World's Roads Now, 2 Billion By 2035: Report url: http://www.greencarreports.com/news/1093560_1-2-billion-vehicles-on-worlds-roads-now-2-billion-by-2035-report 2016. 10. 29.

2.3. Éghajlatváltozás

A Föld éghajlata többet változott az utóbbi 150 évben, mint az elmúlt 420.000 évben összesen. A föld átlaghőmérséklete még mindig emelkedik, és ennek több következménye is lehet a jövőben.[196] Arról még vita folyik, hogy mi a legnagyobb katalizátora ennek a folyamatnak. Akik az emberi tevékenységet okolják a változásokért, úgy gondolják, hogy a szennyezés legnagyobb részét a városok termelik. Ahogy már említettük, a világ népességének több mint a fele városokban él. Ennek többek között az is a következménye, hogy az emberi tevékenységek, a gyártás, a szállítás, az energia előállítása és felhasználása is itt koncentrálódik, amely az ezzel együtt járó környezetszennyezést is koncentrálttá teszi. Így logikus lépés, hogy a szennyezés csökkentését a városokban kell elkezdeni.

2.4. Energia- és vízellátás

A városok kialakulásának egyik alapvető oka a létszükségletekhez való könnyebb hozzájutás volt. A vízellátottság ma is kulcskérdés a városok működésében. A klímaváltozás azonban több térségben megváltoztatta a felszíni vizek mennyiségét, minőségét, eloszlását. A csapadékmennyiség csökkenése vagy megnövekedése az életfeltételek romlását idézték elő. Jelenleg a Föld népességének 40 százalékának nehézséget jelent a vízhez való hozzáférés.[197] A vízhiányt tehetősebb térségekben a tenger sómentesítésével próbálják orvosolni, de ez egy rendkívül drága eljárás, amely nagyon sok energiát igényel. Az aszály arra kényszeríti a népességet, hogy másik városba, országba költözzenek, ezzel is erősítve a demográfiai trendeket.

Az Egyesült Államokban található Flint a vízellátási probléma és az állami tehetetlenség szimbóluma lett 2014-ben. A város vízellátásának forrását költségcsökkentési okokból az addig használt Huron-tóból áthelyezték a sokkal közelebbi Flint folyóba. Azonban a folyóban olyan anyagok voltak, amelyek a vezetéket megrongálva nehézfémeket és más szennyeződéseket juttattak a vízvezetékekbe. Ez a folyamat az egész várost az élhetetlenség határára sodorta, de a politikai életben is komoly hatással járt, mivel az állam tehetetlenségének látszatát keltette az emberekben, hiszen a probléma okát igen, de a szennyezést még ma sem tudták megszüntetni.[198]

2.5. Környezetszennyezés és hulladékgazdálkodás

Az előző fejezettel szorosan összefügg ez a témakör. Az energiaéhség és a fogyasztás mértéke oda vezetett, hogy minden városban komoly kihívást jelent a hulladékkezelés. A legelterjedtebb módszerek közé tartozik a hulladéklerakó és hulladékégetés, de ezek erősen szennyező eljárások, a lerakókhoz nagy terület is szükséges. Már elterjedt megoldás az újrahasznosítás és a hulladéktermelés minimalizálása, de ezeknek a megoldásoknak az aránya még mindig nem kielégítő. A város fejlődését és működését csak úgy lehet fenntartani, ha a keletkezett hulladékot hatékonyan újra lehet hasznosítani.

---

196 Petit, J. R.; Jouzel, J.; Raynaud, D.; Barkov, N. I.; Barnola, J.-M.; Basile, I.; Bender, M.; Chappellaz, J.; Davis, M.; Delaygue, G.; Delmotte, M.; Kotlyakov, V. M.; Legrand, M.; Lipenkov, V. Y.; Lorius, C.; Ritz, C.; Saltzman, E. (1999-06-03). "Climate and atmospheric history of the past 420,000 years from the Vostok ice core, Antarctica". NATURE 399. 1999 pp. 429–436. url: http://www.nature.com/nature/journal/v399/n6735/abs/399429a0.html 2016. 10. 10.

197 Kik is azok a klímamenekültek? Greenfo.hu url: http://greenfo.hu/hir/2016/07/01/kik-is-azok-a-klimamenekultek 2016. 10. 10.

198 Yanan Wang: In Flint, there's so much lead in children's blood that a state of emergency is declared Washington Post 2015 url: https://www.washingtonpost.com/news/morning-mix/wp/2015/12/15/toxic-water-soaring-lead-levels-in-childrens-blood-create-state-of-emergency-in-flint-mich/ 2016. 10. 10.

Ezek a tendenciák arra ösztönözték a városfejlesztőket és a fenntartókat, hogy lépéseket tegyenek és új fenntartható fejlesztési terveket dolgozzanak ki. Azért volt szükség egy új gondolkodásmódra, mert a hagyományos megoldások nem voltak hatékonyak az új környezetben. A városokat nem lehetett bővíteni csak a fizikai térben, mert az egyes szolgáltatásokat (közlekedés, vízellátás, elektromos hálózat) nem lehet biztosítani a város teljes lakosságnak. Az új megközelítés megkövetelte, az innovatív megoldásokat, amit most egységesen okosvárosnak nevezünk.

3. Az okosváros koncepciója

Ha az okosváros meghatározását keressük, több mint száz definíciót találunk, amiből arra következtethetünk, hogy nincs általánosan elfogadott meghatározása. A definíciók nagy száma arra is utalhat, hogy a városok problémáira megoldást kereső informatikai rendszerek nagy számban és változatosan állnak rendelkezésünkre. A változatosság miatt és a különböző városok különböző feltételei miatt rendkívül sokrétű lehet azoknak a megoldásoknak a száma, amit már okosváros megoldásnak nevezhetnek. Ha megpróbáljuk rendszerezni, melyek azok a problématerületek, amelyekre a leghatékonyabb megoldást az IKT eszközök segítségével kaphatunk, hat kategóriát különböztethetünk meg. Ezzel a rendszerezéssel egyben az okosváros lényegét is megfogalmazhatjuk.

Az ENSZ-EGB meghatározása szerint a következő alapokra lehet létrehozni egy jól működő okosvárost: Az okosváros infrastruktúrája hat fő területen alapszik: az okos emberek, okos mobilitás, az okos élet, okos gazdaság, az okos kormányzás és az okos környezet. Az okos városnak nyitottnak kell lennie, rugalmasnak, biztonságosnak, és fenntarthatónak. Részletesebben a következő feltételeket teljesíti:

- Biztosítja a megfelelő és megfizethető lakhatást;
- biztosítja a biztonságos, megfizethető és fenntartható közlekedési rendszereket;
- segíti a befogadó és fenntartható urbanizációt;
- biztosítja a világ kulturális és természeti örökségének védelmét;
- csökkenti a halálesetek számát és a természeti csapások hatásait;
- csökkenti a környezetre gyakorolt hatást;
- univerzális hozzáférést biztosít a biztonságos és elérhető zöld és nyilvános terekhez;
- támogatja a pozitív gazdasági, társadalmi és környezeti kapcsolatokat a városi és vidéki területeken;
- integrálja az innovatív technológiákat az IKT-n belül, a különböző szektorok között.[199]

Több különböző réteget tudunk megkülönböztetni az okos városban, például: városi réteg, érzékelő réteg, hálózatok réteg, adatelemzés réteg, automatizálás réteg, Big Data réteg. Ezek a rétegek külön-külön és együtt is hatással lehetnek az okos város működésére. Ehhez szorosan kapcsolódik a Kevin Ashton által meghatározott Internet of Things (IoT), „... ahol minden tárgy és berendezés csatlakozik az internetre. Az eszközök által rögzített adatokon keresztül a számítógépek szinte mindent tudhatnak az emberekről."[200]

Az Egyesült Nemzetek Európai Gazdasági Bizottsága meghatározott néhány célt a fenntartható fejlődés elérése érdekében. A céljuk az volt, hogy a városlakók életkörülményeit fenntartható módon javítsák egy átfogó stratégia révén, de nem csak a városlakóra vonatozóan. A szolgáltatások, fejlesztések, valamint a környezet védelme is mindenki érdeke. Ugyanakkor a felelősséget tekintve

[199] The United Nations Economic Commission for Europe, Smart Cities characteristics in UNECE Region. URL: http://www.unece.org/housing-and-land-management/projects/housingsmartcities/smart-cities-characteristics.html 2016. 10. 10.

[200] Kevin Ashton: That 'Internet of Things' Thing. URL: http://www.rfidjournal.com/articles/pdf?4986; https://www.scientificamerican.com/article/the-internet-of-things/ 2016. 10. 10.

a szennyezés mértéke egyenesen arányos a város kiterjedésével, így a megoldás is indítható ebbe az irányba. Az infokommunikációs technológiák lehetővé teszik, hogy a társadalmi hálózatok meghaladják a történelmi korlátokat. Képesek egy időben rugalmasak és alkalmazkodóak lenni egyben, köszönhetően annak, hogy a működésük közben decentralizálja a kepeségeit autonóm komponensekre, miközben továbbra is képes koordinálni mindezt a decentralizált, megosztott tevékenységet, amelynek célja a döntéshozatal. A digitális kommunikációs hálózatok gerincét a hálózati társadalom eredményei, az infrastruktúrát (a nagyteljesítményű energiahálózatokat) az ipari társadalom eredményei adják..."[201]

A Nemzetközi Telekommunikációs Unió (ITU) elemzésének eredménye alapján: „Egy okos, fenntartható város (SSC) egy innovatív város, amely az infokommunikációs technológiák (IKT) és egyéb eszközök felhasználásával az életminőség szintjét emeli, a hatékonyabbá teszi a városi üzemeltetését és a szolgáltatásokat, valamint javítja a versenyképességet. Ezen kívül biztosítja, hogy mindez megfeleljen az igényeinek, a jelenlegi és jövőbeni nemzedékeknek, tekintettel a gazdasági, társadalmi és környezeti szempontokra."[202]

Az okosváros koncepciót nem lehet univerzálisan alkalmazni minden városra, hiszen más körülményekkel, kihívásokkal kell szembenézniük az egyes városoknak. Tehát a koncepció nem egy formula csupán, egy modell, amelynek részeit külön is hasznosítani lehet. A városoknak és lakóiknak a saját igényeikhez kell szabniuk, milyen technológiával válna könnyebbé az életük, és a környezetük. „Az eredmények azt mutatják, hogy az okos város fejlődési mintái erősen függnek a helyi viszonyoktól és tényezőktől. Az okosváros létrehozásához vezető úton több olyan tényező és kihívás van, amelyet figyelembe kell venni: a gazdasági fejlődés, a város strukturális változásai, a digitális ellátottság, a földrajzi elhelyezkedés, a város népsűrűsége és az abból fakadó közlekedési problémák."[203]

Ha nem is határozható meg pontosan, mit is jelent az okos város, azonban sokkal közelebb vihet a megértéséhez a következő definíció: A Smart City, vagy okos város olyan települést takar, mely a rendelkezésre álló technológiai lehetőségeket (elsősorban az infokommunikációs technológiát – IKT) olyan innovatív módon használja fel, amely elősegíti egy jobb, diverzifikáltabb és fenntarthatóbb városi környezet kialakítását. Egy várost akkor nevezhetünk „okosnak", ha az emberi tőkébe, a hagyományos infrastrukturális elemekbe (pl. közlekedés), valamint a modern IKT infrastruktúrába történő befektetései ösztönzik és hajtják a fenntartható gazdasági fejlődést, valamint tovább növelik az életszínvonalat, miközben a természeti erőforrásokkal is ésszerűen gazdálkodik. Az okos város tehát az okos technológiát úgy használja, hogy a város infrastrukturális rendszerei és szolgáltatásai sokkal jobban kapcsolódjanak egymáshoz, okosabbak és hatékonyabbak legyenek.[204]

3.1. Technológiai megoldások az okos városban

Az infokommunikációs technológia a mai társadalomban is meghatározó szerepet tölt be. A mindennapok részét képezik az okos eszközök. Az okosváros koncepció által felállított fejlesztési irányok e technológia segítségével valósulhatnak meg a jövőben. Magyarországon is több városban (Pécs, Veszprém, Győr, Budapest …) alkalmaznak már az okos városhoz köthető technológiákat. Általában

[201] Manuel Castells: The Network Society: from Knowledge to Policy The Johns Hopkins University Press, Center for Transatlantic Research Relations, Washington, DC 2006 p. 4. url: http://www.umass.edu/digitalcenter/research/pdfs/JF_NetworkSociety.pdf

[202] ITU-T Focus Group on Smart Sustainable Cities: Smart sustainable cities: an analysis of definitions 2014. p. 13. url: http://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx

[203] Paolo Neirotti, Alberto De Marco, Anna Corinna Cagliano, Giulio Mangano, Francesco Scorrano: Current trends in Smart City initiatives: Some stylised facts Original Research Article Cities, Volume 38, June 2014, p. 25–36. url: http://www.sciencedirect.com/science/ article/pii/S0264275113001935

[204] Smarter cities for smarter growth IBM Institute for Business Value. url: https://www.zurich.ibm.com/pdf/isl/infoportal/IBV_SC3_report_GBE03348USEN.pdf

ezek a városok már „okosnak” nevezik magukat, de ez nem jelenti, hogy a koncepcióban szereplő összes technológiai fejlesztést alkalmazták. A Lechner Tudásközpont kutatásai alapján Magyarországon a következő területeken érdemes okosváros technológiák alkalmazásával fejlesztésbe kezdeni:

a) Okos mobilitás (közlekedés),
b) Okos környezet (környezetvédelem, környezeti fenntarthatóság, levegővédelem, zöld épületek),
c) Okos emberek (tudásmenedzsment, oktatás, képzés, továbbképzés),
d) Okos életkörülmények, életminőség (szociális háló, kultúra, településfejlesztés),
e) Okos kormányzás (információbiztoság, adatvédelem, közbeszerzés, e-aláírás),
f) Okos, fenntartható gazdaság (kereskedelem, szakképzés, kutatás-fejlesztés- innováció[205]

A lista alapján, de más csoportosításokat figyelembe véve olyan területeket emeltünk és fejtünk ki a következő alfejezetekben (mobilitás, környezet kormányzás), amelyek összefoglalnak három nagy problémakört.

Mobilitás

A városi közlekedés, amely nélkülözhetetlen a városok működéséhez több megoldandó problémával szembesült a népesség növekedés miatt. A városok fizikai növekedésével, a közlekedés működőképességének határán egyensúlyozva új szervezési megoldásokra van szüksége. Az egyik lehetséges megoldást a „hálózati társadalom” eszközeiben és megoldásaiban találták meg. Az „Okosváros” koncepció az infókommunikációs technológia segítségével a városi élet egészét új alapokra helyezi. A koncepció egyik fontos területe a közlekedés-szervezés újragondolása. Több, már létező és néhány még megalkotásra váró technológia segítségével mind a közösségi, mind az egyéni városi közlekedést hatékonyabbá teszi. A működési hatékonyságot olyan, már létező technológiák segítik, mint a valós idejű tájékoztató táblák, a forgalomfigyelő rendszerek, az ezzel kapcsolatban álló adaptív jelzőlámpák, a kötött pályás közlekedési hálózat fejlesztése távvezérelt és autonóm járművekkel, amelyek járatok számának növekedését teszik lehetővé és csökkentik a balesetek esélyét. A tervezett technológiai újítások közül a közúti közlekedés adja legnagyobb mozgásteret, mivel a problémák száma is itt a legmagasabb. A megoldások között találhatunk irreális és realistább megközelítéseket is, az utóbbi csoportba tartoznak az okos utak rendszere, a parkolóhely foglaltságát figyelő rendszerek vagy az autonóm közlekedési járművek, amelyek nem csak önmagukban adnak megoldást valamilyen problémára, azonban rendszerbe szervezve többek az egyes elemek összegénél.

A mobilitást érintő innovációk közül kiemelkedik az autonóm közlekedési eszközök fejlesztése. A járművek többsége már ma is rendelkezik valamilyen autonóm működésre képes felszereléssel. Ezek a felszerelések általában csak egy feladatot látnak el, amely lehet aktív biztonsági feladat (menetstabilizátor, blokkolásgátló, követési-távolság tartó elektronika) vagy kényelmi berendezés (sávtartó elektronika, parkolás segítő rendszer, sebesség-tartó automatika). Ezeknek a rendszereknek fontos közös tulajdonságuk, hogy kikapcsolhatóak és csak kiegészítik az emberi irányítást, nem veszik át teljesen a jármű irányítását. Egyes mai járműveket, amelyek nagy számban tartalmaznak és használnak ilyen eszközöket, már fél-autonómnak nevezhetünk. Ezt fejleszti tovább és haladja meg az autonóm jármű, amely egy rendszerbe szervezi a már említett, ma is alkalmazott eszközöket és kiegészíti olyan szenzorokkal, amelyek képessé teszik a fedélzeti számítógépet a jármű irányítására, a vezető beavatkozása nélkül is.

Az autonóm járművek széleskörű katonai felhasználásra is lehetőséget adnak. A már említett Google eszközével párhuzamosan a katonai alkalmazást fejlesztő Oshkosh is létrehozott egy saját járművet. A TerraMax pilóta nélküli szárazföldi jármű technológia integrálja a nagy teljesítményű

[205] Nagy András, Sain Mátyás, Sárdi Anna, Vaszócsik Villa: Településértékelés és monitoring Lechner Tudásközpont url:http://lechnerkozpont.hu/doc/okos-varos/telepulesertekeles-es-monitornig-modszertani-javaslat.pdf 2016. 10. 10.

számítógépeket, érzékelő rendszereket, a mesterséges intelligenciát és a távvezérlő technológiát valamint a teljesen autonóm irányítást. A technológia működhet attól függően, hogy a stratégiai célok mit kívánnak meg, képes működtetni minden funkcióját emberrel, táv vezérelve, vezető-követő és a teljes autonóm vezérléssel is. *Működése abban különbözik a civil autonóm járműtől, hogy a katonai verzióban lehetőség van a távvezérlésre. A katonai járművek döntően nem épített utakon fogják majd igénybe venni a felhasználás során, így amikor kiválasztja az optimális útvonalat, nagyobb felbontású képre van szüksége a környezetéről, ezért jobban támaszkodik a lézeres szenzor és a kamera adataira, mint a geo-információs adatokra.*

Környezet

A városok szennyező tevékenysége mára nyilvánvalóvá vált mindenki számára. A szennyező tevékenység elsősorban a városi polgárok életét nehezíti meg. Az okosváros koncepció fő célkitűzése az „élhető" város létrehozása, amelynek fontos része az emberek egészsége és a fenntarthatóság.

Az infókommunikációs technológiát ma is használják a közműhálózatok optimalizálására. A tervezett okos mérőeszközök, amelyek valós időben közvetítik a központi rendszer felé a villamos energia, víz és gázfogyasztást. Ezzel együtt a fogyasztási tendenciákat is megfigyel, például, ha ismertek az áramfogyasztási igények, az erőművek teljesítményét is optimalizálni lehet. Ugyanezen az elven lehet minden szolgáltatást a fogyasztókhoz igazítani. Ma is léteznek statisztikák, amelyek alapján meg lehet becsülni, milyen teljesítmény szükséges az igények kiszolgálásához. Ebben az esetben a becslések pontatlansága felesleges energiatermelést indukál. Az okos mérőeszközök funkcióit ki lehet bővíteni elemző funkcióval is, ezzel a vízminőséget, illetve a gáz minőségét is ellenőrizni lehet, amivel biztonságosabbá tehetőek ezek az infrastruktúrák.

Azokon a területeken, ahol nem érhető el tiszta ivóvíz (Afrika nagyrésze), szükség van víztisztító eszközökre. A vízellátás megoldásai közé tartozik az olyan víztisztító berendezés is, amely szabadon telepíthető, nem szükséges hozzá vezetékes víz. A kifejezetten fejlődő országok vízellátás szempontjából rossz körülményekkel küzdő területeire tervezett eszköz, az ihatatlan, szennyezett vagy fertőzött vizet is képes ihatóvá tenni, viszonylag gyorsan. Nem igényel hosszas telepítést, hiszen egy komplett szerkezet, de a használata könnyen elsajátítható.

Kormányzás

Az állampolgárok részvétele az állam működési folyamatában mindig a legfontosabb kérdések közé tartozott a politika-tudományban. Ha egy állam képes a polgárait úgy bevonni a működésébe, hogy az állampolgárok elégedettek preferenciái érvényesülnek, akkor az állam működése közelít a tökéletes-hez. Ezt az utópisztikus gondolatot korlátozzák az emberek különböző igényei és elvárásai, valamint hiányzott az a lehetőség, hogy minden polgár közvetlenül és gyorsan kapcsolatban legyen az állam működtetőivel. Az okosváros technológiai megoldásai erre is megoldást nyújthatnak. A közigazgatás ügyeit már eddig is próbálták elektronikus rendszerekkel gyorsítani és egyszerűsíteni. De ezek a megoldások csak részlegesen oldották meg a problémákat.

A politika alrendszeren kívül, az állam más funkcióinak fejlesztése is hozzá tartozik az okosváros koncepcióhoz. A rend- és honvédelem, az egészségügyi ellátás katasztrófa elhárítás, és az oktatás területén is megjelentek olyan megoldások, amelyek a hatékonyságnövelést szolgálják. A város eseményeit ellenőrzés alatt tartani az emberi és más erőforrások nagy részének lekötésével jár. A rendfenntartás minősége változó a különböző városokban, azonban minden városban (államban) elengedhetetlen ennek a szolgáltatásnak a fenntartása. A térfigyelő rendszerek meglévő infrastruktúrájának

fejlesztésével[206] és elemző szoftverek alkalmazásával egy olyan komplex rendszert alakítható ki, amely nem csak a rendvédelem céljaira alkalmazható, de a katasztrófaelhárítás és a mentőszolgálat hatékonyságát is javíthatja. Ezek a szolgáltatások jelenleg a lekötött emberi erőforrások nagy részét a felügyeleti funkcióra használják, amelyet az okos megfigyelőrendszer helyettesíthet.

Technológiai kihívások

Az okosváros működéséhez szenzorokra van szükség, amelyek az adatokat szolgáltatják az adatelemző mesterséges intelligenciák működéséhez. Minden alrendszernek hasonló működési elvű szenzorokra van szüksége. A képfeldolgozás, rádióhullámos érzékelők, lézeres távmérők és annak továbbfejlesztéseivel is operálhatnak a fejlesztők. Az autonóm járművek lézer és radar szenzorokat egyaránt használnak. Mindkét lehetőség egyelőre jelentős korlátokkal működik. A lézer-szenzor,[207] amely kibocsátja és érzékeli, a lézersugarakat másodpercenként tízszer fordul meg, amelyben 64 lézer-generátor és érzékelő a visszaverődő sugarak segítségével összegyűjti a 3D objektumokkal kapcsolatos információkat az autó 150 méteres környezetében.[208] Jelenleg a szenzor számára legnagyobb korlátot az időjárás jelenti, ugyanis ködös vagy esős időben a lézerfényt eltéríthetik az apró vízcseppek így jelentősen csökken az eszköz használhatósága. A radarszenzorok hasonlóan működnek, a tárgyakról visszaverődő hullámok alapján határozzák meg a környezetüket. Ez azonban kisfelbontású pontatlan képet rajzol ki a távoli tárgyakról, így csak bizonyos részfeladatokra és csak korlátozottan alkalmazható. A technológia korlátai más téren is megmutatkoztak. Az autonóm jármű jelenlegi állapotában még nehezen birkózik meg olyan feladatokkal, amelyek nem szerepelnek az adatbázisában. Olyan esetekben, amikor egy váratlan akadályba ütközik, például egy útlezárás, nem képes dönteni, mi a helyes megoldás abban a forgalmi szituációban. Ilyenkor emberi beavatkozás szükséges a szituáció megoldásához. Az eszközök korlátai más területeken is jelentkeznek. A térfigyelő rendszerek több spektrumon is megfigyelhetik a környezetüket.

Az okosvárosban alkalmazott technológiák használhatóságához elengedhetetlen az internet vagy más számítógépes hálózat használata. Ez egyben azt jelenti, hogy ezek az eszközök fokozottan ki lesznek téve a kibertér rosszindulatú szereplőinek. A közlekedésszervezés hatékonyabbá tétele mellett ezek és a hasonló kutatások a céljuk mellett egy másik nagyon fontos tényre is felhívják a figyelmet. A város működését segítő berendezések és maguk a városlakók is, eszközeiken keresztül, folyamatosan információkat szolgáltatnak mozgásukról, helyzetükről, esetleg állapotukról. Ezek az információk nem kizárólag azokhoz jutnak el, akiknek címezték vagy jogosultak kezelni azokat. A rosszindulatú kibertevékenységek egyik eszköze a nyílt forrású hírszerzés. „Annak érdekében, hogy a támadók sikerrel tudják végrehajtani az egyes kritikus infrastruktúra elemek blokkolását, megfelelő információkkal kell, rendelkezzenek a kiválasztott célpont felépítéséről, sebezhetőségéről, képesnek kell, legyenek a támadás megindításakor e rendszerek képességeinek optimális esetben teljes körű szüneteltetésére, adott esetben csökkentett funkciójú üzemelésének elérésére, miközben a saját számítógépes rendszerének működését biztosítják.”[209]

---

[206] Arcfelismerés, távoli retinaszkennelés, baleset felismerés, forgalomfigyelés, bűncselekmény felismerés

[207] Ten astonishing technologies that power google’s self-driving cars url: https://www.national.co.uk/tech-powers-google-car/ 2016. 10. 29.

[208] Oshkodefence Terramax url: http://oshkoshdefense.co.uk/wp-content/uploads/2014/01/EN-UK_Technology_Bro_6-3-2011.pdf 2015. 02. 10.

[209] Bányász Péter − Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, Hadtudomány Elektronikus szám, 2013. p. 194. http://mhtt.eu/hadtudomany/2013_e_Banyasz_Peter_Orbok_Akos.pdf 2016. 10. 10.

3.2. Az okos város kockázatai

Az okosváros meghatározásaiból kiderül, hogy a város működését a technológia segítségével akarja hatékonyabbá tenni. A technológia használatával azonban egy sor olyan kockázat is felszínre kerül, amely addig nem vagy kevésbé volt hatással a biztonságunkra. Ezek a kockázatok jelenleg is fennállnak, csupán nem olyan mértékű a kitettségünk. Hagyományosan a városi infrastruktúra különböző elemekből áll össze, de a kiber-fizikai rendszer összekapcsolja a kiberteret a fizikai infrastruktúrákkal, beágyazott érzékelőket, számítási eszközöket, kommunikációs technológiákat egyaránt. A város által előállított nagy mennyiségű adatot a kiber-fizikai rendszerek rögzíthetik, hogy azonosítsák a problémákat és javítsák a hatékonyságot. Amellett, hogy gyűjtik az adatokat és javaslatokat hajtanak végre a folyamatok hatékonyabbá tétele érdekében, ezek a rendszerek képesek automatikusan irányítani és manipulálni a fizikai infrastruktúrát a változtatásokat végrehajtására. Az így kialakult «rendszerek rendszere», integrálja az okosváros elemeit és képes rövid és a hosszú távon is a hatékony működésre."[210] Azzal, hogy a kibertér és a fizikai világot összekapcsoljuk, sőt a kibertérből irányíthatóvá tesszük, kitesszük magunkat azoknak a veszélyforrásoknak, amelyek eddig „csak" a kiberteret fenyegették.

4. Az Internet of Things jelentette kihívások

A 21. században a nagyvárosokban élők mindennapjait szinte észrevétlenül egyre inkább meghatározzák a különböző technikai újítások, melyek segítségével hatékonyabban tudjuk beosztani az időnket, könnyebben tájékozódunk, egyszerűbben szerzünk információt, vagy éppen kevésbé szennyezzük a környezetünket. Az innovációk térnyerésével olyan új eszközök állnak rendelkezésünkre, melyek akár képesek egymással is kommunikálni, így egyre több tevékenység optimalizálható vagy automatizálható, egyre kevesebb erőforrás elhasználásával egyre több mindent tudunk elvégezni. Az úgynevezett Internet of Things, vagyis a „dolgok internete", ami annak a jelenségnek a leírása, hogy minden, mindennel, mindenhol, mindenkor összekapcsolódik. Az összekapcsolt eszközök között nem csak az „okos" telefonokat, tévéket, órákat, autókat értjük, hanem minden olyan eszközt, amely kapcsolódik az internetre és így egymáshoz is, például a háztartási gépek, csecsemőfigyelők, kamerák, hálózati tárolókat és sorolhatnánk. Ezeknek az eszközöknek és hálózatuknak köszönhetően egyre jobban elmosódnak a határok a kibertér és a fizikai világ között. Valamint így egyre több klasszikus értelemben vett tech-cég válik érdekeltté abban, hogy olyan infrastruktúrát fejlesszenek, amellyel kézzelfogható-an részt vesznek például a városfejlesztésben is. Ennek csak egyik ága a közlekedésoptimalizálásban és az önműködő gépjárművek tervezésében megindult verseny, ahol olyan elsőre szokatlan szereplők jelentek meg, mint a Google vagy az Apple. De ma már szinte minden elektronikai, illetve telekommunikációs cég (IBM, AT&T, Cisco, Samsung, Microsoft, Oracle, GE, LG stb.) foglalkozik olyan megoldásokkal, melyeket kifejezetten a városi szolgáltatások optimalizálására terveztek.[211]

A trend megállíthatatlannak tűnik és ezzel párhuzamosan egyre több szó esik az internetre kapcsolódó eszközök biztonságáról, ami bizony komoly kívánnivalókat hagy maga után. Márpedig a probléma egyre nőni fog, ha az érintettek nem tesznek ellene. A kibertér rosszindulatú szereplőinek általában olyan eszközök ellen éri meg támadásokat intézni, amelyek használóinak száma elér egy kritikus tömeget ahhoz, hogy a támadásokkal megfelelő hasznot lehessen elérni. Az IoT-eszközök feltörésével olyan értékes információkat lehet majd megszerezni, amelyet a felhasználó ellen fordíthatnak vagy bejuthatnak más rendszerekbe is. Egy okostévé esetében hozzá lehet jutni a berendezés által egyébként monitorizált adatokhoz (milyen műsort néztünk, milyen alkalmazásokat futtattunk, milyen

[210] UN Urban Population Trends Url: https://engtechmag.wordpress.com/2014/07/22/un-world-urbanization-prospects-report-half-the-world-lives-in-urban-areas-an-annotated-infographic/ 2016. 10. 10.

[211] Czirják Ráhel: *Okosvárosokkal a globális társadalmi kihívások kezeléséért?* http://www.geopolitika.hu/2016/09/23/okosvarosokkal-a-globalis-kihivasok-kezeleseert/ 2016. 10. 10.

weboldalakat látogattunk meg stb.). Ha pedig a televíziót felszerelték kamerával és mikrofonnal, a hackerek mindent látni és hallani fognak, ami a szobában történik. A testen hordható diagnosztikai eszközök ugyanúgy, ha nem jobban ki vannak téve annak a veszélynek, hogy hozzáférnek az általa mért és közvetített adatokhoz, amelyek révén az orvosok távolról is tájékozódhatnak egy beteg állapotáról. Ezeket az adatátvitelre használt kommunikációs csatorna feltörésével lehet a leginkább támadni, és így rendkívül bizalmas, esetleg értékes egészségügyi adatokhoz jutni.

A járműgyártók egyre több automatizált szolgáltatást építenek be az autókba, amelyek segítségével elkerülhetőek a dugók, és jelentősen könnyebbé válik a járművezetők életét. Azonban a fejlesztésekkel együtt a kockázat mértéke is növekedik, hiszen, ha a számítógépekkel vezérelt, egymással vezeték nélkül kommunikáló járművek rendszerét feltörik, veszélybe kerülhet az utasok vagy a forgalom más szereplőinek élete. Az autonóm járművek fejlesztésében és alkalmazásában civil és katonai területen dolgozó fejlesztők egyaránt nagy lehetőségek látnak több vállalatnál is. Az eszközt 2009-óta fejlesztő Google, már létrehozott több működőképes járművet. Ezeket a forgalomban tesztelik, hogy minél több szituációban vizsgálhassák a teljesítményét. A Google számára nagy előnyt jelentett, hogy rendelkeznek olyan geoinformatikai technológiával és információkkal, amelyeket felhasználhatnak a jármű tájékozódási rendszeréhez. A fedélzeti számítógép navigálásához három fontos információforrásra van szüksége: a nagy felbontási és pontos térképre, a műholdas helymeghatározás adataira és a saját érzékelői által közvetített adatokra, amelyek a jármű közvetlen környezetét térképezik fel. A globálisan tájékozódó, az útvonalakat és a közvetlen környezetét ismerő számítógép képes kiválasztani az ideális útvonalat a cél eléréséhez. Ezt még kiegészítheti azok a még kísérleti stádiumban lévő technológiák, amelyek szintén segítik a biztonságos közlekedést és tájékozódást. Az egyik ilyen technológia az utakba szerelt jeladók hálózatának segítségével információkat közöl a járművekkel, valamint az, amely a járművek számítógépeinek egymás közötti kommunikációját teszik lehetővé.

A technológia már önmagában is előnyökhöz juttathatja az alkalmazóit, a vezető leterheltségének csökkentésével, illetve a biztonságos irányítás képességével. Emellett a katonai felhasználásának további lehetőségei is vannak. A jelenkori konfliktusok kimenetelében kulcsfontosságú – főleg a nyugati országok esetében – a hátország legitimációja, azaz mennyire tudják elfogadtatni a háború szükségességét a lakossággal. A politikai érveken túl, amelyek a közösség meggyőzését szolgálja, nagyon fontos az egyes emberek meggyőzése, akik a harcba küldik hozzátartozóikat. Ennek legjobb módja a szeretteik, a katonák épségének garantálása, de legalább is annak ígérete. Az autonóm járművek ezen a téren nyújtják a legnagyobb lehetőséget, hiszen a vezető életének kockáztatása nélkül lehet olyan feladatokkal megbízni, amit eddig csak katonákkal lehetett megoldani. Ilyen feladatok lehetnek az utánpótlási szállítások a harctérre, aknamentesítő járművek irányítása, harctámogató, harckiszolgáló járművek vezérlése. Ezeknek a járműveknek a fejlesztése jelenleg kísérleti szakaszban jár, de fél-autonóm, illetve távvezérelt eszközöket már rég használnak a hadseregek, gondoljunk a drónokra vagy a bombahatástalanító robotokra.

Etikai és jogi kihívások

A jelentős számú előny mellett, amelyet az autonóm járművekkel elérhetünk, jelentkeznek olyan kérdések is, amelyek kihívássá változtatják a fejlesztésnek ezt az irányát. Az egyik legnagyobb vitát az etikai kérdések okozzák az autonóm járművekkel kapcsolatban. Patrick Lin, a California Polytechnic State University etikai és feltörekvő tudományok kutatócsoport[212] igazgatójának *kérdése: Feláldozhatja-e az autó a saját utasainak életét? Például, ha elkerülhetetlen ütközést észlel egy másik autóval, megpróbálhatja elkerülni a balesetet egy olyan manőverrel, ami biztosan végzetes a saját utasaira nézve?* [213]

[212] https://ww2.kqed.org/science/2016/10/03/how-safe-is-safe-enough-for-a-self-driving-car/ 2016.10.10.

[213] Erik Sofge: The Mathematics of Murder: Should a Robot Sacrifice Your Life to Save Two? Popular Science 2014 http://www.popsci.com/blog-network/zero-moment/mathematics-murder-should-robot-sacrifice-your-life-save-two 2016.10.10.

Ennek a kérdéskörnek a folytatása a jogi dilemma. Ki a felelős a jármű által okozott kárért, illetve, hogy lehet megállapítani, ki vezette a járművet a baleset bekövetkeztekor? Ezekre a kérdésekre jelenleg még nem tudunk megfelelő válaszokat adni. A jelenlegi jogi szabályozás a Bécsi Közlekedési Egyezmény[214] *is ezt veszi alapul, amikor így fogalmaz:* „a vezetőnek a járművét folyamatosan az irányítása alatt kell tartania és minden pillanatban képesnek kell lennie beavatkozni."

Az etikai dilemma a térfigyelő rendszerek esetében is felmerül. A személyiségi jogok és a biztonság elvének szembenállása ma is kihívást jelent a demokratikus államok és rendvédelmi szervei számára. Ha az okosváros működéséhez a város teljes megfigyelése szükséges a biztonság érdekében, akkor a polgárok élete abszolút mértékben kiszolgáltatottá válik a hatóságnak.

4.1. A kibertér kockázata

Az infókommunikációs technológiát használó városok hatékonyabbá válhatnak. Ugyanakkor a technológiai fejlődés magában hordoz több biztonsági kockázatot is. A hálózati társadalomban[215] – amely az információs társadalomra épül és annak újragondolásán alapszik – jelentősen függünk a technológia működésétől. Az IKT használók ma is ki vannak téve a kibertér fenyegetéseinek, de a mai felhasználók élete csak részben függ, ha egyáltalán függ a technológia működésétől. Ezzel szemben az okosváros kiépülésével és a dolgok internete elterjedésével a kitettségünk és függőségünk rendkívül megnő. Minden felhasználó szembesülhet az információs technológia számos kihívásával. A számítógépes fenyegetések száma és kifinomultsága az eszközök számával együtt nő.[216] A kibertér biztonsági kockázatai ma is léteznek, de összehasonlítva azzal az jövőképpel, ahol az élet minden területén jelen lesznek a kiber-fizikai rendszerek, közel sem akkora a hatásuk, mint ma.

A rosszindulatú programok számos célt szolgálhatnak, mint az információszerzés, károkozás, információk törlése, vagy az IKT és egyéb eszközök jogosulatlan használata. A műveletek a céljainak megfelelően lehetnek kifinomultak és primitívek is. Ahogy a fizikai térben is, a kibertérben is a rombolás az egyszerűbb tevékenység, hiszen nem igényel akkora idő, energia és költség ráfordítást, mint egy adathalász vagy más bonyolultabb művelet. A viszonylag „egyszerűbb" műveletek közé tartozik, a szolgáltatásmegtagadással járó támadás (Denial of Service (DoS)), és az elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service (DDoS)) támadások, amelyeknek a megtámadott rendszer megbénítása a célja. Ez a támadásforma viszonylag egyszerűen végrehajtható mivel a támadáshoz szükséges tudás és eszközrendszer szintén megtalálható a kibertérben. Továbbá nem szükséges hozzá nagy költségvetés, ráadásul kis csoportok vagy egy személy is véghezviheti. Mivel könnyen hozzáférhető, sokkal több támadó számára nyújt lehetőséget, mint más bonyolultabb vagy költségigényesebb támadásforma, amit kiegészít az, hogy nehezen lehet az elkövetőket megtalálni, ezért kockázata is nagyobb.

A támadástípusok között léteznek sokkal kifinomultabb eljárások és programok is. Az egyik első, kifejezetten egy célpont megtámadására készített rosszindulatú program a Stuxnet malware volt, amely az iráni Natanz urándúsító centrifugáinak tönkretételére hoztak létre. Habár ennek a támadásnak szintén a rombolás volt a célja, de a feltételei sokkal nagyobb anyagi, idő, emberi erőforrás ráfordítást és hírszerzői képességeket igényeltek. A hasonló számítógépes vírusokkal ellentétben a Stuxnet egy bizonyos célponti rendszerbe kerülve aktiválódott, bár több ezer helyen megtalálták később. A működését tekintve egy több lépcsős programról van szó. Az első lépcsőnek a reprodukció

[214] Bécsi Közlekedési Egyezmény a közúti közlekedésről és jelzésekről. url: http://www.unece.org/trans/welcome.html 2016. 10. 10.

[215] Manuel Castells: The Network Society: from Knowledge to Policy The Johns Hopkins University Press, Center for Transatlantic Research Relations, Washington, DC 2006 p. 4. url: http://www.umass.edu/digitalcenter/research/pdfs/JF_NetworkSociety.pdf 2016. 01. 10.

[216] Attackers Target Both Large and Small Businesses https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf 2016. 10. 29.

volt a feladata, hogy minél nagyobb eséllyel jusson el a célrendszeréhez. A második lépcső csak akkor aktiválódott, ha talált a környezetében bizonyos, a célrendszerrel (a Siemens folyamatirányítási rendszere) megegyező kritériumokat. Ha a rendszer nem azokat az urándúsító centrifugákat vezérelte, akkor a program nem futtatta tovább a következő lépcsőjét és inaktív maradt. Az eset további érdekessége, hogy a natanzi üzemben nem volt külső internetkapcsolat pontosan a kibertámadások hatékonyabb elhárítása érdekében. Tehát a rosszindulatú program valamilyen adathordozón jutott be az üzem rendszerébe, amit egy belépési engedéllyel rendelkező személy kellett, hogy bejuttasson. Azt nem tudhatjuk, hogy aki bejuttatta a programot, milyen indítékokkal rendelkezett, ha egyáltalán tisztában volt azzal, hogy mit tesz, de az biztos, hogy azt a biztonsági rést használta ki, hogy külső adathordozót lehetett csatlakoztatni a rendszerhez. A program végül elérte célját és az irányító rendszerekbe jutva átállította a centrifugák forgási sebességét, amellyel tönkretette a berendezéseket. Ezzel 3-4 éves visszaesést okozott az iráni atomprogramnak.

4.2. A „Big Brother" kockázat

Az okos város modellezésénél figyelembe kell venni azt a lehetőséget is, amikor nem a tervezettnek megfelelő módon használják a technológia nyújtotta lehetőségeket. A szenzorhálózat és a kiber-fizikai rendszerek elterjedése a hatóságok számára olyan lehetőségeket nyújtanak, amellyel minden eseményt megfigyelhetnek és esetleg rögzíthetnek is. A rendfenntartás vagy más érdekekre hivatkozva a hatóság ezzel a lehetőséggel visszaélhet. Ez elsősorban a politikai rendszer diszfunkcióját jelenti, de a technikai háttér felerősítheti a diszfunkció hatásait. A diktatúrák elsőszámú célja a társadalom teljes ellenőrzése, a dolgok internete segítségével egy ilyen rendszer valóban megközelítheti ezt az állapotot. Ilyenkor az állam nem a polgárok érdekében, hanem ellenük cselekszik. A mai biztonsági rendszerek is érzékelőkre és megfigyelési hálózatokra épülnek. Ez a tény már önmagában rejti a hatalommal való visszaélés lehetőségét. Az eseménynek nem szükséges extrém lenni ahhoz, hogy a polgáraik jogait és érdekeit sértse. A dolgok internete nem feltétlenül vezet el a George Orwell által írt 1984-ben elképzelt negatív utópiához, de a visszaélés veszélye mindenképpen fennáll.

Az okosváros, amely a dolgok internetére épülve kiegészíti a technikai fejlődést, társadalmi és kulturális fejlődéssel, az egyik fontos célja, hogy a polgárokat tudatos felhasználókká és azt is meghaladva, az okosváros fejlesztőivé tegye. Ebben az esetben a politikai rendszerek diszfunkciójára is sokkal kisebb az esély, mint egy információ és eszköz és lehetőség hiányban szenvedő társadalomban.

4.3. Mesterséges intelligencia

Valószínűleg ez az a terület, amelynél nagyobb képzelőerőre lesz szükség. A tudattal rendelkező mesterséges intelligencia nem feltétlenül valamilyen szándékos tevékenység eredményeként jöhet majd létre. A világon összesen több mint 3.4 milliárd internet felhasználó van.[217] Ha minden felhasználó csak egy eszközön csatlakozik az internethez, akkor is elgondolkodtató, hány internetes végponttal rendelkező hálózat lenne képes arra, hogy valamilyen tudatot létrehozzon? Azt tudjuk, hogy körülbelül 200 milliárd neuron elég egy tudat működéséhez, ugyanis ennyi idegsejt van az emberi agyban.[218] A kiszámíthatatlanság az egyik olyan tényező, amely miatt aggódhatunk. A tudattal rendelkező mesterséges intelligencia létrehozása morális kérdéseket vet fel. Van-e joga az embernek

[217] http://www.internetlivestats.com/

[218] Azevedo, Frederico A.C.; Carvalho, Ludmila R.B.; Grinberg, Lea T.; Farfel, José Marcelo; Ferretti, Renata E.L.; Leite, Renata E.P.; Filho, Wilson Jacob; Lent, Roberto; Herculano-Houzel, Suzana (2009). „Equal numbers of neuronal and nonneuronal cells make the human brain an isometrically scaled-up primate brain". *The Journal of Comparative Neurology.* 513 (5): 532–541.

mesterséges lényt alkotni? Ha elfogadjuk azt, hogy van, akkor adhatunk-e neki szabad akaratot, vagy be kell tartania Asimov törvényeit?[219] Ha az általunk programozott parancsokat hajt végre a mesterséges tudat, akkor miért hoztuk létre? Mekkora az esélye annak, hogy ellenünk fordul? Ha ellenünk fordul van-e esélyünk ellene? Ha ismerjük ezeket a kérdéseket, logikus döntés lehet a mesterséges tudat létrehozása?

Ray Kurzweil úgy fogalmazott a „Szingularitás küszöbén" című könyvében: „… az ember alkotta technológia változásainak üteme gyorsul, a képességei pedig exponenciálisan nőnek. Az exponenciális növekedés csalóka dolog. Szinte észrevétlenül kezdődik, majd váratlan dühvel kirobban – mármint akkor váratlan, ha az ember nem figyel a pontos pályájára… a számítógépes intelligencia egykor szűk alkalmazási területei is fokozatosan bővülnek, egyre több tevékenységet ölelve fel. Például ma már a számítógépek elektrokardiogramokat és orvosi képeket diagnosztizálnak, repülőgépeket vezetnek, automatizált fegyverek taktikai döntéseit vezérlik, pénzügyi döntéseket hoznak és hiteleket bírálnak el, és sok egyéb feladatot is átvettek, amik egykor az emberi intelligencia közreműködését igényelték"[220]

4.4. Sebezhetőségek és függőségek

Kapcsolódva az előző részhez, a mesterséges intelligencia és a dolgok internete nyújtotta lehetőségek könnyen vezethetnek a társadalom ellustulásához és ezáltal a technológiafüggőség abszolúttá válásához. Ez a függőség már ma is komoly problémát jelent az információs és a hálózati társadalom tagjainak. Jelenleg ez csak lelki függőséget jelent a felhasználók számára, de a későbbiekben már fizikait is jelenhet, ha a környezetünk és a létfeltételeket biztosító eszközök is mind a dolgok internete részeivé válnak. Kurzweil írja, hogy a kibertér a tudás birodalma, amelynek a felfedezése a világ legizgalmasabb hivatásai közé tartozik. Most előttünk a lehetőség, hogy minden ember önmagában, a saját habitusa szerint tehesse meg ezeket a felfedezéseket.[221] Ehhez hozzátartozik, hogy ha a tudás kizárólagos forrásává válik a kibertér, akkor a kiszolgáltatottságunk is jelentősen megnő a technológiától. Az okosváros előnyeinek elterjedése magában hordozza azt a kockázatot, hogy a felhasználó városlakók egyre inkább a technológia foglyaivá válva azokat a döntéseiket is rábízzák, amelyek befolyásolhatják a biztonságukat is. Ha folytatjuk ezt a gondolatot, ezek a technológiák a kényelmüket szolgálják, így előfordulhat, hogy bizonyos döntések, szokások és ismeretek hiányozni fognak az életünkből, amelyeket ma még létszükségnek gondolunk. A függésünk az információtól vagy az internettől ma is problémát jelent az emberek egy részének. Ha egy IoT által működtetett világban élünk majd, a függőségünk mértéke beláthatatlanul megnőhet.

---

[219] Isaac Asimov: Én, a robot. Móra, 1991. Baranyi Gyula fordítása
A robotika három törvénye:
1. A robotnak nem szabad kárt okoznia emberi lényben, vagy tétlenül tűrnie, hogy emberi lény bármilyen kárt szenvedjen.
2. A robot engedelmeskedni tartozik az emberi lények utasításainak, kivéve, ha ezek az utasítások az első törvény előírásaiba ütköznének.
3. A robot tartozik saját védelméről gondoskodni, amennyiben ez nem ütközik az első vagy második törvény bármelyikének előírásaiba.

[220] Ray Kurzweil: A szingularitás küszöbén. The Viking Press 2005, pp. 11–12. 2016. 10. 10.

[221] Ray Kurzweil: The Singularity Is Near. The Viking Press 2005, p. 485. 2016. 10. 10.

5. A város funkcióinak fejlődési lehetőségei, kiemelve a közigazgatást

A kormányzás és a részvétel

Az államok hatékony irányítására számos elméletet különböztet meg a politikatudomány, amelyek közül néhány a közösségeket helyezi előtérbe, néhány az egyént. A demokratikus politikai rendszerekben mindkét álláspontnak lehetnek képviselői, ettől válik az egyének és a közösségek számára is elfogadhatóvá. Azonban a demokráciának is vannak olyan tulajdonságai, amelyek gyengítik a funkcionális működését. Elsősorban a polgárok részvételének elvének biztosítása a döntéshozatalban szenved sérülést, amikor képviseleti demokráciáról beszélünk, hiszen a polgárok csak képviselőik útján vehetnek részt a döntéshozatalban (kivéve a népszavazást). Ebben az esetben a polgárok döntéseiket informáltságuk és képviselőik retorikai képességeik alapján hozzák meg. Ez a folyamat nem teszi lehetővé, hogy az egyének és a közösségek érvényre juttathassák érdekeiket, így sérül a demokrácia alaptétele miszerint a nép uralkodik önmagán. Az alul vagy félreinformáltság komoly demokrácia-deficit.

Ahogy növekszik a polgárok száma, úgy válik egyre alulinformáltabbá az egyes polgár, elsősorban az életkörülményei romlása miatt. Az élhetőbb környezet és az infokommunikációs technológiák fejlődésével ez a tendencia megfordíthatónak látszik. A világháló lehetőséget biztosít a polgároknak, hogy tájékozódjanak, sőt akár maguk is véleményformálóvá váljanak. Legalább is ez lenne a logikus következmény, azonban ma az információk mennyisége akadályozza a legjobban az objektív tájékozódást. A polgárok képtelenek kiválogatni azokat a releváns információkat, amelyek leginkább befolyásolhatják életüket. Ez az internet szabályozatlanságának köszönhető, pont annak a tulajdonságának, amelynek a szólásszabadság kitejesedését kellett volna beteljesítenie. Tehát a világháló valamely szabályozása valószínűleg szükségszerűvé válik annak érdekében, hogy a felhasználó polgárok a számukra releváns információkhoz hozzájuthassanak.

A „technológiai megoldások az okos városban” alfejezetben említett fejlesztési lehetőségeket figyelembe véve láthatjuk a fejlődés lehetséges irányát a politikai részvétel, az állam és a közigazgatás tekintetében.

6. Tudatos tervezés és felhasználók

Az infokommunikációs eszközök elterjedése és összekapcsolódásuk a fejlődés többirányú lehetőségét nyújtja számunkra. Azonban nem szabad eltekinteni a biztonsági kérdésektől. Minden eszköz, amelyet IKT segítségével a hálózat részévé teszünk, egyben egy új veszélyforrás is. A cél az, hogy az új megoldások okozta kockázatokat, már a fejlesztéseket megelőzve képesek legyünk felismerni.

A tervezők részben úgy képzelik el a jövő városát, hogy a polgárok maguk fogják azt irányítani. Mivel az internet tájékozottá tesz bennünket, így jobban informált döntéseket hozhatunk. Okos polgárokká válunk azáltal, hogy változtatunk szokásainkon, hatékonyabb gyakorlatokat és intelligensebb társadalmi normákat fejlesztünk ki az okos városunkban.[222]

Azonban azok, akik csak az informatikai környezetben keresik a megoldást, rossz úton járnak. A hálózat leggyengébb pontja a felhasználó volt és marad is. Ezért a felhasználók fejlesztésére kellene alapozni az okos városfejlesztéseket. Az okos állampolgár lehet az alapja a biztonságos és jól működő okos városnak társadalmi és technológiai értelemben egyaránt. Ebben az esetben a polgárok nem csak képesek lennének biztonságosan használni az okos város előnyeit, hanem képesek lennének a fejlesztésére és javítására is. A folyamatos innováció az okos városokban azért szükséges, mert az okos város nem a városfejlődés csúcsa, hanem a kezdete. A polgárok nem csak a felhasználói a rendszernek, de egyben részét is képezik annak.

[222] Smart citizens How the internet facilitates smart choices in city life Costumerlab Eriksson url: http://www.ericsson.com/res/docs/2014/consumerlab/ericsson-consumerlab-smart-citizens.pdf 2016.10.10.

7. Felhasznált irodalom:

- 1.2 Billion Vehicles On World's Roads Now, 2 Billion By 2035: Report http://www.greencarreports.com/news/1093560_1-2-billion-vehicles-on-worlds-roads-now-2-billion-by-2035-report 2016. 10. 29.
- „Attackers Target Both Large and Small Businesses" https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf 2016. 10. 29.
- Frederico A.C. Azevedo – Ludmila R.B. Carvalho – Lea T. Grinberg – José Marcelo Farfel – Renata E.L. Ferretti – Renata E.P. Leite – Wilson Jacob Filho – Roberto Lent – Suzana Herculano-Houzel (2009): „Equal numbers of neuronal and nonneuronal cells make the human brain an isometrically scaled-up primate brain". The Journal of Comparative Neurology. 513 (5): 532–541. o.
- Bányász Péter − Orbók Ákos: „A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében". Hadtudomány Elektronikus szám, 2013 194. o. http://mhtt.eu/hadtudomany/2013_e_Banyasz_Peter_Orbok_Akos.pdf 2016. 10. 10.
- Bécsi Közlekedési Egyezmény a közúti közlekedésről és jelzésekről. http://www.unece.org/trans/welcome.html
- Czirják Ráhel: „Okosvárosokkal a globális társadalmi kihívások kezeléséért?" http://www.geopolitika.hu/2016/09/23/okosvarosokkal-a-globalis-kihivasok-kezeleseert/
- Erik Sofge: „The Mathematics of Murder: Should a Robot Sacrifice Your Life to Save Two?". Popular Science, 2014. http://www.popsci.com/blog-network/zero-moment/mathematics-murder-should-robot-sacrifice-your-life-save-two
- Isaac Asimov: *Én, a robot.* Móra, 1991. Baranyi Gyula ford.
- „Focus Group on Smart Sustainable Cities: Smart sustainable cities: an analysis of definitions". ITU-T, 2014. 13. o. http://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx
- Kevin Ashton: "That ‚Internet of Things' Thing" http://www.rfidjournal.com/articles/pdf?4986; https://www.scientificamerican.com/article/the-internet-of-things/
- „Kik is azok a klímamenekültek?" Greenfo.hu. https://greenfo.hu/hir/kik-is-azok-a-klimamenekultek/ 2016. 10. 10.
- Manuel Castells: The Network Society: from Knowledge to Policy. The Johns Hopkins University Press, Center for Transatlantic Research Relations, Washington, DC, 2006. 4. o. http://www.umass.edu/digitalcenter/research/pdfs/JF_NetworkSociety.pdf 2016.01.10.
- Nagy András – Sain Mátyás – Sárdi Anna – Vaszócsik Villa: Településértékelés és monitoring. Lehner Tudásközpont http://lechnerkozpont.hu/doc/okos-varos/telepulesertekeles-es-monitornig-modszertani-javaslat.pdf
- Oshkodefence Terramax. http://oshkoshdefense.co.uk/wp-content/uploads/2014/01/ENUK_Technology_Bro_6-3-2011.pdf
- Paolo Neirotti – Alberto De Marco – Anna Corinna Cagliano – Giulio Mangano – Francesco Scorrano: "Current trends in Smart City initiatives: Some stylised facts". Original Research Article Cities, Volume 38, June 2014. 25–36. o. http://www.sciencedirect.com/science/ article/pii/S0264275113001935
- J. R. Petit – J. Jouzel – D. Raynaud – N. I. Barkov – J. M. Barnola – I. Basile – M. Bender – J. Chappellaz – M. Davis – G. Delaygue – M. Delmotte – V. M. Kotlyakov – M. Legrand – V. Y. Lipenkov – C. Lorius – C. Ritz – E. Saltzman (1999. június 3). „Climate and atmospheric history of the past 420,000 years from the Vostok ice core, Antarctica". Natura, 399. 1999. 429–436. o. http://www.nature.com/nature/journal/v399/n6735/abs/399429a0.html
- Ray Kurzweil: The Singularity Is Near. The Viking Press, 2005, 485. pp. 11–12. o.

- Smart citizens – How the internet facilitates smart choices in city life. Costumerlab Eriksson. http://www.ericsson.com/res/docs/2014/consumerlab/ericsson-consumerlab-smart-citizens.pdf
- Smarter cities for smarter growth. IBM Institute for Business Value. https://www.zurich.ibm.com/pdf/isl/infoportal/IBV_SC3_report_GBE03348USEN.pdf
- „Ten astonishing technologies that power google's self-driving cars". https://www.national.co.uk/tech-powers-google-car/
- "The United Nations Economic Commission for Europe, Smart Cities characteristics". Unece. http://www.unece.org/housing-and-land-management/projects/housingsmartcities/smart-cities-characteristics.html
- UN Department of Economic and Social Affairs Population Division World Population, 2012 http://www.un.org/en/development/desa/population/publications/pdf/trends/WPP2012_Wallchart.pdf
- „UN Urban Population Trends". https://engtechmag.wordpress.com/2014/07/22/un-world-urbanization-prospects-report-half-the-world-lives-in-urban-areas-an-annotated-infographic/
- „Worldwide Prius sales top 3-million mark; Prius family sales at 3.4 million" http://www.greencarcongress.com/2013/07/prius-20130703.html
- Yanan Wang: „In Flint, there's so much lead in children's blood that a state of emergency is declared". Washington Post, 2015. https://www.washingtonpost.com/news/morning-mix/wp/2015/12/15/toxic-water-soaring-lead-levels-in-childrens-blood-create-state-of-emergency-in-flint-mich/

8. Felhasznált internetes források jegyzéke

- http://www.bbc.com/news/world-latin-america-30727877
- http://www.demographia.com/db-worldua.pdf
- https://ww2.kqed.org/science/2016/10/03/how-safe-is-safe-enough-for-a-self-driving-car/
- https://www.teir.hu/idosoros-elemzo/

V. SZABÓ ANDRÁS: REFERENCIAARCHITEKTÚRÁK A MOBILVÉDELEMBEN

1. Bevezető

Korunk egyik legkomolyabb kiberbiztonsági kihívását a mobileszközök elterjedése jelenti. A szervezetek számára kulcsfontosságú információk olyan védtelen környezetbe kerülnek például a dolgozók által használt saját okostelefonokon, melyek azonnali beavatkozásra késztetik az elektronikus információbiztonsággal foglalkozó szakembereket. Ezt erősíti meg a jogszabályi elvárás is, hiszen a 2013. évi L. törvény (Ibtv.) és annak végrehajtási rendeletei számos olyan követelményt fogalmaznak meg, melyek a mobileszközökre is érvényesek.

Felismerve azt az igényt, hogy az elektronikus információbiztonsággal kapcsolatba kerülő szakemberek számára hasznos segítséget jelent egy olyan segédlet, mely konkrét műszaki megoldásokat ismertet, a Nemzeti Közszolgálati Egyetem és az Informatikai Vállalkozások Szövetsége egy olyan szakanyagot hozott létre, melynek célja, hogy a közigazgatási szervezetek számára is elérhető termékeken keresztül mutassa be, milyen lehetőségek vannak az okoseszközök védelmére, egyben levezesse, hogy ezek a konkrét megoldások milyen módon segítik az Ibtv.-nek való megfelelést.

A szakanyag létrehozásához köszönetet mondunk a RelNet Technológia Kft., a Sicontact Kft., a NewCo ICT Security Services Kft., az IBM és a Microsoft munkatársainak!

2. Korszerű mobilbiztonság Fortinet és Pulse Secure megoldásokkal biztosítva

Az információvédelem egyik legtöbb kihívást tartogató területének a mobilbiztonság számít, amelyet csak erős architekturális háttérrel és korszerű technológiák bevonásával lehet hatékonyan kiépíteni, valamint fenntartani.

Nem is olyan régen az informatikai biztonság még korántsem volt olyan összetett, komplex terület, mint napjainkban. A szervezetek elsősorban a fizikai biztonságra, a hálózataik határvédelmére és a kártékony programok elleni küzdelemre koncentráltak. Gyakorta lehetett tapasztalni, hogy egy-egy vállalatnál a védelmet egy tűzfal, valamint egy víruskereső biztosította, és jobb esetben volt egy biztonsági szabályzat, amelynek betartását többnyire humán erőforrásokkal lehetett ellenőrizni.

Az informatika rohamos fejlődése azonban az évek során rányomta a bélyegét a védelmi intézkedésekre is, és egyre mélyebb szintű, több rétegű védelem felé terelte a szervezeteket, belekényszerítve azokat a biztonság technológiai, adminisztratív és humán oldalról történő fejlesztésébe. Ennek eredményeként manapság már védelmi architektúrákról beszélünk, amelyek az informatikai infrastruktúrák szerves részét képezik, és mélyen beépülnek a vállalatok, intézmények folyamataiba. Legalábbis abban az esetben, ha egy szervezet valóban komolyan gondolja a kiberfenyegetettségek elleni küzdelmet, vagy éppen valamilyen jogszabályi, iparági követelménynek kell megfelelnie.

Akár arra a következtetésre is juthatnánk, hogy megfelelő szemlélet alkalmazásával ideális védelem alakítható ki, ami korszerű technológiák bevonásával nem is olyan nehéz feladat. Sajnos ez azonban koránt sincs így. Különösen nem azokon a területeken, amelyek nemrégen kezdték el felforgatni az informatika világát. Gondoljunk csak a mobilizációra, a felhő alapú szolgáltatások terjedésére vagy éppen a dolgok internetére (IoT – Internet of Things). E trendek védelmi oldalról történő

lekövetése aggasztó lemaradást képes előidézni, ami sebezhetővé teheti a szervezetek informatikai rendszereit, illetve az általuk kezelt adatokat.

Ezúttal a mobilbiztonságot vesszük górcső alá. Megvizsgáljuk, hogy milyen kockázatokkal kell számolni, és azok kezelésére milyen lehetőségek kínálkoznak. Elöljáróban már most érdemes megjegyezni, hogy egy sokkal kiterjedtebb védelmi területről van szó, mint az elsőre látszik, és önmagában a technológiai oldalról való megközelítése nem elegendő a kockázatok elvárható szintű csökkentéséhez. A biztonság szempontjából egyfajta paradigmaváltásra van szükség, ugyanis a sok éven át folytatott hálózat- és munkaállomás-védelemre kiélezett óvintézkedéseket egy olyan környezetbe kell „átültetni", amelynek nincsenek határai, dinamikusan változik, és ilyen módon nehezen kontrollálható, felügyelhető.

2.1. Mobilbiztonsági kockázatok

Természetesen a mobilbiztonság esetében is igaz, hogy csak akkor lehet hatásos védelmet felépíteni, ha ismerjük a kockázatokat. A veszélyforrások bizonyos szinten általánosíthatók, ugyanakkor fontos hangsúlyozni, hogy a mobilizációval, illetve a mobil munkavégzéssel összefüggő kockázati tényezőket az egyes szervezeteknek saját maguknak kell felmérniük, értékelniük, priorizálniuk, hiszen a kockázatarányos biztonság követelményeinek csak így lehet megnyugtató módon megfelelni. A következőkben azokat a fontosabb fenyegetettségeket vesszük sorra, amelyeket mindenképpen mérlegelni kell a kockázatértékelés során.

A mobil eszközök, különösen az okostelefonok és a táblagépek vállalati és intézményi környezetekben való elburjánzásával az IT-biztonságért felelős szakemberek vállára nehéz teher került. Különösen azért, mert rövid idő alatt a céges és a magán készülékek furcsa szimbiózisba kerültek, és a kontrolljuk roppant körülményessé vált. Persze lehetett volna azt mondani, hogy egy adott szervezetnél munkaidőben nem lehet használni a magántulajdonú eszközöket, de hamar kiderült, hogy ez mind az üzleti, mind a felhasználói érdekekkel szembe megy, és egy csapásra semmibe veszi az úgynevezett BYOD (Bring Your Own Device) trendeket. Ráadásul a vállalati tulajdonban lévő eszközök ettől még ugyanúgy kiszolgáltatottak maradtak volna. Ezért napjaink mobilbiztonságának fő csapásirányát egyértelműen az egységesített, jól felügyelt, fenyegetettség- és kockázatközpontú megközelítések uralják, amik az adatbiztonságot éppúgy középpontba helyezik, mint az adatvédelmet.

A mobilbiztonsági kockázatok képzeletbeli toplistájának élmezőnyében nem más szerepel, mint maga a mobilitás. A legtöbb fenyegetettség ugyanis ahhoz kapcsolódik, hogy a felhasználók szabadon hordozzák az okostelefonjaikat, táblagépeiket, ami nemcsak azzal jár, hogy e – sok esetben értékes üzleti és személyes adatokkal telezsúfolt – készülékek elveszhetnek, elkallódhatnak és idegen kezekbe kerülhetnek, hanem azzal is, hogy a felhasználók azokat nem biztonságos hálózatokhoz csatlakoztatják, kétes szoftvereket töltenek le rájuk stb.

A távoli munkavégzés lehetővé tétele megkérdőjelezhetetlen előnyökkel jár egy szervezet számára. Növeli az alkalmazottak elégedettségét, rugalmasabbá teszi a munkavégzést, és a költségmegtakarításból is kiveheti a részét. Eközben azonban kockázatokat is felvet. Elég, ha csak arra gondolunk, amikor egy alkalmazott az okostelefonjával (vagy akár a notebookjával) akar hozzáférni a munkahelyi fájljaihoz, alkalmazásaihoz vagy éppen az üzleti levelezéséhez akár egy kávézó nyilvános WiFi-jének segítségével. Ez esetben egy csapásra válhatnak teljesen kiszolgáltatottá a céges adatok, a felhasználónevek, a jelszavak és az üzleti kommunikáció. Rosszabb esetben pedig az adott mobil „ugródeszkává" válik a támadók számára, akik azon keresztül érhetik el a vállalati IT-erőforrásokat.

A mobilkészülékekre komoly veszélyt jelentenek a mobilvírusok és a kártékony funkciókkal felvértezett alkalmazások. Ezek az esetek többségében adatlopásra és kémkedésre specializálódnak: könnyedén képesek kiszivárogtatni a címjegyzékeket, az üzeneteket és a tárolt fájlokat, miközben a felhasználó minden lépését követik. Más károkozók közvetlen pénzszerzési célokat szolgálnak a csalók számára, amit leggyakrabban emelt díjas SMS-üzenetek küldözgetésével valósítanak meg.

Az újabb mobil malware-ek pedig már a zsarolástól sem riadnak vissza, és a képernyő zárolásával, rosszabb esetben a mobilon tárolt fájlok titkosításával okoznak károkat, majd váltságdíjat követelnek a készülék tulajdonosától a helyreállításhoz szükséges információkért cserébe. Vagyis az okostelefonok, táblagépek világában is letették a névjegyüket a ransomware programok.

Hiba lenne azt gondolni, hogy a mobilbiztonság szempontjából csakis az ártalmas programok vezethetnek károkozásokhoz. Kockázatkezelésre – csakúgy, mint például a PC-knél – az operációs rendszerek és a legális szoftverek esetében is szükség van. A problémát pedig nem kis mértékben tetézi, hogy a patch-elési folyamat már a gyártók, fejlesztők oldalán is gyakorta akadozik. A két legnépszerűbb mobil operációs rendszer, az Android és az iOS is kedvelt azon biztonsági kutatók körében, akik sérülékenységek feltárásával foglalkoznak. Sokszor jutalmazási programok keretében végzik a munkájukat, és pénzdíj ellenében osztják meg a Google és az Apple fejlesztőivel a felfedezéseiket. A kimutatott sebezhetőségeket e két cég munkatársai általában gyorsan javítják. Az Apple esetében a frissítések többnyire havi rendszerességgel jutnak el a készülékekre, míg ez a folyamat az Android érában már sokkal aggasztóban zajlik. A Google által támogatott Nexus készülékek kivételével a gyártók belátása szerint válnak elérhetővé a patch-ek, sokszor hónapokkal a biztonsági rések feltárását követően. Sajnos az sem szokatlan jelenség, hogy egy-egy viszonylag régebbi típus már nem is kapja meg a szükséges foltokat. A kedvezőtlen androidos helyzetet tovább tetézi, hogy a platform nagyon fragmentált, aminek eredményeként olyan eszközöket kell védeni, amik különféle verziójú operációs rendszereket futtatnak. Nyilván a heterogenitás kockázatait sem szabad figyelmen kívül hagyni.

A mobil alkalmazások sebezhetőségei minden platformot közel azonos módon érintenek. Mind a külső fejlesztők által készített, mind a belső fejlesztésű szoftverek biztonsági réseivel számolni kell a fenyegetettségek listájának összeállításakor. A tapasztalatok azt mutatják, hogy a legtöbb probléma a mobil alkalmazások és az azokhoz tartozó szerverek közötti kommunikáció biztonságával, a tanúsítványok kezelésével, a készülékeken tárolt adatok védelem (titkosítás) nélkül tárolásával és az authentikációs mechanizmusokkal kapcsolatban szokott felmerülni.

Az alkalmazásbiztonság szempontjából külön ki kell térni a rootolt (Android) vagy jailbreakelt (iOS) készülékekre. Ezek ugyanis további aggályokat támasztanak, mivel egy ilyen készüléken tulajdonképpen bármi megtehető, egyebek mellett a védelmi mechanizmusok is megkerülhetővé válhatnak.

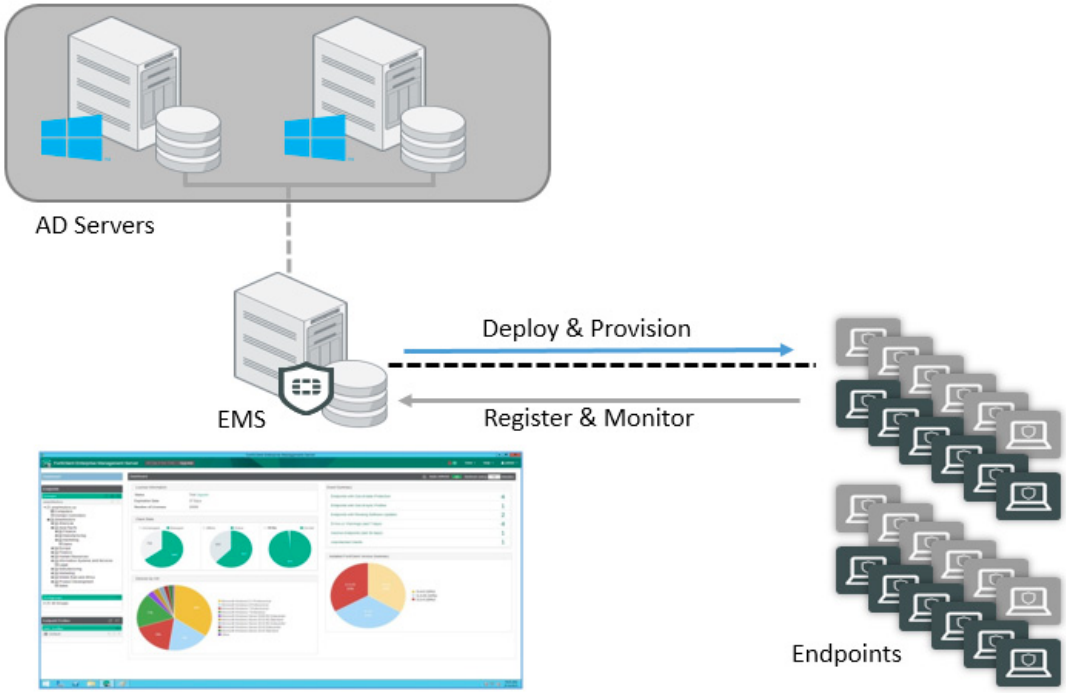
Természetesen a kockázatok listáját olyan „univerzális”, platformfüggetlen fenyegetettségek is növelik, mint amilyen például az adathalászat vagy az üzleti levelezésekkel kapcsolatos visszaélések, azaz a BEC (Business E-mail Compromise).

2.2. Kezdjük a védekezést

Amennyiben az adott szervezetre vonatkozó mobilbiztonsági kockázatok felsorakoztatása megtörtént, akkor kezdetét veheti a védelmi intézkedések kidolgozása. A veszélyforrások számbavétele után hamar láthatóvá válik, hogy a biztonság csak akkor lesz képes megfelelni a zártság, a folytonosság és a kockázatarányosság elveinek, ha teljes védelmi architektúrában gondolkodunk, és a mobilbiztonságot összekapcsoljuk az egyéb védelmi területekkel. Mindez nem kizárólag a digitális értékek megóvását szolgálja, hanem a felügyeletet és az üzemeltetést is nagymértékben megkönnyítheti.

A védelem kiépítése során arra kell törekedni, hogy a mobil eszközök esetében megfigyelhető nagyfokú heterogenitást legalább a biztonsági technológiák szintjén ne tetézzük tovább. Vagyis célszerű olyan gyártó által biztosított platform vagy megoldás mellett letenni a voksot, amely jól integrálható a meglévő rendszerekhez. E megfontolás figyelembevétele nélkül hamar ki fog derülni, hogy a védelem nem lesz hatékony, az informatikai és biztonsági személyzet pedig leterheltté válik. Ez végső soron ahelyett, hogy a biztonságot növelné, a káoszt és az elégedetlenséget fogja fokozni. Nem utolsó sorban pedig hamis biztonságérzet alakulhat ki, ami szintén a támadók kezére játszik.

Ha megvizsgáljuk az alábbi, Fortinet által készített ábrát, akkor egyszerű, ámde annál szemléletesebb módon tárul elénk, hogy egy védelmi megoldásnak miként kell beépülnie egy meglévő infrastruktúrába:



1. ábra: Az informatikai infrastruktúra és a védelmi technológiák integrációja
Forrás: Fortinet, Inc.

Az ábrából kitűnik, hogy a biztonságot felügyelő összetevők a középpontban csoportosulnak, és szorosan kapcsolódnak az Active Directory címtárhoz, ami nyilván bármilyen más LDAP megoldás is lehetne. A központosított felügyeletet, vezérlést és a biztonsági házirendek kialakítását, betartatását elősegítő (EMS – Enterprise Management Server) összetevők az AD mellett erős viszonyt ápolnak a végpontokkal, amik lehetnek szerverek, asztali, illetve hordozható munkaállomások, és nem utolsó sorban mobil eszközök. Az ábrán e készülékek szétválasztására szándékosan nem került sor, ugyanis pontosan az a cél, hogy a védelem hatóköre alá bevont okostelefonokat és tableteket éppolyan biztonságmenedzsment vegye körül, mint például a PC-ket.

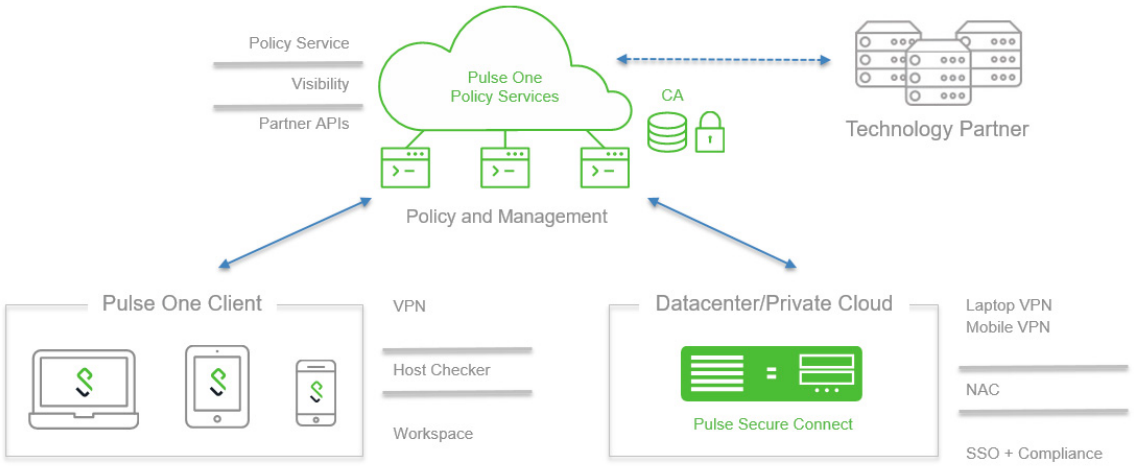
Természetesen a fenti, leegyszerűsített ábra a végtelenségig bővíthető, és számos egyéb biztonsági technológiával egészíthető ki. A következő kérdés egyből adódik: milyen védelmi szolgáltatásokra van szükség?

2.3. Védelmi funkciók

Mivel a megvalósítandó védelmi szolgáltatások és intézkedések alapvetően épülnek a szervezetfüggő kockázatfelmérés eredményeire, ezért a szükséges funkciók meghatározását is az egyedi igények mentén kell megtenni. Az alábbiakban egy olyan – a Pulse Secure iránymutatásai alapján készült – lista látható, amely a leggyakrabban szóba kerülő védelmi képességekre világít rá.

Alkalmazásbiztonság – mobil alkalmazások telepítésének kontrollja – távoli szoftvertelepítés – fehér- és feketelisták alkalmazása – alkalmazáseltávolítás akár távolról	**Adatbiztonság** – szeparált fájlrendszer – másol/beilleszt műveletek tiltása az izolált adatterületek között – távoli zárolás és adattörlés
Végpontok menedzsmentje – csoport, felhasználó, alkalmazás és eszköz alapú biztonság – többszintű házirendkezelés – központosított felügyelet – jelentéskészítés	**Adatvédelem** – A magán és a vállalati adatok, alkalmazások, illetve kommunikáció szétválasztása.
Eszközkezelés – rootolás/jailbreakelés detektálása – USB-debug tiltása – teljes körű titkosítás	**Azonosítás** – eszközökön az authentikáció megkövetelése – jelszóházirendek érvényre juttatása
Távoli hozzáférések kezelése – VPN-elérés biztosítása – tanúsítványalapú hitelesítés – helyfüggő bejelentkeztetés	**IOS-specifikus védelem** – iCloud mentés tiltása – Siri tiltása – képernyőképek készítésének meg-akadályozása – beépített kamera tiltása

A fenti szolgáltatások megvalósítására alkalmas architektúra felépítése:

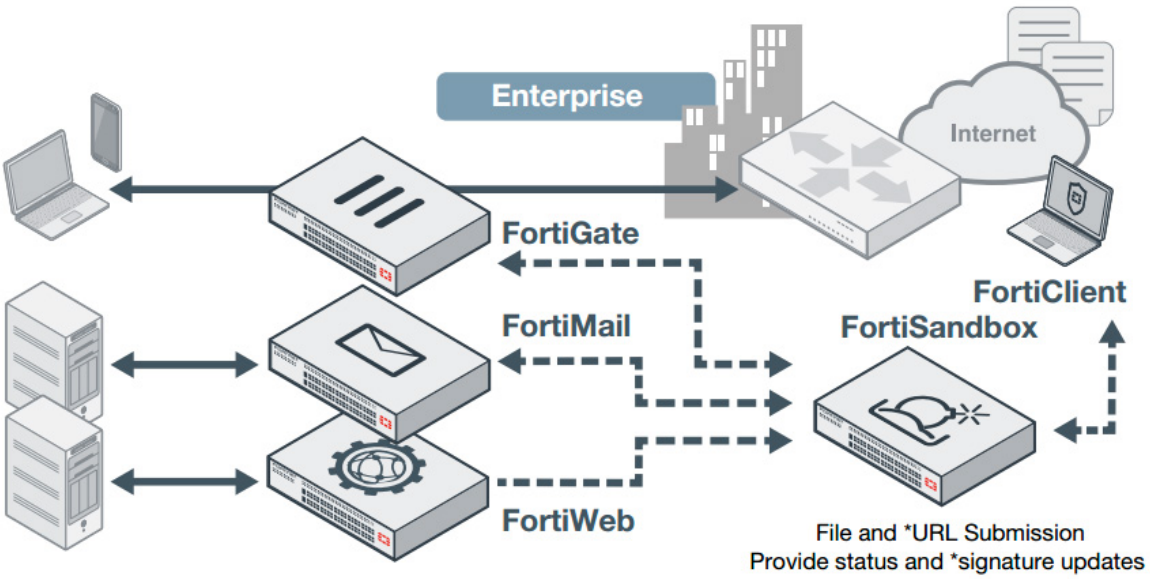


2. ábra: Korszerű mobilbiztonsági architektúra
Forrás: Pulse Secure, LLC

2.4. Alkalmazásbiztonság

A mobilbiztonsági kockázatok kezelésének egy jelentős része az alkalmazásokkal kapcsolatos nehézségek leküzdésére irányul. Ez persze nem meglepő, hiszen a mai okostelefonokra, táblagépekre pillanatok alatt lehet telepíteni szoftvereket, elég csak ellátogatni valamely alkalmazásáruházba. Ezt a felhasználók is megtehetik, sőt számukra mindez sokkal egyszerűbb, mint például egy átlagos Windows-os alkalmazást installálni. Így aztán a mobil készülékeken gyakorta hemzsegnek a legkülönfélébb programok, amik között sajnos ártalmasak is feltűnnek. Különösen akkor, ha a felhasználó nem a hivatalos alkalmazásboltokból (Google Play, Apple App Store) szerzi be a szoftvereket. Noha például a Playről is több esetben bizonyosodott már be, hogy a háttérrendszere nem minden esetben képes detektálni a káros alkalmazásokat, azért a kockázatok még mindig jóval kisebbek, mint ami például egy kínai, orosz stb. áruház kapcsán felmerül. Ezért vállalati környezetben lényeges, hogy kikényszerítsük a megbízható helyekről történő, akár fehér- vagy feketelistákkal körülbástyázott alkalmazástelepítést. Eközben annak a lehetőségét is meg kell teremteni, hogy ha véletlenül vagy szándékosan mégis felkerül egy káros app egy vállalati adatok kezelésére is használt mobilra, akkor azt a lehető leggyorsabban, akár távolról is el lehessen távolítani.

Vannak olyan gyártók, amelyek már elkezdték a sandbox technológiák mobil alkalmazásbiztonságba történő bevonását. Ennek köszönhetően még a szoftverek telepítése előtt a vállalati vagy akár egy külső biztonsági cég által üzemeltetett sandbox környezetben alaposan górcső alá kerülhetnek a programok. Így még időben kiszűrhetővé válhatnak a nemkívánatos alkalmazások. Természetesen mindez csak akkor tud igazán hatékonyan működni, ha a sandbox integrált részét képezi a teljes védelmi arzenálnak.



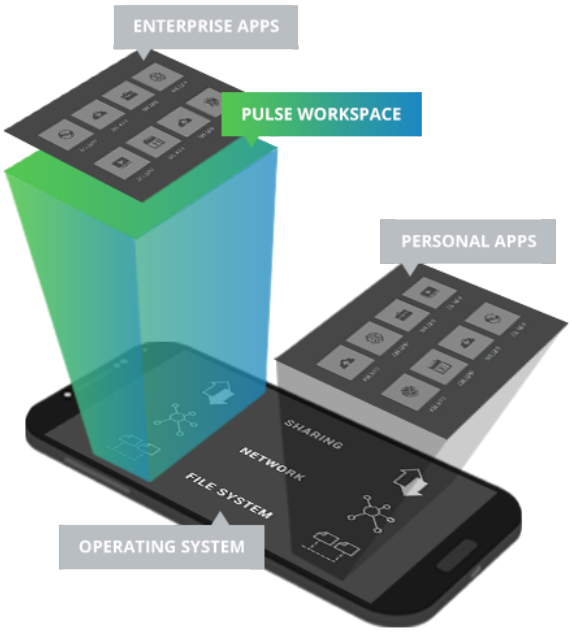
3. ábra: Sandbox integráció
Forrás: Fortinet, Inc.

Az alkalmazásbiztonság egy következő szintjére azok a technológiák vezetnek el bennünket, amelyek izolációval biztosítják a károk megelőzését. Az első generációs megoldások többnyire meglehetősen komoly korlátokat állítottak a szervezetek elé, mivel nem voltak képesek minden alkalmazás esetében garantálni az üzemszerű működést. A használatukhoz gyakorta magukat az appokat

is módosítani kellett, és SDK-k, valamint app wrapper technikák révén lehetett elérni a szoftverek védelembe történő bevonását.

Az újabb generációs alkalmazásvédelmek már korántsem ennyire rugalmatlanok. A Pulse Secure által kifejlesztett technológia az alkalmazás virtualizáció vívmányainak kihasználásával bármilyen Android és iOS kompatibilis szoftvert képes biztonságos környezetbe illeszteni, majd annak használatát a vonatkozó biztonsági házirendeknek megfelelően szabályozni.

A virtualizáció védelembe történő bevetésénél azonban nem állt meg a fejlődés, ugyanis egy manapság szintén divatos technológiai is a középpontba került, amely nem más, mint a konténerizáció. Esetünkben ennek azért van lényeges szerepe, mert a segítségével a felhasználó készülékén létrehozható egy üzleti és egy magán adatterület, ami aztán egymástól függetlenül menedzselhető, kezelhető. Az izoláció szigorú és mély szintű annak érdekében, hogy az üzleti és a személyes alkalmazások, adatok ne keveredhessenek.



4. ábra: Szeparált munkaterületek a mobil készülékeken
Forrás: Pulse Secure, LLC

Az alkalmazásbiztonsági funkciók sorában a következő lépés a szoftverek sérülékenységvizsgálata. Egy szervezetre mind a nyilvánosan elérhető – sokszor biztonságosnak gondolt – alkalmazások, mind a saját fejlesztésű appok sebezhetőségei veszélyt jelenthetnek. Mielőtt a biztonsági vagy informatikai csapat egy alkalmazás használatát jóváhagyja, vagy a fejlesztett szoftvert átveszi, azelőtt gondosan elvégzett vizsgálatokat, teszteket kell végrehajtania. Sokféle módszer kínálkozik minderre, kezdve az adott program által igényelt engedélyek szemrevételezésétől, az adattárolási és kommunikációs eljárások elemzésén át egészen a statikus és dinamikus kódelemzésekig bezárólag. Ezek a feladatok sok erőforrást köthetnek le, de sajnos ezzel még nincs vége a teendőknek. A mobil appok a hagyományos szoftvereknél is gyorsabban változnak, rendszeresen jelennek meg az újabb verzióik, ami azt is jelenti, hogy az említett biztonsági vizsgálatokat nem elég egyszer lefolytatni, rendszeres tesztekre van szükség. Amennyiben egy olyan mobil alkalmazás engedélyeztetéséről van szó, amelyet például az oktatási intézmények a diákok rendelkezésére bocsátanak, vagy egy önkormányzat lakossági szolgáltatásokat biztosít azon keresztül, akkor a sérülékenységekből fakadó kockázatok kezelését kiemelten kell kezelni.

A fentiek a 41/2015. (VII. 15.) BM rendeletben meghatározott alábbi funkciókat valósítják meg:

- Sérülékenységteszt
- Frissítési képesség
- Előzetes tesztelés és megerősítés
- Nem futtatható szoftverek
- Futtatható szoftverek
- Elektronikus információs rendszerelem leltár
- A szoftverhasználat korlátozásai
- A felhasználó által telepített szoftverek
- Kártékony kódok elleni védelem

2.5. Adatvédelem

Legyen szó bármilyen hordozható, adattárolásra alkalmas eszközről, az elvesztésből, eltulajdonításból eredő kockázatok fokozottan jelentkeznek. Amennyiben egy ilyen nemkívánatos esemény bekövetkezik, és az adott készülék (vagy adathordozó) nincs kellően védve például megfelelő hitelesítéssel és titkosítással, akkor annak beláthatatlan következményei lehetnek. Már csak azért is, mert az okostelefonok, táblagépek tárolókapacitásának folyamatos növekedésével egyre nagyobb mennyiségben kerülnek fel rájuk értékes adatok. Ez pedig az adatlopás, illetve az adatszivárgás veszélyét is növeli.

Amennyiben egy mobilnak nyoma veszik, akkor azt célszerű zárolni és/vagy a rajta tárolt adatokat törölni. Ehhez természetesen megfelelő eszközmenedzsment eszközökre is szükség van. Az első generációs MDM (Mobile Device Management) megoldások is tudták már mindezt. Sőt napjainkban egyes gyártók, illetve biztonsági cégek is nyújtanak olyan szolgáltatásokat, amik segítségével az ilyesfajta műveletek távolról (interneten keresztül) elvégezhetők.

A korai MDM technológiáknak azonban viszonylag hamar felszínre tört az egyik nagy hátrányuk: ha távoli adattörlést kellett végezni, akkor minden veszett. Ez pedig komoly adatvédelmi aggályokat vetett fel azon mobilok esetében, amelyek a felhasználók tulajdonában voltak. Mit is gondolt egy alkalmazott: „A cégem miért törli le a személyes adataimat, telefonkönyvemet, családi fényképeimet?”. A felvetés nagyon is jogos volt, miközben a cég csak a saját adatait akarta védeni.

Az ellentmondás feloldása érdekében a gyártók és a biztonsági cégek arra a következtetésre jutottak, hogy a magán és a vállalati adatokat el kell szeparálni. Vagyis nemcsak a már korábban említett alkalmazásizolációra van szükség, hanem az adatok, sőt a teljes kommunikáció felosztására is. Amennyiben ez megvalósul, akkor a szervezet kizárólag a vállalati munkaterület felett rendelkezhet, azt törölheti, kontrollálhatja, monitorozhatja, felügyelheti. A felhasználó magán adatterületére pedig még a vállalati adminisztrátoroknak sincs rálátásuk, tehát a privát szféra nem sérül. Mindez nagymértékben megkönnyíti a készülékek ellopásakor meghozandó védelmi intézkedéseket (például az adattörlést), de akkor is jól jöhet, amikor az alkalmazott elhagyja a munkahelyét. Ekkor a céges adatokat törlik az okostelefonjáról, míg a saját adatai, fényképei, videó sértetlenek maradnak.

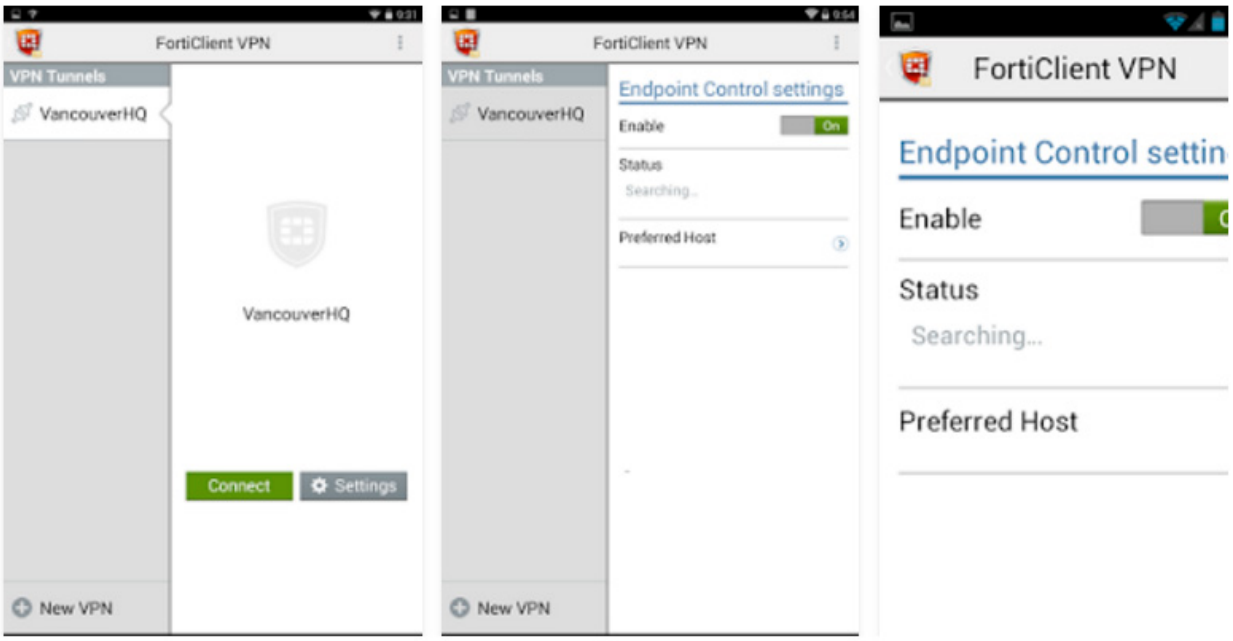
A fentieken túl a privát és az üzleti területek szétválasztásának van még egy további fontos előnye, ami az adatszivárgások megelőzésében, azaz a DLP (Data Loss Prevention) technológiák bizonyos szintű kiterjesztésében mutatkozik meg. Ennek köszönhetően az adott szervezet a vállalati munkaterület kapcsán meghatározhatja, hogy azt milyen adatok hagyják el. Tilthatja a másol/beilleszt műveleteket, a képernyőképek létrehozását vagy akár az iCloud mentések készítését is.

2.6. *Távoli hozzáférések védelme*

A mobil munkavégzés által jelentett rugalmasság, gyorsaság és kényelem akkor nyeri el értelmét, ha egy szervezet lehetőséget ad a munkavállalói számára, hogy a vállalati IT-erőforrásokat távolról elérhessék, legyen szó adatbázisokról, alkalmazásokról, intranetes weboldalakról, fájlokról vagy levelezésről. Ugyanakkor ehhez szigorú kontrollkörnyezetet kell felépíteni, hogy átláthatóvá és felügyelhetővé váljanak a különféle hozzáférések.

A távoli elérések védelmében az egyik legalapvetőbb szerepet a VPN (Virtual Private Network) technológiák játsszák. Ezek nem kizárólag mobilbiztonsági kockázatokat kezelnek, hiszen akár telephelyek közötti összeköttetést is biztosíthatnak. Ennek ellenére mind a biztonság, mind az üzemeltetés szempontjából az az ideális, ha az általános VPN-hozzáféréseket biztosító megoldások mobil eszközök felé történő kiterjesztése valósul meg.

A virtuális magánhálózatok esetében napjainkban az IPsec, illetve az SSL VPN technológiák hódítanak. Ezekhez a legtöbb gyártó mobil klienseket is biztosít, így semmi akadálya nincs annak, hogy egy okostelefonról vagy táblagépről csatlakozzon a felhasználó a céges hálózathoz. Ugyanakkor a korszerű eszközök olyan extra szolgáltatásokat is biztosítanak, amelyeket célszerű fontolóra venni egy beruházás előtt, mert valóban hasznosnak bizonyulhatnak a mindennapokban, sőt egyes megfelelőségi követelmények miatt akár kötelező is lehet a használatuk. Például, ha egy vállalatnak PCI DSS megfelelőségét kell igazolnia, akkor rögtön elengedhetetlenné válik a távoli hozzáférések kétfaktoros azonosítással történő ellátása. Emellett célszerű olyan VPN-eszközt választani, amely képes együttműködni a meglévő címtárakkal és a mobil eszközmenedzsmenttel. Fontos, hogy a megoldás megfelelő szinten naplózzon, és a munkamenetek teljes életciklusát lefedje, beleértve a kapcsolati időtúllépésből eredő teendőket is. Hasznos lehet, ha képes az egyszeres bejelentkeztetések (SSO) kezelésére, és az már csak hab a tortán, ha még lokáció alapú házirendkezelést is biztosít. Ez utóbbi esetben lehetővé válhat, hogy a felhasználó – az eltérő kockázati szinteknek megfelelően – más-más hozzáférési jogokat kapjon attól függően, hogy az otthonából vagy éppen egy kávézóból csatlakozik a munkahelye hálózatához.



5. ábra: FortiClient VPN alkalmazás Androidra
Forrás: Google Play, Google Inc.

Mielőtt egy-egy technológia mellett letesszük a voksunkat célszerű azt is átgondolni, hogy milyen szintű rendelkezésre állásra van szükség. Amennyiben a szolgáltatáskiesések nem, vagy csak kis mértékben tolerálhatók, akkor olyan védelmet kell választani, amely támogatja a redundáns működést (akár aktív/passzív, akár aktív/ formában).

Pulse Secure Appliance
Forrás: Pulse Secure, LLC

A távoli elérések biztosítása során érdemes külön figyelmet fordítani a fájlok, megosztások védett hozzáférhetővé tételére. Ennek oka, hogy sok szervezetnél megfigyelhető a Dropbox és egyéb, felhős tárhelyszolgáltatások kontroll nélküli igénybevétele felhasználói oldalon is. Ez pedig az adatszivárgások kockázatát növeli. Ezért sokkal célravezetőbb, ha a saját megosztásokat tesszük hozzáférhetővé távolról, kellően felügyelt módon.

A fentiek a 41/2015. (VII. 15.) BM rendeletben meghatározott alábbi funkciókat valósítják meg:

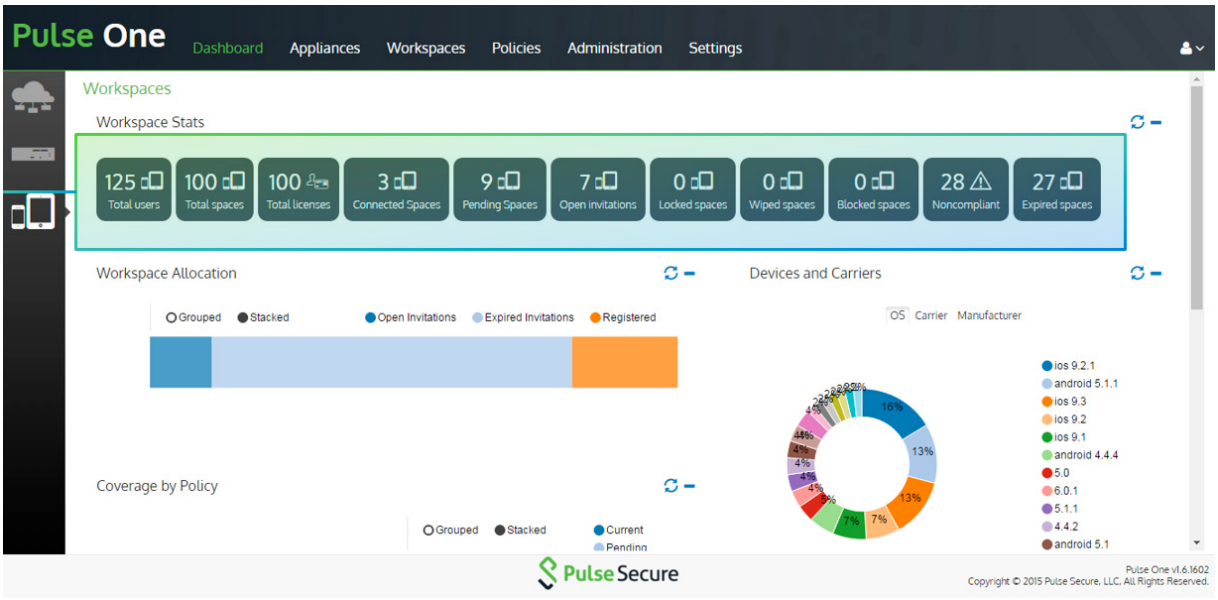
- Hozzáférés az adatátviteli eszközökhöz és csatornákhoz
- Azonosítás és hitelesítés
- Hozzáférés ellenőrzés

2.7. Minden szál egybefut

Az eddigiekben ismertetett mobilbiztonsági megfontolásokból láthatóvá vált, hogy egy igen összetett és szerteágazó, sokszor nagyon heterogén környezeteket lefedő védelmi területről van szó. Ezért egy vállalat, intézmény életében már néhány tucat mobil eszköz kordában tartása is lehetetlen feladatnak bizonyulhat akkor, ha nem áll rendelkezésre megfelelő biztonságmenedzsment támogatás. Márpedig általában ennél jóval több készülék felügyeletét kell ellátni, amelyek több száz vagy ezres nagyságrendben kerülhetnek be a vállalatokhoz.

Egy korszerű mobilfelügyeleti rendszer akkor tud igazán hatékony lenni, ha minden eszközt, alkalmazást lefed. Nagyon előnyös helyzet alakítható ki abban az esetben, ha ez a felügyelet összekapcsolódik egyéb központi védelmi és riasztó rendszerekkel, SIEM (Security Information and Event Management), illetve naplózó megoldásokkal.

Egy jól használható, központi mobilfelügyelet lehetőséget ad a házirendek létrehozására, karbantartására, csoport-, felhasználó- és eszközszintű szabálydefiniálásra, az előírások betartatására, és minden olyan tevékenység egy felületről történő elvégzésére, amelyeket a korábbiakban említettünk, beleértve a kontrollált alkalmazástelepítést, valamint a távoli szoftvereltávolítást, törlést és zárolást is. Mindezek mellett nélkülözhetetlen a jelentéskészítés, amely biztonsági, üzemeltetési és compliance szempontból is lényeges.



6. ábra: Pulse One menedzsment felület
Forrás: Pulse Secure, LLC

Mivel a mobil eszközök és azok biztonsága kapcsán sok teendővel kell számolni, ezért minden esetben megfontolás tárgyát kell képeznie az automatizálhatóságnak. Mindezt elő lehet segíteni úgy, hogy a mobil eszközfelügyelet (jó esetben teljesen integrált módon) kiegészül egy önkiszolgáló felülettel. Ezen a felhasználók a számukra engedélyezett alapvető tevékenységeket (például jelszóváltoztatást) végrehajthatják anélkül, hogy ehhez a help desket kellene hívniuk. A mobil készülékek esetében egyes gyártók arra is adnak módot, hogy szigorúan szabályozott módon az új mobilok automatikusan bekerüljenek a rendszerbe, majd felkerüljenek rájuk a felhasználó üzleti célú alkalmazásai és akár a levelezési beállítások is. Ezzel nemcsak a manuális konfigurálásban rejlő hibalehetőségeket lehet kizárni, hanem számottevő emberi erőforrás is felszabadulhat az IT-csoportban.

A fentiek a 41/2015. (VII. 15.) BM rendeletben meghatározott alábbi funkciókat valósítják meg:

- Munkakörök, feladatok biztonsági szempontú besorolása
- A biztonsági események kezelése
- Automatikus eseménykezelés
- Információ korreláció
- Az elektronikus információs rendszer felügyelete
- Automatizálás
- Riasztás

2.8. *Részösszefoglalás*

Aki mobilbiztonsággal foglalkozik, az nagyon szövevényes terepen dolgozik. Márpedig állni kell a sarat, mivel egy kritikus védelmi területről van szó, amit nem szabad félvállról venni. Jó hír, hogy gondosan megtervezett, alaposan átgondolt, kellő szintű technológiai támogatással megerősített rendszerrel a kockázatok nagymértékben csökkenthetők, és a megfelelőségi követelmények teljesíthetővé válhatnak. Mindehhez újfajta szemléletre van szükség, és többrétegű, magas fokon integrált rendszer kialakítására kell törekedni. E szemléletet pedig a felhasználók felé is tolmácsolni kell, hiszen az emberi tényezők kezelése, a biztonságtudatosság fokozása a mobilbiztonság területén hatványozottan érvényesül.

3. ESET Endpoint Security for Android, Remote Administrator (MDM) modellje

3.1. Bevezetés

A kínált megoldás *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet* ***3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK*** bekezdésének ***3.3.11. Rendszer és információ sértetlenség***, azon belül a ***3.3.11.4.*** pont ***Kártékony kódok elleni védelem***nek feleltethető meg.

3.2. ESET Remote Administrator feladata

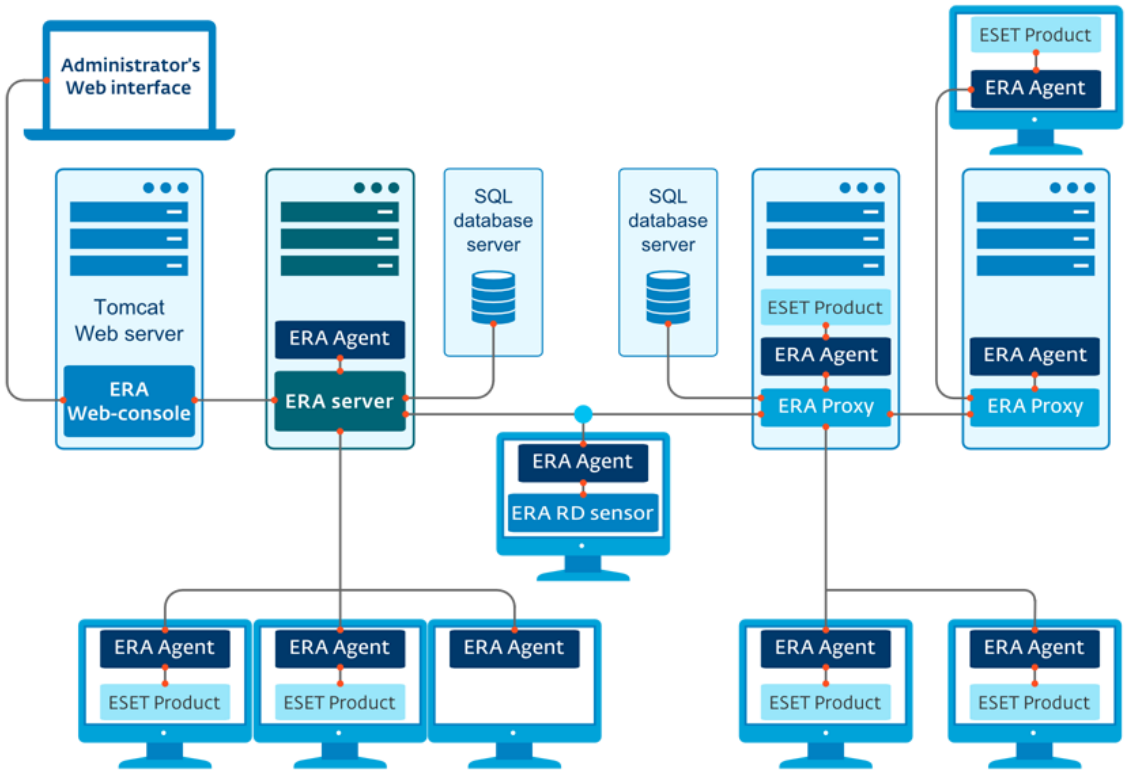
A teljes számítógépes hálózat, valamint kapcsolódó mobil eszközök vírus- és kémprogramok elleni védelme bárhonnan, egyetlen helyről menedzselhető. A rendszer segítségével azonnal információ kapható a munkaállomások, szerverek, valamint mobil eszközök vírusvédelmének állapotáról, frissítéseiről, riasztásairól. A felügyelt számítógépeken kényszerített csoportházirend alkalmazható, a beállítás-módosítások és a különböző víruskeresési feladatok távolról végrehajthatóak. A távadminisztráció segítségével nagyobb hálózatok vírusvédelme is átláthatóvá válik, a program távoli telepítési lehetőséggel, elemzésekkel és statisztikákkal segíti a rendszergazdák munkáját. A központi menedzsment működéséhez TCP/IP kapcsolat elegendő. Active Directory vagy NT domain megléte nem szükséges, de ha rendelkezésre áll, használható.

3.2.1. A távadminisztrációs rendszer részei

A távadminisztrációs program struktúrájának központi része az ESET Remote Administrator Server (röviden ERAS), amely egy szolgáltatásként fut a szerverként működő gépen. Ezzel áll összeköttetésben az ESET Remote Administrator Web Console, amelyen egy bárhonnan indítható webes konzol, ezen a felületen végezhető el a védelemmel kapcsolatos bármely feladat. Minden olyan számítógépre (mobil eszközöket kivéve), amelyet központilag szeretnénk kezelni, szükséges feltelepíteni az ESET Remote Administrator Agent programot. Ez a szolgáltatás végzi a kommunikációt az adott kliensen telepített végpontvédelemmel, ez továbbítja a klienssel kapcsolatos információkat és eseményeket a távadminisztrációs szerver felé és ez hajtatja végre a szerveren létrehozott feladatokat és módosításokat a klienseken. Tulajdonképpen tekinthető egyfajta lokálisan telepített, leegyszerűsített távadminisztrációs szervernek. Azáltal, hogy lokálisan tárolja a kliensekre vonatkozó policy-ket (házirendeket), csoportbeállításokat és az adott eseményekre beállított automatikusan futtatandó feladatokat, a kliens gépek távadminisztrációja offline állapotban is aktív marad.

A távadminisztrációs struktúra további komponensei a webes konzol felületét biztosító Apache Tomcat Server, a kliensek adatbázisát kezelő Microsoft SQL Server Express, a hálózaton található védelem nélküli kliensek felderítését végző Rogue Detection Sensor és az opcionálisan telepíthető, a távadminisztrációs szerver felé irányuló kommunikációt összefogó és ezáltal minimalizáló Remote Administrator Proxy. Ez a proxy nem összekeverendő az Apache HTTP Proxy-val, amely a vírusdefiníció adatbázis tükrözését valósítja meg http protokollon keresztül.

A Mobil Device Connector szintén opcionálisan telepíthető, az Android-os okoseszközök védelmét ellátó ESET Endpoint Security for Android programok központi kezeléséhez szükséges és az iOS eszközök központi menedzsmentjét biztosítja.



7. ábra: ESET Remote Administrator részei és egymáshoz való viszonyuk

3.2.2. Használt portok

A 7. ábrán látható hálózatok kapcsolatokat a rendszer különböző szolgáltatások igénybevételével biztosítja. Az alábbi táblázat felsorolja a használt TCP portokat (amennyiben a hálózaton a szerver és a kliensek közé tűzfalak is vannak telepítve, akkor azokon e TCP portok engedélyezése szükséges).

Protokoll	Port	Használat	Leírás
TCP	2222	ERA Server figyeli	Kommunikáció az kliensek és az ERA Server között
TCP	2223	ERA Server figyeli	Kommunikáció az ERA Web Console és az ERA Server között, távtelepítéshez használatos
UDP	1237	Broadcast	Wakeup call küldésére
TCP	2223		ERA Web Console
TCP	443		HTTP SSL Web Console hívás
TCP	3128		HTTP Proxy (frissítés gyorsítótárazás)
TCP	2222		Proxy
TCP	139	Célport az ERA Server szemszögéből	Az ADMIN$ megosztás használata
TCP	445	Célport az ERA Server szemszögéből	Közvetlen elérés a megosztott erőforrásokhoz TCP/IP-n keresztül a távtelepítéshez (alternatív megoldás a TCP 139 helyett)

Protokoll	Port	Használat	Leírás
UDP	137	Célport az ERA Server szemszögéből	Névfeloldás a távtelepítés folyamán
UDP	138	Célport az ERA Server szemszögéből	Böngészés a távtelepítés folyamán

3.2.3. Rendszerkövetelmények

Operációs rendszer	• Támogatott Windows operációs rendszerek listája • Támogatott Linux operációs rendszerek listája
Adatbázis	• MySQL 5.5 vagy újabb • Microsoft SQL Server
Egyéb	• Java Runtime Environment 7 vagy újabb

3.2.4. Hardverkövetelmény

Az ESET Remote Administrator Server zökkenőmentes működéséhez az alábbi konfiguráció javasolt:

- 2 GHz Dual-Core processzor
- 4 GB RAM
- 20 GB szabad lemezterület
- 1 Gbps Network Adapter

3.3. ESET Endpoint Security for Android

Az ESET Endpoint Security for Android olyan károkozók ellen nyújt gyors és megbízható védelmet, amelyek célpontja az Android operációs rendszert futtató okostelefonok és a táblagépek. Az alkalmazás heurisztikus vírusvédelmének és alacsony erőforrásigényének köszönhetően a telefon vagy tablet teljesítményének befolyásolása nélkül képes teljes körű védelmet nyújtani, az SMS/MMS spam-szűrő pedig a kéretlen üzenetektől is megkíméli a felhasználót. Ezeken kívül jelszavas védelmet, lopásvédelmi modult (SIM kártya azonosítás, táv-törlés, táv-lezárás, GPS helymeghatározás), hívás szűrést, eszközbiztonsági modult is tartalmaz.

3.3.1. Tulajdonságok

Egyszerű használat

Az alkalmazás fejlesztésekor, a felhasználói élmény növelése érdekében a felhasználók valós szükségletei lettek középpontba állítva. Az új felhasználói felületnek köszönhetően annak használata, valamint a funkciók közötti navigálás érthetőbbé és egyszerűbbé vált. A program grafikus felületének struktúrája megegyezik az új ESET Endpoint megoldásokéval, beleértve az ESET Remote Administrator 6 menedzsment konzolt és az ESET Endpoint Antivirus/ESET Endpoint Security kliens szoftvereket is, így ismerős érzés lehet bármelyik termék használata anélkül, hogy korábban ismertük volna azt.

Alkalmazásfelügyelet

Az alkalmazásfelügyelet funkció lehetővé teszi a rendszergazdáknak, hogy figyeljék a telepített alkalmazásokat, letiltsák meghatározott alkalmazások elérését és csökkentsék a fertőzés kockázatát azáltal, hogy bizonyos alkalmazások eltávolítására kérik a felhasználókat. A rendszergazda az alkalmazásokra vonatkozó különféle szűrési módok közül választhat: kategóriaalapú letiltás, engedélyalapú letiltás, letiltás forrás szerint, manuális letiltás.

Továbbfejlesztett Antivírus modul

- Rövidebb valós idejű ellenőrzési idők
- Beépített ESET Live Grid
- 2 szintű ellenőrzés: optimalizált és mindenre kiterjedő
- Kézi indítású víruskereső háttérellenőrzés funkcióval
- Ütemezett ellenőrzés
- Ellenőrzés töltéskor: automatikusan elindul egy ellenőrzés a készülék tétlen állapotában (teljesen fel van töltve és egy töltőhöz csatlakozik)
- A vírusdefiníciós adatbázis frissítésével kapcsolatban a rendszergazda megadhatja a szokásos frissítések időzítését, és kiválaszthatja az eszközök által használt frissítési módot (rendszeres frissítés, tesztelési mód, helyi tükör)
- Az ellenőrzés eredményét tartalmazó részletes naplókat a rendszer elküldi az ESET Remote Administrator 6 alkalmazásnak.

Eszközbiztonság

Ezzel a funkcióval a rendszergazdák általános biztonsági házirendeket érvényesíthetnek több mobileszközön.

A rendszergazda például:

- megadhatja a képernyő-zárolási kódok minimális biztonsági szintjét és összetettségét;
- beállíthatja a sikertelen feloldási kísérletek maximális számát;
- megadhatja az időtartamot, amelyet követően a felhasználóknak módosítaniuk kell a képernyő-zárolási kódjukat;
- beállíthatja a zárolási képernyő időzítőjét;
- korlátozhatja a kamera használatát.

Üzenet megjelenítése

Készülékek távoli kezelésekor a rendszergazda egyéni üzenetet küldhet egy adott készüléknek vagy készülékek csoportjának. Így átadhat egy sürgős üzenetet a felügyelt készülékek felhasználóinak. Az üzenet felugró üzenet formájában jelenik meg, így nem kerüli el a felhasználó figyelmét.

Távoli kezelés

Az összes alkalmazás-beállítás konfigurálható és megadható távoli házirenden keresztül az Antivirus, az SMS- és hívásszűrő és az Eszközbiztonság beállításaitól az Alkalmazásfelügyelet korlátozásain át egyéb beállításokig. Ez lehetővé teszi a rendszergazdáknak a vállalati biztonsági házirend betartatását a teljes hálózatban, beleértve a mobileszközöket is.

Az ESET Endpoint Security for Android új verziója továbbfejlesztett jelentéskészítést tartalmaz, amely az ESET Remote Administrator Webkonzolról látható. Ez lehetővé teszi a rendszergazdáknak, hogy azonnal felismerjék a problémát okozó eszközöket, és megkeressék a probléma forrását.

Hívásblokkolás

Előre meghatározott vagy ismeretlen (a telefonkönyvben nem szereplő) számokról érkező hívások elutasítása akár előre megadott engedélyező/tiltó lista alapján.

Kéretlen SMS/MMS szűrés

Az SMS- és hívásszűrő védelmet nyújt a felhasználóknak a nemkívánatos hívásokkal, SMS- és MMS-üzenetekkel szemben. Ez a funkció kétféle szabályt kínál: a rendszergazdai és a felhasználói szabályokat, ahol a rendszergazdai szabályok mindig elsőbbséget élveznek.

Időalapú tiltás: a felhasználó vagy a rendszergazda letilthatja a megadott időben beérkező hívásokat és üzeneteket. A legutóbbi hívó vagy üzenetküldő, telefonszám, kapcsolatcsoport, rejtett vagy ismeretlen számok egyérintéses letiltására is lehetőség van.

Lopásvédelem

A lopásvédelmi funkciók lehetővé teszik a rendszergazdáknak a készülék védelmét és megkeresését az elvesztése, illetve ellopása esetén. A lopásvédelmi intézkedések az ERA alkalmazásból vagy távoli parancsokkal aktiválhatók.

Az ESET Endpoint Security for Android a korábbi verziójában is alkalmazott távoli parancsokat (Zárolás, Törlés, Keresés) használja. Emellett az alábbi teljesen új parancsok is elérhetők:

- Feloldás: Feloldja a zárolt készüléket.
- Gyári beállítások visszaállítása: A parancs gyorsan eltávolítja a készüléken elérhető összes adatot (a fájlok fejléce megszűnik), és visszaállítja a készüléket a gyári alapbeállításokra.
- Sziréna: Az elvesztett készülék zárolva lesz, és erős hangjelzést ad ki még akkor is, ha néma üzemmódra van állítva.

Megjegyzés

A következő funkciók nem elérhetőek azokon a táblagépeken, amelyek nem rendelkeznek üzenetküldési és hanghívás funkcióval: távlezárás, távtörlés GPS helymeghatározás, SIM ellenőrzés, rendszergazda kapcsolatok, hívásblokkolás, kéretlen SMS/MMS szűrés.

Az Android 4.4 vagy újabb operációsrendszert futtató készülékeken az SMS/MMS, valamint a bejövő hívások kezelési irányelvei a korábbi verziókhoz képest megváltoztak, ezért az említett rendszert futtató eszközökön az ESET Endpoint Security for Android SMS- és hívásszűrő funkciója nem elérhető. Ezen telefonok esetében erre a változásra egy felugró információs ablak is felhívja a figyelmet.

3.3.2. Rendszerkövetelmények

- Képernyő felbontása: min. 480x800
- Lemezterület: 20+ MB
- CPU: ARM processzor ARMv7-es utasításkészlettel
- Operációs rendszer: Android 4 vagy újabb verzió

3.4. A távadminisztrációs rendszer telepítése, előkövetelményei

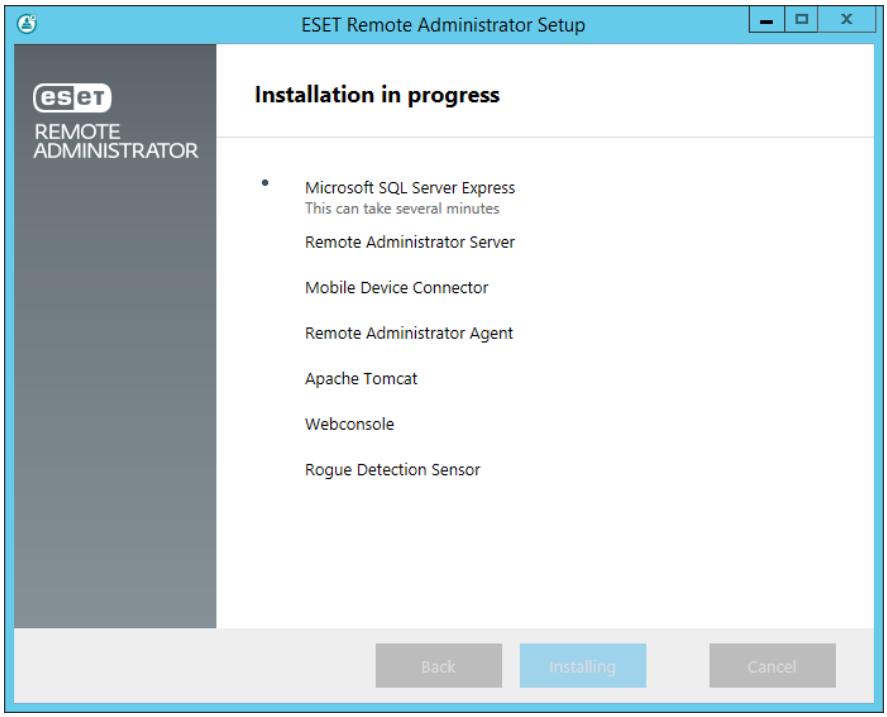
3.4.1. Telepítés

A telepítőcsomagok elérhetőek a http://www.eset.hu/letoltes/vallalati/tavadminisztracio oldalon.

A központi menedzsment rendszer az összes komponensével telepíthető egyszerre, egyetlen telepítő futtatásával, vagy telepíthető akár komponensenként is, amennyiben a rendszer bizonyos részeit már korábban telepítette, vagy rendelkezik saját MySQL vagy MS SQL adatbázis szerverrel és azt kívánja használni az automatikusan települő helyett.

A sikeres telepítéshez szükséges három további program meglétét a szerveren, a **.Net 3.5**-ös keretrendszer, a **Java Runtime Environment** legfrissebb verziója a webes felület működéséhez, illetve a **WinPcap** program a hálózaton található védtelen eszközök felderítéséhez. Utóbbi kettőt a gyártó honlapjáról töltheti le (a telepítőből néhány kattintással elérhető), míg a .Net keretrendszert a Szerepkörök és szolgáltatások hozzáadása varázsló segítségével telepítheti a szerveren.

Ezen felül amennyiben nem szeretne ESET Remote Admininstratort használni rendelkezésre állnak különböző plugin-ek a távmenedzsment megoldások használatára, így például Kaseya, Labtech, Autotask AEM, Autotask PSA, Tigerpaw, Connectwise.

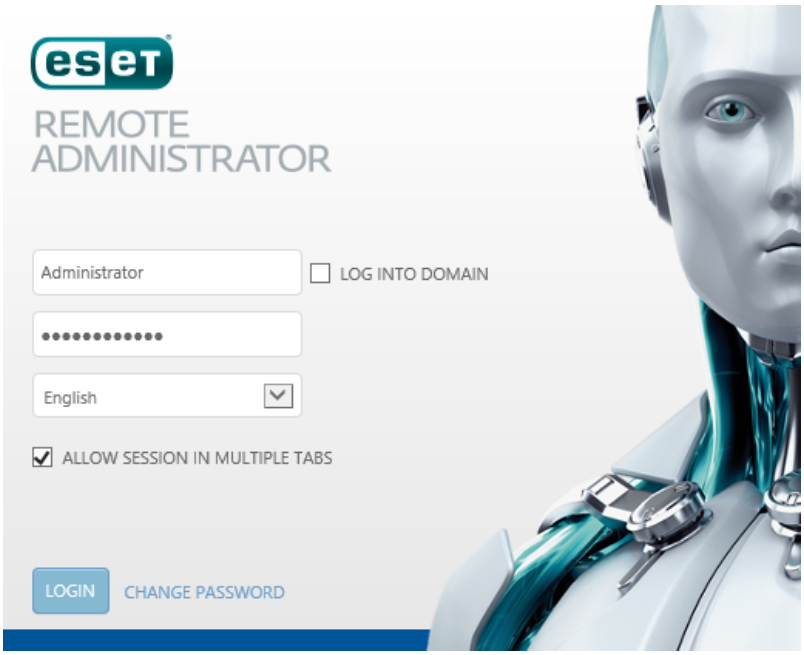


8. ábra: ESET Remote Administrator telepítő-varázsló

A Mobile Device Connector-t abban az esetben szükséges telepítenie, ha az ESET Endpoint Security programokat Android rendszeren működő eszközök esetén is szeretné központilag kezelni, ezen felül természetesen az Apple iOS eszközök menedzsmentjét is ebben a formában szeretné megoldani.

A legelső lépésben kiválasztható Remote Administrator Proxy-t csak nagy hálózatok vagy több telephely esetén érdemes telepíteni a távadminisztrációs program hálózati forgalmának csökkentéséhez.

A telepítés során megadható a licenclevélben megkapott Licenckulcs, de azt később is hozzá lehet adni a távadminisztrációs programhoz.

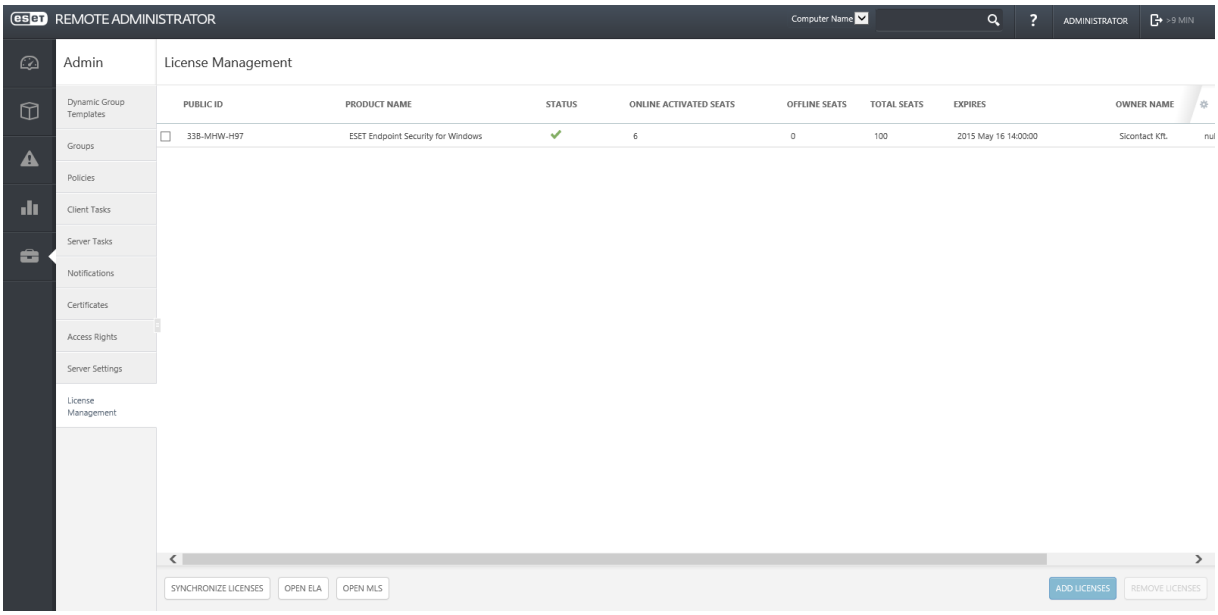


9. ábra: ESET Remote Administrator belépési képernyő

A belépés történhet az ESET Remote Administratorban definiált felhasználókkal, vagy a kijelölt AD csoport felhasználóival.

Licencek kezelése

A telepítés befejeztével már csatlakozhatunk is a távadminisztrációs szerverhez a webes felületen. Amennyiben nem adott meg licenckulcsot a telepítés során, ezt megteheti az **Admin** (szerszámosláda ikon) -> **Licence Management** részen az **ADD LICENSES** gombra kattintva. Ezt követően ugyanitt követhető nyomon, hogy hány licenc került felhasználásra a hálózaton.



10. ábra: ERA Web Console licenckezelő felülete

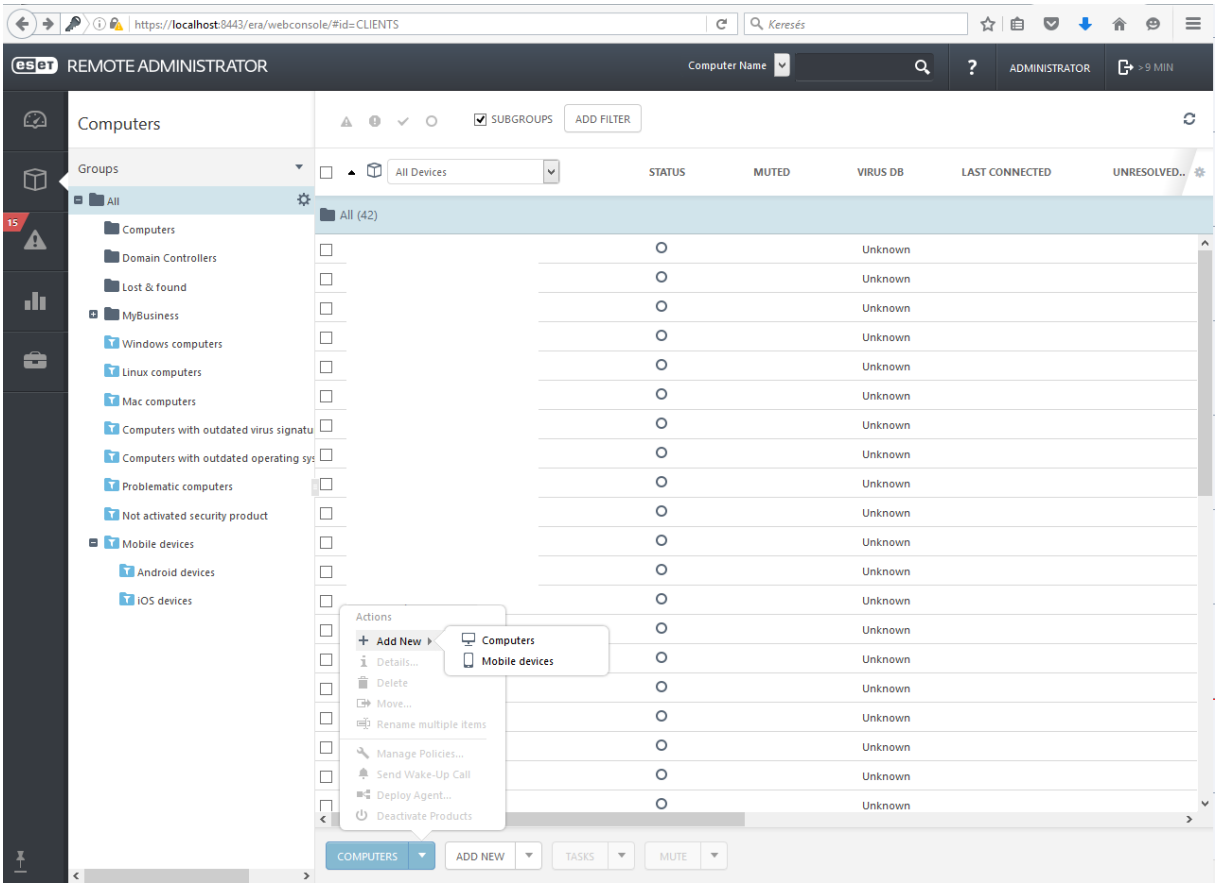
3.4.2. *Számítógépek felderítése*

A hálózaton található számítógépek felderítésére legegyszerűbben az Active Directory szinkronizálásával van lehetőség, de amennyiben nem domain-es környezetben telepítette a távadminisztrációs programot, lehetősége van akár kézzel is hozzáadni a klienseket azok nevei vagy IP címei alapján, vagy importálhatja is azokat ugyanezen tulajdonságaik alapján egy CVS fájlból.

Az Active Directory-val való szinkronizálás feladat az **Admin → Server Tasks** menüben a **Static Group Synchronization** elemet kiválasztva a **NEW…** gombra kattintva hozható létre. A feladat részletei között a **Settings** részt lenyitva adható meg, hogy mely csoportba szinkronizálja le a felderített számítógépeket, illetve az Active Directory helyét és az eléréséhez szükséges hitelesítő adatokat. A **Finish** gombbal hagyhatók jóvá a módosítások, ezt követően a feladat nevére kattintva a **Run now…** opció kiválasztásával futtatható le az. A feladat futásának állapota a feladat nevére kattintva, a Details lehetőséget kiválasztva az Executions fülön tekinthető meg.

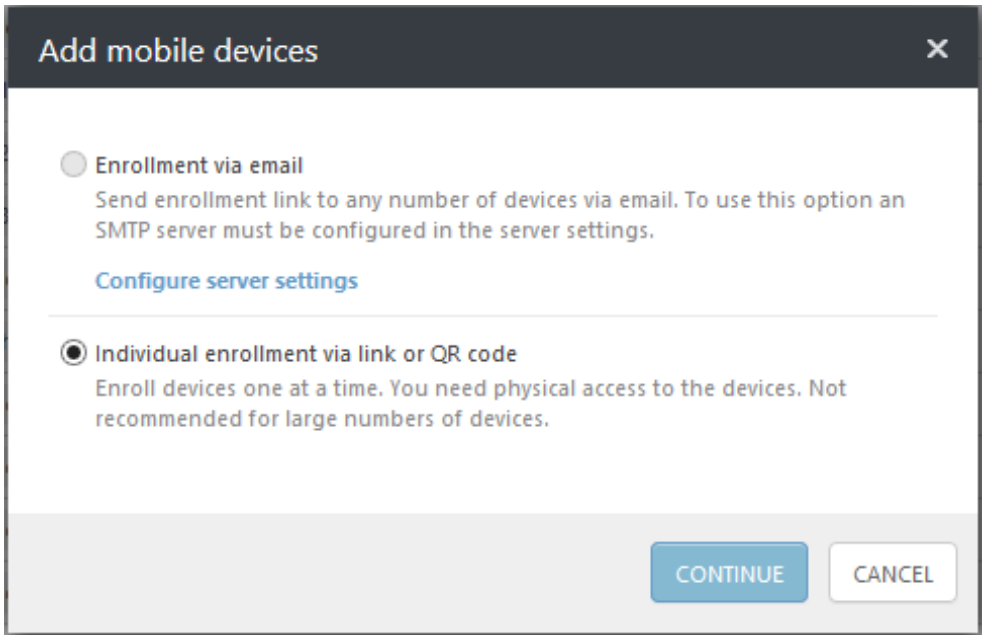
3.4.3. *Mobil eszköz hozzáadása*

Android és iOS operációs rendszerű készülékek felvételére nyílik lehetőség egyenként vagy csoportosan. Új eszköz felvételéhez nyissa meg a tetszőleges böngészőben az *ESET Remote Administrator Web Console*-t, majd a bal oldali menüben kattintson a *Computers* sorra, ezután az *All* szóra a fastruktúrában. Az ablak alsó részén található *COMPUTERS* gombra kattintva válassza az *Add new* opciót és ezen belül a *Mobil Devices* lehetőséget.



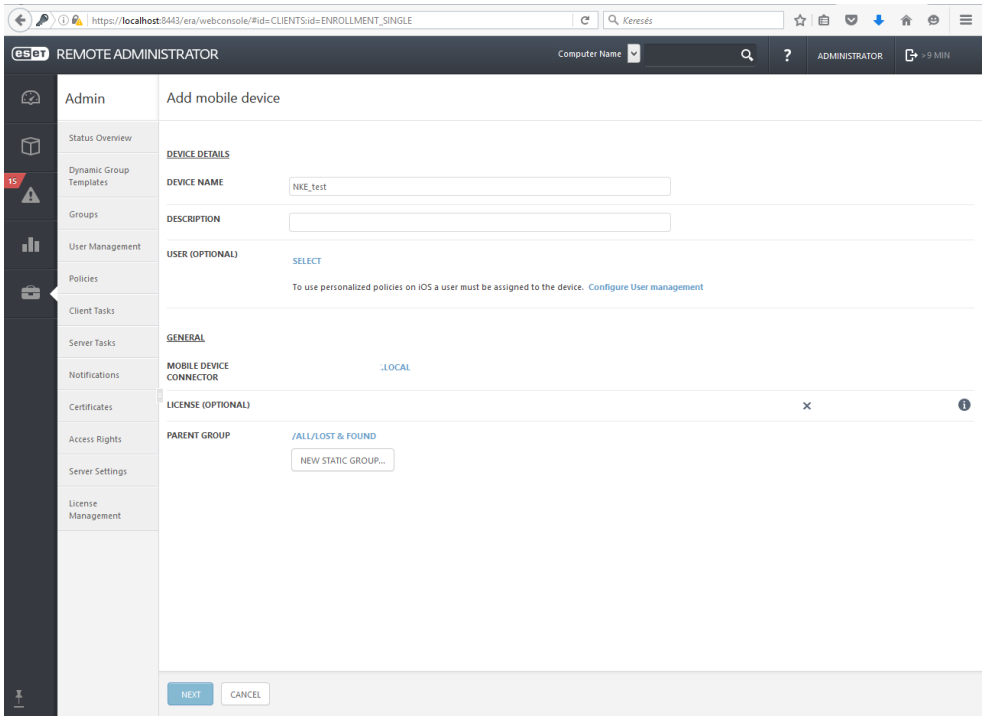
11. ábra: Mobil eszköz hozzáadása az ERA Web Console-on belül

Ezután két lehetőség közül választhat, hogy e-mailben küldi el a telepítő csomagot a bevonni kívánt eszköz(ök)re, vagy QR kódot leolvastatva, természetesen az utóbbi nem szerencsés nagyobb mobil eszközpark esetén. Miután kiválasztotta a deployment módját, kattintson a CONTINUE gombra.



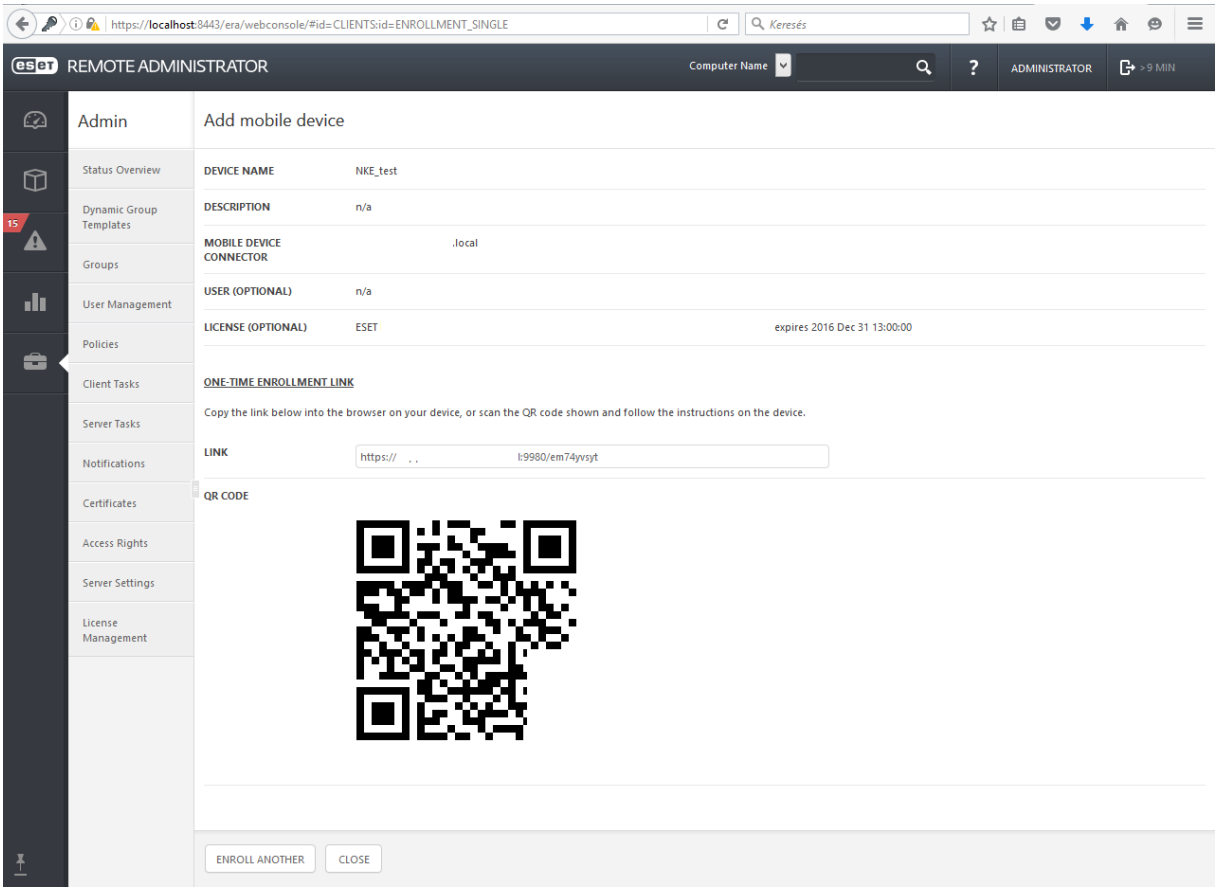
12. ábra: Mobil eszköz enrollment módjának kiválasztása

A megjelenő ablakban adja meg az eszköz nevét, leírását, amennyiben iOS eszközt is be szeretne vonni a távmenedzsmentbe, rendeljen hozzá egy felhasználót az eszközhöz, továbbá adja meg a használni kívánt licencet és a szülő csoportját is válassz ki ezeknek az eszközöknek, majd nyomja meg a NEXT gombot.



13. ábra: Mobil eszköz hozzáadásnak részletes beállítása

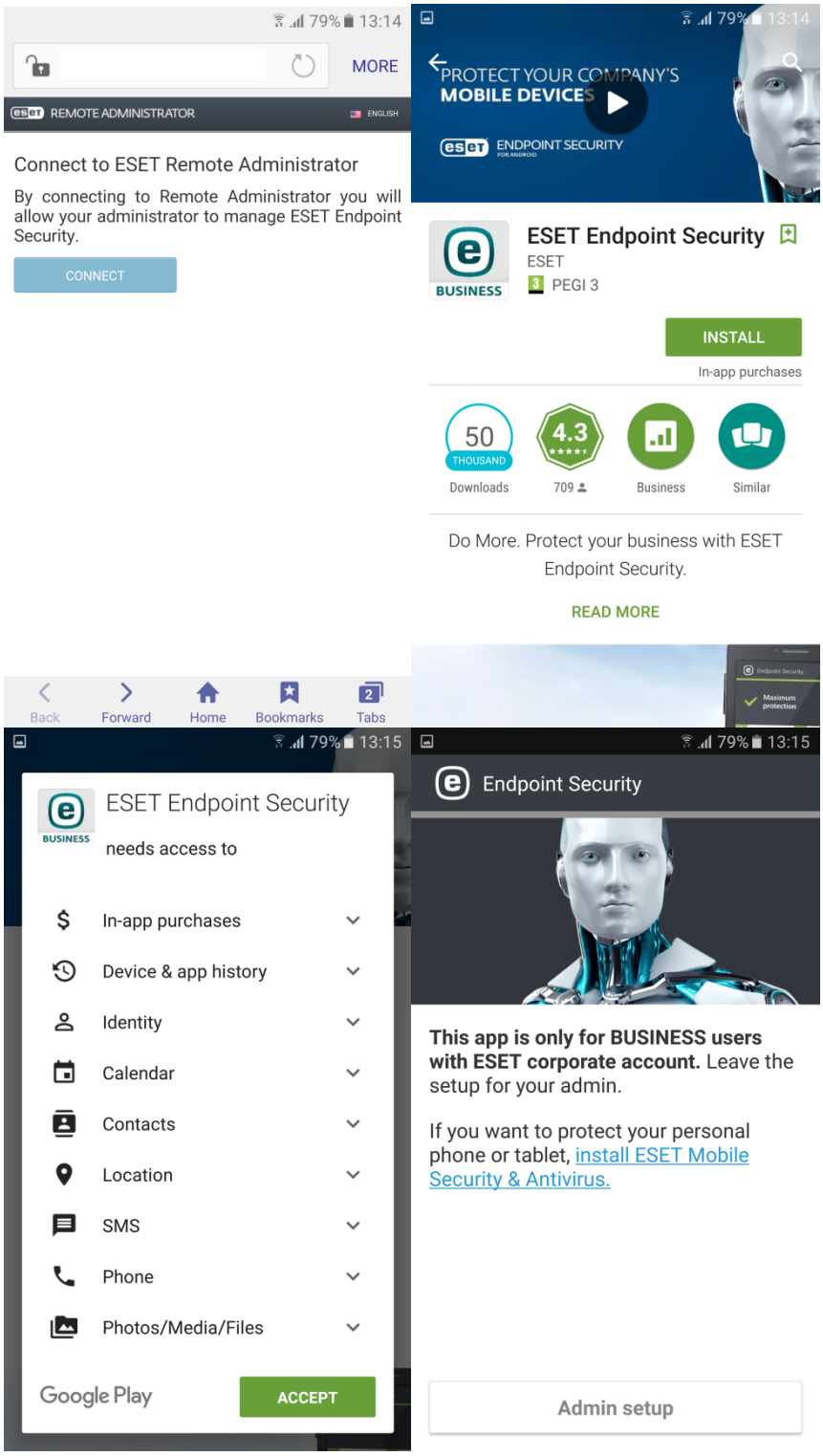
A következő ablakban megjelenik a QR-kód, ha ezt az opciót választotta a 12. ábrán látható pontban, amennyiben az e-mailben való kiküldést, akkor az eszközön található levelezőkliensben találja a szükséges adatokat és az egyszer használatos linket is, amit elküldhet az adott telefonra e-mailben is külön.



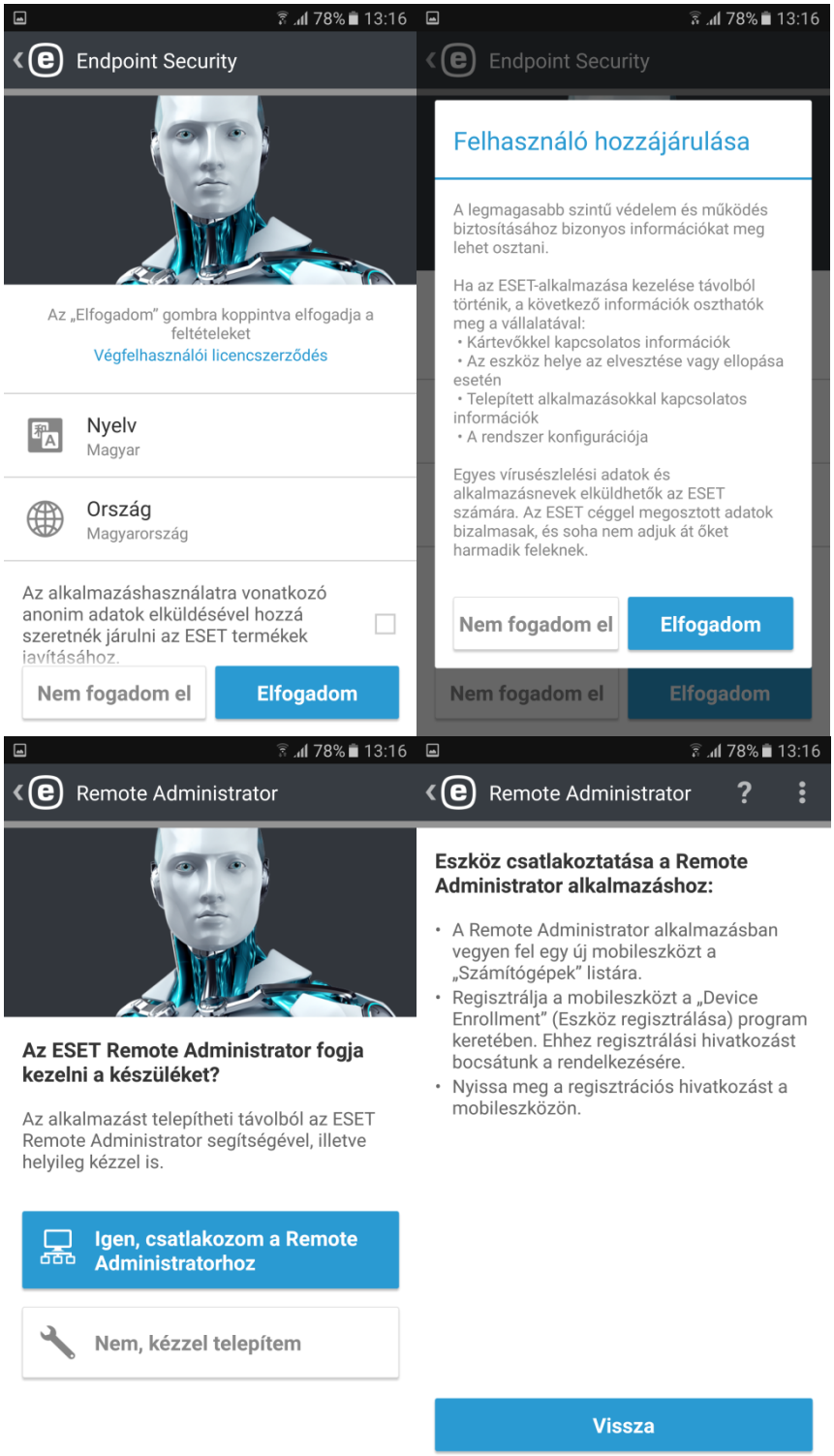
14. ábra: Telepítéshez szükséges QR-kód

3.4.4. Végpontvédelem telepítése mobil eszközökre

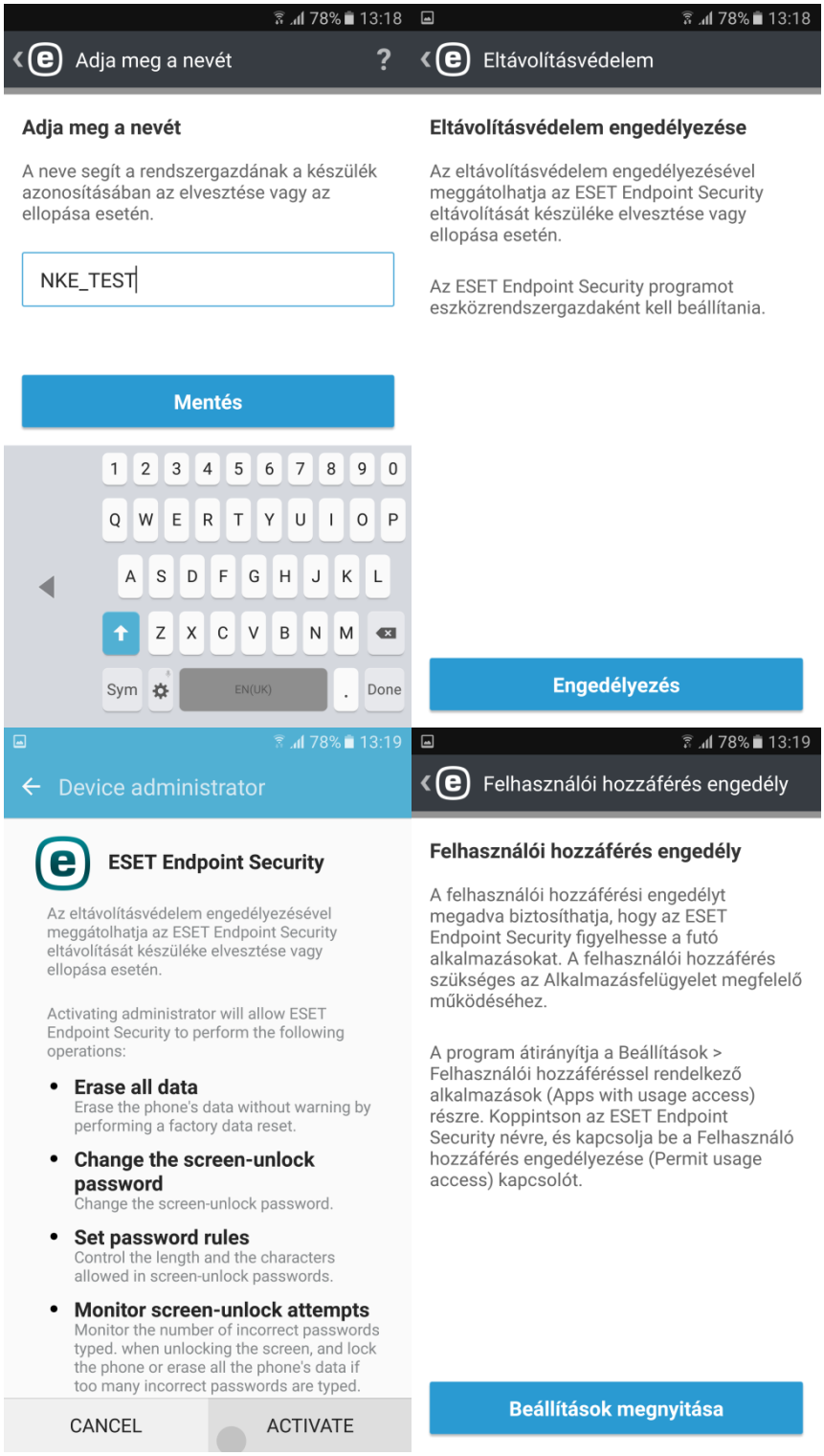
A telepítés lépéseit a következő ábrák mutatják



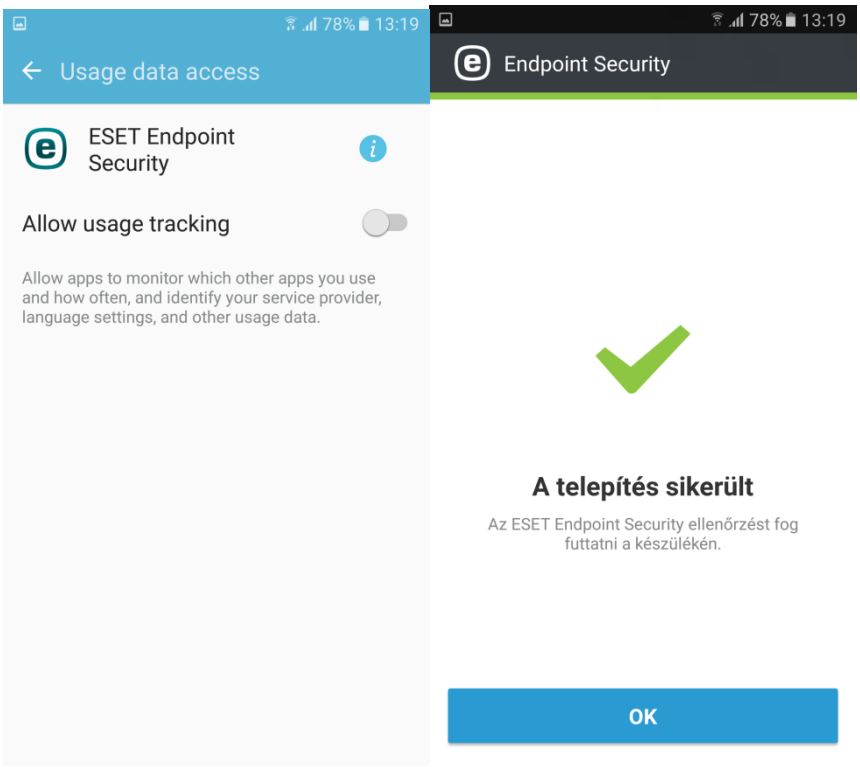
15. ábra


78% 13:16
Endpoint Security
Az „Elfogadom” gombra koppintva elfogadja a feltételeket
Végfelhasználói licencszerződés
Nyelv
Magyar
Ország
Magyarország
Az alkalmazáshasználatra vonatkozó anonim adatok elküldésével hozzá szeretnék járulni az ESET termékek javításához.
Nem fogadom el
Elfogadom
Endpoint Security
Felhasználó hozzájárulása
A legmagasabb szintű védelem és működés biztosításához bizonyos információkat meg lehet osztani.
Ha az ESET-alkalmazása kezelése távolból történik, a következő információk oszthatók meg a vállalatával:
• Kártevőkkel kapcsolatos információk
• Az eszköz helye az elvesztése vagy ellopása esetén
• Telepített alkalmazásokkal kapcsolatos információk
• A rendszer konfigurációja
Egyes vírusészlelési adatok és alkalmazásnevek elküldhetők az ESET számára. Az ESET céggel megosztott adatok bizalmasak, és soha nem adjuk át őket harmadik feleknek.
Nem fogadom el
Elfogadom
Remote Administrator
Az ESET Remote Administrator fogja kezelni a készüléket?
Az alkalmazást telepítheti távolból az ESET Remote Administrator segítségével, illetve helyileg kézzel is.
Igen, csatlakozom a Remote Administratorhoz
Nem, kézzel telepítem
Remote Administrator
Eszköz csatlakoztatása a Remote Administrator alkalmazáshoz:
• A Remote Administrator alkalmazásban vegyen fel egy új mobileszközt a „Számítógépek” listára.
• Regisztrálja a mobileszközt a „Device Enrollment” (Eszköz regisztrálása) program keretében. Ehhez regisztrálási hivatkozást bocsátunk a rendelkezésére.
• Nyissa meg a regisztrációs hivatkozást a mobileszközön.
Vissza

16. ábra

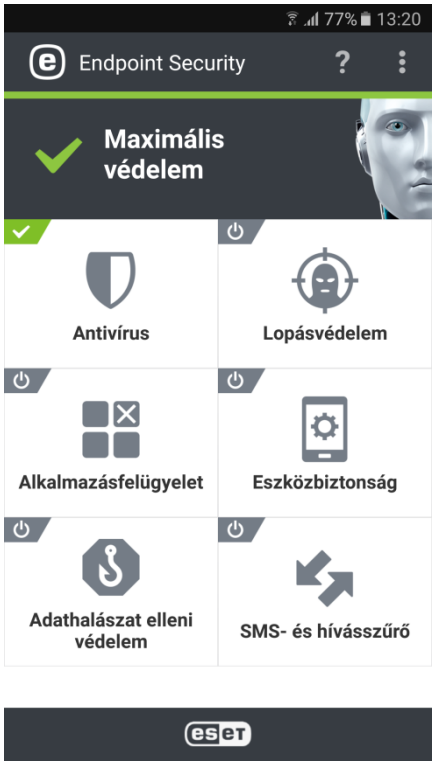

78% 13:18
Adja meg a nevét
Adja meg a nevét
A neve segít a rendszergazdának a készülék azonosításában az elvesztése vagy az ellopása esetén.
NKE_TEST
Mentés
78% 13:18
Eltávolításvédelem
Eltávolításvédelem engedélyezése
Az eltávolításvédelem engedélyezésével meggátolhatja az ESET Endpoint Security eltávolítását készüléke elvesztése vagy ellopása esetén.
Az ESET Endpoint Security programot eszközrendszergazdaként kell beállítania.
Engedélyezés
78% 13:19
Device administrator
ESET Endpoint Security
Az eltávolításvédelem engedélyezésével meggátolhatja az ESET Endpoint Security eltávolítását készüléke elvesztése vagy ellopása esetén.
Activating administrator will allow ESET Endpoint Security to perform the following operations:
Erase all data
Erase the phone's data without warning by performing a factory data reset.
Change the screen-unlock password
Change the screen-unlock password.
Set password rules
Control the length and the characters allowed in screen-unlock passwords.
Monitor screen-unlock attempts
Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
CANCEL
ACTIVATE
78% 13:19
Felhasználói hozzáférés engedély
Felhasználói hozzáférés engedély
A felhasználói hozzáférési engedélyt megadva biztosíthatja, hogy az ESET Endpoint Security figyelhesse a futó alkalmazásokat. A felhasználói hozzáférés szükséges az Alkalmazásfelügyelet megfelelő működéséhez.
A program átirányítja a Beállítások > Felhasználói hozzáféréssel rendelkező alkalmazások (Apps with usage access) részre. Koppintson az ESET Endpoint Security névre, és kapcsolja be a Felhasználó hozzáférés engedélyezése (Permit usage access) kapcsolót.
Beállítások megnyitása

17. ábra



18. ábra

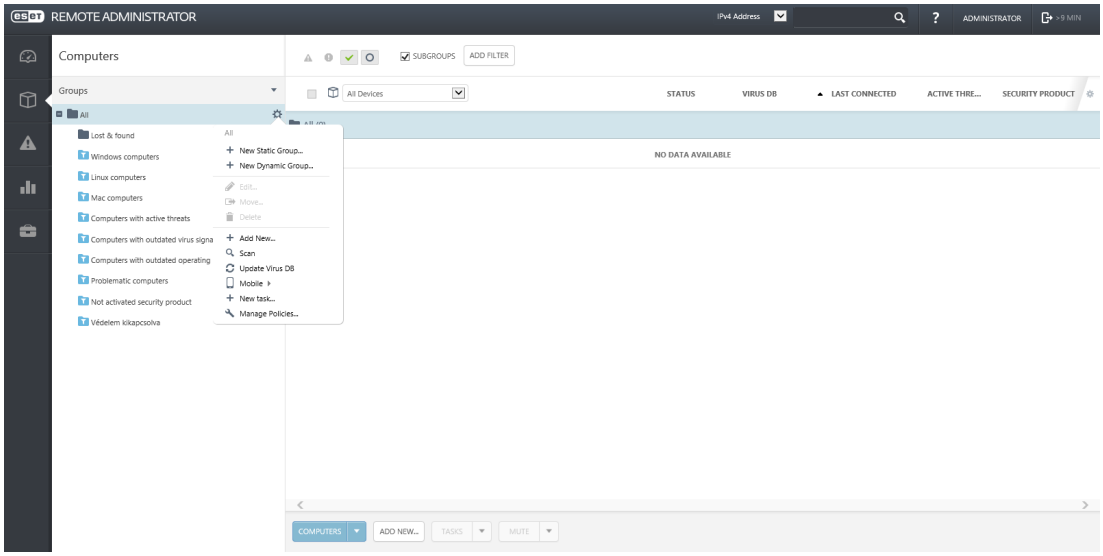
A telepítés után az Androidos eszközön megjelenik a telepített és aktivált vírusellenőrző program, aminek a beállításait a központi menedzsmenten keresztül policy-k (házirendek) segítségével módosíthatunk.



19. ábra: Telepített védelem kezdőképernyője

3.4.5. *Csoportkezelés*

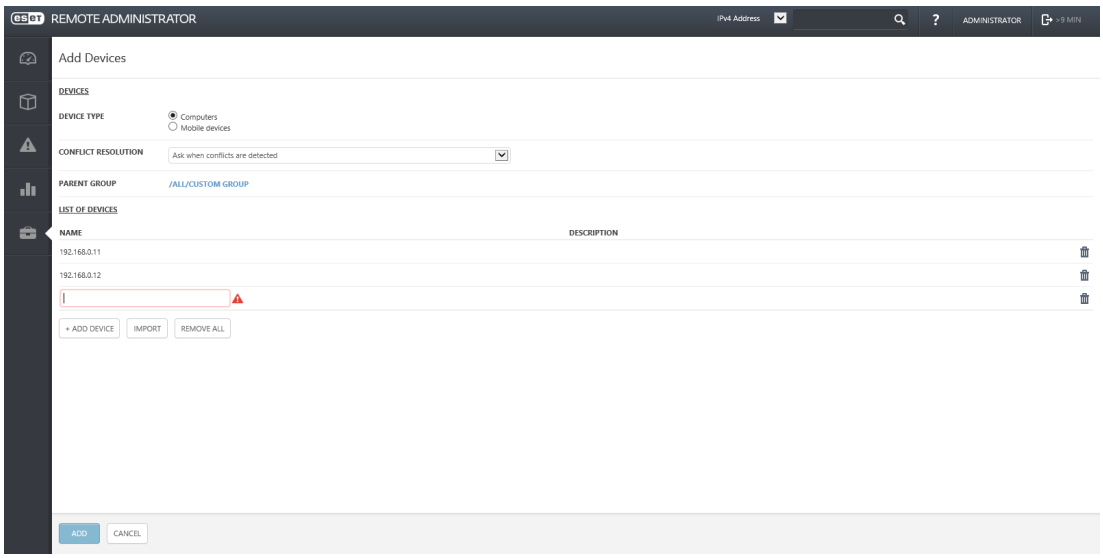
Egy távadminisztrációs program elengedhetetlen része a számítógépek logikai csoportokban történő egyszerű kezelése. Az ESET Remote Administrator erre kétféle lehetőséget biztosít, statikus és dinamikus csoportok létrehozásával.



20. ábra: Csoportkezelő ablak

3.4.6. *Statikus csoportok*

A statikus csoportok kezelése egyszerűbb, de nevükből fakadóan kevésbé rugalmasak és kevesebb funkcionalitás is köthető hozzájuk. A csoportot egyszerűen létre kell hozni, elnevezni, majd megmondani, hogy mely számítógépek legyenek a tagjai. Egy számítógép egy statikus csoportból csak kézi eltávolítás útján kerülhet ki, vagy magának a csoportnak a törlése esetén. Statikus csoport létrehozása a **Computers** menüpontban az All nevű csoport sorának végén lévő **fogaskerékre** kattintva a **New Static Group…** elem kiválasztásával történik. Létrehozása után a csoportot kiválasztva az **ADD NEW…** gombbal adhatók hozzá számítógépek, mobil eszközök.

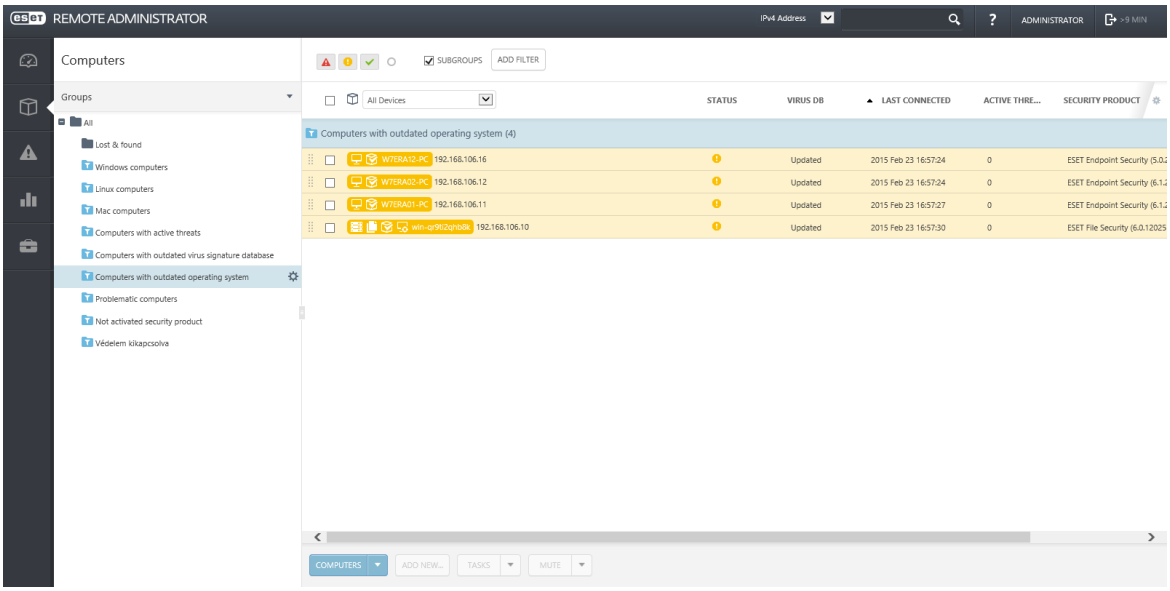


21. ábra: Eszköz hozzáadása IP-cím alapján

Statikus csoportokat az Active Directory lekérdezésével is fel lehet tölteni, ennek menete a Számítógépek felderítése bekezdésben már ismertetésre került.

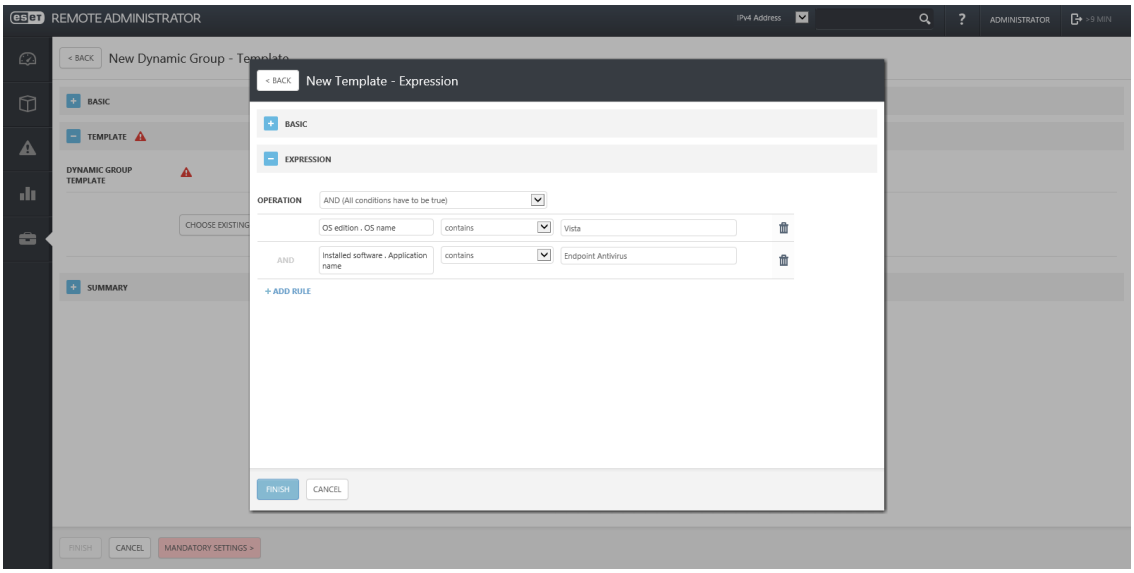
3.4.7. Dinamikus csoportok

A dinamikus csoportok tagsága egy feltételhez kötött, azok létrehozásakor kell definiálni, hogy milyen feltétel teljesülése esetén kerül egy számítógép a csoport tagjai közé. Dinamikus csoport létrehozása a **Computers** menüpontban az **All** nevű csoport sorának végén lévő **fogaskerékre** kattintva a **New Dynamic Group…** elem kiválasztásával történik. A csoport létrehozásakor annak elnevezése után a **Template** részen kiválasztható az előre definiált vagy már korábban létrehozott feltételek egyike a **CHOOSE EXISTING…** gombra kattintva, vagy a **NEW…** gombra kattintva létrehozható egy általunk összeállított új feltétel-együttes, amelyek különböző logikai kapcsolókkal köthetők össze (AND, OR, NAND stb.). A dinamikus csoportok és azok feltételei a számítógépeken futó Agentek-ben tárolásra kerülnek azok következő bejelentkezését követően, így egy számítógép ezentúl akkor is bekerülhet egy a dinamikus csoport valamelyikébe (és kaphatja meg annak policy-jét), ha épp nem csatlakozik a távadminisztrációs programhoz.



22. ábra: Dinamikus csoport a nem aktuális vírusdefiníciós adatbázissal rendelkező gépekkel

A dinamikus csoportok feltételei egyrészt lehetővé teszik, hogy adott állandó tulajdonságaik alapján kerüljenek a munkaállomások egy könnyen kezelhető logikai egységbe (pl. számítógépnév-maszk, IP cím, IP tartomány, operációs rendszer típusa, hardver elemek, stb.), másrészt dinamikusan kezelik a klienseket azok változó tulajdonságai alapján (adatbázis naprakészsége, védelem állapota, operációs rendszer naprakészsége, stb.).

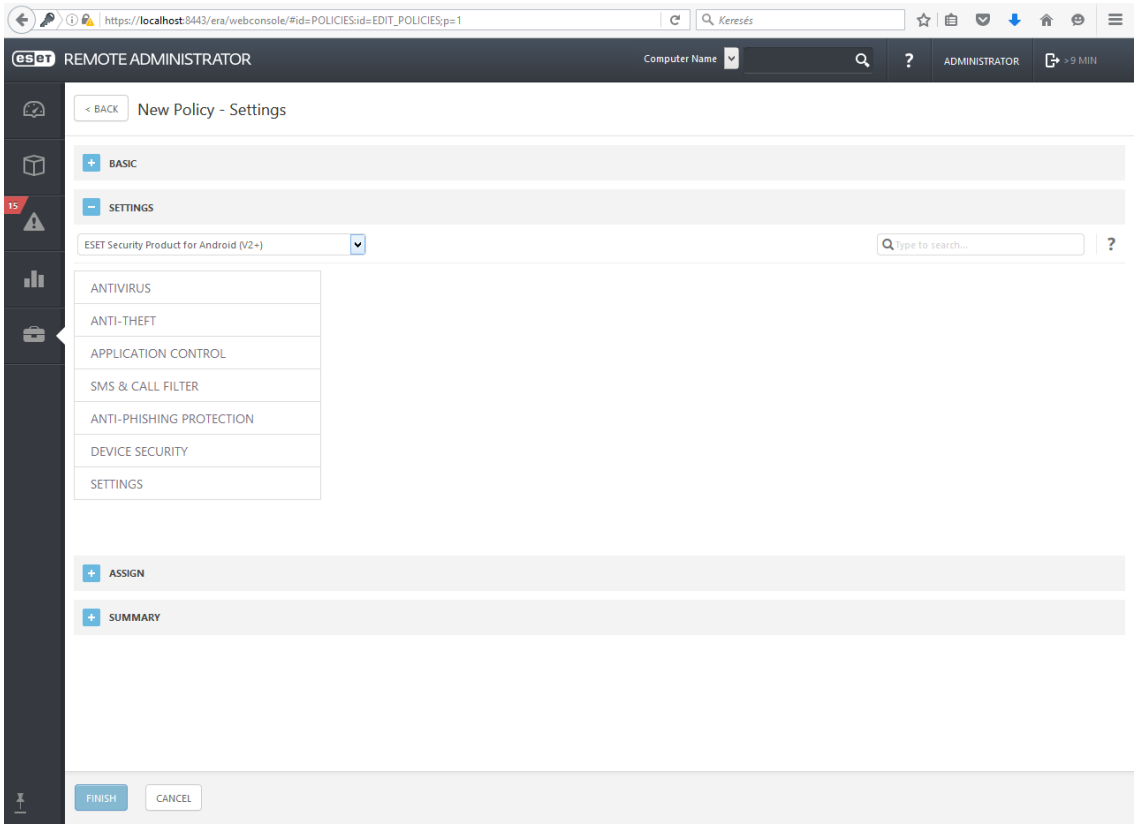


23. ábra: Dinamikus csoport létrehozása különböző feltételek alapján

Egy dinamikus csoportba történő belépés kiváltó eseményéül szolgálhat bármilyen folyamatnak, ezáltal egy jól végiggondolt csoportosítással lehetőség nyílik az esetlegesen felmerülő problémák automatikus kezelésére.

3.4.8. Policy-k kezelése

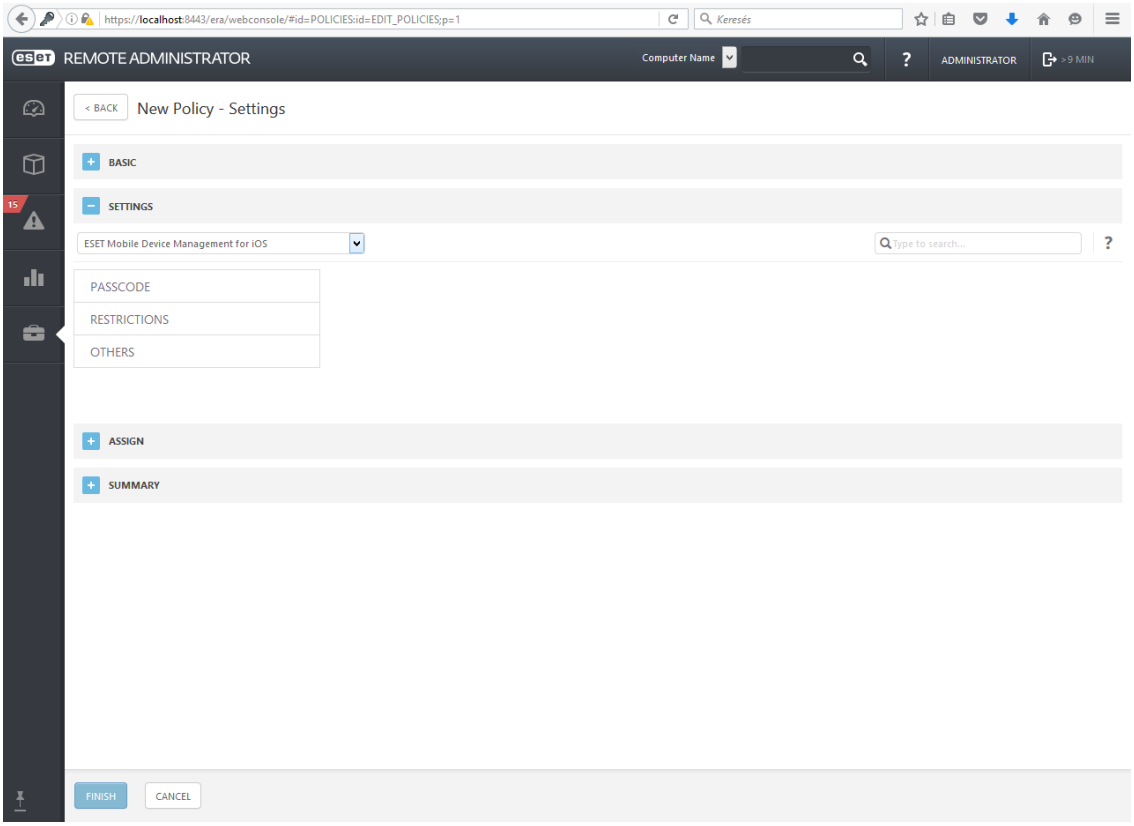
A policy (házirend) egy beállításjegyzés, amely tartalmazza egy kliens (végpontvédelem, szervervédelem, Agent, stb.) azon beállításai, amelyek megváltoztatása nem engedélyezett a felhasználók számára. A policy-k kezelése az **Admin → Policies** menüpontban történik, itt meg lehet tekinteni az előre definiált policy-ket és a korábban hozzáadott saját policy-ket, továbbá a jobb oldali részen a **Groups** illetve **Clients** fülön, hogy mely csoportokra és munkaállomásokra érvényesek, a **Settings** fülön pedig hogy milyen beállításokat tartalmaznak.



24. ábra: Policy szerkesztő Android-os eszközök esetén

Android-os eszközön a következő funkciók menedzselhetőek:

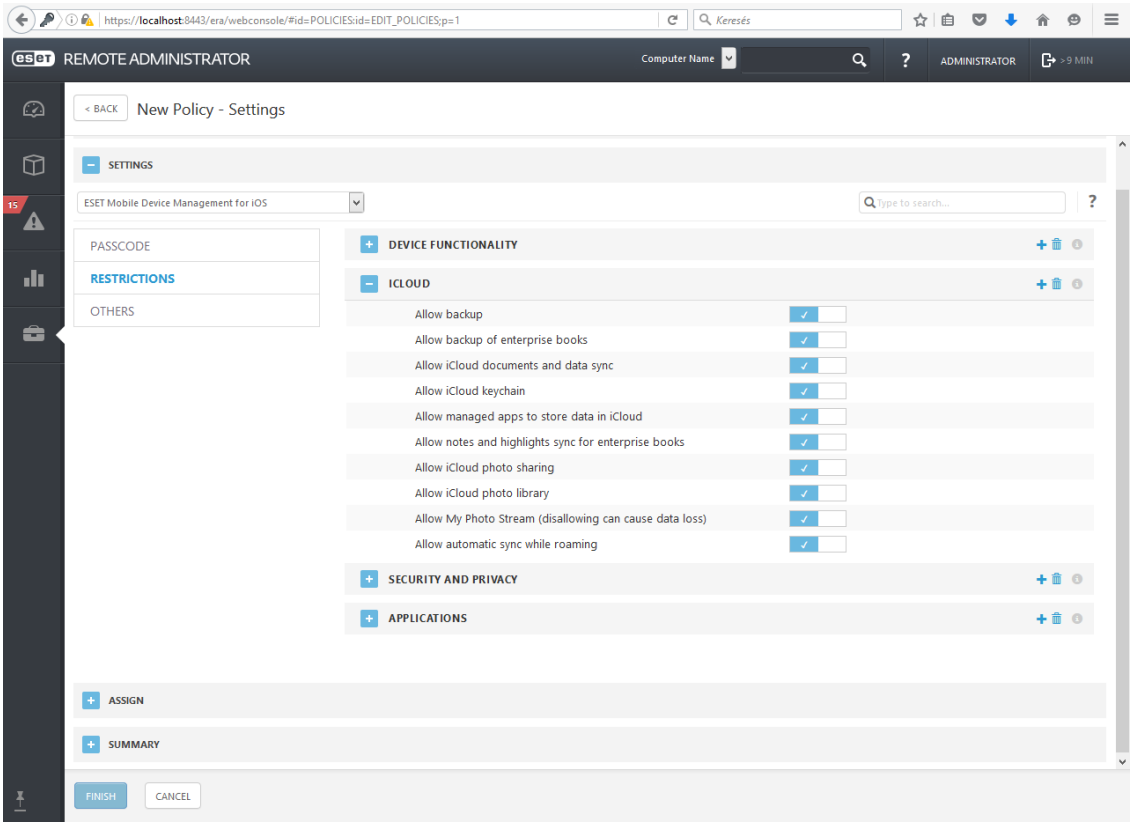
- Antivírus
- Lopásvédelem
- Alkalmazáskontroll
- SMS- és hívásszűrés
- Adathalászat elleni védelem
- Eszközbiztonság
- További beállítások



25. ábra: Policy szerkesztő Apple iOS eszközök esetén

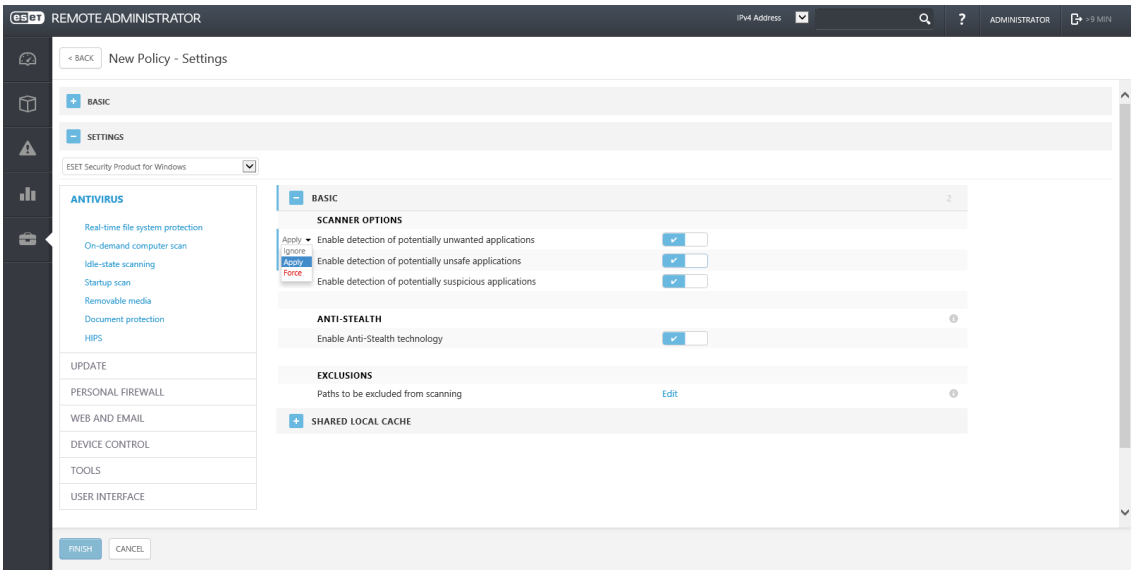
Apple iOS eszközökön elérhető MDM-funkciók:

- Passcode követelmények testreszabása
- Korlátozások és engedélyek (kamera SIRI és iCloud használat, biztonsági beállítások, alkalmazáskontroll)
- Internetkapcsolattal és felhasználói fiókokkal kapcsolatos beállítások



26. ábra: Policy szerkesztő Apple iOS esetén az iCloud működésének szabályozására

Új policy létrehozása a **POLICIES** gombra kattintva megjelenő lehetőségek közül a **New…** kiválasztásával történik. A policy elnevezését követően a **Settings** részen meg kell adni, hogy milyen típusú termékekre vonatkozzon, majd módosítani vagy megjelölni a fenntartandó beállításokat a megjelenő beállítások között. Az itt látható beállítás teljes egészében megegyezik egy kliens lokálisan módosítható részletes beállításaival, így a beállítások kezelése könnyebben elsajátítható.



27. ábra: Beállítás három lehetséges állapota

Egy adott beállítás három szinten képezheti részét egy policy-nek. **Ignore** állapotban egy beállítás nem része a policy-nek, alapértelmezetten az összes beállítás ebben az állapotban van. **Apply** állapotban a beállítás része egy policy-nek, de egy másik policy felülírhatja azt, amennyiben az később kerül kiértékelése, vagy később kerül alkalmazásra az adott kliensen. A **Force** állapot mindenképpen alkalmazásra kerül egy kliensen és úgy is marad, még akkor is, ha egy később alkalmazásra kerülő policy más értéket adna szintén Force jelölővel.

Az **Assign** részen az **ASSIGN…** gombra kattintva jelölhetjük ki, hogy az imént definiált beállításjegyzék mely kliensekre vagy mely csoport összes tagjára vonatkozzon.

3.4.9. Események, feladatok, automatizálás

Az ESET távadminisztrációs rendszerének egyik legnagyobb előnye annak automatizálhatósága. Előre beállított események hatására automatikus feladatok üzemezhetők be, amelyek segítségével a rendszergazda távollétében is kezelésre kerülnek az esetlegesen felmerülő problémák.

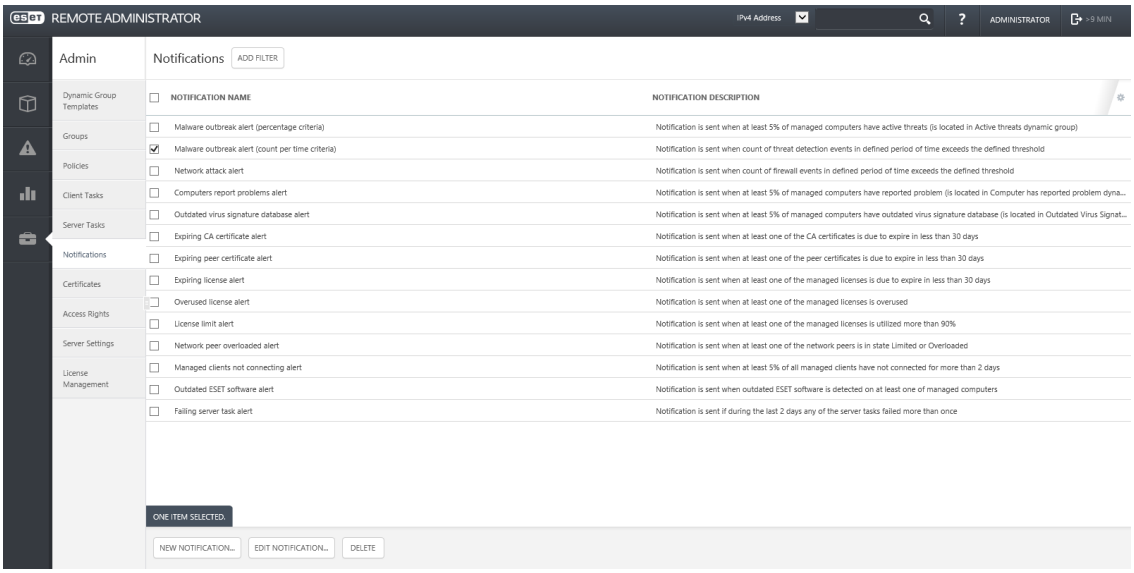
Feladatok

Az ESET Remote Administrator szerteágazó feladatok formájában végzi a klienseken vagy a szervereken eszközölt változtatásokat vagy folyamatokat. Szerverfolyamatnak számít az Agent távtelepítése, az Active Directory szinkronizálása és a különböző riportok készítése. Az összes többi folyamat a klienssel vagy az azon futó ESET programmal kapcsolatos, ezek futását az Agent vezérli lokálisan, így ezek kliensfolyamatnak számítanak. A kliensfolyamatok vonatkozhatnak az operációs rendszerre (rendszerfrissítés, program telepítése/eltávolítása, parancs futtatása, üzenet megjelenítése), lehetnek ESET specifikusak is (frissítés, aktiválás, ütemezett feladat futtatása stb.), vonatkozhatnak mobil eszközökre (lopásvédelmi funkciók aktiválása, eszköz ellenőrzése, szoftver telepítése), illetve vonatkozhat magára a távadminisztrációs programra (komponensek telepítése, RD sensor adatbázisának törlése, stb.).

Szerverfeladatokat az **Admin → Server Tasks** részen, kliensfeladatokat pedig az **Admin → Client Tasks** részen lehet felvenni az adott feladat típus kiválasztását követően a **NEW…** gombra kattintva. Előredefiniált vagy már korábban létrehozott feladatot a feladat nevére kattintva a **Run now** opció kiválasztásával lehet ismételten lefuttatni (amennyiben az nem eseményhez kötött). A feladat futásának állapota a feladat nevére kattintva, a Details lehetőséget kiválasztva az Executions fülön tekinthető meg.

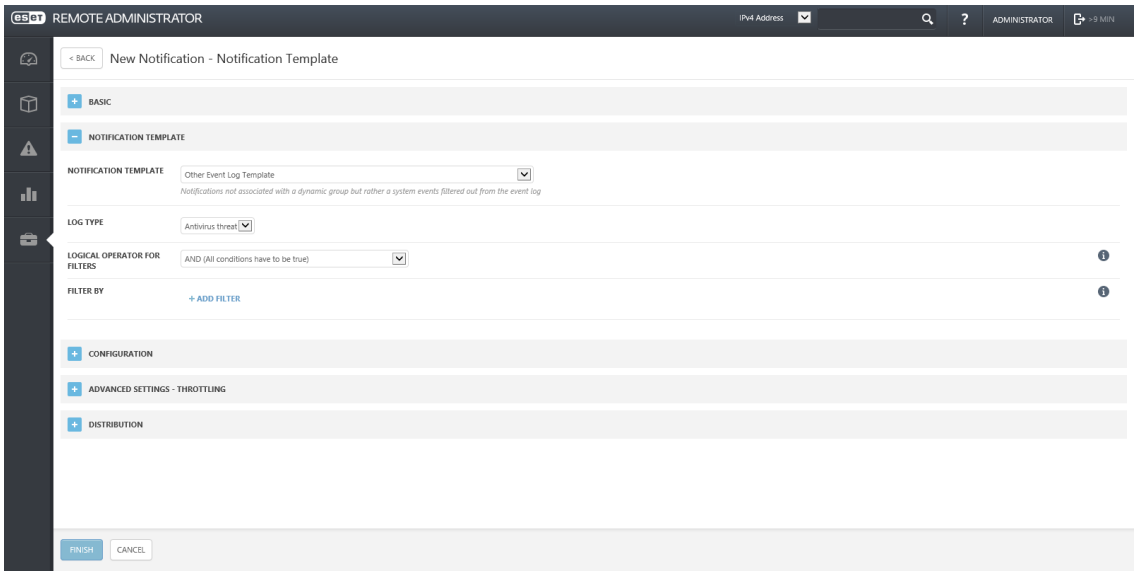
Értesítések

A távadminisztrációs szerver értesítési funkciója bizonyos események hatására email-ben tájékoztatja a rendszergazdát. Az értesítések kezelése az **Admin → Notifications** menüpontban történik. Itt megtekintheti és szerkesztheti az előre definiált értesítéseket, vagy létrehozhat újakat is a **NEW NOTIFICATION…** gombra kattintva, igényeinek megfelelően.



28. ábra: Értesítések konfigurálása

Az értesítések tekinthetők tulajdonképpen olyan e-mail-küldési feladatoknak, amelyek a kiváltó eseményeik statisztikai gyakoriságát is figyelembe vehetik. Tehát definiálható, hogy a távadminisztrációs program csak bizonyos számú eseményt követően küldjön értesítést, vagy csak abban az esetben, ha az egy adott számban jelentkezik egy bizonyos időtartamon belül. Az értesítés típusa a **NOTIFICATION TEMPLATE** részen választható ki, az üzenet szövege és formátuma a **CONFIGURATION** részen adható meg, a különböző számbeli vagy időbeli statisztikák pedig az **ADVANCED SETTINGS – THROTTLING** részt lenyitva definiálhatók. Ezt követően a **DISTRIBUTION** részen adható meg, hogy milyen e-mail címre szeretné eljuttatni az imént felvett feltételek teljesülése esetén elküldött értesítést.

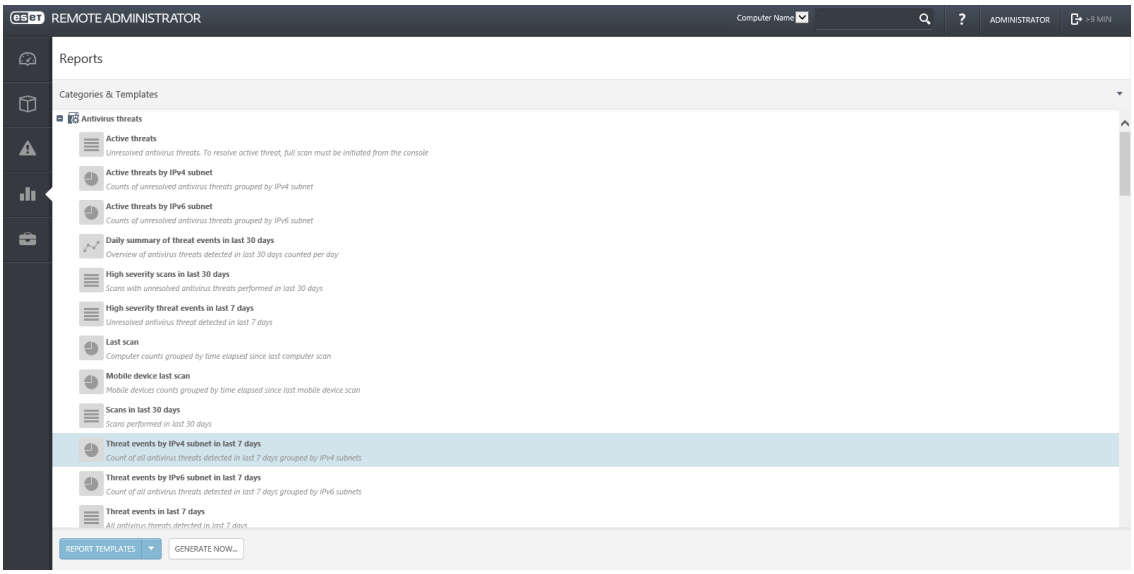


29. ábra: Új értesítés template létrehozása

Riportok

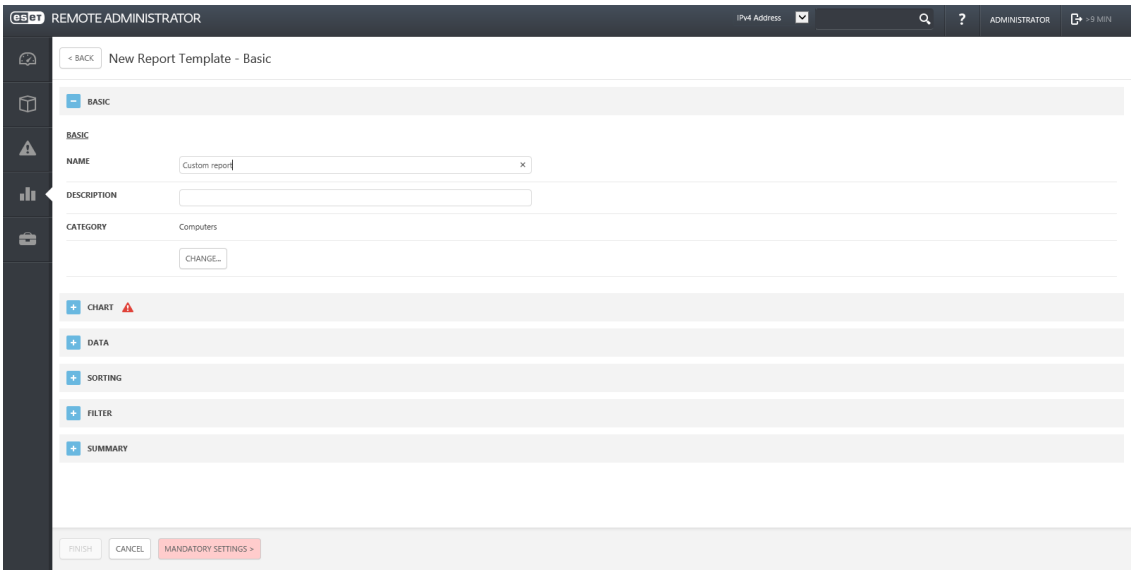
Az ESET Remote Administrator számtalan előredefiniált riport készítésére és elküldésére alkalmas, de ugyanúgy készíthetők vele átfogó, testre szabott kimutatások is.

A riportokat a webes felület főablakán, a balról beúszó menüben a **Reports** menüpontra kattintva kezelheti.



30. ábra: Riportvarázsló

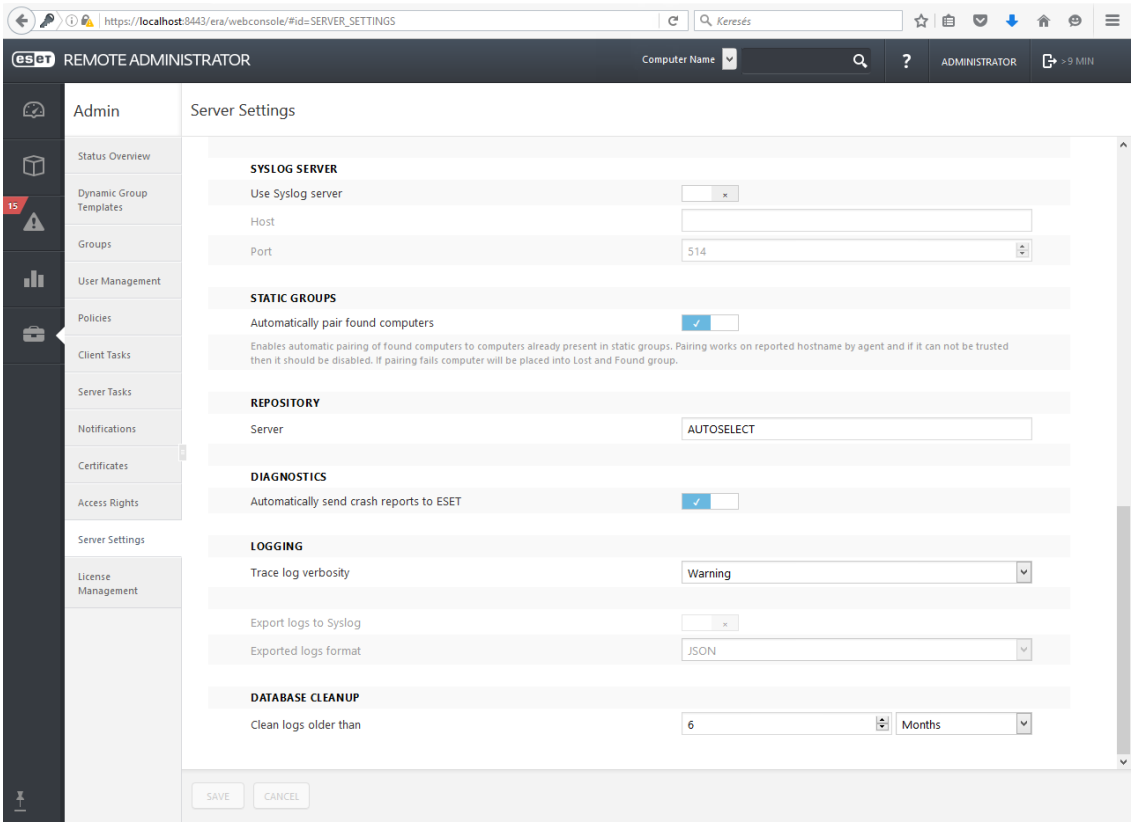
Részletesen testre szabható riportokat ugyanezen az oldalon a **REPORT TEMPLATES** gombra kattintva a **New Report Template…** opciót kiválasztva készíthet.



31. ábra: Új riport template létrehozása

Naplókezelés

Az ESET Remote Admininstrator Server által készített naplófájlok a c:\ProgramData\ESET\Remote-Administrator\Server\EraServerApplicationData\Logs\ elérési úton találhatóak, de természetesen van lehetőség egy tetszőleges Syslog szerverre is továbbítani a naplóbejegyzéseket. Ennek beállítása az ERA Web Console, Admin, Server Settings menüpontjában található.



32. ábra: Syslog szerver beállítás

3.5. Részösszegzése

A fentiek a 41/2015. (VII. 15.) BM rendeletben meghatározott alábbi funkciókat valósítják meg:

- Közösségi média szűrése
- ADATHORDOZÓK VÉDELME
  - ERA – Cserélhető adathordozók tiltása, adott típusú adathordozók engedélyezése
- Hozzáférés-ellenőrzés
  - Mobil – Távoli lezárás
  - ERA – 2FA felhasználókezelés
- Automatizálás
  - ERA – adatbázis elavultsága esetén automatikus frissítés task
  - ERA – adathordozó behelyezése esetén figyelmeztető üzenet (kérje a rendszergazda jóváhagyását)

4. Mobilvédelem és megvalósítása Sophos Mobile Control megoldással

4.1. Bevezetés

Jelen fejezet bemutatja, hogy a Sophos Mobile Control milyen módon támogatja a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről egyes előírásait.

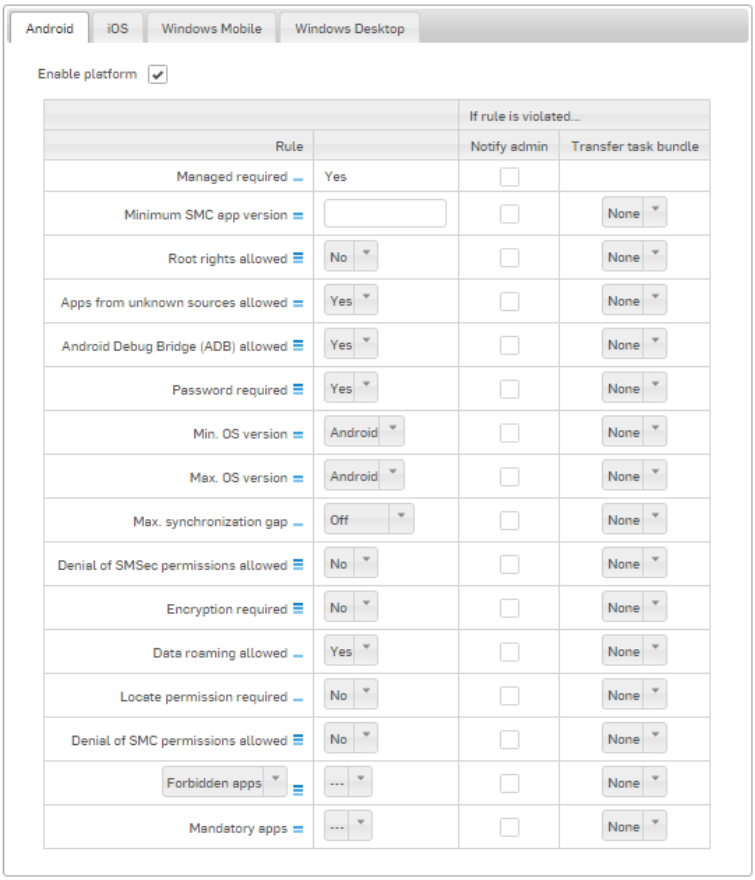
4.2. A biztonsági események kezelése

Automatikus eseménykezelés (3.1.5.2)

A rendszer lehetőséget ad **Compliance rules**, azaz **Megfelelőségi szabályok** beállítására különböző készülékcsoportok számára. Segítségükkel automatikus válaszreakciók hozhatók létre a különböző eseményekhez, mint például:

- Hozzáférés korlátozás fertőzött vagy Root-olt/Jailbreak-elt készülékek esetén
- Titkosítás hiánya esetén
- Adatbarangolásra (Data Roaming)
- Előírt alkalmazások hiányára (Mandatory apps)
- Tiltott alkalmazás telepítésére (Forbidden apps), stb…

Beállítása: Configure/Compliancerules/Createcompliancerules



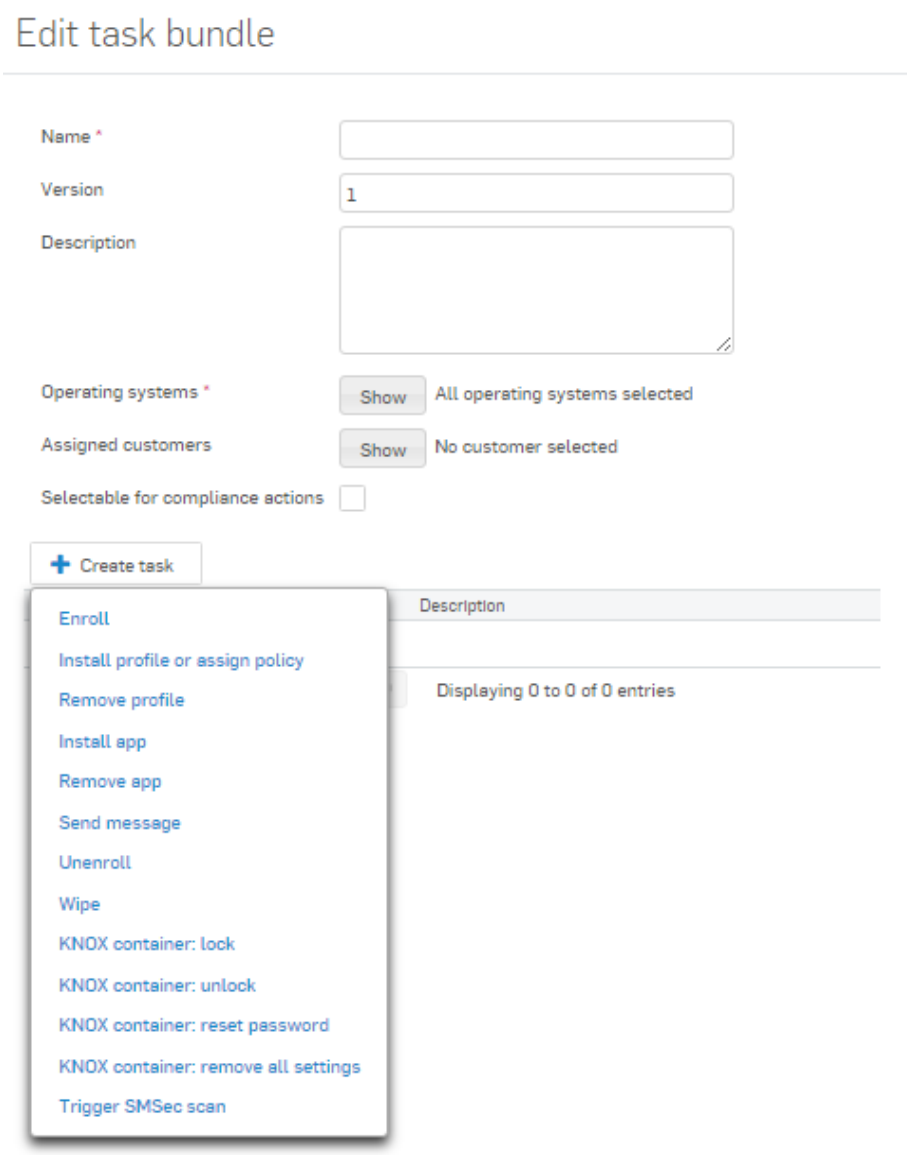
33. ábra: Android platform Compliance rules beállítási lehetőségei

Megjegyzés: *A beállítási lehetőségek platformonként és verzióként (Android, iOS, Windows Phone, Windows Desktop) eltérőek lehetnek!*

Ezekre az eseményekre külön-külön válaszreakciókkal reagálhatunk a készülékeken, ilyen lehet:

- Riasztás küldése az adminisztrátornak (**Beállítása:** Compliancerule-on közvetlenül)
- **„Taskbundles”**, azaz Feladat csomagok létrehozása, mint például
  - ✓ Üzenet küldése a felhasználónak
  - ✓ Alkalmazás eltávolítása
  - ✓ Telefon tartalmának törlése (Wipe)
  - ✓ Telefon kiregisztrálása az SMC környezetből (Unenroll), stb…

Beállítása: Configure/TaskBundles



34. ábra: Taskbundles létrehozása (például Android készülékekhez)

4.3. Emberi tényezőket figyelembe vevő (személy)biztonság

Munkakörök, feladatok biztonsági szempontú besorolása (3.1.6.2)

Jogviszony létesítése (Készülékek bevonása az SMC rendszerbe)
A készülékek bevonására több lehetőség is kínálkozik attól függően kinek a kezdeményezésére indul a csatlakoztatási folyamat. A bevonást kezdeményezhetik:

- a kijelölt **adminisztrátorok** vagy
- maguk a **felhasználók**, amennyiben erre jogot biztosítunk részükre az **Önkiszolgálói portálon keresztül (Self Service Portal)**

Készülékek bevonása az adminisztrátorok által
A folyamat segítségével a bevonni kívánt készülék közvetlenül az adott felhasználóhoz és készülék csoporthoz rendelhető, menete:

Beállítása: Manage/Devices/Add/Adddevicemanually/…

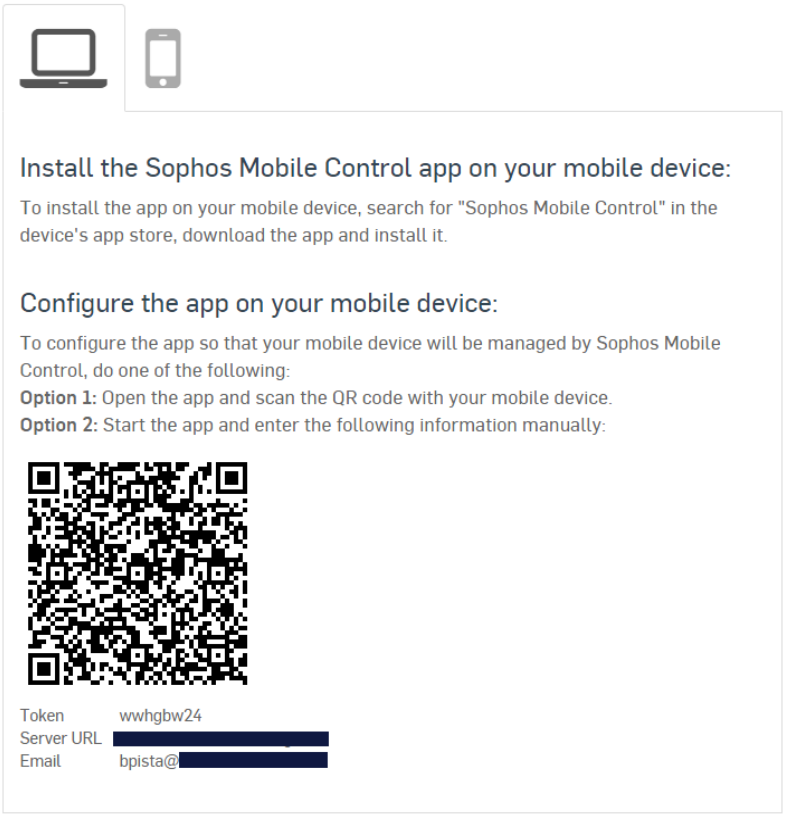
1. Adjuk meg a készülék nevét és leírását (Name, Desciption)!
2. Válasszuk ki a tulajdonlás típusát (Owner: Company, personal)!
3. Adjuk meg a felhasználó email címét (címtár integráció estén kiválaszthatjuk a felhasználót is)!
4. Válasszunk készülék csoportot (Device Group)!
5. Rendeljük hozzá a megfelelő **Compliance Rule**-t!

Megjegyzés: *A *-al jelölt mezők kitöltése kötelező!*

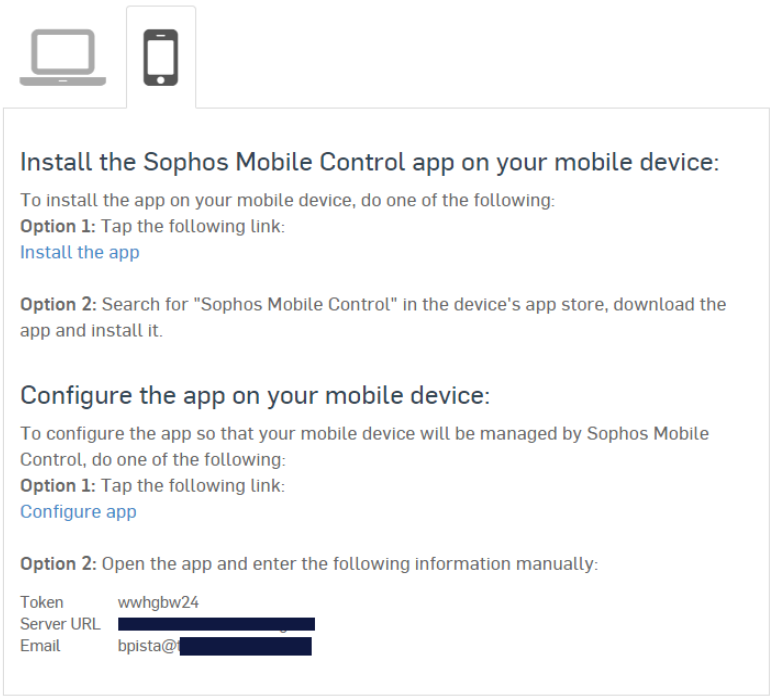
A fenti folyamat varázsló segítségével is elvégezhető, mely megtalálható az alábbi menüpont alatt: Manage/Devices/Add/Enrollment wizard/…

Készülékek bevonása a felhasználók által
Amennyiben a SMC rendszert úgy konfiguráltuk, hogy a felhasználók a **Self Service Portal**-on keresztül regisztrálhatják készülékeiket, úgy a következő folyamat segítségével az üzemeltetés leterhelése nélkül interaktív módon kezelhetünk nagyobb eszközparkot.

1. Lépjen be a felhasználó a **Self Service Portal**-ra egy böngésző segítségével! A felhasználók a címtár integráció segítségével saját, már megszokott felhasználói nevüket és jelszavukat használhatják. (URL: https://szervercím)
2. Kattintson az **Enrollnewdevice** gombra!
3. Fogadja el a megadott felhasználási feltételeket!
4. Válassza ki a készülék platformját!
5. Válassza ki a tulajdonlás típusát (Owner: Company, Personal)!
6. Kövesse a megjelenő utasításokat a készülék csatlakoztatására attól függően, hogy milyen eszközről kezdeményezte a mobilkészülék bevonását (PC-ről vagy magáról a mobilkészülékről)

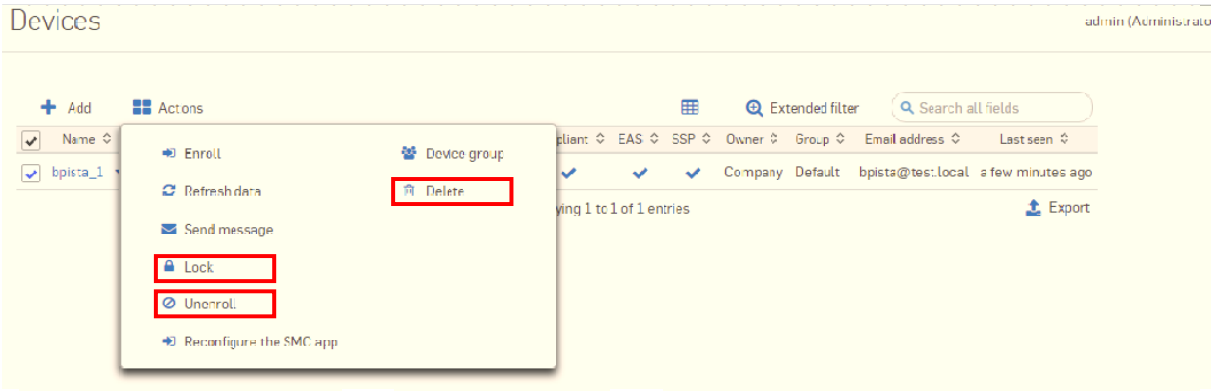


35. ábra: Készülékek bevonása a felhasználók által – PC-ről kezdeményezve



36. ábra: Készülékek bevonása a felhasználók által – mobilkészülékről kezdeményezve

Jogviszony megszüntetése (Készülékek blokkolása, kivonása az SMC rendszerből vagy törlése)
A munkaviszony megszűnése vagy a készülék elvesztése esetére több lehetőség is kínálkozik a készüléken tárolt, illetve elért érzékeny adatokhoz való hozzáférés megakadályozására.

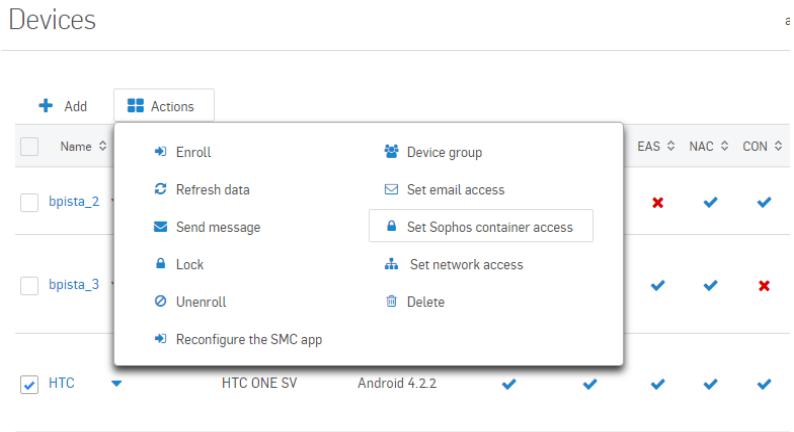


37. ábra: Készülék hozzáférésének korlátozása

Hozzáférés azonnali megvonása

1. **Lock** funkció: Készülék zárolása a teljes hozzáférés megakadályozása például elvesztés esetére. A készüléken tárolt információk megmaradnak, viszont nem lesznek elérhetők az illetéktelenek számára.

   Megjegyzés: *Ebben az esetben amennyiben az adatok tárolására a Sophos konténerizált szolgáltatásait alkalmaztuk az érzékeny információkat fájl szintű hozzáférés esetén sem érhetik el az illetéktelenek.*
2. Amennyiben a Sophos konténer szolgáltatásait használjuk részlegesen is letilthatjuk ehhez a hozzáférés a **Set Sophos container access** beállítás használatával, melyek az alábbiak lehetnek:
   - **Deny** – Tiltott
   - **Allow** – Engedélyezett
   - **Automode** – Compliancerule-hoz kötött, azaz, hogy a készülék éppen megfelel-e a beállított megfelelőségi szabályoknak



38. ábra: Set Sophos containeraccess beállítás

Hozzáférés visszavonása felhasználó cseréjéhez

Unenroll funkció: Rendszer kivonása a menedzsment fennhatósága alól, olyan esetben válik szükségessé, amennyiben a készüléket át akarjuk adni egy másik dolgozónak. Ebben az esetben a Sophos Mobile Control készülék oldali alkalmazása visszaáll menedzselés nélküli módban, a kapcsolódó Sophos konténerizált szolgáltatásai az alábbi állapotba kerülnek:

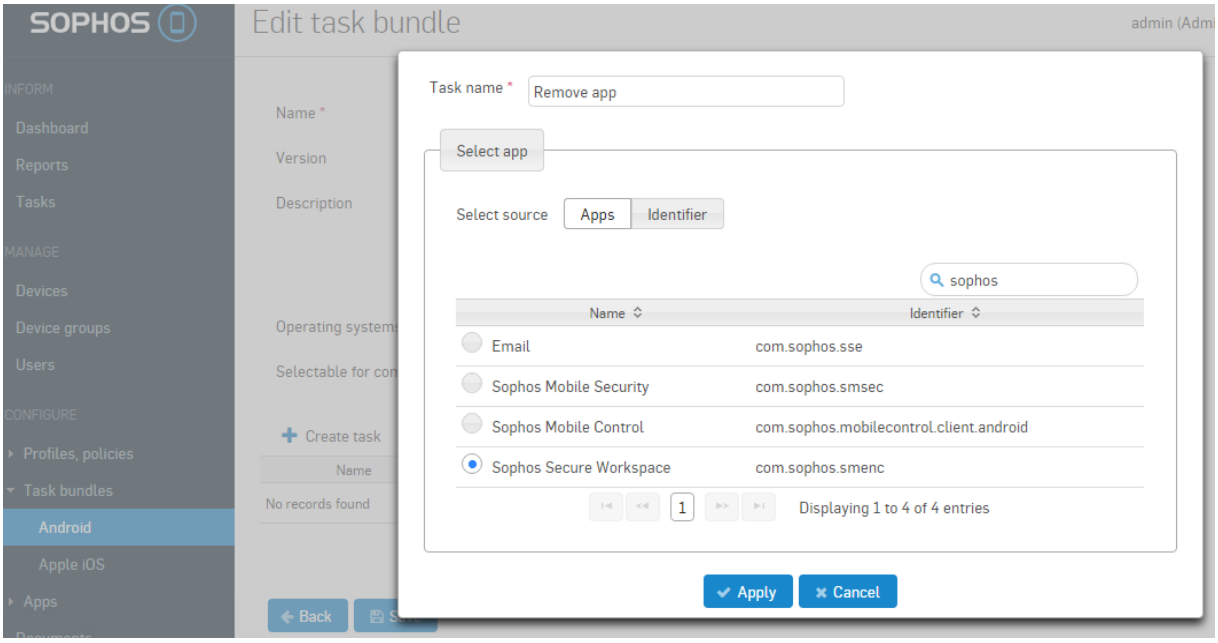
Android esetén: Sophos konténerizált szolgáltatásai lockolásra kerülnek az adatok tikosított formában a készüléken maradnak. Az új felhasználóhoz való hozzárendeléskor a régi felhasználó adatai automatikusan törlésre kerülnek.

iOS, Samsung SAFE, Windows 10 Mobile esetén: A vállalati adatok automatikusan törlésre kerülnek.

Ezt követően a készüléket a Sophos komponensek telepítése nélkül újra menedzselt állapotba hozhatjuk.

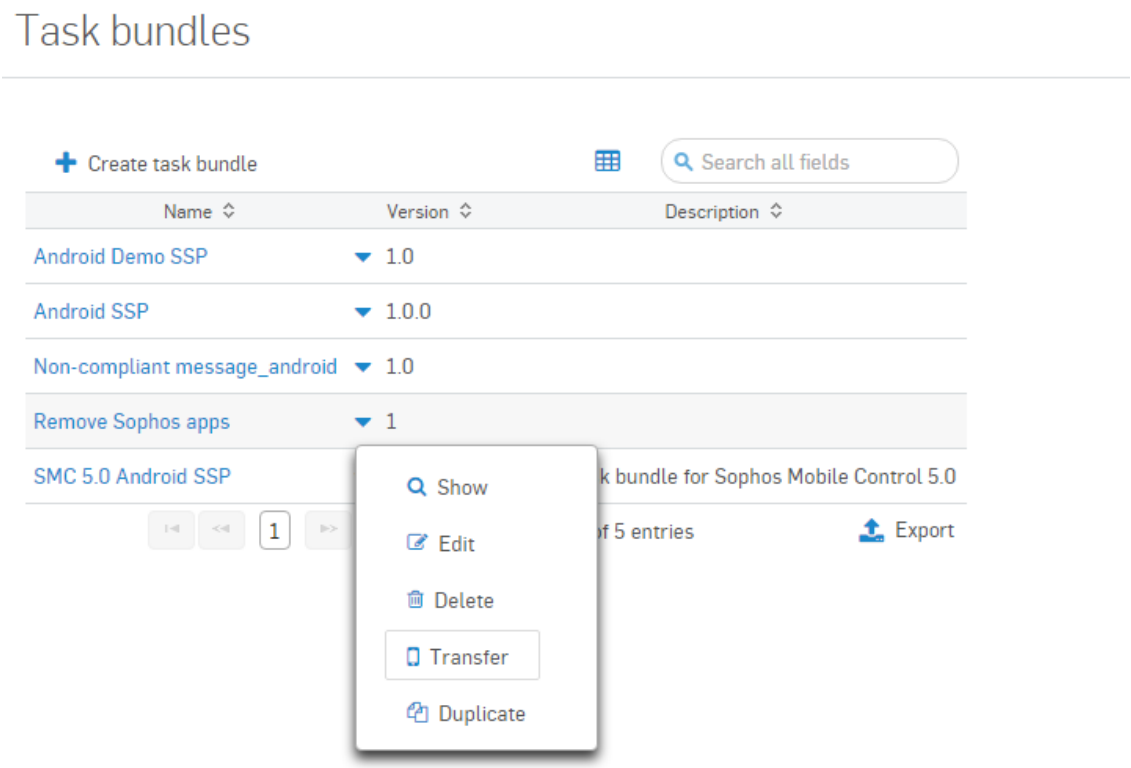
Hozzáférés megszüntetése (például a készülék selejtezése esetén)

1. **Wipe** funkció: Egy lépésben elvégezhetjük a készülék teljes tartalmának törlését. Ezt a készüléken a gyári beállítások visszaállítása funkcióval végezhetjük el távolról (Remotefactoryreset). A készüléken lévő ÖSSZES ADAT TÖRLÉSRE kerül!
2. **Szelektív törléssel** (távolról az SMC felületén keresztül):
   (1) Távolítsuk el a készülékről a Sophos alkalmazásait a konténerizált szolgáltatásokhoz tartozó tárolt tartalmak megszüntetéséhez. Ehhez a **Taskbundles** közül hozzunk létre **Removeapp** típusú feladatot és adjuk hozzá az eltávolítandó alkalmazásokat.



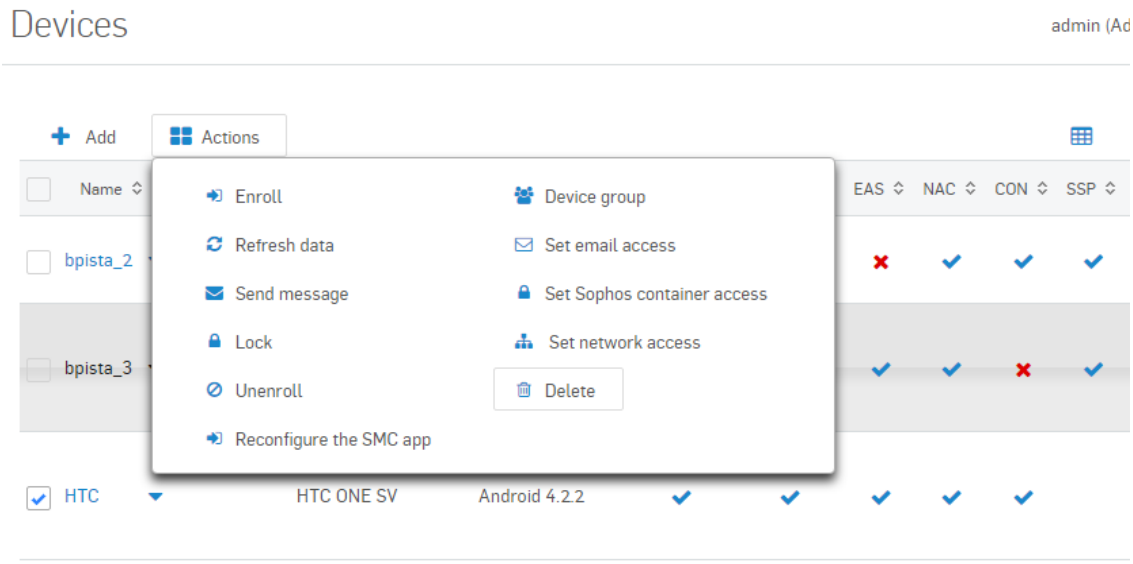
39. ábra: Remove app feladat létrehozása

(2) A létrehozott feladatot hajtsuk végre a készülékeken a **Transfer** funkció segítségével!



40. ábra: Adott feladat végrehajtása a készülékeken

(3) Töröljük a készüléket a központi menedzsmentből a **Delete** funkció használatával!



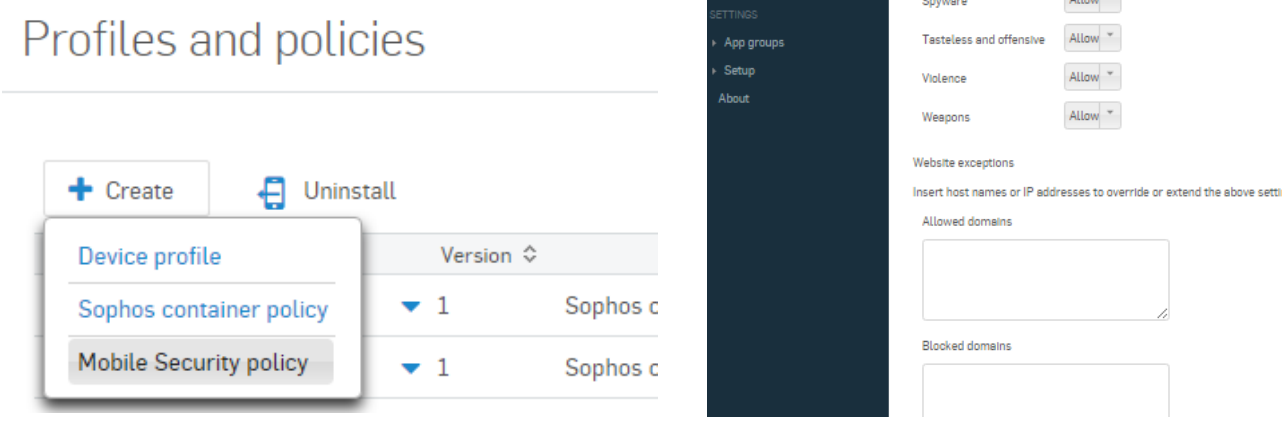
41. ábra: Delete funkció használata

Viselkedési szabályok az interneten, tartalomszűrés (3.1.6.9.2)

A felhasználók internetezési szokásainak megregulázására és a kártékony tartalmak elkerülésére a készülékeken az alábbi lehetőségeket kényszerít-hetjük ki:

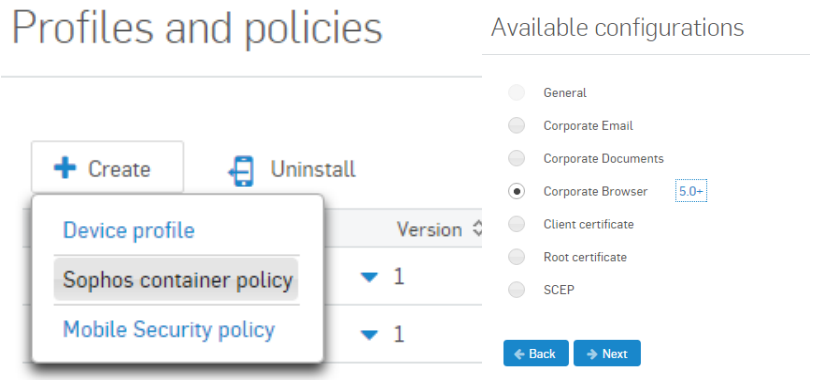
1. **Web kategóriák** engedélyezése (Allow), engedélyezése figyelmeztetéssel (Warning) vagy tiltása (Block).
2. **Egyedi URL vagy IP címek** fehér és fekete listázása

A beállításokat platformonként (Android, iOS) eltérő módon a **Configure/Profiles, policies/…** menüpont alatt állíthatjuk be a különböző vonatkozó policykben.



42. ábra: Web szűrés beállítása Android rendszerű készülékeken

3. **Érzékeny információt** tartalmazó vállalati oldalak konténerizált, védett böngészőn történő megtekintésének beállítása pl.: intranetes siteok (Android 5,0+ és iOS esetén).
   (1) Hozzunk létre egy **Sophos container policyt!**
   (2) Válasszuk ki a **Corporate Browserhez** tartozó konfigurációs lehetőséget!
   (3) Adjuk meg kikényszerítendő URL-eket az **Add domain** funkció segítségével!



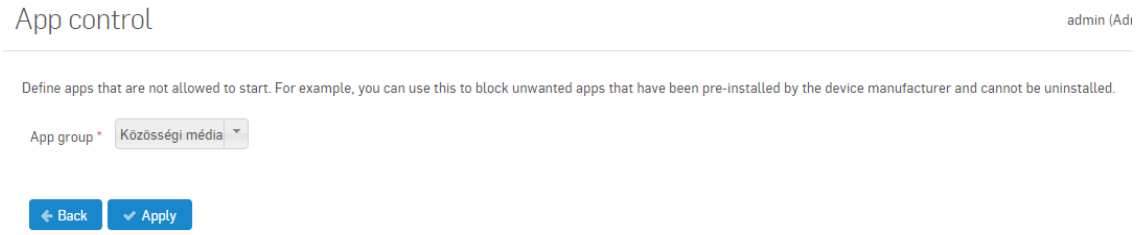
43. ábra: Érzékeny információt tartalmazó weboldalak védett böngészőbe történő irányítása

Közösségi média szűrése, böngészőn keresztüli elérés korlátozása (3.1.6.9.1.3/1.)

A közösségi média elérését két oldalról is korlátoznunk szükséges. Egyrészt a böngésző alapú **weblapok eléréseinek korlátozásával** a korábbi fejezetben foglaltak alapján, illetve a közösségi médiát elérő **kliensalkalmazások futtathatóságának korlátozásával.**

Közösségi média szűrése, kliens alkalmazások korlátozása (3.1.6.9.1.3/2.)

A készülékeken telepített alkalmazások listájából vagy meghatározott alkalmazásokból tetszőleges csoportokat hozhatunk létre. Ezt követően a létrehozott csoportokat a készülékekre ható policyban használhatjuk, mint **kötelezően telepítendő, tiltott** vagy **engedélyezett** alkalmazások. A közösségi média korlátozásához hozzunk létre alkalmazás csoportot a tiltandó kliensalkalmazásokkal, majd rendeljük azokat **Deviceprofile**-ok **Forbiddenapps** (iOS, Windows Mobile)/**Appcontrol** (Android) beállításaihoz.



44. ábra: AndroidAppControl funkciójának beállítása

4.4. Karbantartás

Külső eszközhozzáférések korlátozása (3.3.7.4.3.1.)

Az érintett szervezet megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan elektronikus információs rendszerből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a szervizelt rendszer biztonsági képességekkel.

A pont teljesítéséhez a jelen dokumentum 3.1.6.2/7-ben leírt folyamat alkalmazható!

3.3.7.4.3.3. Amennyiben a 3.3.7.4.3.1. szerinti eljárást nem lehet lefolytatni és a 3.3.7.4.3.2. pont szerinti eljárás nem került elvégzésre, a szervizelés végrehajtását követően át kell vizsgálni az elemet a lehetséges kártékony szoftverek miatt, mielőtt visszakapcsoljak az elektronikus információs rendszerhez.

Android platform esetén távolról is kikényszeríthető a készüléken a **kártékony szoftverek keresése a Configure/Taskbundles/Android/TriggerSMSecscan** feladat indításával.

4.5. Konfigurációkezelés

Aláírt elemek (3.3.6.5.4.)

A szervezet által meghatározott szoftver- és az úgynevezett firmware (vezérlőeszköz) elemek esetében meg kell akadályozni az elemek telepítését, ha azok nincsenek digitálisan aláírva ismert és jóváhagyott tanúsítvány alkalmazásával.

Ez a pont a mobilkészülékek esetében csak részben alkalmazható technológiai sajátosságuk miatt, azonban az eszközök kezelésekor a **Compliancerule**-okkal előírható az elvárt minimális és maximális OS verzió (firmware) használata.

Nem futtatható szoftverek (3.3.6.7.3.)

Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját, és megtiltja ezek futtatását.

Futtatható szoftverek (3.3.6.7.4.)

Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben jogosultan futtatható (engedélyezett, úgynevezett fehérlistás) szoftverek listáját, és engedélyezi ezek futtatását, az ettől eltérő szoftver futtatását egyedi engedélyhez köti.

Elektronikus információs rendszerelem leltár (3.3.6.8.)

Az SMC **Reports** menüpontja számos lehetőséget kínál a kezelt készülékek nyilvántartásához és azokon futó alkalmazások leltárazásához. Az előre definiált reportok Excel és CSV formátumba exportálhatók, univerzális lehetőséget kínálva az egyéni nyilvántartások készítéséhez.

A szoftverhasználat korlátozásai (3.3.6.10.)

A rendszerben lehetőségünk van különböző alkalmazáscsoportok létrehozásához. Ezt követően ezeket a csoportokat felhasználhatjuk a készülékek beállításaiban, mint **kötelezően telepítendő, tiltott** vagy **engedélyezett** alkalmazások.

Adathordozó-ellenőrzés (3.3.7.3.2.)

Az érintett szervezet ellenőrzi a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

Az Android rendszerű készülékek esetén van értelmezve és biztosítható a kártékony programok elleni védelem (alkalmazás telepítéskor és időzítetten), valamint a csatlakoztatott tárolók pl.: SD kártyák ellenőrzésére a **Sophos Mobile Security** alkalmazással. Az SMS alkalmazás a központi menedzsmenten keresztül átfogóan kezelhető és felügyelhető (Lásd még jelen dokumentumban a **3.3.7.4.3.3.** fejezetet).

A számítógépes rendszerre csatlakoztatott mobilkészülékek hordozható médiaként való alkalmazására pedig a végpontvédelmek szabályozott beállítása az irányadóak (USB scan beállítás).

4.6. Hozzáférés ellenőrzése

Letiltás (3.3.10.2.8.)

Azonnal le kell tiltani a kockázatot jelentő felhasználók fiókjait.

A lehetőségeket a 3.1.5. fejezet tartalmazza.

Sikertelen bejelentkezési kísérletek (3.3.10.7.)

Az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire.

A hitelesítést kérő szolgáltatásoknál meghatározható a **belépési kísérletek száma**, amelynek megsértése esetén az adott szolgáltatás **zárolásra** (Lock) vagy a készüléken lévő adatok **törlésre** (Wipe) kerülnek (ez a lehetőség szolgáltatásonként eltérő).

Képernyőtakarás (3.3.10.10.2.)

A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel – ami a zároló személy nevét is tartalmazhatja – kell eltakarni.

A Sophos konténerizált szolgáltatásai minden esetben biztosítják, hogy az érzékeny információkat a felhasználók csak **megfelelő hitelesítés után érhessék el**. Amennyiben kiléptek az alkalmazásból a következő belépésnél újra hitelesítés szükséges, ha a **Graceperiodinminutes** beállításban meghatározott idő letelik.

A konténer beállításainál szabályozható, hogy az érzékeny adatokkal mit végezhet a felhasználó, azok kikerülhetnek-e a kontérnerből (pl.: copy/paste).

Beállítása: Configure/Profiles, policies/<<Platform>>/Create/Sophos container policy/Add configuration/…

Vezeték nélküli hozzáférés (3.3.10.14.)

3.3.10.14.1.1. Belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán.

Valamennyi platform esetén lehetőség van Wifi hálózat konfigurációjának leküldésére a készülékekre.

Beállítása: Configure/Profiles, policies/<<Platform>>/Create/Deviceprofiles/Add configuration/Wifi

Mobil eszközök hozzáférés-ellenőrzése (3.3.10.15.)

Belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre.

Külső elektronikus információs rendszerek használata (3.3.10.16.)

Meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez.

Működtetését a **Compliancerule-ok** biztosíthatják, melyekkel megakadályozható a vállalati adatokhoz való hozzáférés valamely szabálysértés esetére pl.: fertőzés esetén, rootolt/jailbreakelt eszközök esetén, stb… (Lásd még a **3.1.5.2.** fejezetet!)

4.7. Rendszer- és információsértetlenség

Kártékony kódok elleni védelem (3.3.11.4.)

Csak Android eszközök esetén értelmezhető a kártékony kód elleni védelem.

Compliancerule segítségével ellenőrizhető és biztosítható a védelemben a **szkennelések közötti időközök** minimális értéke. A készülékre alkalmazott **Compliancerule**-ok megsértése esetén automatikusan kikényszeríthető a pl.: kártékony kód ellenőrzése a **Configure/Taskbundles/Android/TriggerSMSecscan** feladat indításával. (Lásd még a **3.1.5.2.** fejezetet!)

A szkennelések ütemezetten is elvégezhetők a **Sophos Mobile Security** alkalmazás policy beállításában.

Automatizálás (3.3.11.5.2.)

Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.

Riasztás (3.3.11.5.4.)

Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

Az SMC rendszer működésének vonatkozásában annak állapotáról folyamatos emailes tájékoztatást kapnak a beállított adminisztrátorok. Ezen felül a készülékek esetén **Compliancerule**-onként beállítható, hogy megsértésük esetén, melyik adminisztrátor kerüljön értesítésre a rendszer által. (Lásd még a **3.1.5.2.** fejezetet!)

Sértetlenség ellenőrzés (3.3.11.8.2.)

Az elektronikus információs rendszer sértetlenség ellenőrzést hajt végre a meghatározott szoftverekre és információkra, a rendszer újraindításakor, vagy biztonsági esemény bekövetkezését követően, vagy meghatározott gyakorisággal.

A készülékre alkalmazható **Compliancerule**-ok megsértése esetén automatikusan kikényszeríthető a kártékony kód ellenőrzése a **Configure/Taskbundles/Android/TriggerSMSecscan** feladat indításával.

Végrehajtható kód (Végrehajtható kód) (3.3.11.8.6.)

Az elektronikus információs rendszer megtiltja az olyan bináris vagy gépi kód használatát, amely nem ellenőrzött forrásból származik, vagy amelynek forráskódjával nem rendelkezik.

Android és iOS rendszerű készülékek esetén megtiltható az **alkalmazások felhasználó általi telepíthetősége**. Mindemellett Android platform esetén értelmezhető és megtiltható az is, hogy **más forrásból származó alkalmazásokat telepíthessen a felhasználó**, mint a Play Store. Mindezeket a korlátozásokat az adott profile **Restrictions** beállításaival végezhetjük el.

4.8. Rendszer- és kommunikációvédelem

Együttműködésen alapuló számítástechnikai eszközök (3.3.13.12.)

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

A SMC jelenlegi verziójában (6.1.4) nincs lehetőség az ilyen jellegű komponensek távoli eszközön történő bekapcsolására. Ellenkezőleg, a beállítási lehetőségek ezen komponensek korlátozására terjednek ki.

5. Mobil eszközök kezelése IBM Maas360 –nal

IBM MaaS360 olyan képességekkel rendelkezik, amely segít az IT szervezeti egységeknek felügyelet tartani a mobil eszközöket, alkalmazásokat és dokumentumokat megőrizve a felhasználói elégedettséget és a vállalati adatbiztonságot is. Jól skálázható, több előfizetésre tervezett architektúra, egyszerű kezelhetőség, megfizethető és azonnal használatba vehető megoldás az IBM MaaS360.

5.1. IBM MaaS360 Mobile Device Management

IBM MaaS360 átfogó és biztonságos megoldást biztosít az összes komolyabb mobil platformhoz nagyvállalati környezetben. Legyen szó iOS-ről, Androidról, BlackBerry vagy Windows Phone eszközről, MaaS360 a teljes életciklusát lefedi az eszköznek: felügyelet alá vonás, biztonság, monitoring, alkalmazás management és végfelhasználói támogatás. Fontosabb területek, amire a MaaS360 képes:

- Email, Wi-Fi, és VPN profilok konfigurálása over the air (OTA)
- Jelkód, titkosítás kierőszakolása
- Eszköz funkcionalitás korlátozása
- Elveszett vagy ellopott eszköz helyzetének meghatározása
- Távoli zárolás és törlés
- Szelektív törlés, mely csak a vállalati adatokat érinti
- Végfelhasználói önkiszolgáló felület
- Automatikus compliance management
- Meglévő vállalati rendszerekhez való integráció (Exchange, AD/LDAP, tanúsítványok, stb.)
- Alkalmazások telepítése a vállalati alkalmazás katalógusból
- Vállalati dokumentumok disztribúció
- Adatforgalom kezelése

5.2. MaaS360 Secure Productivity Suite

MaaS360 Secure Productivity Suite (SPS) olyan cross-platform megoldás, aminek a segítségével el lehet választani a vállalati adatokat (névjegyek, naptár események, tennivalók, levelezés, vállalati alkalmazások) a személyes adatoktól. Az SPS igazi ereje a BYOD (Bring Your Own Device – alkalmazott saját tulajdonú eszköze) eszközöknél mutatkozik meg. MaaS360 az egyetlen felhő alapú megoldás, amely lehetőséget kínál a vállalati adatokhoz való biztonságos hozzáféréshez anélkül, hogy a munkavállaló saját eszközének használatában kényelmetlenséget okozna.

MaaS360 SPS megoldása adatvesztés ellen is véd. Legyen szó authentikációról, authorizációról, csak a korábban jóváhagyott felhasználók férhetnek hozzá a szenzitív adathoz. A secure container házirendeken keresztül szabályozható az adathoz való hozzáférés módjai, azok megosztása, csatolmányok továbbítása, de akár a másolás-beillesztés is. Az elveszett vagy ellopott eszközökről szelektíven, csak a vállalathoz köthető dokumentumok, alkalmazások, profilok, tanúsítványok egy mozdulattal eltávolíthatók.

- MaaS360 Secure Mail – intuitív irodai programcsomag e-mail, naptár és névjegy funkcióval.
- MaaS360 App Security – mobil alkalmazás konténer, amelyen a házirendek segítségével kikényszeríthető az elvárt titkosítást, biztonságot és az adatszivárgás ellen is véd.
- MaaS360 Secure Document Sharing – olyan biztonságos dokumentumkonténer, amely lehetővé teszi a dokumentumok biztonságos hozzáférését, megtekintését, megosztását fájlok és email csatolmányok esetében.
- MaaS360 Secure Browser – teljes értékű böngésző, amely kikényszeríti a biztonsági és HR házirendeket és biztonságos hozzáférést biztosít a vállalati intranet oldalakhoz.

5.3. Igaz Mobility-as-a-Service (MAAS)

A biztonságos, multi-tenant architektúrával rendelkező felhő alapú kialakításnak köszönhetően, a MaaS360 rendkívül gyorsan és egyszerűen bevezethető. Nincs szükség helyi szerverek telepítésére, kialakítására és konfigurálásra. Csak létre kell hozni egy felhasználói fiókot és már kezdődhet is az

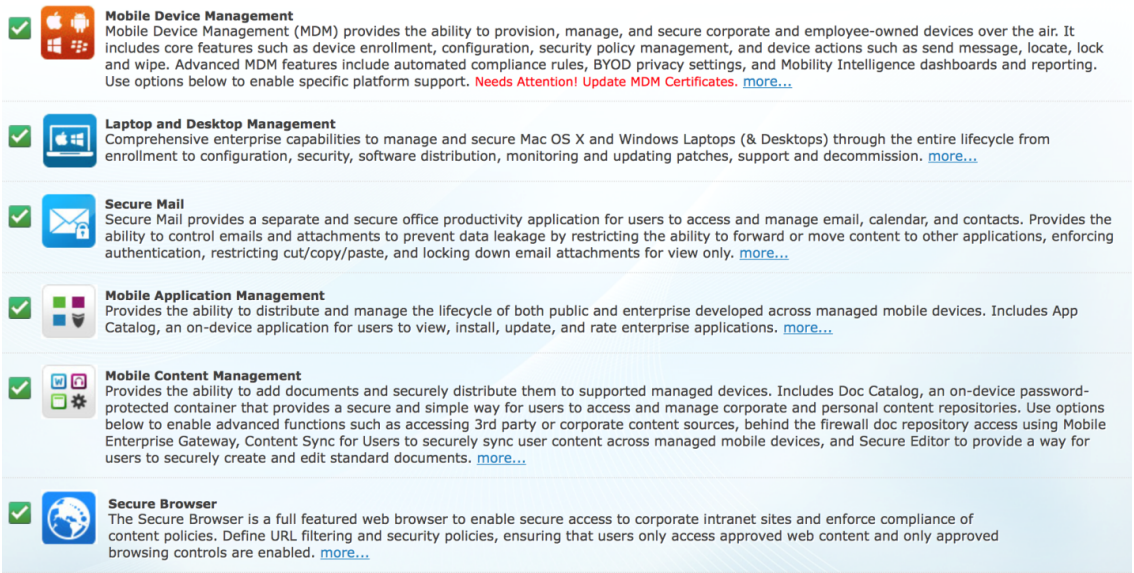
eszközök felügyelet alá vonása. A MaaS360-nak köszönhetően azonnali betekintést kaphatnak az adminisztrátorok az eszközállományba, a telepített alkalmazásokba, erőforrás-hozzáférésekhez.

A MaaS360 szolgáltatása előfizetés alapú, hozzáférhetősége az interneten keresztül történik. A felhasználók mindig a legfrissebb verzióval rendelkeznek, nincs szükség manuális telepítésre. Csak az igénybe vett szolgáltatásokért kell fizetni és csak akkor, amikor szükség van rá.

5.4. A megoldás részleteiben

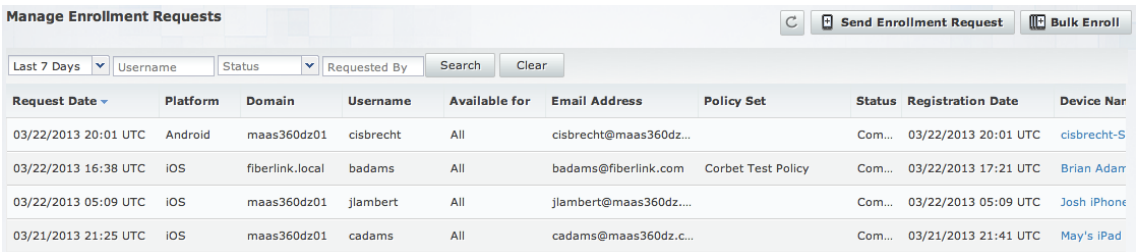
A MaaS360 egyedülálló módon teszi lehetővé a mobil stratégia által megfogalmazott igények kielégítését oly módon, hogy a felhasználók képesek legyenek a vállalati adatokhoz és erőforrásokhoz hozzáférni a saját tulajdonukban lévő eszközökről, legyen szó okostelefonról, tabletről vagy notebookról a szükséges biztonsági óvintézkedések mellett. Az alábbi lista csak a főbb képességeket szemlélteti, amelyet szerettünk volna kiemelni.

Támogatja a ma ismert összes fontosabb készülékgyártót, beleértve az Apple iOS 4.0+, Android 2.2+, Samsung SAFE/ELM eszközöket, Windows Phone 7.5 és 8/8.1, Windows 10, BlackBerry 5.0. Laptopok esetében, a MaaS360 Windows eszközök esetében Windows XP SP3-tól, Apple Mac OS X eszközök esetén 10.5 verziótól napjainkig.



45. ábra: A MaaS360 főbb funkció

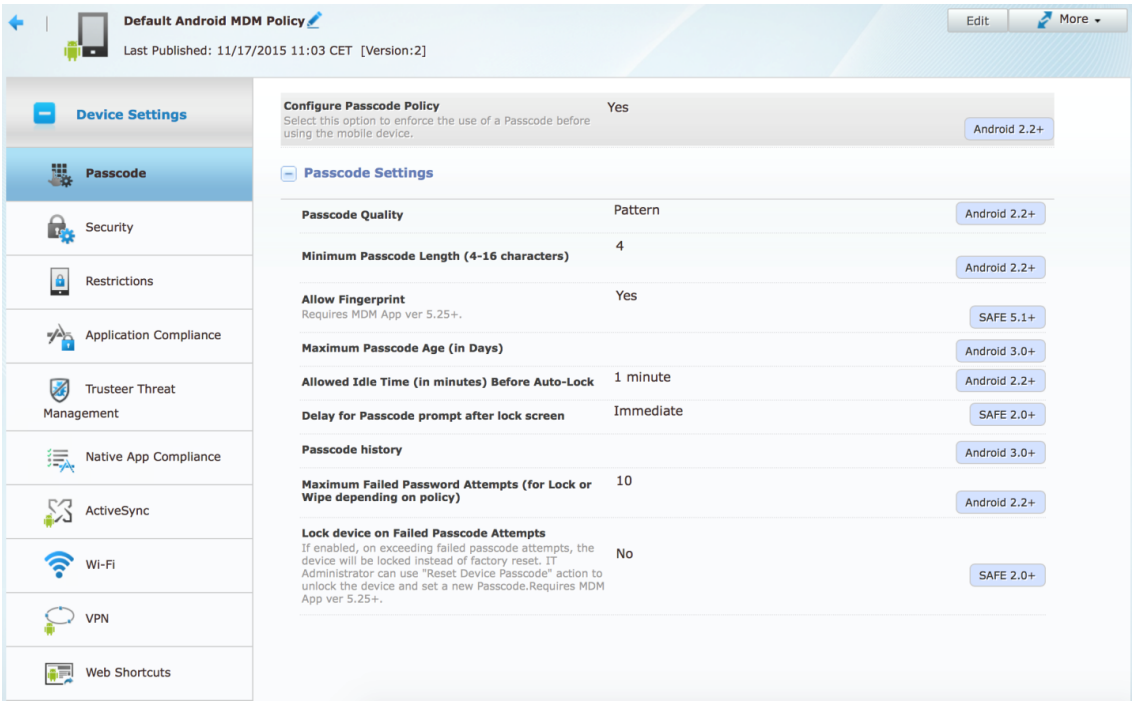
A MaaS360 képes felfedezni azokat az új eszközöket, amelyek megpróbálnak csatlakozni a vállalati erőforrásokhoz. Ezekre az eszközökre felügyelet alá vonási kérelmet is küldhetünk. Ezzel a képességgel megakadályozható, hogy olyan eszköz csatlakozzon, amely korábban nem lett jóváhagyva.



46. ábra: A hálózati erőforrásokhoz való hozzáférés naplózása

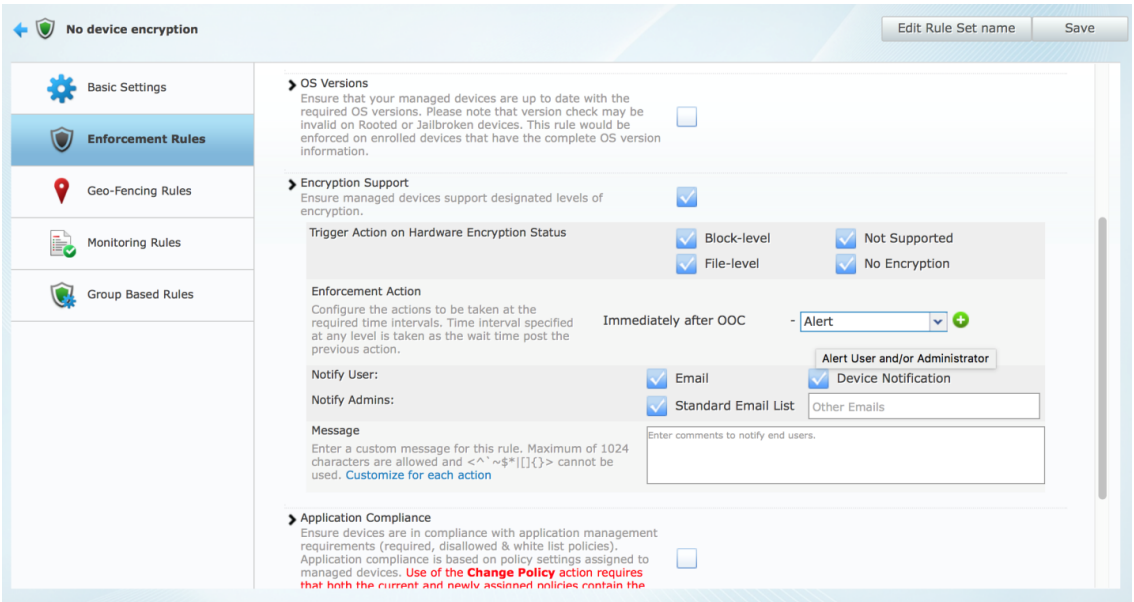
A MaaS360 házirendeket használ, hogy az eszközök biztonságosak maradjanak. Ezek a házirendek számos dolgot szabályozhatnak, kezdve a jelkódtól, az automatikus zároláson át, bizonyos alkalmazások letiltásáig.

A házirendeket a készülékek automatikusan letöltik. A felhasználónak nem szükséges a vállalati hálózathoz csatlakoznia, minden házirend módosítás az interneten keresztül kerül a készülékre.



47. ábra: Házirend

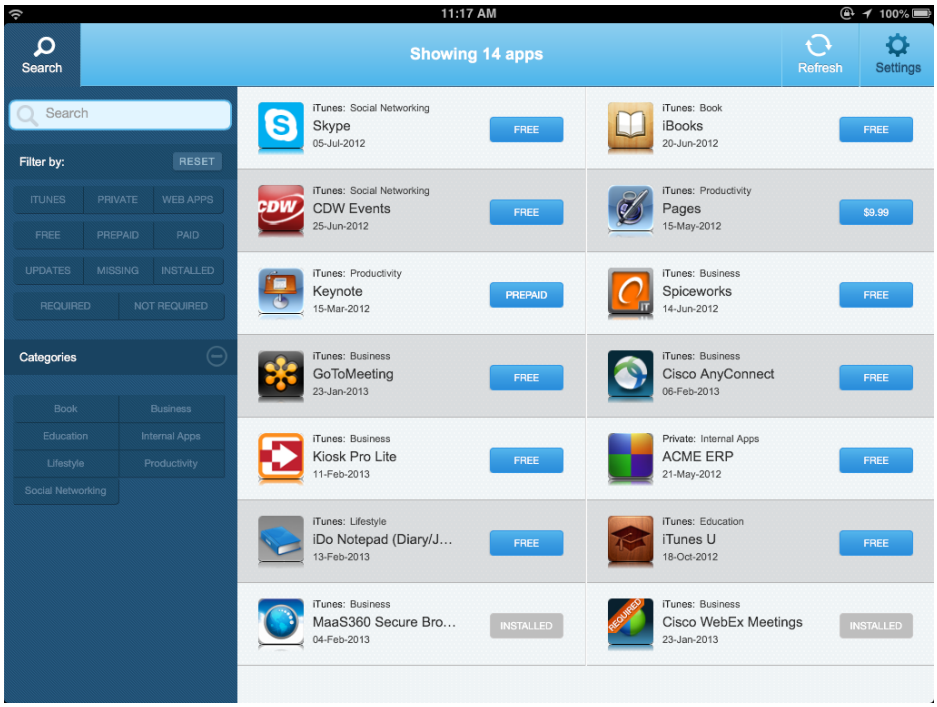
A MaaS360 Compliance Engine mindig gondoskodik róla, hogy a mobil eszközök megfeleljenek a házirendeknek. Bármely pillanatban, ha egy eszköz megszegi a házirendet, a MaaS360 érzékeli és végrehajtja a korábban definiált akciót.



48. ábra: Biztonsági szabályrendszer ellenőrző funkció (MaaS360 Compliance Engine)

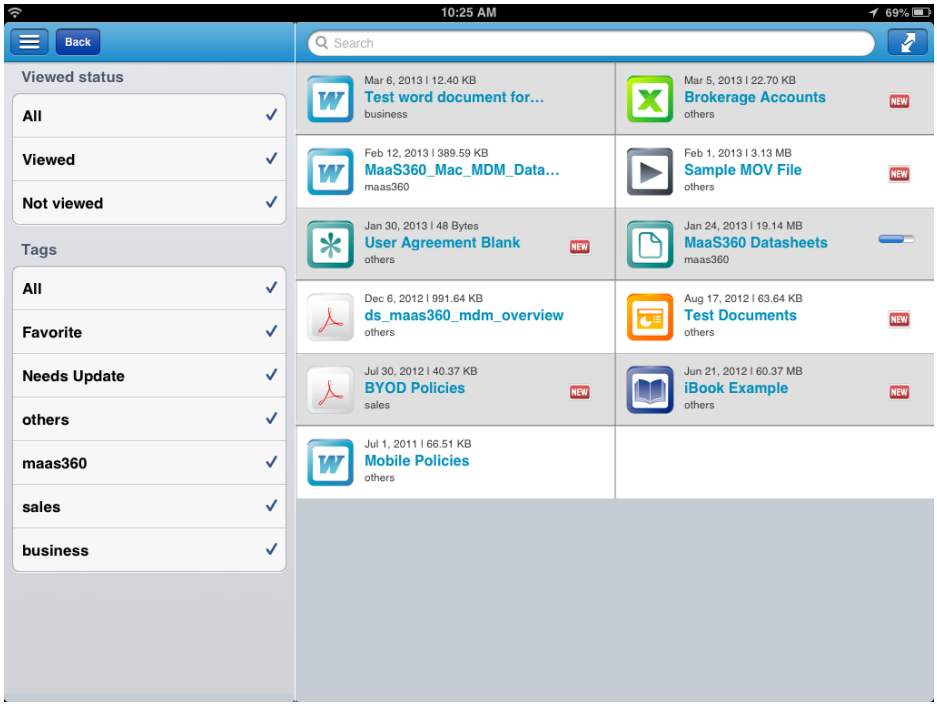
A MaaS360 intuitív vállalati alkalmazás katalógust is biztosít iOS-re, Androidra és Windows eszközökhöz egyaránt. Ebben a katalógusban definiálhatók a felhasználók számára, hogy milyen publikusan is letölthető alkalmazások legyenek telepíthetőek, de akár házon belül fejlesztett alkalmazásokat is tartalmazhat a lista.

Az alkalmazások lehetnek kötelezőek, megengedettek, vagy éppen tiltottak is, ezen állapotoknak a kezelését a MaaS360 végzi.



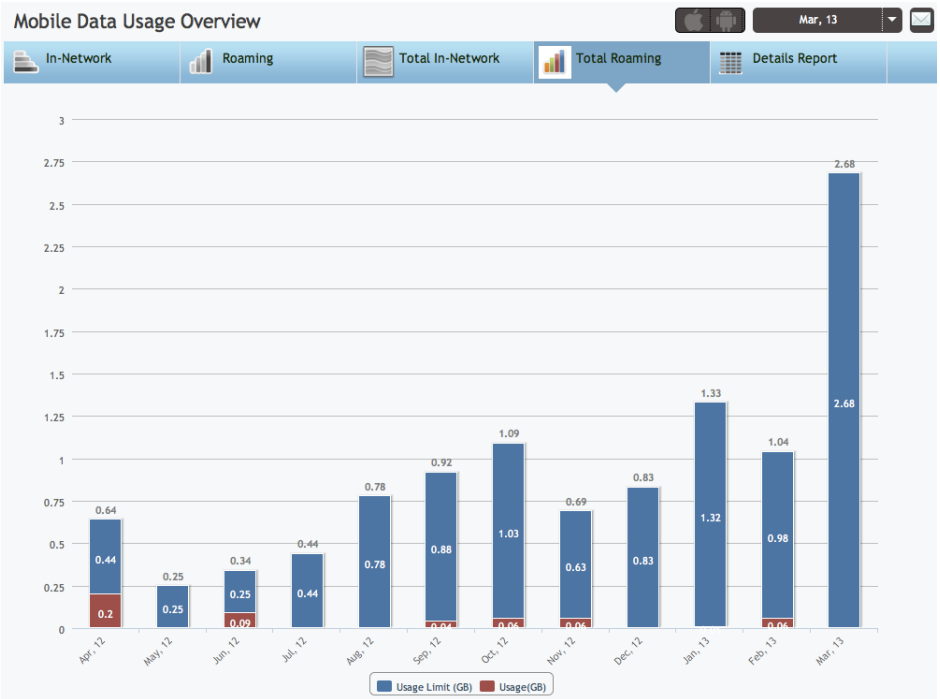
49. ábra: A telepíthető alkalmazások listája

A MaaS360-ban egyszerűen lehet a különböző vállalati dokumentumokat elérhetővé tenni a mobil eszközökön. Csak néhány kattintás az IT által és a dokumentum már feltöltésre is került, és elérhetővé vált az eszközökön, továbbá az utóbbiról statisztikai adatokat is kaphatnak. A dokumentumokat lejárati dátummal is el lehet látni, így annak lejáratakor a dokumentum automatikusan törölve lesz. Amikor egy új dokumentum elérhetővé vált, az érintett felhasználók azonnal értesítést kapnak, így nem szükséges folyamatosan frissíteni. Támogatott formátumok között szerepel a ma is ismert és széles körben használt Microsoft Office formátumok, PDF-ek, Google dokumentumok, csakúgy, mint videó- és hanganyagok.



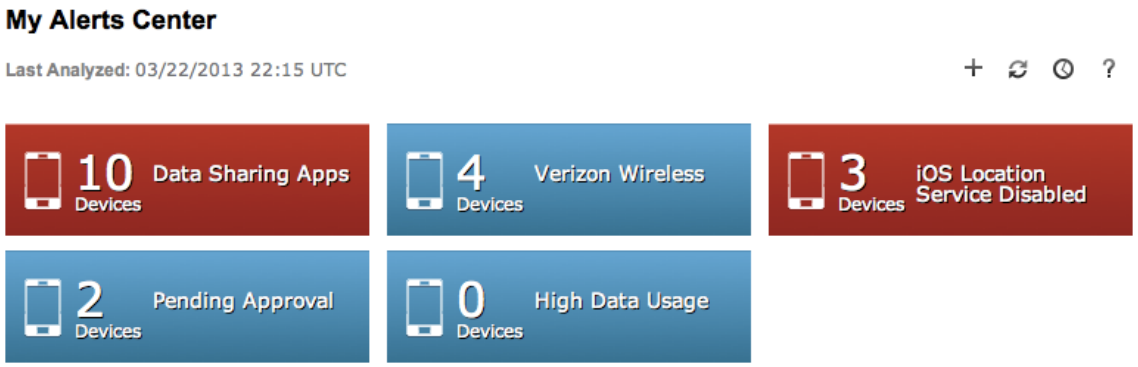
50. ábra: A szervezeten belüli dokumentum megosztás (kollaborációs szolgáltatás)

A ma használt mobileszközök illetve alkalmazások több adatforgalmat generálnak, mint eddig korábban, így a MaaS360 segítségével könnyedén megtehetik az IT adminisztrátorok, hogy az adathasználati kereteket bizonyos határok közé terelje, legyen az hazai vagy roaming adathasználat. A felhasználó értesítést fog kapni, ha hamarosan eléri a beállított határértéket, további használat esetén akár az adathozzáférés is letiltható. A hozzátartozó riport funkciók lehetővé teszik az eszköz specifikus, illetve a teljes szervezet által használt adatmennyiségek riportjainak megtekintésére.



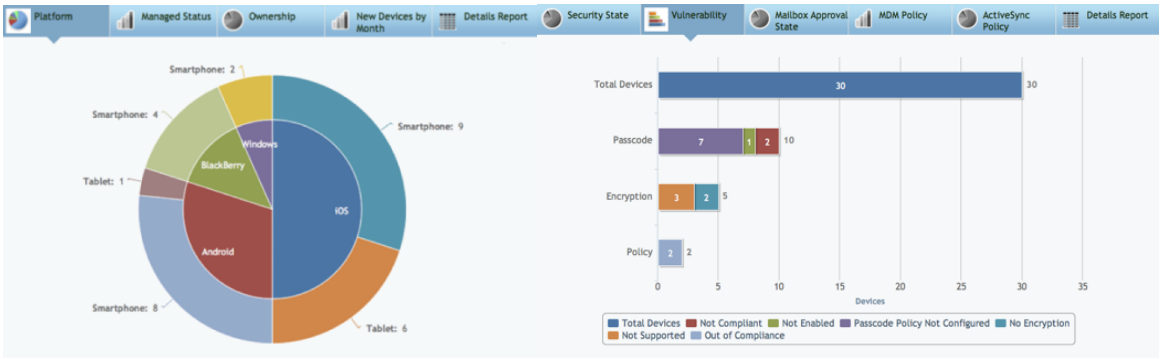
51. ábra: Felhasználói statisztikák

A MaaS360 adminisztrációs felületén, a My Alerts Center segítségével gyorsan és könnyeden kaphatunk áttekintő képet arról, hogy az aktuálisan kezelt eszközparkban milyen eszközök jelenthetnek problémát, de arról is, hogy hány új eszköz került aktiválásra az elmúlt 7 napban. Természetesen használhatóak a gyárilag előre konfigurált figyelmeztetések, de mi magunk is létrehozhatunk egyedileg újakat.



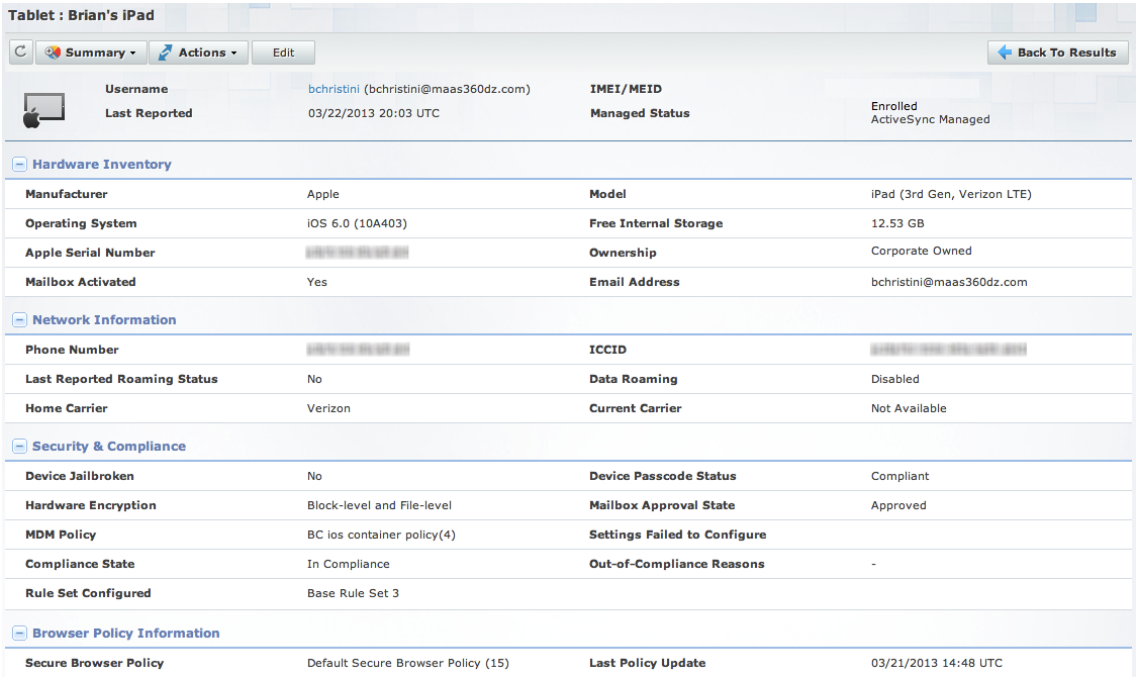
52. ábra: A MaaS360 adminisztrációs felülete

A MaaS360 továbbá biztosít ún. executive és operational felületeket, ahol nyomon követhetők a vállalati és alkalmazottak által használt eszközállomány tulajdon megoszlása, lehetőség van platform szerinti szűrésre, továbbá, hogy átlagosan hány új eszköz kerül nyilvántartásba, és a rengeteg mért információ mentén akár még mélyebbre is lehet fúrni.



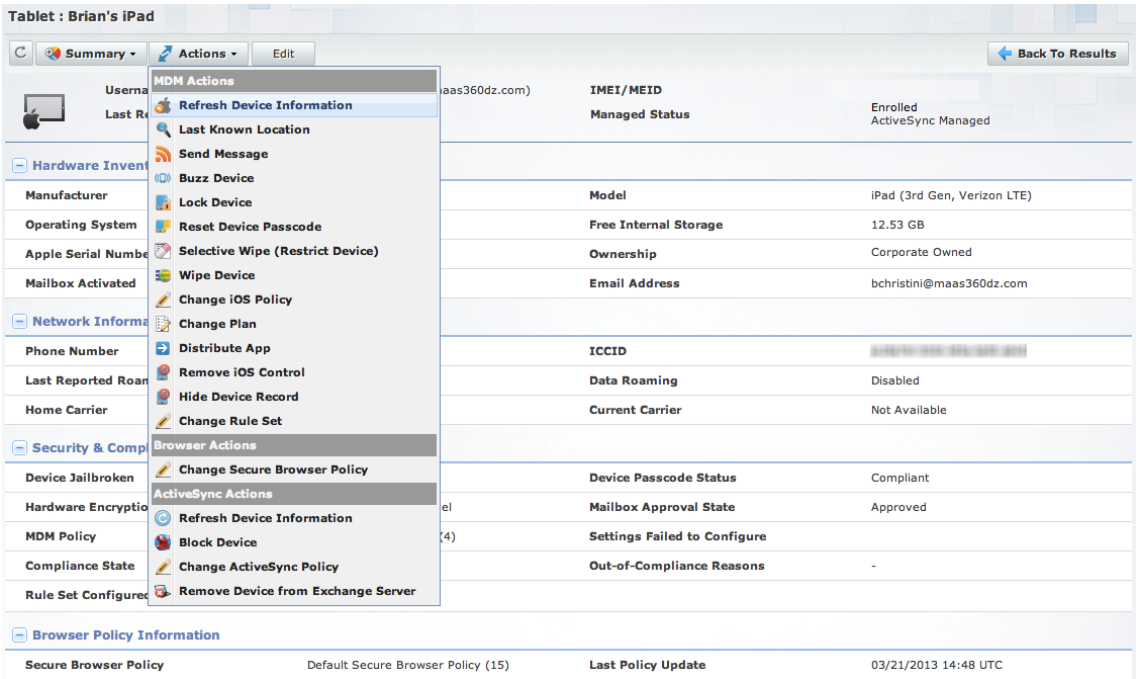
53. ábra: Néhány példa a statisztikák megjelenítésére

A MaaS360 minden adatot, amit az eszközről összegyűjtött, a Device View nézetben tekinthető meg. Ideális képernyő hibakereséskor, továbbá az alapvető ügyfélszolgálati munkákhoz. Az adminisztrátorok ezenfelül megtekinthetik a készülék hardver képességeit, a telepített alkalmazásokat, biztonsági beállításokat, aktív házirendeket stb.



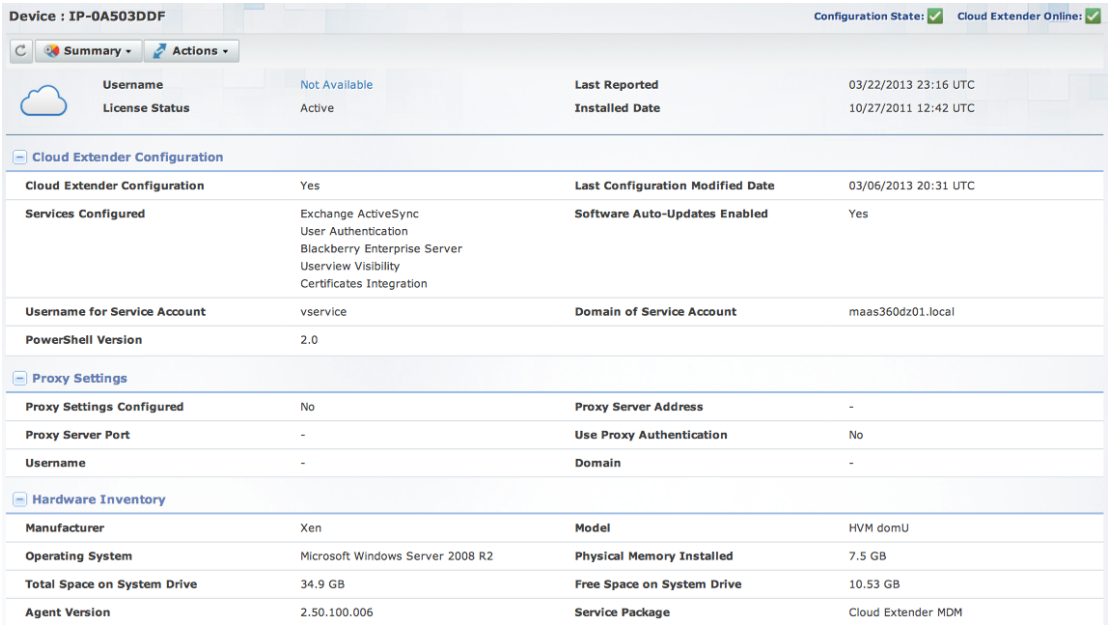
54. ábra: Device View nézet segítségével egy felügyelt eszköz adatai (hardver paraméterek, hálózati, biztonsági beállítások)

Attól függően, hogy milyen gyártótól származik az eszköz, különféle tevékenységeket hajthatunk rajtuk végre. Ilyen tevékenység lehet az eszköz távolról történő zárolása, üzenet küldése, email hozzáférés felfüggesztése, alkalmazás telepítése, vagy épp távolról történő törlés.



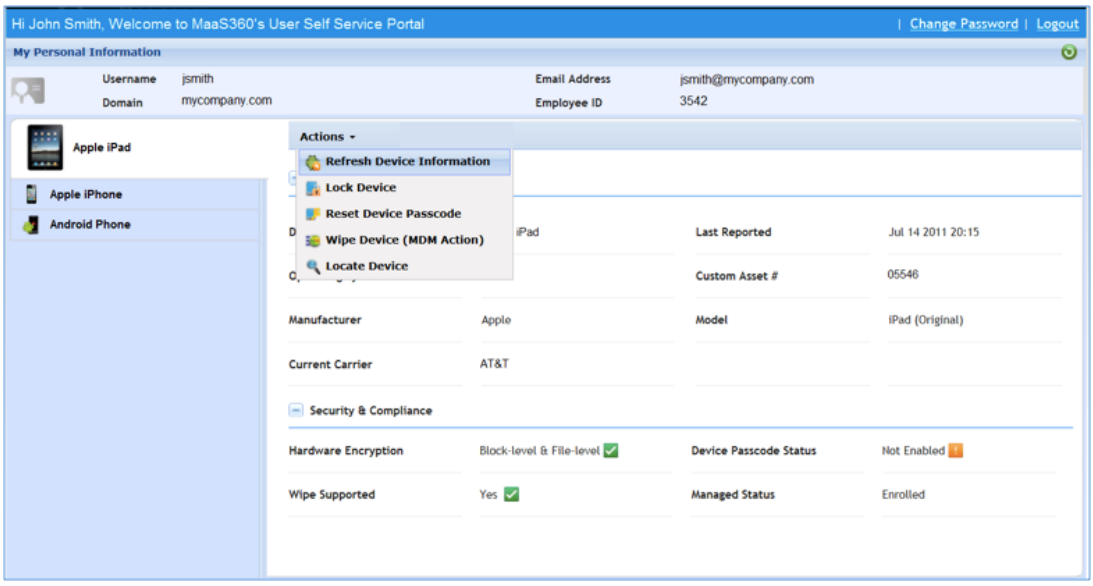
55. ábra: A lehetséges tevékenységek a vizsgált eszköz menedzselésére (pl.: távoli törlés, zárolás, távoli alkalmazástelepítés stb.)

A MaaS360 Cloud Extender (CE) egy olyan addicionális szolgáltatás, amellyel az átlagos háttérrendszereket integrálni lehet. Ilyen háttérrendszer lehet a Microsoft Exchange ActiveSync (2007, 2010, 2013 és Office365), BlackBerry Server, Lotus Notes Traveler, Active Directory, és Certificate Authorities. A CE képes adatokat ezekből a rendszerekből importálni ill. együttműködni is velük (tanúsítványok letöltése az eszközökre). A Cloud Extender nem egy inline proxy, éppen ezért például az e-mail-forgalom nem megy rajta keresztül.



56. ábra: A Cloud Extender beállítási felülete

A Bring Your Own Device (BYOD) eszközökhöz is széleskörű támogatást nyújt a megoldás. Ezek közé tartozik a gyorsított és egyszerűsített, interneten keresztül elvégezhető felügyelet alá vonás, az önkiszolgáló felület, testre szabható és könnyen megérthető végfelhasználói egyezmények, automatikus eszköz jóváhagyás, valamint biztonsági oldalról nézve az adminisztrátoroknak a korábban bemutatott lehetőségek (távoli törés, compliance szabályok stb.).



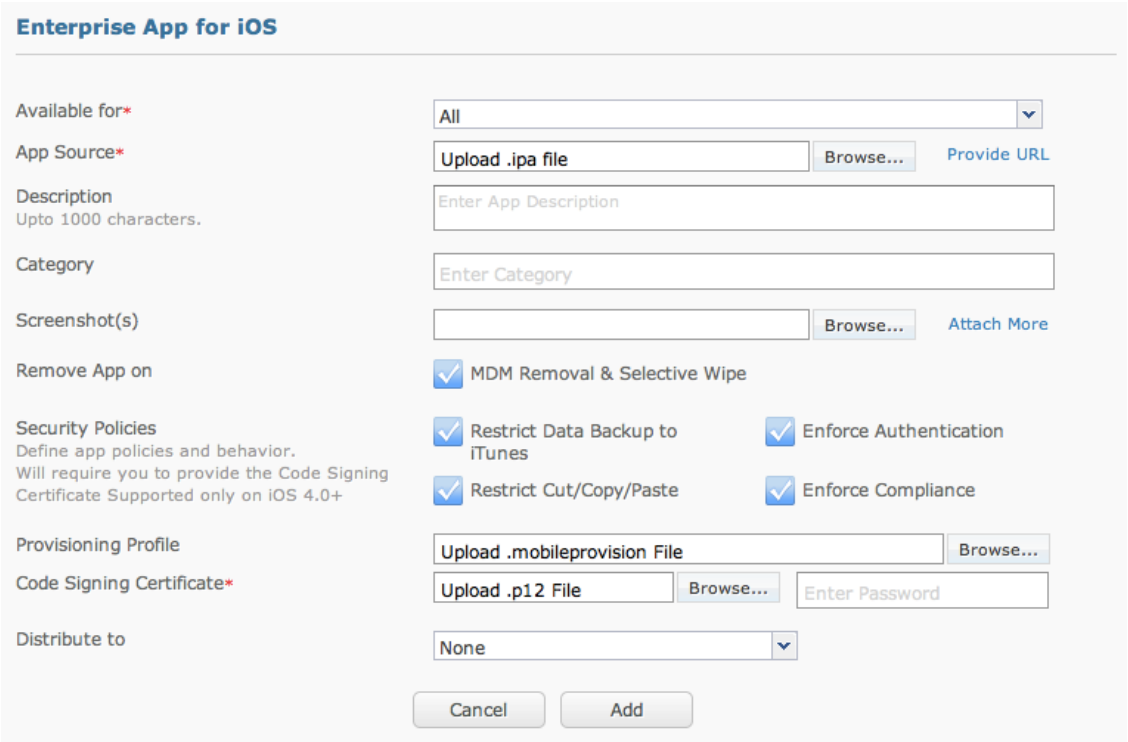
57. ábra: BYOD-eszközök menedzsment felülete

A dokumentum korábbi fejezeteiben már említettük, hogy a MaaS360 SPS csomag további szintekre emeli a biztonsági lehetőségeket és az azokhoz tartozó lehetőségeket. Részleteiben viszont még nem mutattuk meg, mire is képes az IBM MaaS360 Secure Productivity Suite. A korábbi távoli törlés, authentikáció és authorizáció mellett az alábbiakra is lehetőség van:

- Teljes értékű PIM alkalmazás, névjegyekkel, naptárral és levelezéssel
- Emailek feletti teljes felügyelet (szöveg és csatolmány egyaránt)
- FIPS 140-2 megfelelés, AES-256 titkosítás iOS-en és Androidon
- Cloud alapú levelezés támogatása: Office 365 és Gmail
- Authentikáció engedélyezése és zárolás téves vagy hibás hozzáférési kísérlet után
- Online és offline hozzáférés ellenőrzés az email megnyitása előtt
- Csatolmányok közvetlen megtekintése az alkalmazásban
- Csatolmányok törlése szelektíven
- Levél továbbítása, mozgatása más alkalmazásba, Kivágás-Másolás-Beillesztés opcionális tiltása, képernyőkép készítésének letiltása

MaaS360 App Security lehetővé teszi az alkalmazás szintű konténerizációt, mely segítségével az erre a működésre felkészített alkalmazások csak a konténerben futhatnak. További előnye, hogy így addicionális biztonsági intézkedések is kikényszeríthetőek:

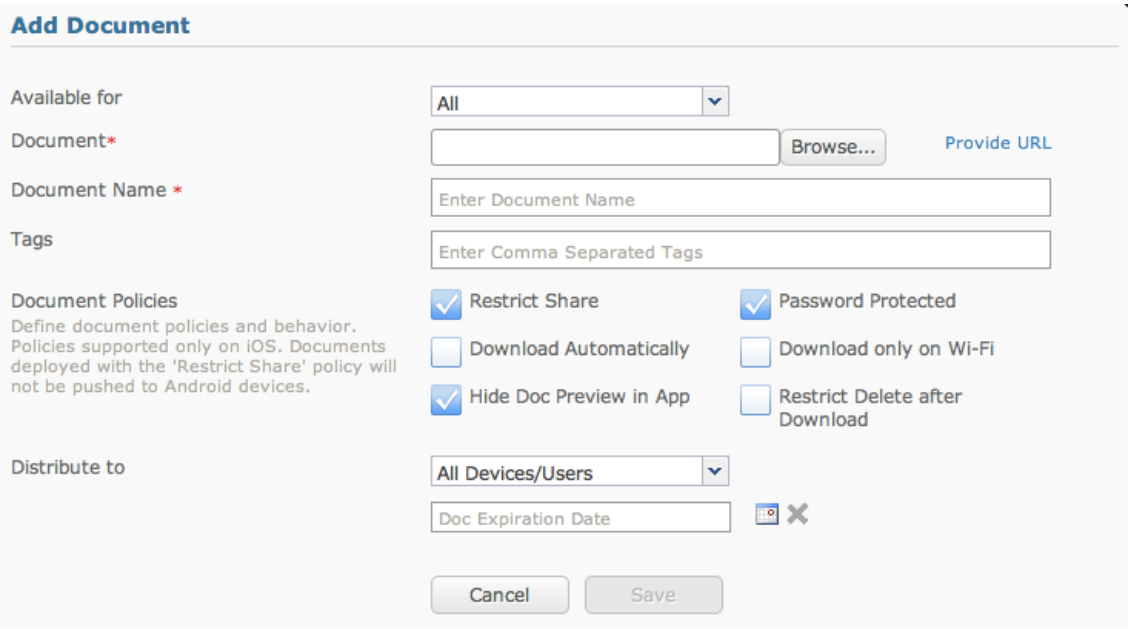
- Authentication és authorizáció kikényszerítése
- A házirendeknek való megfelelés kikényszerítése
- Kivágás-Másolás-Beillesztés tiltása, biztonsági mentés tiltása
- Házirend megszegése esetén valós idejű értesítés és az előre konfigurált akciók végrehajtása
- Alkalmazások integrálása a MaaS360 SDK-val vagy az ún. App wrapping képességgel
- Alkalmazás szintű tunneling (nincs VPN) a biztonságos hozzáféréshez



58. ábra: Belső fejlesztésű alkalmazások megosztása

A MaaS360 Secure Document Sharing egy kiterjesztése a Doc Catalognak, így további lehetőségek állnak majd rendelkezésre:

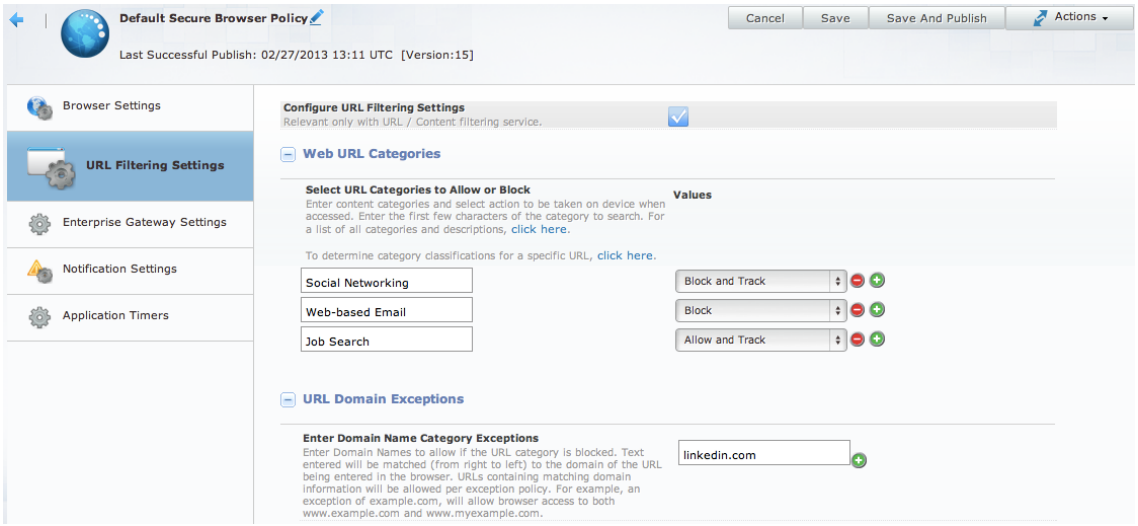
- Nem csak megnézni lehet a fájlokat, hanem meglévőket szerkeszteni, újakat létrehozni.
- Fájlok megosztása a konténeren kívülre (publikus alkalmazásba például).
- Vállalati Sharepoint vagy Windows file share hozzáférés
- Fájlok szinkronizálása több eszköz esetén
- Idő alapú lejárati dátum és annak elérkezésekor törlés
- Gyakori formátumok támogatása: Word, Excel, PowerPoint, text és PDF
- Felhasználói authentikáció kierőszakolása
- Granuláris hozzáférés kezelés



59. ábra: A MaaS360 Secure Document Sharing ablaka

A MaaS360 Secure Browser-el lehetőség nyílik a vállalati intranet oldalak megtekintésére VPN kapcsolat kialakítása nélkül. Továbbá létrehozhatunk úgynevezett fehér és fekete listákat, amelyeket meg lehet vagy éppen nem lehet megnyitni az eszközről. További előnye még a böngészőnek, hogy a megszokottól eltérő minimum biztonsági szint is beállítható (például a self-signed tanúsítvánnyal rendelkező oldalakat ne lehessen megnyitni). További funkciók:

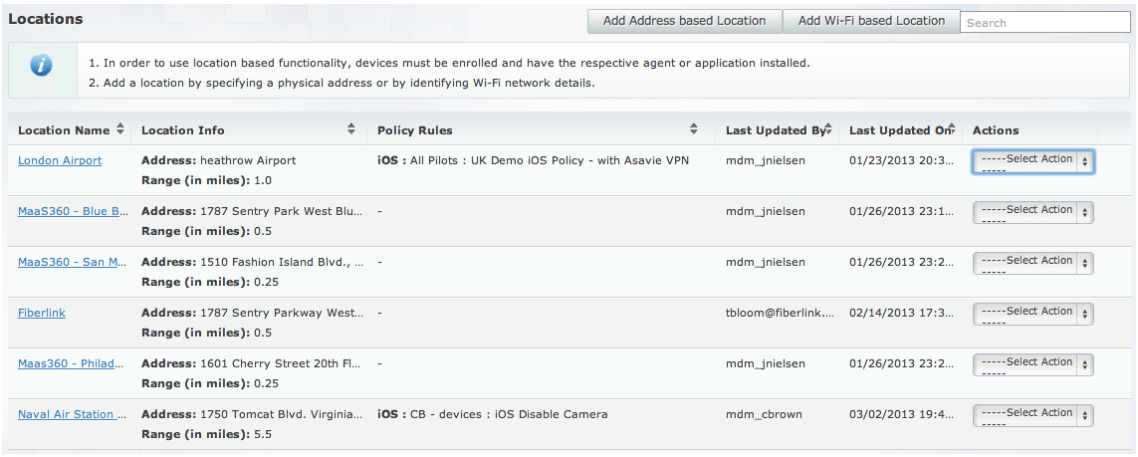
- Felhő alapú, központi felügyeleti platform
- Könnyen lehet házirendeket létrehozni, majd azokat OTA-n kézbesíteni
- Valós idejű védelem
- Oldalak tiltása
- VPN nélküli, de biztonságos vállalati hozzáférés
- Sütik használatának, nyomtatás lehetőségének, fájl letöltésének meggátolása
- Valós idejű értesítés és riporting
- Észrevétlen integráció a többi MaaS360 alkalmazásokkal
- Legalább Android 4.0 és iOS 5.0 szükséges hozzá.



60. ábra: MaaS360 Secure Browser

A MaaS360 lehetőséget kínál az úgy nevezett lokáció alapú házirendek kialakítására is. A helymeghatározás több módon is lehetséges: vagy GPS alapú koordináták alapján, vagy a konfigurált vezetéknélküli hálózati pontok mentén. Az ilyen szabályokkal akár alkalmazásokat is le lehet tiltani, de akár külföldi adatforgalom felügyeletére is használható. Felhasználási példák:

- Amikor az eszköz egy autógyár hálózatára csatlakozik, a kameraalkalmazás letiltásra kerül. Amikor elhagyja ezt a hálózatot, újra lehet fényképezni.
- Ha az eszköz elhagyja az országot, a roamingszolgáltatás letiltásra kerül.



61. ábra: Lokáció alapú házirendek

6. A Windows 10 mobil eszközök védelmi megoldásai

6.1. Bevezető

A Microsoft fejlesztései során nagy hangsúlyt fektet az informatikai biztonsági megoldásokra, különös tekintettel a mobil eszközök használatának elterjedésével.

Ma már elengedhetetlen a mindennapos munkavégzésben az, hogy a munkavállalók okos mobil eszközöket használjanak. A mobil eszközök funkcionalitása egyre bővül, ugyanakkor a közösségi, vagy szórakoztató funkciók kínálata is egyre szélesedik. A felhasználói élmény érdekében a gyártók alkalmassá teszik eszközeiket arra, hogy mind a vállalati, mind a közösségi/szórakoztató alkalmazások egyaránt elérhetők legyenek a mobil eszközökön.

A szervezeteknek tehát alkalmazkodniuk kell az IT gyakorlatokhoz, és ki kell alakítaniuk azokat a vállalati szabályokat, be kell vezetniük azokat a biztonsági intézkedéseket, amelyek biztosítják a mobil eszközök biztonságos használatát úgy, hogy az távoli munkavégzésre is teljes mértékben alkalmas maradjon.

A szervezetek védelmi szabályainak követniük kell az egyre szigorodó adat- és információvédelmi szabályozást, el kell érniük, hogy mobil eszközeik megfeleljenek az előírásoknak. Az állandóan változó kiberfenyegetettség megnehezíti ezt a munkát. A káros kódok újabb változatainak terjesztése, az adathalász tevékenység és a terheléses támadások mindennaposak, ez különösen veszélyezteti a mobil eszközöket is.

Annak biztosítására, hogy a szervezetek megvédjék a felhasználókat és információkat a támadások ellen, teljes körű mobil védelmi rendszer kiépítése szükséges. A Windows 10 Mobil minden szinten képes biztonsági védelmet nyújtani úgy, hogy a szervezet által központi biztonsági eszközmenedzsment beállítások mellett a felhasználói élmény teljes marad.

6.2. Azonosítás és hozzáférés-ellenőrzés

A Windows 10 operációs rendszert használó eszközökre, így a Mobil eszközökre is azonosítás- és hozzáférés-felügyelet integrálható az Active Directory-n[223] (a továbbiakban: AD) keresztül. Ennek célja, hogy a felhasználók biztonságos azonosítása azelőtt megtörténjen, hogy hozzáférnének a szervezet hálózatához, alkalmazásaihoz és adataihoz.

Az azonosítási és hozzáférés-felügyelet magába foglalja az AD, az SSO, a multifaktoros azonosítás, a biometrikus azonosítás, a szabályérvényesítés beállításait és a VPN egyszerű elérését.

Biometrikus azonosítás

A Windows Hello a Windows 10 eszközökön lehetővé teszi a felhasználók számára a könnyű és természetes, ugyanakkor biztonságos módon történő azonosítást a helyi eszköz és távoli szolgáltatások felé. Ennek az egyszerűségét biometrikus eszközök biztosítják, a biztonságát pedig az eszközbe épített kriptográfiai eszköz (TPM) segítségével történő kétfaktoros hitelesítési lehetőség adja.

A felhasználó biometrikus adatai nem mennek keresztül a felhasználó eszközein és nem történik felhő alapú központi tárolás. A biometrikus kép, amelyet az érzékelő leolvasáskor készít, algoritmi-

[223] Az Active Directory címtár az adatbázisból és az azt futtató Active Directory szolgáltatásból áll. Fő célja a Windowst futtató számítógépek részére autentikációs és autorizációs szolgáltatások nyújtása, lehetővé téve a hálózat minden publikált erőforrásának (fájlok, megosztások, perifériák, kapcsolatok, adatbázisok, felhasználók, csoportok stb.) központosított adminisztrálását. Számos különböző erőforráshoz (megosztott mappák, nyomtatók, levelezés stb.) egyetlen felhasználónév/jelszó páros megadásával biztosít hozzáférést (Single Sign On, SSO). Lehetőséget nyújt a rendszergazdák számára házirendek kiosztására, szoftverek és szoftverfrissítések telepítésére a szervezeten belül. Az Active Directory az információkat és beállításokat egy központi adatbázisban tárolja.

kus formába kerül átalakításra, az eredeti kép pedig visszafordíthatatlanul megsemmisül. A további védelem érdekében a felhasználónak a biometrikus azonosítással együtt meg kell adnia a PIN kódját is arra az esetre, ha a kamera nem működne. A PIN szintén magán az eszközön biztonsági megoldásokkal védett, továbbá eszköz-specifikus.

VPN

A Win10 mobil beépített VPN-t alkalmaz azért, hogy a belső rendszerekhez, intranethez és alkalmazásokhoz gyors hozzáférést biztosítson a felhasználók számára. Amennyiben az IT az automatikus VPN csatlakozást beállítja, a felhasználó Microsoft Passport hitelesítő adataival mobil vagy tablet eszközén a belépést követően automatikusan eléri azt.

A Win10 mobil eszközök több VPN alkalmazást is képesek használni. Az IT meg tudja határozni azt is, hogy bizonyos alkalmazások mely VPN kapcsolatot használják, pl. alacsonyabb biztonsági elvárások esetén VPN-A-t, magas biztonsági fokozat esetén a VPN-B-t, a vállalati források lehető legbiztonságosabb elérésének érdekében.

6.3. Információvédelem

Attól függően, hogy információ tárolás az eszközön, vállalati felhőben, vagy helyi adatközpontban történik, a Win 10 mobil rugalmas, de hatékony védelmet nyújt az adatlopás ellen. Az eszköztitkosítás és az információ jogosultság-kezelés a mobil eszközmenedzsment részeként beépítésre került és teljeskörűen segíti az adatbiztonság megvalósítását.

Eszköztitkosítás

A Win10 mobil BitLocker technológiát alkalmaz, hogy a belső adattárolók titkosítására, ide értve az operációs rendszert és az adattárolási partíciókat.

Az eszköztitkosítást a felhasználó közvetlenül is tudja aktiválni; a vállalati eszközmenedzsment szabályokat az IT részleg állítja be. Amikor az eszköztitkosítás bekapcsolásra kerül, a telefonon tárolt minden adat automatikusan titkosítva lesz. Ha egy védett Win10 mobil eszköz elvész, vagy ellopják, az eszközvédelem erőssége és az adattitkosítás rendkívül megnehezíti, hogy egy jogosulatlan személy a szenzitív adatokhoz hozzáférjen, vagy visszaállítsa azokat.

Vállalati adatvédelem (Windows Information Protection – WIP)

A vállalati adatvédelmi megoldás (a továbbiakban: WIP) ez év második felétől lesz elérhető szélesebb körben. A WIP a jövőben újfajta megközelítést alkalmaz a vállalati adatvédelem terén.

Ma egy felhasználó mobil eszközén számtalan alkalmazást használ. Az egyes szerepekhez (pl. személyes-vállalati) kötött alkalmazásokba a felhasználónak minden esetben újra be- és ki kell lépnie, újra és újra azonosítani kell magát. AWIP automatikusan alkalmazza a vállalati szabályokat, titkosítja a fájlokat és adatokat, ha azok a vállalati rendszerből érkeznek, vagy vállalati alkalmazások.

Például, ha egy felhasználó olyan emailt kap, amelyben .xlsl melléklet van, a Win10 mobil automatikusan meghatározza, hogy annak tartalma vállalati adat-e. Amennyiben igen, titkosítja azt arra az időre, amíg az az eszközön tárolódik. Amennyiben a szervezet úgy állította be a védelmi szintet, hogy megakadályozza a személyes alkalmazásokkal és adattárolóval való megosztást, a felhasználó a vállalati rendszeren belül tudni fogja másolni a melléklet részét vagy egészét más vállalati alkalmazásokba, (pl. másolás Word dokumentumba, majd mentés vállalati OneDrive-ra). Ugyanakkor a mellékletből az adatot, fájlt, dokumentum részét vagy egészét nem lehet átmásolni személyes alkalmazásokba, menteni nem vállalati publikus, vagy más privát felhőbe.

Nyomon követés

A szervezeteknek a WIP használatával lehetőségük lesz arra, hogy blokkolják, vagy ellenőrizzék a nem megfelelő adatmegosztást. Megengedhető lesz ugyan, hogy a felhasználók megszegjék a korlátozást, de ekkor a rendszer figyelmeztetést ad ki, hogy informálja az érintetteket a szabályszegésről, egyidőben az MDM rendszer naplózza a tevékenységet.

Kiegészítő alkalmazások adatbiztonsága

A megbízható alkalmazások menedzselése integrálható a rendszerbe, az engedélyezett alkalmazásokban minden adat automatikusan titkosítva és védve lesz. A WIP megengedi, hogy ezek az alkalmazások hozzáférjenek az adatokhoz és adatokat tároljanak biztonságos környezetben. Attól függetlenül, hogy ezek az alkalmazások hol futnak, a ki- és bejelentkezés szintén automatikus.

A WIP alkalmazásával tehát korlátozhatók és titkosíthatók a vállalati adatok, de nem érintik a személyes használatú alkalmazásokat; az eljárás attól függ, honnan származik az adat.

Biztonságos adathozzáférés és tárolás

A WIP lehetővé teszi a rendszergazdák számára, hogy meghatározzák, mely helyben, vagy felhőben nyújtott szolgáltatások, adattárolók és hálózatok megbízhatóak.

Bizonyos mentett adatokat és dokumentumokat nem kell titkosítani annak érdekében, hogy azok más engedélyezett vállalati felhasználók számára is elérhetők legyenek. Az IT képes lesz beállítani azoknak a vállalati IP-címeknek vagy tartománylistáknak a körét, amelyek hozzáférhetnek a hálózathoz. Azok a felhasználók, akik jogosultak a dokumentumok megtekintésére, a hitelesítő adataik alapján automatikusan elérhetik azokat. Ezért a titkosítás csak akkor kerül alkalmazásra, ha az adatok tárolása a mobil eszközön történik, vagy a felhasználó által átkerül egy nem megbízható helyre.

A titkosítási kulcsokat és a WIP korlátozásokat az MDM rendszer bármikor képes menedzselni, így a vállalkozás teljes ellenőrzése alatt képes tartani az adatokat.

Részleges és teljes törlés

A WIP azt is lehetővé teszi, hogy az arra jogosult adminisztrátorok a vállalati adatokat távoli hozzáféréssel töröljék a felhasználó eszközéről, miközben a felhasználó személyes tere nem sérül.

A Win10 mobil eszközök esetén a távoli menedzsment segítségével az eszköz távolról zárolható, értesítés küldhető, és nyomon követhető. Az elveszett vagy ellopott telefon nyomonkövetésére web alapú alkalmazás segíti a felhasználót abban, hogy az eszközét távolról zárolja, térképen követni tudja annak helyét vagy hangosan megcsöngettesse még akkor is, ha a telefon hangereje le van véve. A lopás elleni védelem azt is megakadályozz, hogy az eszközt illetéktelenek újra indítsák. Ha egy lopásra bejelentett vagy elveszett mobil eszköz előkerül, speciális kód segítségével a zárolása feloldható.

Tartalomvédelmi szolgáltatások (Azure Information Protection – AIP)

Az Azure Information Protection (AIP) a Microsoft EMS szolgáltatás része, amely lehetővé teszi a tartalom létrehozója számára hozzáférési jogok kijelölését a Microsoft Office dokumentumok, PDF-ek, vagy e-mail üzenetek esetén, amelyeket a felhasználó másoknak is el kíván küldeni.

Az IT, vagy az azonosított felhasználó titkosítja az adatokat, jogvédett dokumentumokat vagy e-mail üzeneteket, és meg tudja adni, mely jogosult felhasználók férhetnek hozzá a titkosított tartalmakhoz speciális jogosultságuk által. A beállított jogosultságok alapján érvényesíthető a dokumentum hozzáférési szintje (pl. csak olvasható), megakadályozható a dokumentummásolás és -beillesztés más

dokumentumba vagy üzenetbe, illetve megakadályozható a dokumentum vagy üzenetnyomtatása. Az AIP használatával beállítható egy e-mail-üzenet továbbítása is; megadható, hogy csak szervezeten belül, vagy egyáltalán ne lehessen továbbítani.

A tartalomvédelmi szolgáltatás alapvetően képes javítani a szervezet általános adatbiztonsági helyzetét, tovább növeli a vállalati adatok belső és külső védelmét. A Windows 10 mobil eszközök egyedülálló képessége az, hogy az AIP-t saját környezetében futtatja, amely lehetővé teszi a felhasználók számára, hogy teljes mértékben részt vegyenek AIP-sel védett e-mail kommunikációban és hozzá tudjanak férni az AIP-sel védett dokumentumokhoz mobil eszközeiken. Az AIP kiterjeszthető nem Windows eszközökre is. Az ügyfelek vagy az üzleti partnerek iOS vagy Android eszközeire is adhatók dokumentum-hozzáférési jogosultságok.

6.4. Rosszindulatú támadás elleni védelem

A rosszindulatú támadások (malware) egyre kifinomultabbak és számuk továbbra is növekszik. A támadók keresik a hozzáférést az értékes személyes és vállalati adatokhoz csalás, zsarolás, vagy egyenesen a szellemi tulajdon eltulajdonítása céljából.

A mobil eszközök használatával megnőtt a támadható felületetek száma, több százezer rosszindulatú program jelenik meg minden évben mobil eszközökre. A vállalatok által biztosított mobil eszközöket, amelyek elérik a vállalati erőforrásokat olyan módon kell menedzselni, amely biztosítja az eszközökön tárolt rendszerek, alkalmazások és adatok biztonságát.

A Win10 mobil eszközök kriptográfiailag védik a forrásrendszereket és alkalmazásokat, hogy csökkentsék a malware fenyegetettséget és adathalász tevékenységet. A hardveralapú védelmi funkciók célja, hogy megakadályozzák az illetéktelen belépést.

Eszközsértetlenség

Minden Win10 mobile eszköz része a biztonságos rendszerindítás technológia, amely ellenőrzi a rendszerindításhoz szükséges komponenseket. Minden komponens rendelkezik digitális aláírással, amelyet az indításnál érvényesíteni kell. Az eljárás tehát biztosítja, hogy csak a jogosult felhasználó tudja elindítani a készüléket és az operációs rendszert.

Miután ez a kezdeti biztonsági ellenőrzést elvégezte, a Trusted Boot[224] átveszi a teljes operációsrendszer-indítási folyamatot, így a felhasználó el tudja kezdeni használni a mobil eszközt. A Trusted Boot előírja, hogy az operációs rendszer minden kódjának – beleértve az OEM illesztőprogramokat és alkalmazásokat is – Microsoft által aláírtnak kell lennie, ezáltal biztosítva a következő réteg védelmét, biztosítva ezzel a platform sértetlenségét.

Eszközvédelem (Device Guard)

A Win10 mobil védelem célja, hogy megakadályozza a rosszindulatú programok bejutását az eszközökbe, s így az alkalmazások kompromittálódjanak. A védelmi intézkedések biztosítják, hogy a felhasználók csak megbízható alkalmazásokhoz férjenek hozzá és biztosítják az alkalmazások sértetlenségét az alkalmazások használatának megkezdése előtt.

A Device Guard a Wind10 mobil eszközt úgy zárolja, hogy csak akkor futtathatók az alkalmazások, ha azok egy megbízható kiadótól származtatott kulccsal aláírtak. A Windows Store-ból, vagy egyéb megbízható forrásból származó alkalmazásokat a szervezeti politikának megfelelően kell használni.

[224] A Trusted Boot alkalmazás a rendszer gyorsabb indítását teszi lehetővé. Az alkalmazás csak aláírt rendszerbetöltő állományoknak adja át az indítási folyamatot, tehát a felhasználónak engedélyt kell erre adnia. Ezzel a rendszer indulásakor csak azok a driverek töltődnek majd be, amelyek megfelelő aláírással rendelkeznek.

A megbízható alkalmazások működése közben, kivéve, ha valamilyen biztonsági esemény történik, az operációs rendszer csak azoknak az alkalmazásoknak a használatát engedi, amely a szervezet által engedélyezett. Abban az esetben, ha egy nem megbízható alkalmazás került telepítésre a készüléken, a Device Guard megakadályozza az alkalmazás futtatását, így védi a rendszer, az alkalmazások és az adat bizalmasságát és sértetlenségét.

Sandbox[225] *alkalmazás*

A Win10 mobil biztosítja, hogy minden alkalmazás saját Sandboxban fusson a legalacsonyabb jogosultsággal. A Sandbox a benne elindított programok számára normál Windows környezet imitál, de az összes fájlhozzáférést elfogja és külön tartományban futtatja. Így egy kártékony szoftver nem tud többé hozzáférni a rendszerfájlokhoz vagy más egyéb módon károkat okozni.

Alkalmazáshozzáférés-védelem

A szervezetek felhasználóiknak további mobil alkalmazásokhoz adhatnak hozzáférést a Windows Store-on vagy vállalati portáljukon keresztül. A telefonokon megosztott alkalmazásoknak, függetlenül a terjesztés módjától, meg kell felelniük a Win10 mobil eszközökre vonatkozó biztonsági korlátozásoknak. A Windows Store alkalmazások Microsoft által aláírtak, amely biztosítja azok eredetiségét. Használatba vétel előtt a LOB-alkalmazásokat[226] is alá kell írnia a szervezeteknek. A vállalatok további, vállalati tanúsítvánnyal ellátott alkalmazásokat adhatnak a felhasználóknak Mobile Device Management rendszerükön keresztül.

Böngésző alapú védelem

A Win10 mobil eszközökön a Microsoft Edge SmartScreen szűrője védelmet nyújt az adathalász oldalak ellen. Ha a SmartScreen egy oldalt gyanúsnak minősít, blokkolja azt. SmartScreen megvédi a felhasználókat a káros szoftvereket tartalmazó közösségi oldalakon. A Microsoft Edge keresések külön alkalmazás tárban futnak, biztosítva ezzel, hogy a káros szoftverek ne férhessenek hozzá a készülékhez. A böngésző a Mobile Device Management korlátozásokat is tudja kezelni úgy, hogy korlátozza a weboldalakhoz való a hozzáférést és átirányítja a forgalmat proxy ellenőrzésre.

Megfelelési vizsgálat az állami és önkormányzati szervek elektronikus információbiztonságról szóló jogszabályi előírások szerint

A Microsoft Magyarország a Microsoft Windows 10 alapú mobilplatformok kormányzati szintű bevezetésének és használatának tárgyában szakértői vélemény elkészítésére kérte fel a Cyber Services Zrt-t. A vizsgálat a Nokia Lumia 950-es készülékre telepített Microsoft Windows 10 Mobile szoftverkészleten folyt le.

6.5. Jogszabályi környezet

A vizsgálat során a Cyber Services Zrt. az eszköz alkalmazhatóságát Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és kapcsolódó 41/2015. (VII. 15.) BM rendelet (a továbbiakban: Rendelet) szerinti biztonsági környezetben ellenőrizte.

[225] A Sandbox a rendszereden belül leárnyékolt terület, ahol a programokat úgy lehet futtatni, hogy azok ne tudják megtámadni az eszközt.

[226] Line Of Business: üzletmenet szempontjából kritikus alkalmazások

A vizsgálat célja az volt, hogy a Nokia Lumia 950 hardverre telepített Microsoft Windows 10 mobilplatform az információbiztonság szempontjából megfelel-e az állami és önkormányzati szervek elektronikus információs rendszere részeként történő üzemelésre, és a megfelelés milyen, a jogszabály által meghatározott biztonsági szinten értelmezhető.

6.6. Alapkiépítésen felüli szoftverigények

A vizsgálati peremfeltételként megjelölt *Mobil Device Management* (a továbbiakban: MDM) szoftver alkalmazása az állami és önkormányzati szervek információs rendszereiben erősen ajánlott a Windows Phone biztonságos használata és hatékony felügyelete érdekében. A Windows Phone alapértelmezésű beállítási lehetőségei *(General Settings)* nem támogatják a központi felügyelet számos olyan funkcióját, amely csak az MDM felügyelete mellett valósítható meg, ezek azonban várhatóan szükségesek a hivatkozott törvényi szabályozás előírásainak helyi megvalósítása során. Az MDM funkcionalitásának kihasználása érdekében – gyártói ajánlás alapján – a felügyeletet ellátó szervnek szüksége lehet az MDM-el együttműködő *Azure ID Premium Edition* típusú azonosítók alkalmazásra is. A naplózási funkciók elérése érdekében a *Field Medic* applikáció telepítése és aktiválása célszerű, mivel a készülék hasonló képességgel alapkiépítésben nem rendelkezik.

Az Ibtv. szabályozása alá eső adatok rendeltetésszerű tárolása, az érintett rendszerek üzemszerű működése Magyarországon, az Európai Unió tagállamai, esetleg az EGT-államok területén engedélyezett. Minden, ettől eltérő helyszínre történő adattovábbítás tilos, azaz megvalósulása esetén a Windows Phone kizárását jelenti az állami és önkormányzati szektorban való felhasználásból.

6.7. Biztonsági osztályok és szintek

Az Ibtv. értelmezésében a „biztonsági osztály” az elektronikus információs rendszer védelmének elvárt erőssége, ugyanakkor a „biztonsági szint” a szervezet felkészültségének mértékét jellemzi az Ibtv-ben és a Rendeletben meghatározott biztonsági feladatok kezelésére.

Az információs rendszerek besorolása az egyes rendszerek áttekintése, a kezelt adatok jellege, a rendszerek sajátosságai és kockázatbecslés alapján lehetséges. Az állami és önkormányzati szervek legmagasabb biztonsági osztálya és szintje a Rendelet 2. mellékletének meghatározása szerint várhatóan a 2–5. biztonsági osztály közé fog esni, saját becslésük szerint.

A legmagasabb 5. biztonsági osztály előfordulása jelentős számú szerv esetében reális, ebből nem zárható ki az önkormányzati szektor sem.

Az 5. biztonsági szint eléréséhez az 1. szinttől 5. szintig terjedően valamennyi biztonsági szervezeti szint követelményeit meg kell valósítani a 2. mellékletben foglaltak szerint. Az egyes rendszerekre lebontott intézkedéscsomag (a Rendelet 3. és 4. melléklete alapján) 5. osztályra és szintre vonatkozó követelményeket kell figyelembe venni, így az ilyen szerveknél az intézkedés-táblázat sorainak túlnyomó részére reagálási kötelezettség jelentkezik, illetve azok mentén kell kialakítani a működő információbiztonsági rendszert. Mivel egy állami vagy önkormányzati szervet kiszolgáló elektronikai eszköz – mint például a Windows Phone – optimális esetben alkalmas az előforduló legmagasabb biztonsági követelmények közepette is megfelelő üzemelésre, ezért az állami és önkormányzati szektorban bármely rendszerben használható mobil platformnak – saját szerepkörében – támogatnia kell a Rendelet szerinti 5. biztonsági szintet.

6.8. Megengedett eltérések minimalizálása

A Rendelet 4. melléklete az információs rendszerek egyenszilárdságának fenntartása mellett a taxatív intézkedéscsomag előírásaitól bizonyos feltételekkel eltéréseket engedélyez. Megengedett a működtetési környezettel, a fizikai infrastruktúrával, a nyilvános hozzáféréssel, a biztonsági szabályozással kapcsolatos előírások szűkebb értelmezése, illetve a csak egyes speciális technológiai megoldásokra értelmezhető rendelkezések elhagyása.

6.9. Helyettesítő intézkedések figyelembe vételének kizárása

Hasonlóképpen nem érvényesíthetőek a vizsgálatban az egyes rendszerek biztonsága érdekében helyileg előírt helyettesítő intézkedések sem, amelyek a Rendelet 4. mellékletében értelemszerűen nem szerepelnek. A rendszerek felépítésének sokfélesége és a szabályozások eltérései következtében nem garantálható az, hogy a Windows Phone egy adott rendszerbe illesztve a biztonsági elveknek megfelelően, de a rendszerben minden elvárt funkciójában helyesen működni fog, bár az adott biztonsági szint követelményeinek megfelel. Helyettesítő intézkedésre azonban egyedi esetekben szükség lehet, hiszen a vizsgálat az információbiztonságra korlátozódik és nem veheti figyelembe annak az állami, önkormányzati szervnek a lokális információs követelményeit, amelyek visszacsatolással bírhatnak a biztonsági beállításokra.

6.10. A Windows Phone készülékkel szemben támasztott biztonsági követelmények és azok támogatása

A Rendelet 4. mellékletéből azokat az intézkedési kategóriák kerültek vizsgálatra, amelyek relevánsak az eszközzel kapcsolatban, illetve amelyek direkt módon érinthetik a Windows Phone alkalmazását egy rendszerben. Ezeket a tevékenységeket, folyamatokat az eszköznek támogatnia szükséges. A Windows Phone-ra, mint mobil platformra nem értelmezhető, illetve specifikusan az információs rendszer központi elemeire vagy általánosan a rendszer egészére alkalmazható előírások a vizsgálat szempontjából nem relevánsak. A vizsgálat a Windows Phone mellett a MDM felügyeleti szoftver és az Azure ID Premium Edition account-ok egyidejű alkalmazásával is számol, azok együttműködését feltételezi.

Alapértelmezésként figyelembe vett biztonsági szint: 5. szint.

6.11. A vizsgálat általános megállapítása

A vizsgálat alapján a Windows Phone alapvetően megfelel az állami és önkormányzati elektronikus információs rendszerekben való felhasználásra.

A megfelelés a legmagasabb, 5. biztonsági osztályra és szintre is értelmezhető.

Néhány biztonsági előírás szigorú megkövetelése azonban korlátozhatja a Windows Phone alkalmazhatóságát a legmagasabb biztonsági osztály és szint kiszolgálására. Ilyen esetekben a Windows Phone használhatósága a 3., szélsőséges esetben az 1. biztonsági osztály és szint kiszolgálására korlátozódhat. A helyi szabályozás célszerű súlyozásával, helyettesítő megoldásokkal, vagy egyes követelmények kockázatbecslésen alapuló elhagyásával a Windows Phone alkalmassága az 5. biztonsági osztályon és szinten tartható. Az alternatív megoldások bevezetését azonban a felügyelő hatóságnak is jóvá kell hagynia.

6.12. Jellemző feltételek, korlátozások, eltérések az alkalmazás során

- A biztonsági követelmények megvalósítása a Windows Phone aktuális képességein túl a vizsgálati peremfeltételként megjelölt, kapcsolódó szoftveres megoldásokkal együttesen történhet: *MDM, Azure ID, Field Medic application*.
- Az autentikációs eljárásokat támogató tanúsítvány-kezelés során figyelembe kell venni, hogy a rendszer csak a PKCS#12 formátumú (vagy az e formátumra átalakított) tanúsítványokat kezeli, emellett visszavonási listákat *(Certificate Revocation List)* nem tárol, így előnyös, ha az érintett szerv informatikai rendszerében saját tanúsítványok kiadására és kezelésére képes *Certification Authority* működik.
- Nem valósíthatók meg a kártékony kódok elleni határvédelem és ezzel kapcsolatos szolgáltatások a Windows Phone készüléken. Az előírás teljesítésére helyettesítő megoldás kidolgozása javasolt.
- A Cyber Services Zrt. véleménye szerint biztonsági kockázatot jelent a privilegizált felhasználói fiókok Windows Phone útján történő elérése, ezért ezt a lehetőséget nem javasolja engedélyezni a 3. biztonsági szint fölött.
- A tulajdonság alapú hitelesítés alkalmazásakor figyelembe kell venni, hogy a Windows Phone a beépített retina letapogató eredménytelen azonosítási kísérletét követően automatikusan a jelszavas belépés lehetőségét biztosítja a felhasználó számára, amely az azonosítás gyengülését eredményezi a rendszerek elérésekor.

Fenti megállapítások ellenére is előfordulhat, hogy valamely szolgáltatás, folyamat, beállítás nem értelmezhető egy adott információs rendszeren. A rendszer alaprendeltetéséből adódóan, meglévő technikai megoldásai következtében, vezetői szinten definiált követelmény teljesítése érdekében, a fejlesztések kockázat/haszon elvű elemzését követően vagy más jelentős okból megvalósított helyettesítő megoldások okozhatják egyes biztonsági, felügyeleti funkciók elérhetetlenségét. Ilyen esetben is a hivatkozott jogszabályoknak való megfelelést fenn kell tartani, de nem garantált a legmagasabb biztonsági osztály és szint követelményeinek teljesítése.

A megfelelőségi vizsgálta alapján a Windows Phone a megfelelő beállításokat követően alkalmazható a legmagasabb biztonsági osztályba tartozó elektronikus információs rendszerekben is.

7. DESlock+ mobil védelmi megoldás

7.1. A DESlock+ alapjai

A DESlock+ első használata előtt érdemes áttekinteni a titkosító algoritmusok és kulcsok használatát, valamint azt, hogy mely adatokat tekintünk védendő adatnak és milyen módszerekkel kívánjuk ezeket megvédeni. *Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet* – 3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK pontjának ***Hozzáférés ellenőrzése*** intézkedési típusának ***3.3.10.15.2. Titkosítás*** pontját fedi le!

7.2. A védendő adatok kategorizálása

A védendő adatok kategorizálása alapján választhatjuk ki a védelem megfelelően biztonságos módszereit.

Mozgó és pihenő adat

A mozgó adat olyan két felhasználó közt megosztott információ, amely nem biztonságos hálózaton vagy nyilvános csatornán keresztül közlekedik, és bizalmassága részletesen leírt titkosítási eljárással biztosítandó. Pihenő adat a merevlemezen vagy külső adathordozón tárolt adat, statikus információ.

Szelektív titkosítás

Szelektív titkosítás alatt az egyes állományok, könyvtárak és e-mailek titkosítását értjük. Az állomány- és e-mail-titkosítás lehetővé teszi, hogy a felhasználók biztonságos módon cseréljenek információt akkor, amikor az adat mozgásban van. Saját gépünkön, a merevlemezen levő könyvtárak és a cserélhető adathordozók titkosítandóak. A DESlock+ lehetővé teszi a titkosított virtuális kötetek és tömörített archív állományok kialakítását.

A titkosított könyvtárakban, virtuális kötetekben levő állományok transzparens módon elérhetőek, ha a felhasználó bejelentkezett a DESlock+ programba és rendelkezik a megfelelő titkosító kulcsokkal. Ha a merevlemezt vagy a cserélhető adathordozót más számítógépbe teszik át, csak a titkosított könyvtárak és fájlok védelmet élveznek.

Teljes körű védelem

A teljesen megnyugtató megoldás érdekében a DESlock+ teljes merevlemez titkosítást is biztosít Windows rendszereken olyan váratlan helyzetek kezelésére, mint a számítógép vagy adathordozó eltulajdonítása, elvesztése. A teljes merevlemez titkosításhoz a DESlock+ Pro licenc szükséges. A teljes merevlemez titkosítás védelmet nyújt a merevlemez számára a gép kikapcsolt vagy hibernált állapotában. A Windows nem indítható ebben az állapotban a felhasználói jelszó megadása nélkül. Ha a merevlemezt kiemelik, és más rendszerben próbálják olvasni, az titkosított marad. A DESlock+ cserélhető adathordozókat is képes teljes mértékben titkosítani.

7.3. DESlock+ titkosítási kulcsai

Titkosítási kulcsok

Egy titkosító kulcs a titkosítási eljárással együtt határozza meg, hogyan alakítjuk át az olvasható szöveget titkosítottá és vissza. Ez azt jelenti, hogy a fájljaink, dokumentumaink vagy merevlemezünk titkosítása egyedileg fog függni a használt titkosító kulcstól.

Megosztott titkosító kulcsok

Más titkosító termékekhez hasonlóan a DESlock+ is képes közös jelszóval titkosított állományokat, archívumokat, e-maileket stb. több felhasználó között megosztani. De a jelszavakat a rendszergazdák nem tudják lementeni, a felhasználók szinte sohasem írják fel és gyakran elfelejtik. A megosztott információ titkosító kulccsal való bizalmassá tétele viszont sokkal inkább kezelhető megoldás: sokkal nehezebben feltörhető és biztosítható, hogy a felhasználó ne tudja magát kizárni.

Más rendszerek aszimmetrikus titkosítási eljárásokkal igyekeznek ezt megoldani, ami a tapasztalt felhasználók számára hatékony ugyan, de az átlagember számára nehezen kezelhető.

A DESlock+ ezt a kérdést máshogy oldja meg és egyidejűleg 64 titkosító kulcs használatát teszi lehetővé. Ezek a titkosító kulcsok különböző, akár egymást átfedő felhasználói csoportokban lehetnek közös használatban egyidejűleg. Ezek a titkosító kulcsok a mindennapi életben használt kulcsokhoz hasonlóan nyitják és zárják a titkosított dokumentumokat.

7.4. A DESlock+ titkosító algoritmusai

A DESlock+ Windows-ban a következő adattitkosító algoritmusokat támogatja:

3DES

Az IBM által 1974-ben kifejlesztett DES (Data Encryption Standard) egy változata. A 3DES 2x56 bites kulcsokat használ, ezzel 112 bites effektív kulcshosszt nyerve (gyakorlatilag háromszorosan végzi el az adatok titkosítását DES algoritmussal).

Blowfish

1993-ban fejlesztette ki Bruce Schneier, kriptográfus, IT biztonsági szakértő és számos szakkönyv szerzője. A Blowfish egy 64-bites blokktitkosító kombinálva egy 128 bites titkosító kulccsal.

AES

Az Advanced Encryption Standard (fejlett titkosítási szabvány) algoritmusát Rijndael néven fejlesztette ki Joan Rijndael és Vincent Rijmen, két belga kritptográfus, akik a leuven-i egyetemen szereztek PhD fokozatot. A Rijndael-t 2000 októberében fogadták el AES-ként, a DES utódjaként. A DESlock+ az AES-t 256 bites kulcshosszig támogatja.

RSA

Az RSA aszimmetrikus titkosítási eljárást Ronald Rivest, Adi Shamir és Leonard Adelmann MIT (Massachusets Institute of Technology) számítógéptudományi kutatókról nevezték el, akik kifejlesztették 1977-ben. A DESlock+ is használ RSA titkosítást és aszimmetrikus titkosítási technológiákat (PKI) minden olyan művelthez, amikor titkosító kulcsokat továbbít nem biztonságos, nyilvános csatornákon keresztül, mint pl. email, fájlmegosztás stb.

7.5. Telepítés és licencszelés

A DESlock+ szoftvert telepítési feltételei a következők Windows rendszeren:

- Legalább 64MB szabad merevlemez terület,
- 128 MB memória,
- Internet Explorer 6 vagy újabb webböngésző.

Kompatibilis operációs rendszerek:

- Windows XP 32 bit Service Pack 3
- Windows XP 64 bit Service Pack 3
- Windows Vista 32 bit
- Windows Vista 64 bit
- Windows 7 32 bit
- Windows 7 64 bit
- Windows Server 2003 32bit
- Windows Server 2008 64bit beleértve RDS
- Windows Server 2008 R2 beleértve RDS

A DESlock+ használható egyénileg is, de vállalati környezetben célszerű a felhasználókat egy DESlock+ Enterprise Server segítségével központilag kezelni. Ehhez a DESlock+ Essential vagy Standard Edition illetve a DESlock+ Pro licencek szükségesek. A DESlock+ Personal Edition példányai nem kezelhetőek központilag.

	Personal Edition	Essential Edition	Mobile Edition	Standard Edition	DESlock+ Pro
Teljes merevlemez titkosítás	–	–	–	–	✓
Cserélhető adathordozók titkosítása	–	–	–	✓	✓
DESlock+ Go Portable titkosítás	–	–	–	✓	✓
Fájl- és könyvtártitkosítás	✓	✓	–	✓	✓
Outlook bővítmény - email és csatolmány titkosítás	✓	✓	✓	✓	✓
Szöveg és vágólap titkosítás	✓	✓	✓	✓	✓
Titkosított virtuális kötetek és tömörített állományok	✓	✓	–	✓	✓
Központi menedzsment	–	✓	✓	✓	✓

62. ábra: DESlock+ licenctípusok és funkciólista

Frissítés a központilag kezelt felhasználók esetén

Alapesetben a rendszergazda végzi a szoftverfrissítést, vagy biztosít egy olyan telepítő csomagot, amely a szervezet számára lett elkészítve. A telepítéshez rendszergazdai jogok szükségesek. A rendszert újra kell indítani a frissítés befejezéséhez

Megjegyzés: A DESlock+ bármelyik verzióját érvényes DESlock+ éves előfizetés mellett illetve érvényes támogatással és DESlock+ öröklicenc mellett lehet telepíteni. Lejárt DESlock+ előfizetés mellett vagy lejárt támogatással DESlock+ öröklicenc mellett a DESlock+ azon verzióit lehet telepíteni, amelyek a támogatási időszak végéig jelentek meg. Ha a DESlock+ előfizetés lejárt, csökkentett funkciókészlet érhető el. Öröklicenc esetében a teljes funkcionalitás olyan verzió mellett van meg, amely a támogatási szerződés idején jelent meg. Újabb verziók esetén azonban ismét csak limitált funkciók érhetőek el.

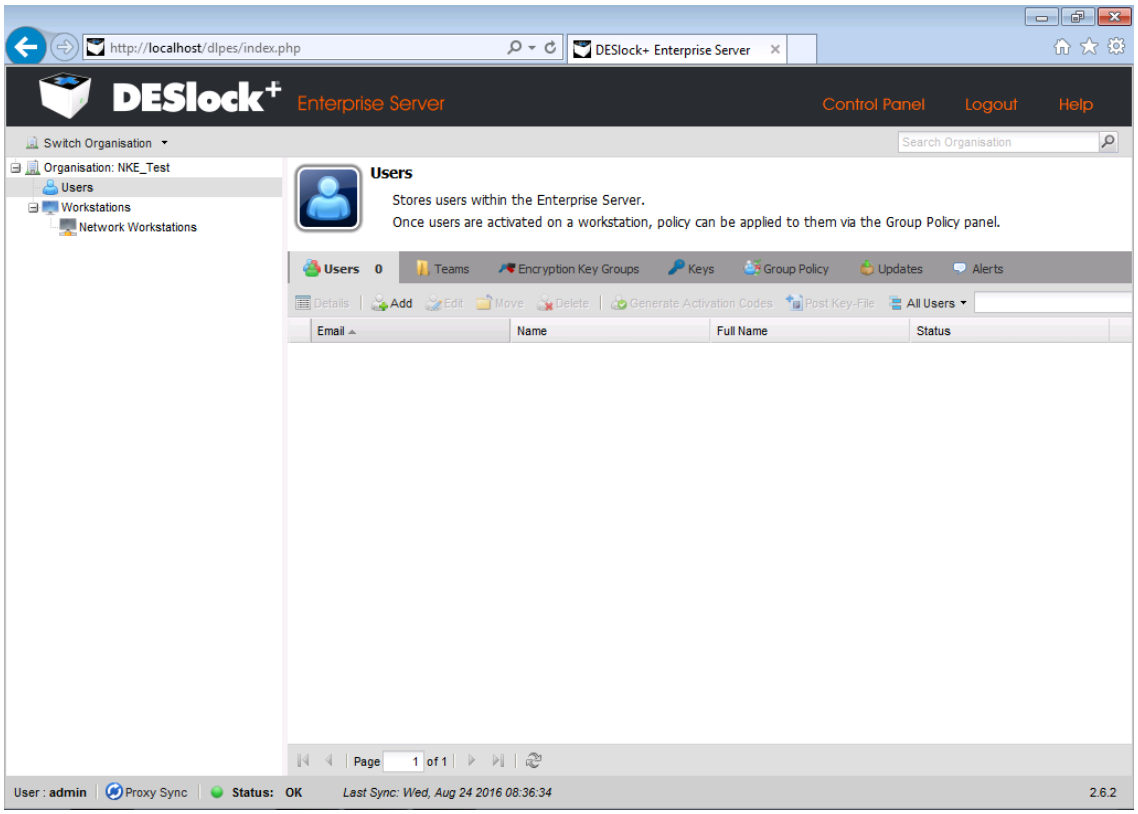
7.6. A központi menedzsment, azaz Enterprise Server-alapok

A DESlock+ Enterprise Server böngésző alapú megoldás, amely a DESlock+ adattitkosítási megoldásokat futtató számítógépek és felhasználók központi kezelésére szolgál. Lehetőséget biztosít a rendszergazdák számára, hogy definiálják a biztonsági szabályozásokat és beállításokat, hogy minél magasabb biztonsági szintet érhessenek el. A kommunikáció a felhasználói végpontok és az Enterprise Server között történhet a szervezeten belül, de lehet akár felhős proxy server alapú is. A kommunikáció teljes mértékben titkosított és a DESlock+ Enterprise Proxy serveren tárolt adatok is titkosított formában tárolódnak.

FIPS 140-2 szabványnak megfelelő 256 bites AES titkosítás használható az összes típusú titkosításhoz.

Az Enterprise Server vezérlőfelületének részei:

- Navigation Panel
- Subject Title
- Subject Details
- Tab and Menu Bar
- Main Control Bar



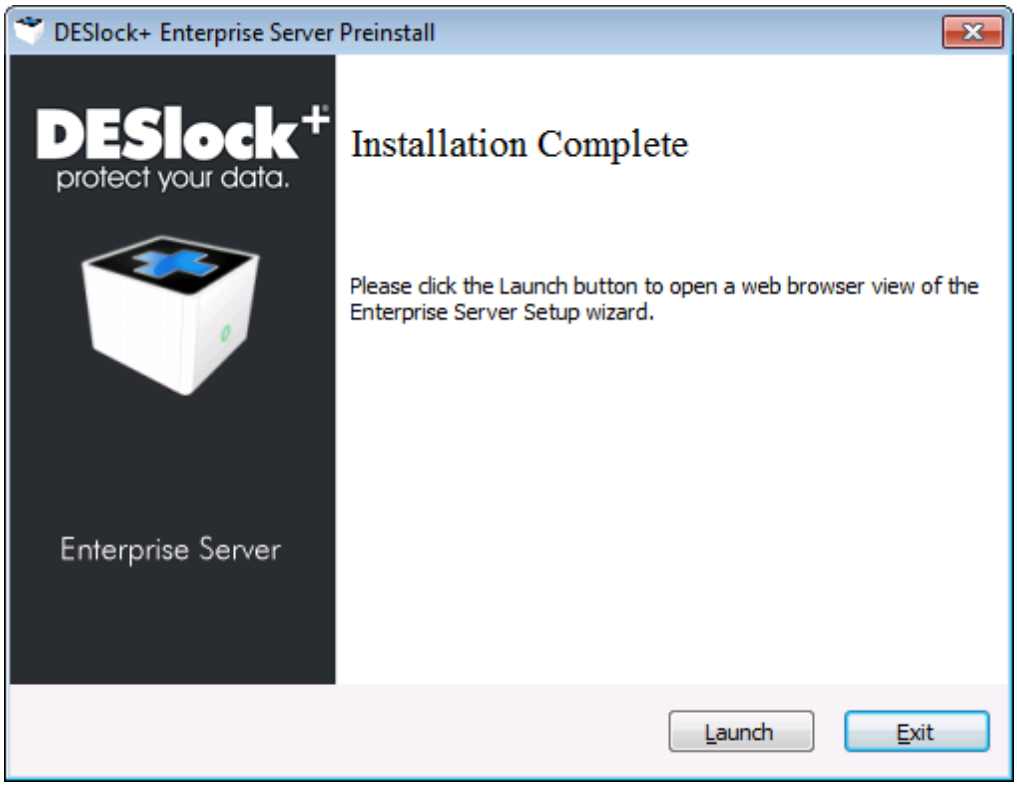
63. ábra: Az Enterprise Server központi felülete

7.7. Rendszerkonfiguráció és telepítés

Telepítés

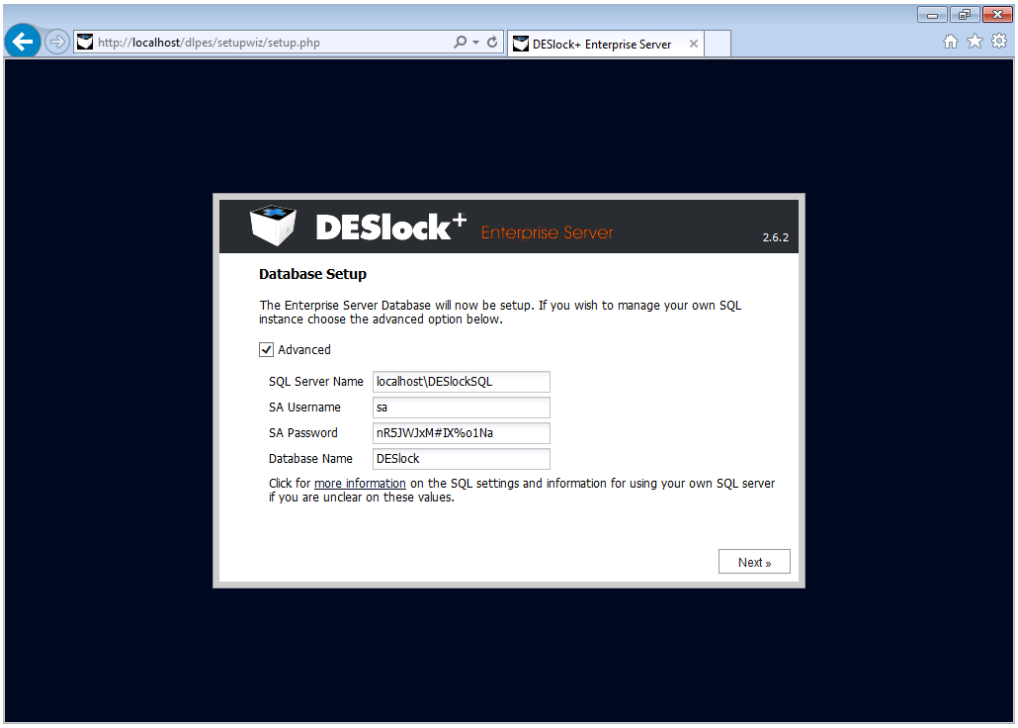
A DESlock+ Enterprise Server telepíthető minden Windows XP (SP3) vagy annál újabb operációs rendszerre. Javasolt ezen, fizikai vagy virtuális gép biztonsági mentése az adatvesztés megakadályozása érdekében.

1. Töltse le a http://www.eset.hu/letoltes/vallalati/adattitkositas oldalról a kívánt telepítőcsomagot, majd futtassa. Az „all in one” telepítő segítségével a következő komponenseket is telepíti a rendszerre: Apache, PHP, .NET, SQL Express
2. Kövesse a telepítővarázsló lépéseit, majd a telepítés végén, nyomja meg a Launch gombot.

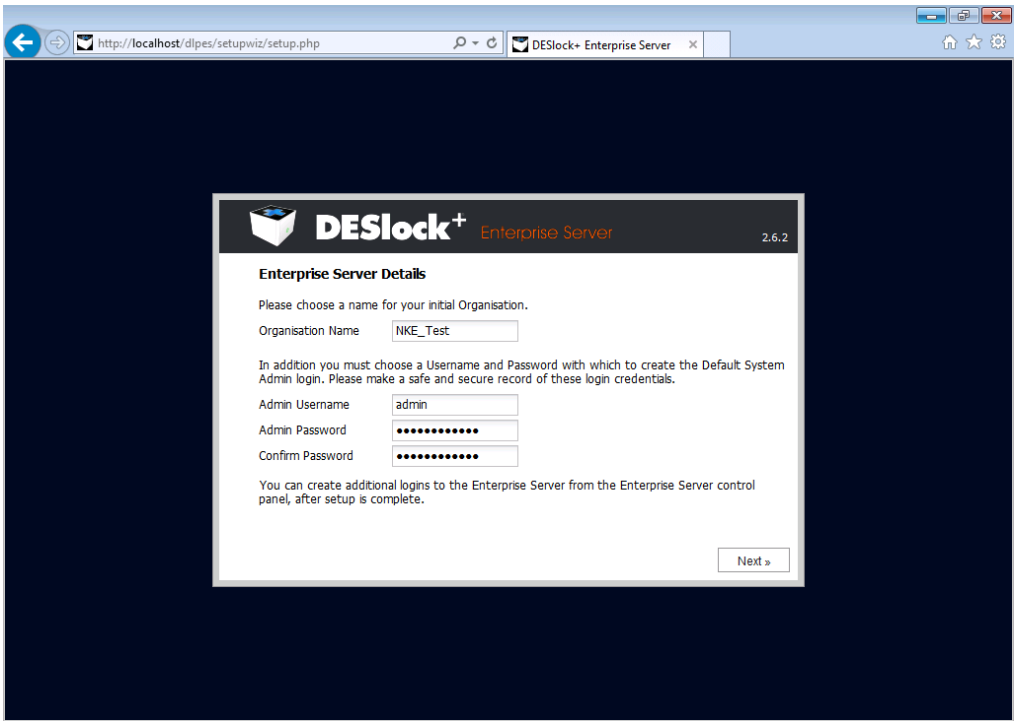


64. ábra: Telepítővarázsló utolsó lépése

3. Az Enterprise Server beállításaihoz kövesse a képernyőn megjelenő utasításokat, amelyek a licenc-adatokra, adatbázis beállításokra és a bejelentkezési adatokra vonatkoznak.



65. ábra: Enterprise Server által használt adatbázis beállításai



66. ábra: Enterprise Serverre való belépéshez szükséges rendszergazdai jelszó megadása

Konfiguráció

Mielőtt használatba venné a DESlock+ Enterprise Servert, szükséges elvégezni az alapkonfigurációt a telepítés során.

Ezek a következők:

- telepítés helye
- Internet Proxy beállítása
- almappa helyét, hogy elérhető legyen a web szerveren: http://localhost/dlpes
- SQL Server paraméterek (név, felhasználónév, jelszó, adatbázis név)
- Enterprise Server pataméterek (szervezet neve, admin felhasználónév, admin jelszó)
- DESlock+ Proxy ID

Minimális rendszerkövetelmények

Enterprise Server:

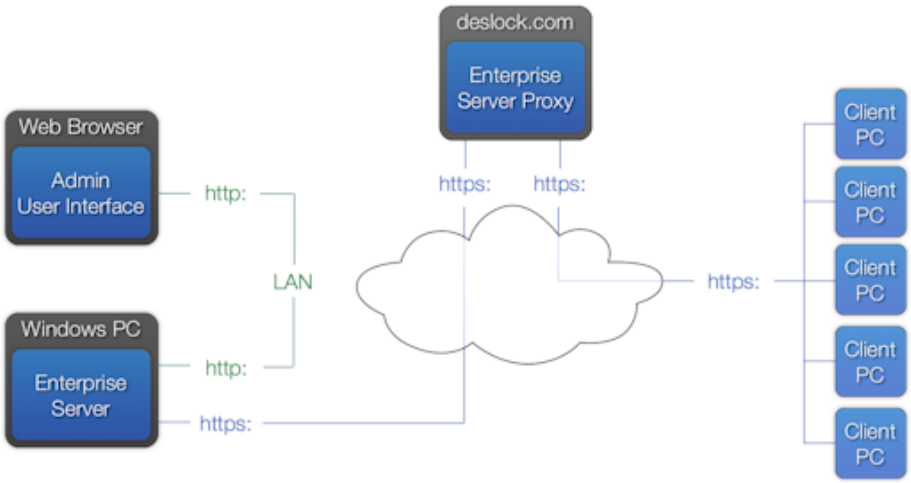
- Host Operációs rendszer
- Legalább 1GB RAM
- 30GB szabad hely a merevlemezen
- 32 bit OS – XP SP3 vagy újabb
- 64 bit OS – Windows 2003 vagy újabb

Előtelepített szoftverek

- SQL Server 2005 Express
- Apache 2.2 vagy IIS 6+
- PHP 5.3.x VC9

További követelmények A 443 port engedélyezése az Internet felé a felhőben működő proxy és a licencszerver elérése érdekében

Opcionális SMTP



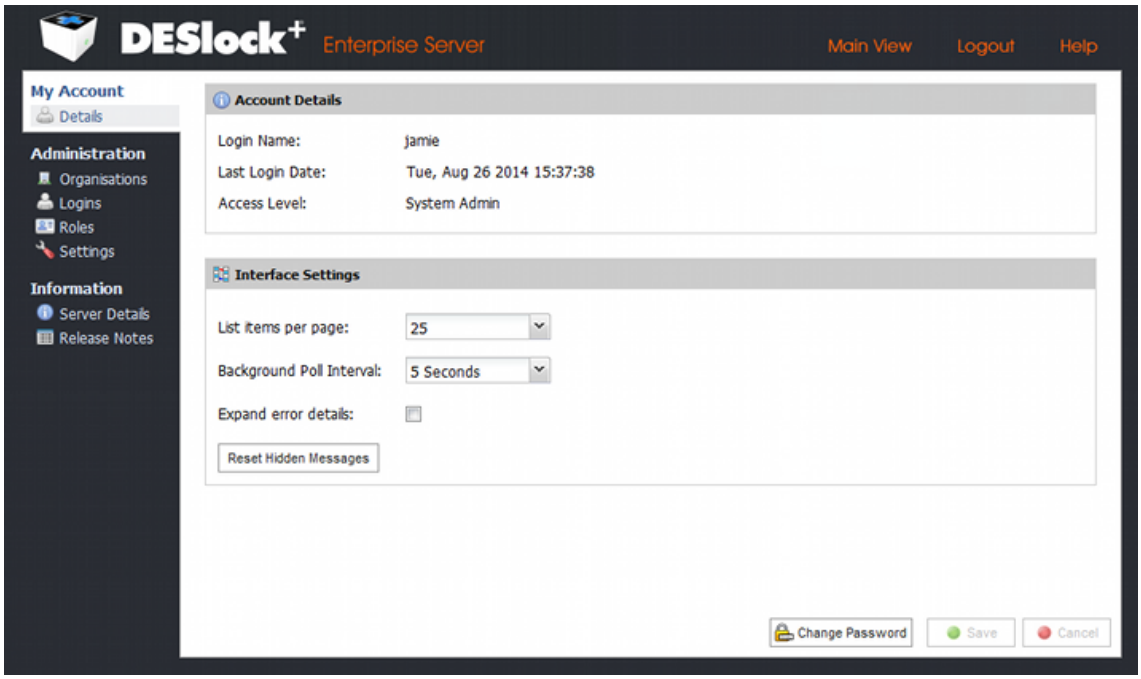
67. ábra: Az Enterprise Server kommunikációjának sematikus rajza

Miután telepítette a központi menedzsment szoftvert és elindította, a web böngészőben a beállítás varázsló elindul és végigvezet az első lépéseken. Ez egy szükséges lépés a központi menedzsment használata előtt.

A DESlock+ Enterprise Server használatba vételéhez jelentkezzen be a felületre a lenti képen látható ablakban.

68. ábra: Az Enterprise Server bejelentkezési felülete

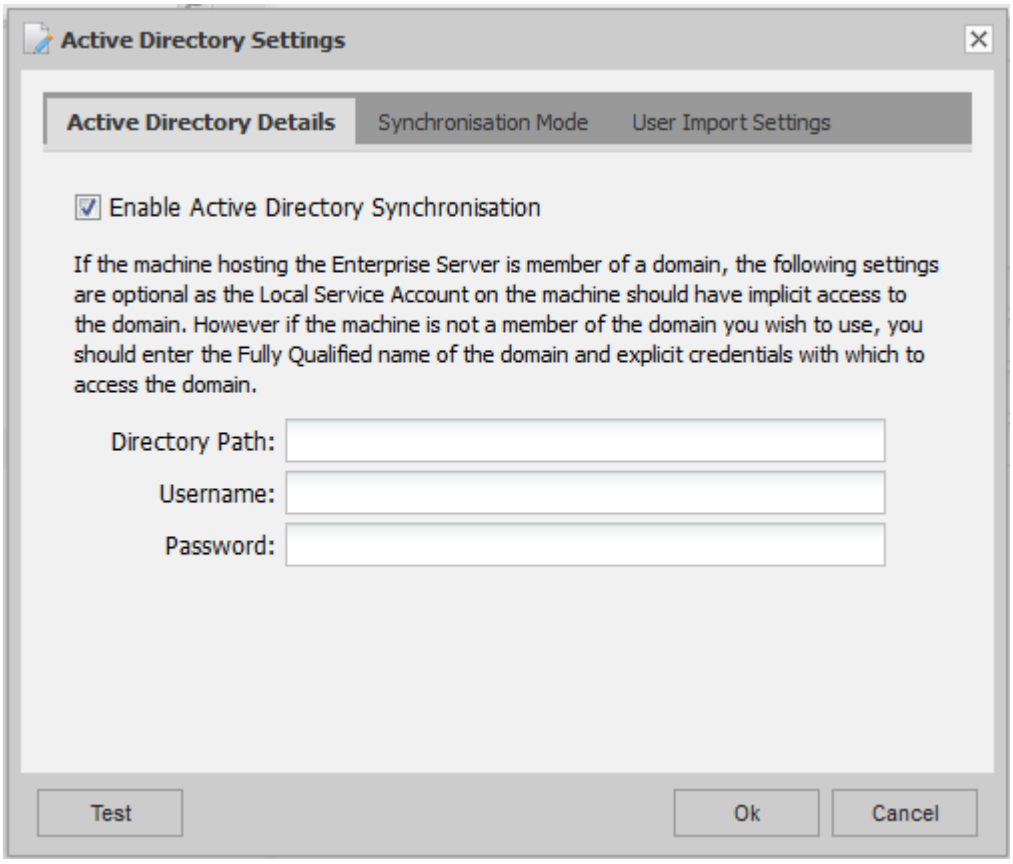
Három típusú standard felhasználói szerepkör áll rendelkezésre. (system administrator, administrator és helpdesk), a system administratornak van lehetősége új szabályokat létrehozni és ezt hozzárendelni a számítógépekhez vagy felhasználókhoz.



69. ábra: Az Enterprise Serverben a felhasználói fiók beállítási lehetőségei

7.8. Active Directory beállítások

Az Active Directory beállításainak elvégzéséhez és/vagy módosításához, kattintson „Control Panel” „Organisation” menüpontjában a kezelt szervezetre, majd itt az „Active Directory Settings” gombra a Details panel jobb alsó részén. Tiltani és engedélyezni tudja az AD integrációt és módosíthatja a szinkronizálás lehetséges beállításait és felhasználók importálásának módját.



70. ábra: Az AD-szinkronizálás beállításai

7.9. Policy beállítások

Két típusú policy mód konfigurálására van lehetőség (annak érdekében, hogy finomhangolhassa a program működését a végpontokon). Ez a két típusú házirend: a *Workstation Policy* és a *Group Policy.*

A *Workstation Policy* szabályozza, hogy az Enterprise Server, felhasználók és munkaállomások milyen módon kommunikáljanak, továbbá a külső adatforrásokhoz való hozzáférést is. A Workstation Policy beállításai a DESlock+ kliensprogram telepítése után rögtön érvényesülnek.

A *Group Policy* a bejelentkezett felhasználóra érvényesül, kontrollálja a DESlock+ funkciókat és szabályozza, hogy a felhasználók milyen menüpontokat és funkciókat érhessenek el. A Group Policy a felhasználók bejelentkezése után felülírhat bizonyos Workstation Policy beállításokat.

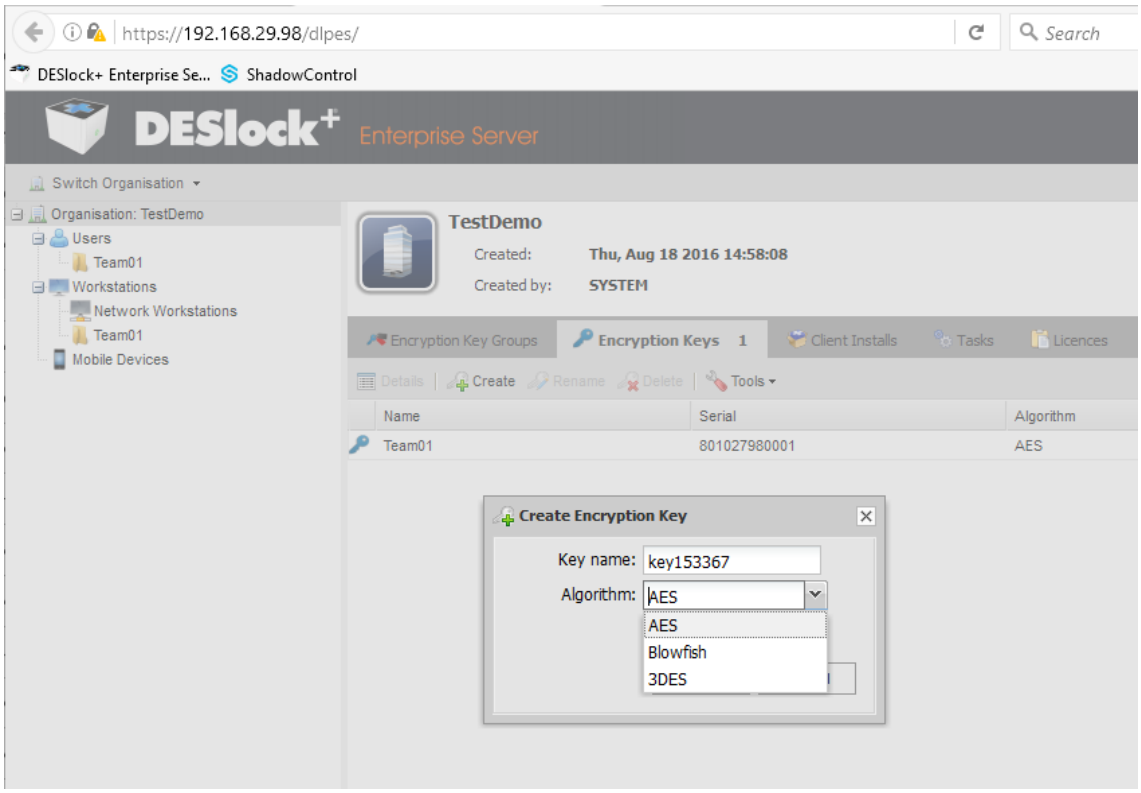
7.10. Encryption Groups and Keys

Nincs meghatározott sorrend, hogy az *Encryption Key Group*-ot vagy az *Encryption Key*-t szükséges először létrehozni.

Titkosítási kulcs létrehozása

Titkosítási kulcsokat központilag kezelt felhasználók számára a rendszergazda hozza létre az Enterprise szerveren. Ez a *„Main View” „Organisation”* menüpontjában történik.

Adja meg a kulcs nevét és válassza ki a használni kívánt algoritmust (Blowfish, 3DES vagy AES) és kattintson az *Add* gombra.



71. ábra: Titkosításikulcs-kezelő a DESlock+ Enterprise Serveren

A központilag kezelt felhasználók esetében a titkosítási kulcsokat és a kulcsállományt a DESlock+ Enterprise Servert kezelő rendszergazda felügyeli, és a felhasználó csak megnézni tudja, mely kulcsok állnak rendelkezésre. A központilag kezelt felhasználók tehát nem tudnak titkosítási kulcsokat létrehozni vagy törölni.

Titkosítási kulcsok archiválása

A titkosítási kulcsok mentése különösen fontos, hiszen, ha a kulcs többé nem hozzáférhető, akkor a vele titkosított adatokhoz sem lehet hozzáférni. A mentési folyamat során a teljes kulcsfájl mentésre kerül a benne levő összes titkosítási kulccsal együtt.

Titkosítási kulcsok megosztása egymás közt

A titkosítási kulcsok átadását a kulcsátviteli varázslóval *(Key Transfer Wizard)* tudjuk megoldani. Amikor ezt a varázslót elindítjuk, a következő lehetőségekből választhatunk:

- Kulcs igénylése más felhasználótól
- Kulcs kiadása más felhasználónak
- Kulcsfájl frissítése más felhasználótól

A kívánt művelet kiválasztása után a varázsló végigvezet a szükséges műveleteken. A varázsló által elkészített átviteli állományokat azután átadhatjuk más felhasználónak e-mailben vagy hálózati megosztásokon keresztül.

Kulcs átadásakor be lehet állítani, hány lépésben lehet még a kulcsot legfeljebb továbbadni: ez a *„Terminator Count”* érték.

Encryption Groups

A *Navigation* panelen válassza az Organization menüpontot és kattintson az *Encryption Groups* fülre. Új kulcs csoport hozzáadásához kattintson a *Create* feliratra a menüben. A *Create Encryption Key Group* ablakban adja meg a csoport nevét, és kattintson az *Add* gombra.

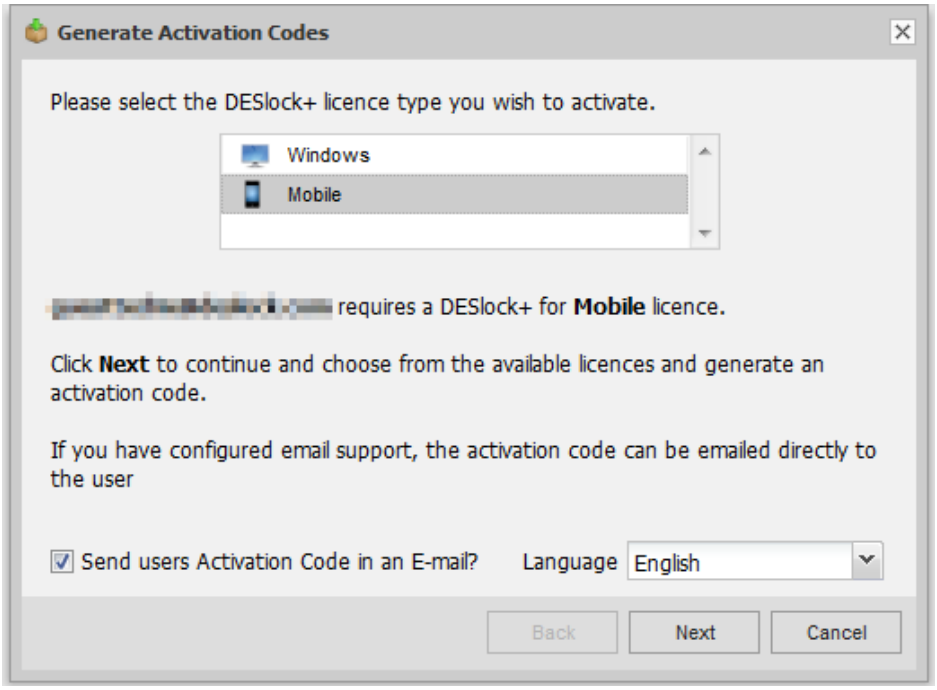
A *Navigation* panelen válassza az Organization menüpontot és kattintson az *Encryption Groups* fülre. Válassza ki a kívánt csoportot és dupla kattintással megkapja a *Details* ablakot és az Encryption Key részletei ablakban nyomja meg az *Add* gombot. Ezzel a kulcs hozzáadódott a csoporthoz, így a benne lévő tagokhoz is, viszont ezek a tagok piros színre fognak változni, mivel szükséges a kulcsfájl frissítése a megfelelő működéshez.

7.11. Mobil eszközök hozzáadása

Jelenleg csak az iOS rendszer támogatott, de az Android alapú rendszerek támogatása is hamarosan érkezik. Első körben szükséges a DESlock+ iOS applikáció letöltése és telepítése. A telepítés után, amíg az aktiválás nem történik meg a védelem ingyenes azaz free üzemmódban fut.

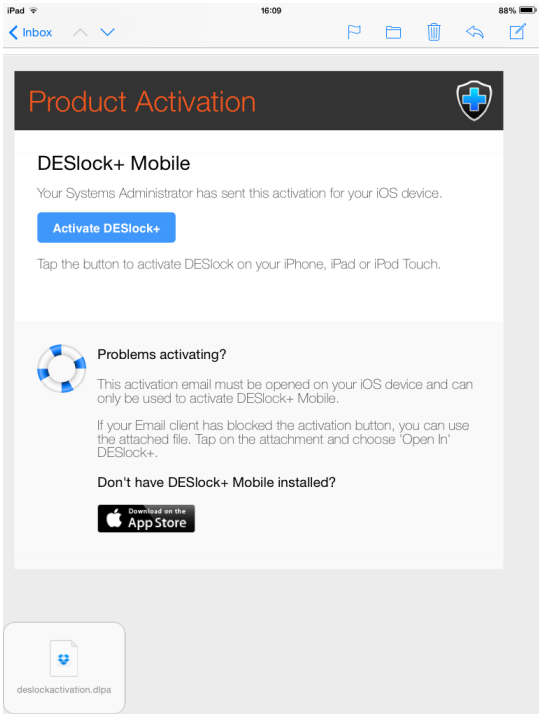
A DESlock+ letöltése az Apple Store-ból:
https://itunes.apple.com/us/app/deslock+-for-ios/id880602467?ls=1&mt=8

Az aktiválási kulcs generálását az Enterprise Serveren belül tudja elvégezni, az alábbi képen látható ablakban a Mobile opciót választva. Vegye figyelembe, hogy szükséges a mobilok védelmét ellátó licenc hozzáadása az Enterprise Serverhez a védelem biztosításához (Main View / Organisation Licenses).



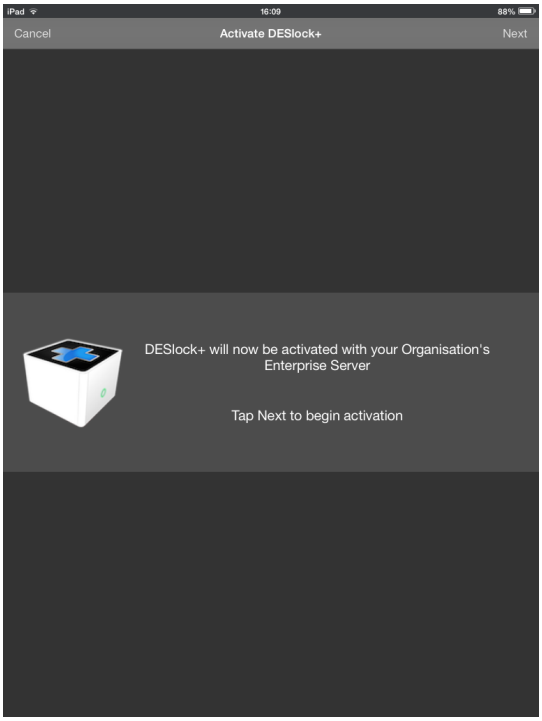
72. ábra: Az Enterprise Server aktiválási kulcs generáló ablaka

Vegye figyelembe, hogy az aktiválási kulcs kiküldése e-mailben történik, így fontos, hogy egy valós e-mail címmel rendelkezzen az érintett felhasználó. Az e-mail megérkezése után, nincs más teendő, csak rákattintani az Activate gombra, amennyiben ez nem működik, kérjük, nyissa meg a levél csatolmányát, ami ugyanazt a funkciót látja el, mint a gomb alatt lévő link.



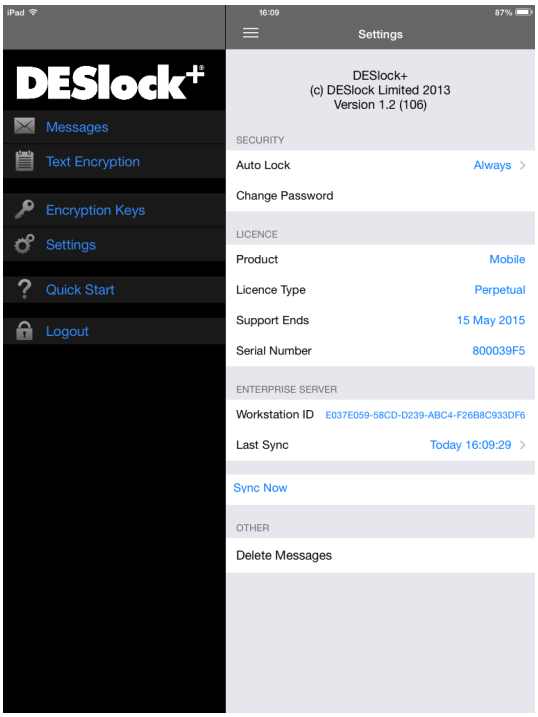
73. ábra: Aktiválási információkat tartalmazó e-mail

Az aktiválás elvégzése után a program elindul és arra kéri a felhasználót, hogy állítson be egy jelszót a kulcsfájlhoz.



74. ábra: Aktiválási ablak

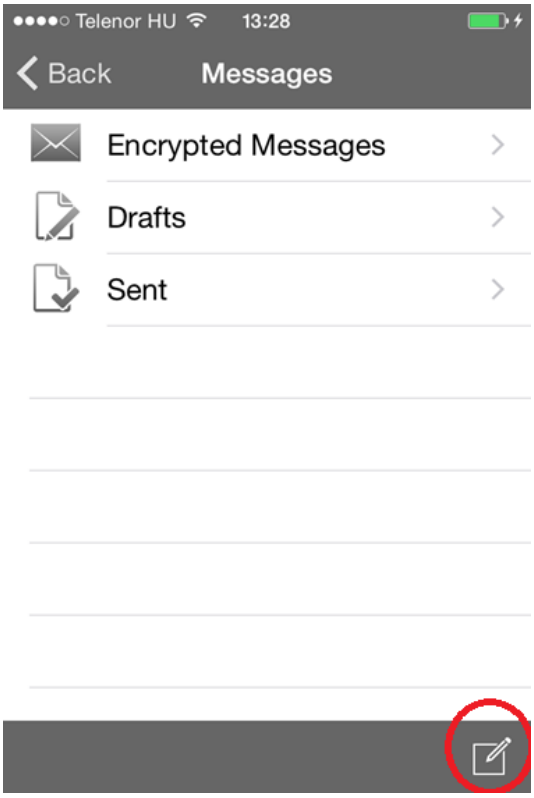
Az aktiválási folyamat lezárulta után (74. ábra) a program aktivált státuszba kerül és lehetőséget biztosít a titkosító kulcsokhoz való hozzáféréshez, amelyeket az „Encryption keys” menüpontban találunk.



75. ábra: DESlock+ vezérlőfelülete iOS rendszeren

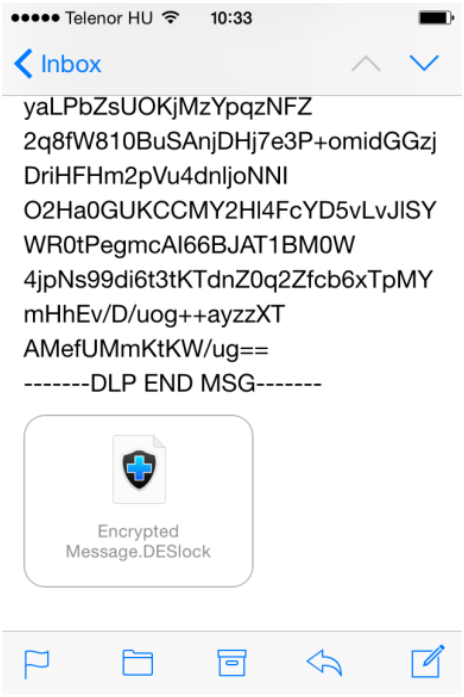
Az applikáció segítségével felhasználóbarát módon lehetséges az iOS Mail programjából titkosított levelezést folytatni, („Messages” menü). Egyéb szoftverek esetében a szövegtitkosítás („Text encryption”) használható vágólap közvetítésével.

A beépített levelezőkliens használatakor titkosított levél küldése esetén a DESlock+ alkalmazásból kezdeményezzük az üzenetküldést (Lásd:76. ábra).



76. ábra: Levelezés titkosítása

A varázslón végighaladva tudjuk megadni a használt titkosítási kulcsot és a címzettet is. Befejezéskor a DESlock+ alkalmazás automatikusan továbbítja a levelet a beépített Mail kliensnek, amely elküldi azt a megfelelő címzettnek. Titkosított levél fogadásakor a beépített Mail kliens egy csatolmány megnyitásához alkalmazza a DESlock+ alkalmazást (77. ábra).

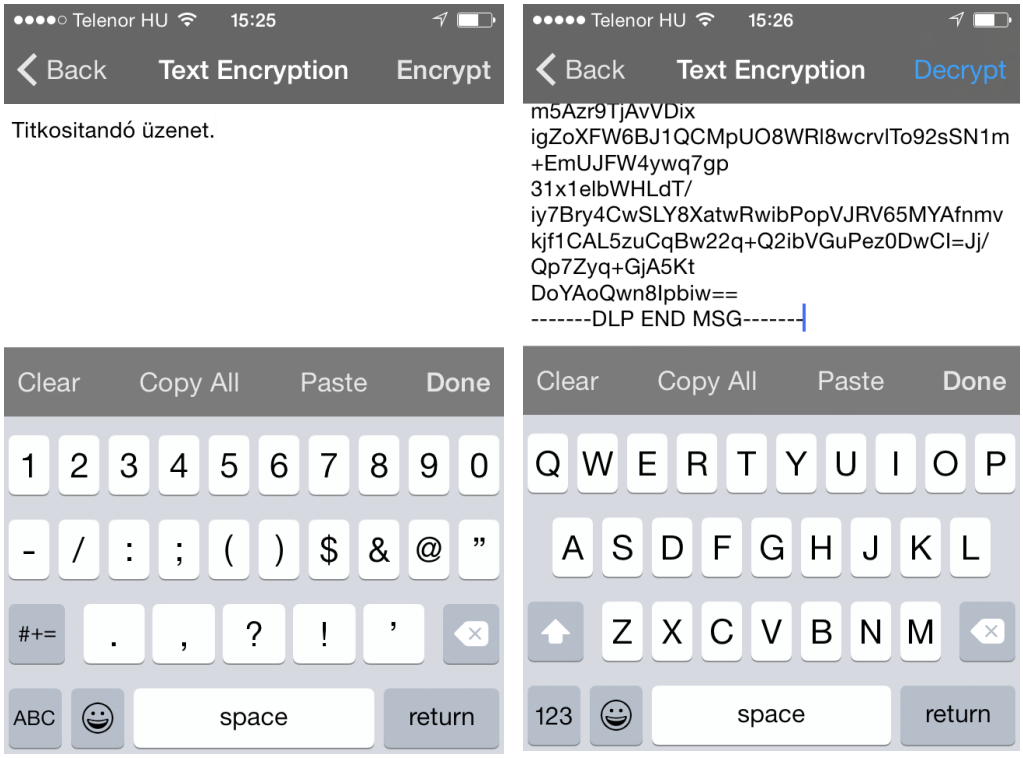


77. ábra: Titkosított e-mail

A csatolmányra „koppintva” megnyílik a DESlock+ alkalmazás, ahol amennyiben a megfelelő kulcs/jelszó rendelkezésre áll, az üzenet olvashatóvá válik a fogadó fél számára is!

78. ábra: Visszafejtett e-mail

Amennyiben nem a beépített levelezőprogramot használjuk, a szövegtitkosítás funkció használata szükséges. Titkosítani az „Encrypt” gomb segítségével lehetséges (79. ábra, bal oldali pillanatkép).



79. ábra: Szövegtitkosítás

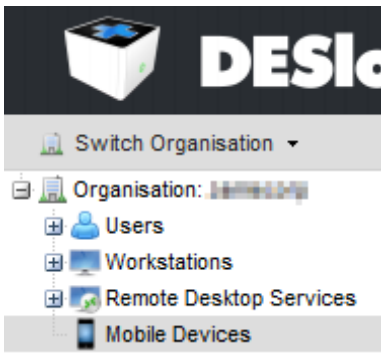
A varázsló felajánlja rendelkezésre álló kulcsokat és a jelszavas titkosítás lehetőségét, majd megjelenik a titkosított üzenet.

A titkosított szöveget vágólapon („Copy All” segítségével) lehet más applikációk felé továbbítani.

Decryptáláskor erre a felületre szükséges vágólapon keresztül bemásolni a titkosított üzenetet, majd a jobb felső „Decrypt” gomb megnyomása után (Lásd: 79. ábra, jobb oldali pillanatkép) a rendelkezésre álló titkosító kulcsokkal, illetve a megadandó jelszóval történik a visszafejtés.

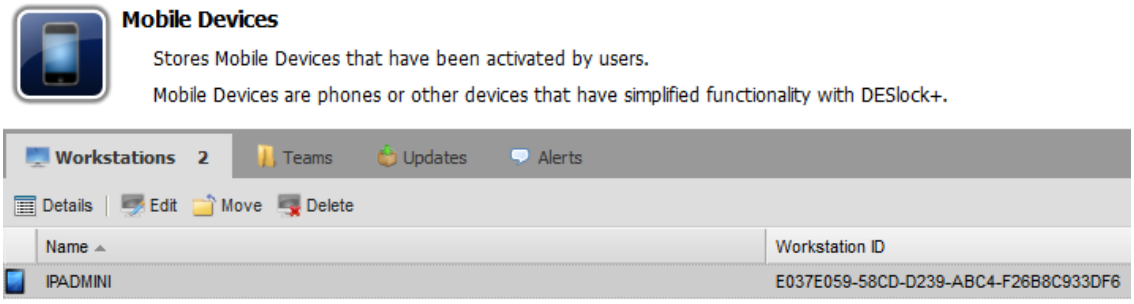
7.12. A mobil védelem Enterprise Serverben való menedzsmentje

Az első mobil eszköz aktiválása után az Enterprise Serverben egy új team (csoport) jön létre *Mobil Devices* néven, ahol az összes aktivált eszköz megjelenítésre kerül.



80. ábra: Enterprise Server team struktúra

A mobil eszközök több dologban eltérnek a normál végpontoktól, hiszen nem érvényesül rajtuk a Workstation Policy, nem futtatható rajtuk teljes merevlemez titkosítás, de más szempontból hasonlóan működnek, hiszen láthatóak az eszközállapotok és riasztások, ezen felül alcsoportok is létrehozhatók.



81. ábra: Aktivált mobil eszközök listájának ablaka

7.13. Egyéb lehetőségek

Központi menedzsment-környezetben használhatunk munkaállomásokhoz rendelhető házirendeket, (Workstation Policy) amelyek segítségével letilthatjuk vagy szabályozhatjuk a nem tikosított adathordozó eszközök használatát.

A házirend cserélhető adathordozókhoz való hozzáférést szabályzó beállításai:

- Nyitott (Open): bármely cserélhető adathordozó használata engedélyezett
- Blokkolt (Blocked): az összes cserélhető adathordozó elérése le van tiltva
- Csak olvasható (Read Only): a cserélhető adathordozók olvasása engedélyezett, írása tiltott

Ezeket a beállításokat a DESlock+ Enterprise Server-en az Enterprise Server adminisztrátorok alkalmazhatják.

Központilag nem menedzselt hálózatok esetén DESlock+-ba bejelentkezve a Key-File házirend szabályozza a hozzáféréseket. Titkosítatlan adathordozó esetén a felhasználónak felajánlható az eszköz titkosítása, amennyiben az szükséges. Központilag menedzselt környezetben az eszköz titkosításának felajánlása házirenddel szabályozható.

A titkosítás és a titkosítás feloldása, valamint a DESlock+ további funkciói csak abban az esetben használhatóak, ha a DESlock+ telepítve van, és a felhasználó be van jelentkezve.

Egyetlen kivétel a DESlock+ Go alkalmazás, ahol a licenccel rendelkező felhasználó jelszó megadása segítségével hozzáférést adhat a korábban titkosított adatokhoz. A titkosított adat abban az esetben lesz elérhető, ha telepített DESlock+ program jelenléte esetén rendelkezünk a megfelelő titkosítást feloldó kulccsal vagy ha az adathordozón található Deslock+ Go hordozható alkalmazásban megadjuk a jelszót. Ez a módszer olyan munkaállomásokon is hozzáférést biztosít a titkosított információkhoz, ahol a DESlock+ nincs telepítve illetve licencelve.

Központilag menedzselt rendszer esetén a DESlock+ Go az adminisztrátor által szabályozott, funkciói pedig a házirend szerint kerülnek beállításra.

7.14. További funkciók, amelyek a Windows környezetben érhetőek el

Teljes merevlemez titkosítás

A DESlock+ lehetővé teszi teljes merevlemez(ek) vagy partíciók titkosítását 256-bites AES algoritmussal. Használata mellett a felhasználónak a rendszerbetöltés előtti azonosítania kell magát a rendszerhez való hozzáféréshez. A teljes merevlemez titkosításhoz a DESlock+ Pro licenc szükséges.

A központilag menedzselt felhasználók esetében a teljes merevlemez titkosítás felügyelt módban valósul meg. Ilyenkor a DESlock+ Enterprise Server rendszergazdája határozza meg a beállításokat az egyes számítógépek számára. Általában ilyenkor a belépési jelszót is központilag adja meg a rendszergazda, de szükség esetén a titkosítási feladat delegálható a felhasználónak is biztonságos módon. Az Enterprise Server konzol használatának további előnye, hogy a jelszó elfelejtése esetén a szerverről megkapható a helyreállító kód. A szerver használatával oldható meg a jelszó cseréje, illetve a számítógép elérhetetlenné tétele egy esetleges lopás esetén. A teljes merevlemez titkosításához megfelelő DESlock+ szoftverlicenc szükséges.

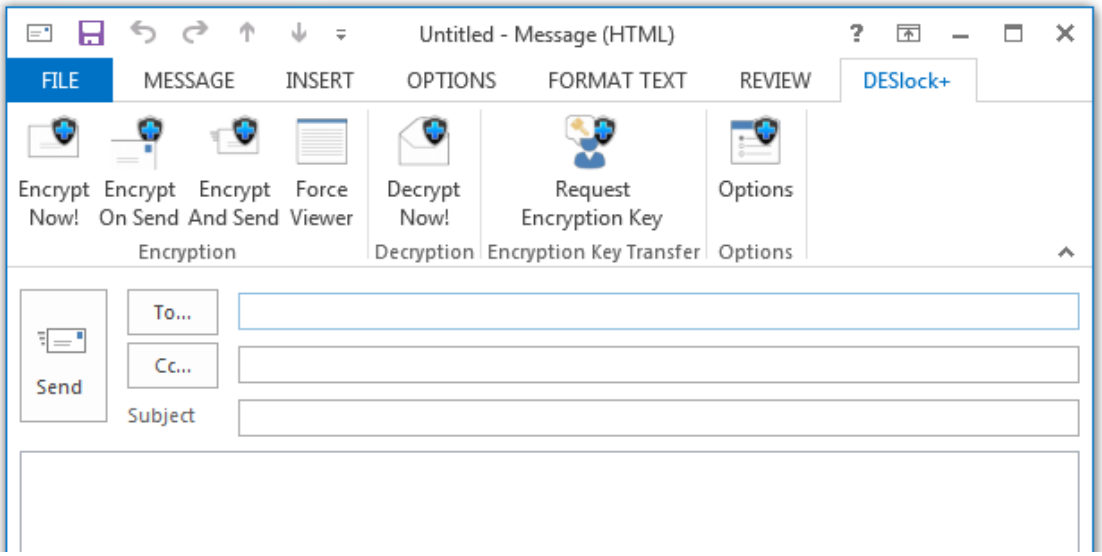
A teljes merevlemez titkosítás a teljesítménytől és a mérettől függően kb. egy óráig tart. A merevlemez titkosítástól függetlenül szükséges egyes fájlokat vagy e-maileket titkosítani, amennyiben bizalmas adatokat viszünk át hálózaton vagy e-mailben.

Az Outlook plug-in használata

A DESlock+ Outlook plugin segítségével titkosíthatja e-mailjeit és azok mellékleteit.

Amennyiben Outlook levelező klienst nem használnak a rendszerben, úgy az e-mailek, üzenetek és mellékletek titkosítása a file- és szövegtitkosítás funkciókkal végezhető el.

Az Outlook programból való titkosított levél küldéséhez kattintson a levelezőprogramban a „New Email” vagy „Új e-mail” gombra. Az új e-mail ablak megjelenésekor az e-mail titkosítás opcióinak eléréséhez kattintson a DESlock+ fülre.



82. ábra: A DESlock+ Outlook bővítménye által biztosított funkciók

A levél szövegezését követően az „Encrypt Now!” gombra kattintva a küldendő e-mailek teljes mértékben titkosíthatóak. Amennyiben a levélnek csak egy részét szeretné titkosítani, írja be a levélbe a titkosítandó szöveget, kattintson az „Encrypt Now!” gombra, majd folytassa a levelet a nem titkosítandó szöveg bevitelével, végül a levél elküldéséhez kattintson a „Send” vagy „Küldés” gombra.

A levelek titkosítási kulccsal vagy jelszóval titkosíthatóak (központi felhasználó-kezelés esetén akkor, ha a jelszóval való titkosításhoz a felhasználó jogosultságai biztosítottak).

A titkosítás módszerét (biztosítási kulccsal vagy jelszóval) a címzett titkosítás-feloldási lehetőségeit (kulcsait) figyelembe véve érdemes kiválasztani. Például, ha a címzett nem rendelkezik telepített DESlock+ alkalmazással, akkor a jelszóval való titkosítás lehet a megfelelő választás. A jelszóval titkosított levél elolvasásához a címzettnek használhatja az ingyenes DESlock+ Reader programot, amely a következő linken érhető el: https://www.deslock.com/deslock+_reader.php

DESlock+ Go használata

A DESlock+ Go-val a DESlock+ telepítése, illetve a megfelelő titkosító kulcs nélkül is lehetőség nyílik a titkosított cserélhető vagy adathordozó olvasására.

DESlock+ nélküli gépek esetén:
Helyezze be az adathordozót, válassza ki a számítógépben a hordozható adattárolót, a DESlock+ Go elindításához kattintson duplán a DLPgo.exe állományra! A DESlock+ Go elindulását követően adja meg a szükséges jelszót, amelynek hatására a hordozható adattárolón titkosított lemezterület egy külön meghajtóként elérhetővé válik.

A DESlock+ Go további előnye, hogy olyan számítógépen is megnyithatóak a titkosított állományok, ahol ugyan a DESlock+ telepítve van, de a kulcsállomány nem tartalmazza az állomány titkosításának feloldásához szükséges kulcsot. Ilyen esetben az adathordozó behelyezését követően a DESlock+ program nem fog megfelelő kulcsot találni a titkosítás feloldásához, így a hordozható adattárolón titkosított állományok eléréséhez a program jelszót fog kérni. A jelszó megadásával a titkosítás feloldásra kerül.

7.15. A szoftver eltávolítása

A program eltávolításakor szükséges figyelembe venni, hogy a szabályos eltávolításkor az összes korábban titkosított állomány visszaállításra kerül. Ezért központilag kezelt telepítés esetén az eltávolítást érdemes jelszó megadásához kötni. Az eltávolítás csak a teljes merevlemez titkosítás visszaállítása után lehetséges. Az e-mailek titkosítva maradnak, amennyiben a titkosítás nélküli tárolást Workstation Policy segítségével megtiltotta a rendszergazda. Mind a mobil eszközről, mind a Windows rendszer esetében a megszokott módon történik a termékek eltávolítása. Újratelepítéskor a központilag kezelt felhasználó visszakapja a számára kiosztott titkosítási kulcsokat, így a titkosított kollaboráció helyreáll.

A fentiek a 41/2015. (VII. 15.) BM rendeletben meghatározott alábbi funkciókat valósítják meg:

- Aláírt elemek
  Mivel az Apple Store-ból kell az alkalmazást letölteni, harmadik fél nem módosíthatja azt, ezt az Apple ellenőrzi.
- Adathordozók védelme
  Emailek, szövegek részben vagy egészben történő kriptográfiai védelme.
- Azonosítás és hitelesítés
  A felhasználó magának állít be jelszót az alkalmazáshoz és a kulcstárhoz. Ennek hiányában a kriptált tartalom nem olvasható.
- Hozzáféréskontroll – Felhasználói fiókok kezelése
  A DESlock Enterprise Server az AD szinkronizált felhasználóknak osztja ki a titkosítási kulcsokat. A kulcsok a szerverről rendszergazdai jogkörben megvonhatóak, így a hozzáférés kontrollálható a szervezet fizikai határain belül és kívül is.
- Letiltás
  A DESlock Enterprise Server az AD szinkronizált felhasználóknak osztja ki a titkosítási kulcsokat. A kulcsok a szerverről rendszergazdai jogkörben megvonhatóak, így a hozzáférés azonnal megvonható a szervezet fizikai határain belül és kívül is.
- Felhasználói szempontból: e-mail- és szövegtitkosítás, kulcskiadás-megvonás.

FOGALOMTÁR

- *29-es Munkacsoport:* a 95/46/EK irányelv 29. cikkében meghatározott, a tagállamok adatvédelmi biztosaiból, illetve adatvédelmi hatóságainak képviselőiből álló független tanácsadó, véleményező és konzultatív fórum. Állásfoglalásaival és javaslataival segíti az Európai Bizottság munkáját az európai polgárok információs önrendelkezési jogának védelme érdekében.
- *Adaptív jelzőlámpa:* a forgalmi viszonyoknak megfelelően szabályozza a szabad jelzések ciklusait.
- *Adat:* közlésre, megjelenítésre vagy további feldolgozásra alkalmas entitás, amely számos megjelenési formát vehet fel (pl.: alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása.
- *Adatalany:* bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.
- *Adatbiztonság:* az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében.
- *Adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).
- *Adatintegráció:* az elmúlt időszak trendjeit figyelve látható, hogy az okoseszközökön (és nem csak ott) futó alkalmazások mind nagyobb integrációra törekednek egymással, a kapcsolódó felhőszolgáltatásokkal, az eszközök más funkcióival, de akár a közösségi médiával is. Ezek az integrációs törekvések mára odáig jutottak, hogy egyes appok telepítése során alapértelmezetten kérik le az adatokat az eszköz kontaktlistájából, az elérhető közösségi médiából vagy más, kommunikációra (is) használt alkalmazásból. Ezek a kapcsolódások és adatintegrációk ma még sok esetben kellően tudatos felhasználói magatartással csökkenthetők, de sokszor az ilyen korlátozások az alkalmazások funkcionalitásának a korlátait is jelentik. Céges környezetben használt okoseszközök esetén persze elvárás lenne az ilyen összekapcsolások korlátozása, illetve megtiltása, de az imént említett funkcióvesztés ennek az egyik legfőbb akadályozó tényezője. Azt is meg kell említeni, hogy lehetnek olyan esetek, amikor az adatok átadása és szinkronizálása – ha ellenőrzött körülmények között zajlik – a biztonság fokozását szolgálhatja. Ilyen eset lehet például az, ha egy lokális címjegyzék nem csak lokálisan, hanem – egy megfelelően védett környezetben – máshol letárolódik.
- *Adatfeldolgozó:* az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.
- *Adathordozó:* sok esetben elég nehéz elválasztani az adathordozókat a hardver elemektől. Ami a fő különbséget jelenti az az, hogy ezeket az elemeket arra tervezték, hogy hosszabb-rövidebb ideig megőrizzék és tárolják az információt. Ilyen módon az adatok jelentősen koncentrálódnak az információs rendszernek ezeken az elemein. A koncentrálódás pedig érzékennyé teheti ezeket az elemeket az információ sértetlensége és bizalmassága szempontjából egyaránt. Az „okos” eszközök többnyire beépítetten és csatlakoztatható módon is tartal-

maznak adathordozókat, amelyeknek a kontrolja egyértelmű elvárás az információbiztonság szemszögéből.

- *Adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése.
- *Adatkezelés jogalapja:* főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés.
- *Adatkezelés elvei:* a célhoz kötött adatkezelés követelménye, valamint az adatminőség követelménye. Ez utóbbi magában foglalja a pontos, teljes és naprakész adatok igényét, valamint az adatfelvétel és az adatkezelés tisztességes és törvényes mivoltát.
- *Adatkezelő:* az a személy vagy szervezet, aki az adatok kezelésének a célját meghatározza, és az adatkezelésre vonatkozó (beleértve a felhasznált eszközt) döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.
- *Adattovábbítás külföldre:* személyes adatok továbbítása az EGT-n (*Európai Gazdasági Térség,* vagyis az Európai Unió országai, továbbá Izland, Norvégia és Liechtenstein) kívül, harmadik országban adatkezelési tevékenységet folytató adatkezelőhöz.
- *Adatvagyontv.:* a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény.
- *Adatvédelem:* az adatkezelés jogszerűségét biztosító, főként szabályozási tevékenységek – elsősorban a védelmet biztosító szabályok és eljárások –, valamint az adatkezelési eszközök és módszerek összessége.
- *Adatvédelmi incidens:* személyes adat jogellenes kezelésének vagy feldolgozásának, így különösen a jogosulatlan hozzáférésnek, megváltoztatásnak, továbbításnak, nyilvánosságra hozatalnak, törlésnek vagy megsemmisítésnek, valamint a véletlen megsemmisülésnek és sérülésnek az esetei. Ez a fogalom-meghatározás összhangban van az Ibtv. által alkalmazott biztonsági esemény fogalmával, ezek együttes értelmezésével az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosítása – jogi szempontból – könnyebben elvégezhető.
- *Android:* egy *Linux* kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobileszközökre (okostelefon, táblagép) tervezve.
- *Automatizált adatfeldolgozással hozott döntés:* az érintett – kérelemre történő – tájékoztatásának a kötelezettségét írja elő az alkalmazott módszerről és annak lényegéről, azzal a kitétellel, hogy ez esetben az érintett részére lehetőséget kell biztosítani az álláspontjának a kifejtésére. További szabály, hogy az érintett személyes jellemzőinek az értékelésén alapuló döntés meghozatalára csak akkor kerülhet sor, ha a döntést az érintett kezdeményezésére valamely szerződés megkötése vagy teljesítése során hozták, vagy ezt olyan törvény teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja (pl. személyiség alapú online tesztek).
- *Autonóm jármű:* A jármű önmagát képes irányítani (vezet és navigál is)
- *Avtv.:* Az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. Ez a rendszerváltás utáni első adatvédelmi törvény, amely 2011. december 31-ig volt hatályban. 2012. január 1-től hatályon kívül helyezte az Infotv.
- *Belső adatvédelmi felelős:* az adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki a szervezet nevében felelős az adatvédelmi szabályok betartásáért és a személyes adatok védelméért.
- *Bécsi Közlekedési Egyezmény:* A közlekedési szabályok, jelzéseket és szimbólumok egységesítésének az egyezménye.

- *Big Data:* a cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és az ügyfelek számára.
- *Bitcoin:* egy virtuális fizetőeszköz, amely titkosított csatornán keresztül teszi lehetővé a fizetést. Ennél fogva különösen népszerű az illegális cselekmények finanszírozásában, legyen szó kábítószer- és fegyverkereskedelemről vagy akár a terrorizmus finanszírozásáról.
- *Bizalmasság elve:* az elektronikus információs rendszernek az a tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot és információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.
- *Biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
- *Biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek a felszámolása, a bekövetkezés okainak és felelőseinek a megállapítása, valamint a hasonló biztonsági események jövőbeni előfordulásának a megakadályozása érdekében végzett tervszerű tevékenység.
- *Biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége.
- *Biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének a meghatározása.
- *Biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.
- *Biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.
- *CERT (Computer emergency response teams):* számítógépes szükséghelyzeteket kezelő csoportok.
- *Célhoz kötött adatkezelés:* személyes adat kizárólag előre meghatározott célból kezelhető, valamely jog gyakorlása vagy kötelezettség teljesítése érdekében. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének pedig tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és – ha az adatkezelés céljára tekintettel szükséges – naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.
- *Clickjacking:* a felhasználó beleegyezésének megszerzése, amivel az áldozat rákényszerül, hogy olyan dolgot telepítsen, amit nem is szeretett volna.
- *Cloud computing* („számítástechnikai felhő” vagy „felhő alapú informatika”): a számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe vagy vállalati számítóközpontja, hanem egy távoli szerver vagy a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek és virtuális munkaállomások. Felhő alapú informatikai alapon működnek például a milliók által használt internetes levelező rendszerek (pl. *Gmail*) és az online tárhelyek (pl. *Dropbox*). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy költenie kellene az ehhez szükséges drága beruházásokra és személyzetet alkalmaznia a rendszerek fenntartásához szükséges kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok

ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját – főleg marketing – céljára is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni.

- *Cookie-k („sütik”):* rövid adatfájlok, amelyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse és kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl. egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl. egy honlap nyelvi beállítása), amely addig marad a számítógépen, amíg a felhasználó azt le nem törli. Az Európai Bizottság irányelvei alapján cookie-kat (kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek) csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetők a felhasználó böngészési szokásai.
- *Crime as a Service:* szolgáltatásszerű bűnözés.
- *Dark Web (Dark Net):* a *Deep Web* része, ahol alapvetően illegális cselekmények folynak.
- *DDoS (Distributed Denial of Service) támadás:* lásd elosztott szolgáltatásmegtagadással járó támadás.
- *Deep Web (Deep Net):* az internetnek az a része, amit nem indexelnek a különböző keresőmotorok.
- *DGYS:* Magyarország Digitális Gyermekvédelmi Stratégiája.
- *DJP:* Digitális Jólét Program.
- *DOS:* Magyarország Digitális Oktatási Stratégiája.
- *DoS (Denial of Service vagy DoS) támadás:* lásd szolgáltatás-megtagadással járó támadás.
- *Dokumentumok, dokumentáció:* az adattárolás és megőrzés hagyományos formája a (papíralapú) dokumentumok létrehozatala. Ha ezt a rendszerelemet ilyenformán értelmezzük, akkor az információbiztonsági vonatkozások – elvárás szintjén – nagyban megegyeznek az adathordozókéval. Ha azonban ezt a rendszerelemet úgy értjük, mint a dokumentumokban megjelenő információt, akkor valójában magával a védelem tárgyával állunk szembe, azaz ezeket kell megvédenünk. Az okoseszközök kapcsán általában nem igazán jelenik meg a papíralapú dokumentumok kérdésköre, a tárolt és feldolgozott adatok annál inkább. Ilyen módon fontos felmérnünk, hogy mihez férhet hozzá az eszköz, illetve mit lehet rajta tárolni.
- *DNFP:* Digitális Nemzet Fejlesztési Program.
- *eIDAS rendelet:* az uniós szintű elektronikus tranzakciókkal kapcsolatos bizalom, amely az online köz- és magánszolgáltatások, valamint az e-kereskedelem hatékonyságának növelése érdekében közvetlenül alkalmazandó általános hatállyal bíró rendelkezéseket tartalmaz a tagállamok számára.
- *Elektronikus információs rendszer:* az adatok és információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.
- *Elektronikus információs rendszer biztonsága:* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.
- *Elosztott szolgáltatás-megtagadásos támadás:* az informatikai szolgáltatás teljes vagy részleges megbénítása vagy a helyes működési módjától való eltérítése. Egy meghatározott al-

kalmazás vagy operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A támadás lényege, hogy lehetőség szerint megakadályozza a célgép elérését.

- *Első generációs adatvédelmi szabályozás:* a szabályozás középpontjában a számítástechnika fejlődéséből eredően az állami nyilvántartások adatai elektronikus tárolásából, és az adatoknak a nyilvántartásokban való keresésének a lehetőségeiből adódó kérdések és azok jogi reflexiója állt. A technológiai fejlődés lehetővé tette a nagytömegű automatizált adatfeldolgozást, amely a központi nyilvántartások kialakításának irányába mutatott. Az állam, mint nagy adatkezelő jelent meg, amely egy egyedi azonosítószám alkalmazásával kívánta kezelni a nyilvántartásokat és az azokban tárolt személyes adatokat. Ez vezetett odáig, hogy Európában – főként a jóléti államok körében – sorra jelentek meg az első szabályzók. A szabályozás elsődleges célja a fentiekben említett nagy állami adatbázisok átláthatóságának a megteremtése volt, amely alapvetően az automatizált adatkezelésekre terjedt ki, és hangsúlyos szerepet kapott benne a konkrét technológia szabályozása. Mindemellett ezek a szabályzók az egyén részére nem garantálták az általános rendelkezési jogot a személyes adataik felett. A szabályozás már ekkor is tartalmazta az adatvédelemi rendelkezések felett őrködő felügyeleti szervek feladat- és hatásköreit.
- *ENISA:* Európai Hálózat- és Információbiztonsági Ügynökség.
- *EUROCITIES:* olyan program, amely a stratégiaalkotás és a kutatás-fejlesztés területén hat tematikus témakörben (kultúra, gazdaság, környezet, tudásalapú társadalom, mobilitás, társadalmi ügyek, együttműködés) történő információ átadással segíti a partnervárosokat. Budapest is a program tagja.
- *Európa Tanács Adatvédelmi Egyezménye:* az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény (az Európa Tanács ún. 108-as Egyezménye). Az első jelentős, az aláíró államokra nézve kötelező erejű nemzetközi jogi dokumentum az adatvédelem terén. Magyarországon az 1998. évi VI. törvény hirdette ki, 1998. február 27-én.
- *Érintett:* lásd *adatalany*.
- *Érintett jogai:* az adatalanyt még az adatkezelés megkezdése előtt, de ezen felül kérésére bármikor egyértelműen tájékoztatni kell az adatkezelés minden részletéről. Az érintett kérheti az adatai helyesbítését, bizonyos esetben a törlését is, valamint törvényben meghatározott esetekben tiltakozhat a személyes adatainak a kezelése ellen.
- *Észlelés:* a biztonsági esemény bekövetkezésének a felismerése.
- *Felhasználó:* egy adott elektronikus információs rendszert igénybe vevők köre.
- *Fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszernek vagy az elektronikus információs rendszer elemeinek a védettségét és biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét és biztonságát.
- *Feketekalapos (black-hat) hacker:* azok a hackerek, akik tudásukkal visszaélve, haszonszerzés vagy károkozás céljából jogosulatlanul betörnek számítógépekbe vagy számítógép-hálózatokba. Sok *black-hat* válik később *white-hat* hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon *white-hat* hackerként, hogy előtte sohasem próbált betörni egy számítógépbe sem. Így a határ inkább az etikus és az etikátlan hackerekre osztható. A *black-hat* hackerek csoportjába tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba.
- *Fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelző-

rendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás védelme, a sugárzott és vezetett zavarvédelem, a klimatizálás és a tűzvédelem.

- *Folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.
- *Globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezeken a rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese.
- *Hacktivizmus:* olyan cselekedet, amelyben a támadók számítógép-hálózatokba hatolnak be, és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag bár nem azonos, mégis számos közös pont van a kiberterrorizmussal. Mindkettőre jellemző, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat a támadásokat, amelyeknek az a célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Bár a hatásuk elenyésző, mert nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport.
- *Harmadik generációs adatvédelmi szabályozás:* az infokommunikációs szolgáltatások térhódítása, az internet világméretű elterjedése és a fokozódó felhasználó igények (a közösségi oldalak elterjedése) miatt vált szükségessé a harmadik generációs adatvédelmi szabályozás kialakítása, amely jelenleg is tart (és szükség van a kiegészítésére vagy új generációs szabályozásra a kihívások kezeléséhez). A tartalomszolgáltatás megváltozása mellett ez a térhódítás óriási méretű adatbázisok kialakulását is jelentette, amely együtt jár az adatbányászati tevékenységgel. Komoly kockázatot jelent a mobileszközök elterjedése és ezzel összefüggésben a helymeghatározáson alapuló szolgáltatások elterjedése, ami nem más, mint a személy valósidejű tartózkodási helyének a közvetítése ismeretlen számú adatkezelő irányába. Ugyanakkor egyre nagyobb igény mutatkozik a felhő alapú szolgáltatások igénybevételére, amely alapjaiban rendezi át az adatok tárolásának a módját.
- *Hashtag:* a hashtaget először a Twitter vezette be és terjesztette el más platformokra. Ez egy olyan egyszerű címkerendszert takar, amin keresztül az eltérő forrásokat szűrni és kategorizálni lehet, és ami könnyed átjárást jelent egy téma mentén a különböző bejegyzésekben. Hashtaget a # szimbólummal kezdődően lehet elhelyezni.
- *Hardver:* az információs rendszerek (talán) legegyértelműbb eleme, amely magában foglal minden olyan eszközt vagy részelemet, amely az információ feldolgozásában, továbbításában és tárolásában részt vesz. Az „okos” eszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, amelyek ideiglenesen vagy állandó módon csatlakoztathatok az eszközhöz.
- *Hozzájárulás:* az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Különleges adatok esetében csak írásos formában adható meg.
- *HUMINT (Human intelligence):* emberi erővel folytatott hírszerzés.
- *Ibtv.:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.
- *Infotv.:* az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.
- *Információ:* valamilyen megfigyelés, tapasztalat vagy ismeret, amelyből következtetéseket lehet levonni és döntések alapjául szolgálhat. Az információ, ha úgy tetszik, nem más, mint jelentéssel felruházott adat, azaz az adatból akkor lesz információ, ha valamiről informál.
- *Információbiztonság:* olyan követelményrendszer, amelynek a középpontjában a bizalmasság, a sértetlenség és a rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt

hordozó adat milyen megjelenési formát vesz fel (pl. alfabetikus, numerikus, grafikus vagy képi forma) és milyen adathordozón jelenik meg.

- *Információszabadság:* a közérdekű, valamint a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog, amely elősegíti a közhatalom gyakorlásának demokratikus kontrollját és a közintézmények átláthatóságát (transzparencia).
- *Információs rendszer felhasználásával elkövetett csalás:* ha valaki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz.
- *Információs rendszer vagy adat megsértésének bűncselekménye:* ha olyan személy, akinek amúgy megvan a jogosultsága a szankcionált magatartásra (információs rendszerbe való belépésre, adat megváltoztatására és törlésére), túllépi a jogosultságának a kereteit, akkor már bűncselekményt követ el. Az információs rendszerbe való jogosulatlan adatbevitel önmagában nem szankcionálandó magatartás, csak abban az esetben, ha az további nem kívánt következményekhez vezet, így a rendszer működését akadályozza. Az alaptényállás vétség, amelyet a Btk. kétévi szabadságvesztéssel rendel büntetni.
- *Információs rendszer védelmét biztosító technikai intézkedés kijátszásának bűncselekménye:* akkor valósul meg, ha az elkövető az információs rendszer felhasználásával elkövetett csalás, illetve az *információs rendszer vagy adat megsértésének bűncselekménye* elkövetése céljából ehhez szükséges vagy ezt megkönnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz, illetve jelszó vagy ilyen számítástechnikai program készítésére vonatkozó gazdasági, műszaki vagy szervezési ismereteit más rendelkezésére bocsátja.
- *Információvédelem:* összetettsége miatt a definíciós meghatározás helyett azokat a tevékenységeket rögzítjük, amelyekkel maga a védelmi tevékenyég leírható. Ide sorolható az információt hordozó entitások (személyek és eszközök) védelme, azaz az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az iratés dokumentumvédelem, valamint a személyi védelem is. Az információvédelem célja – hasonlóan az adatvédelemhez – a jogosulatlan hozzáférés, módosítás vagy megsemmisítés elleni védelem és az információk folyamatos rendelkezésre állásának a biztosítása.
- *Internet of Things (Iot):* a *dolgok internete* kifejezés különböző, egyértelműen azonosítható objektumokra és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg *Kevin Ashton*, de a koncepció ötlete először 1991-ben vetődött fel. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, mérni és ezt egy másik eszköz felé kommunikálni is. Lehet ez egy okostelefon, egy vérnyomásmérő vagy az autónk fedélzeti számítógépe (ECU). Ezeknek az eszközöknek nincsenek sem méretbeli, sem pedig felhasználási megkötései.
- *iOS:* az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- *IS (Islamic State):* önmagát Iszlám Államnak nevező terroristacsoport.
- *ISO 2700x szabványcsalád:* az információbiztonsági menedzsment rendszerek mára alapvetővé vált szabványcsaládja. Története (az elődszabványaival együtt) a 90-es évek közepéig nyúlik vissza, és mára meghatározó szerepet tölt be a szervezetek információbiztonsági rendszereinek kialakításában és tanúsításában. A jelenlegi törekvések szerint ebbe a szabványcsaládba rendezi az ISO minden olyan szabványát, mely többé-kevésbé szorosan kapcsolódik az információbiztonsághoz. Ennek megfelelően igen népes a 2700x szabványcsalád, több tíz szabványból áll. Alapja az ISO/IEC 27001, amely alapvetően nem technikai, hanem egy menedzsment szabvány, még akkor is, ha tartalmaz technikai vonatkozású elvárásokat is. A felépítését tekintve két részből áll. A szabvány törzse tartalmazza a menedzsment rendszerekre vonatkozó elvárásokat, az A melléklet pedig az információbiztonsági

kontrollkövetelményeket. Ez utóbbiak kiterjedésükben és jellegükben hasonlóak a 41/2015. (VII. 15.) BM rendelet mellékleteiben megtalálható követelményekhez. Kockázatmenedzsment szempontból érdemes kiemelni ebből a családból az ISO/IEC 27005 szabványt, amely az információbiztonsági kockázatmenedzsmenttel foglalkozik. Logikája és felépítése hasonló a már korábban említett ISO 31000-hez, ugyanakkor több a kifejezetten információbiztonsági vonatkozása, és a mellékletei sok segítséget jelentenek egy kockázatkezelési eljárás kialakításához, illetve tartalommal való feltöltéséhez.

- *ISO 31000-es szabványok:* A kockázatelemzés elvégzéséhez az egyik legelterjedtebb módszertani segítséget nyújtó szabvány(család) az ISO 31000-es. Történetét tekintve nem egy réges-régen kialakult családtól beszélünk. Kiadásában és sikerében a különböző ISO szabványokon alapuló irányítási és menedzsment rendszerek (minőségirányítás, környezetközpontú irányítás és információbiztonsági irányítás), elterjedése, és kockázati alapokra helyezése játszotta a legnagyobb szerepet Mint általában az ilyen menedzsment jellegű szabványok, ez sem konkrét megoldást vagy egyszerűen, lépésről lépésre alkalmazandó technikát definiál, hanem azt a folyamatot, amit egy kockázatelemzés során végig kell vinni. Megadja, hogy milyen szempontokat kell figyelembe venni, amikor kiválasztjuk, illetve kialakítjuk a saját működésünknek leginkább megfelelő kockázatelemzést. Definiálja a kockázatelemzés-értékelés folyamatát, és a 31010-es szabvány különböző eszközöket mutat be, értékelve azokat abból a szempontból, hogy melyiket mikor érdemes használni a kockázatfelmérés során. Ezt a szabványt haszonnal forgathatja mindenki, aki segítséget szeretne kapni a saját eljárásainak kialakításában.
- *Jailbreaking:* olyan eljárás, amelynek folyamán az *Apple* telefonon keresztül a felhasználó *superuser*évé válik, vagyis egy olyan felhasználóvá, akinek teljes hozzáférése van minden utasításhoz és fájlhoz az operációs rendszerben.
- *Kiberbiztonság:* a kibertérben meglévő kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatokat elfogadható szinten tartják, és a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.
- *Kiberbűnözés:* célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, akiknek a tagjai rendkívüli adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ebben a területben rejlő lehetőségeket.
- *Kiberhadviselés:* az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még leginkább a konvencionális hadviselés támogatására.
- *Kiberkémkedés:* az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzés. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület.
- *Kibervédelem:* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését.
- *Kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az általa okozott kár nagyságának a függvénye
- *Kockázatazonosítás:* célja azoknak a helyzeteknek, lehetőségeknek és eseményeknek a felismerése, amelyek a kitűzött céloknak való megfelelést befolyásolhatják. Az azonosításnak a lehetőségek felmérésén túl magában kell foglalnia mindazokat a tényezőket, amelyek a kockázat kialakulásának a környezetét jelentik. Ebben ki kell térni azokra a folyamatokra, szabályozókra, technikai eszközökre, emberekre, rendszerekre, hardver és szoftver tényezőkre stb., amelyek relevánsak a kockázat és a környezet megértésének a szempontjából.

- *Kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.
- *Kockázatértékelés:* választ kaphatunk olyan kérdésekre, mint hogy kell-e kezelni egy kockázatot; ha igen, milyen sorrendben; megkezdhető-e egy adott beruházás vagy folyamat a jelenlegi paraméterekkel; a különböző lehetséges megoldások közül melyiket kell választani. A különböző besorolások és értékelése értelmezésére a legtöbb esetben nem két (elfogadható és nem elfogadható) hanem három (elfogadható, feltételekkel elfogadható és nem elfogadható) kategóriát célszerű létrehozni.
- *Kockázatfelmérés:* a kockázatoknak egy olyan növelt megértését nyújtja a döntéshozóknak és felelős résztvevőknek, amely befolyásolhatja a célok elérését és az irányítás megfelelőségét és hatékonyságát a szóban forgó helyen. Ez alapot ad a döntéshez, hogy a leginkább megfelelő megközelítést használják a kockázatok kezeléséhez.
- *Kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása. A kockázatokkal arányos védelem azt jelenti, hogy a védelmi intézkedésekre fordított költségeknek arányosnak kell lenniük a fenyegetések által okozott lehetséges károk értékével.
- *Kockázatkezelési terv:* összefoglalja mindazokat az intézkedéseket, amelyeket a szervezetnek el kell végeznie a különböző kockázatok megszüntetésére, átruházására és csökkentésére. A kockázatkezelési terv tartalmazza az intézkedéseket azok részletes bemutatásával együtt, az összerendeléseket, hogy egy intézkedés melyik azonosított kockázatra van hatással, a kockázatcsökkenés mértékét, illetve ebből következően a maradványkockázat értékelését, valamint az egyes maradványkockázatok elfogadását.
- *Korai figyelmeztetés:* olyan aktív szervezeti cselekvés, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni.
- *Közérdekű adat:* az állami/önkormányzati feladatot, illetve egyéb közfeladatot ellátó szerv kezelésében lévő és a tevékenységére vonatkozó vagy a közfeladatának az ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül a kezelésének a módjától, önálló vagy gyűjteményes jellegétől (így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre és annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat).
- *Kritikus adat:* az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;
- *Különleges adat:* a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallási vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, illetve a kóros szenvedélyre vonatkozó adat, valamint a bűnügyi személyes adat.
- *Létfontosságú információs rendszerelem:* a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azok az elektronikus információs létesítmények, eszközök vagy szolgáltatások, amelyeknek a működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné a vagy működőképességüket jelentősen csökkentené.
- *Linux:* egy operációs rendszer, a szabad szoftverek és a nyílt forráskódú programok egyik legismertebb példája.
- *Logikai védelem:* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.

- *Magyar kibertér:* a globális kibertér elektronikus információs rendszereinek az a része, amelyek Magyarországon találhatóak, továbbá a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.
- *Malware:* az angol *malicious software* (kártékony szoftver, káros szoftver vagy rosszindulatú szoftver) összevonásából kialakított mozaikszó, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (*worm*), kémprogramok (*spyware*), agresszív reklámprogramok (*adware*), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (*rootkit*).
- *Man-in-the-middle:* közbeékelődéses támadás, amely során mindkét fél azt hiszi, hogy közvetlenül egymással kommunikálnak, pedig mindketten csak a csatornát irányító rejtett szereplővel állnak kapcsolatban.
- *Mavtv.:* a minősített adat védelméről szóló 2009. évi CLV. törvény.
- *Második generációs adatvédelmi szabályozás:* a szabályozás kialakítását sürgette annak az álláspontnak az Európai Unión belüli térnyerése, amely szerint az adatok szabad áramlását úgy kell biztosítani, hogy a magánszféra és a személyes adatok védelme garantálva legyen. A második generációs szabályozás fő eleme, hogy a technológiai megközelítés helyett az adatkezeléssel érintett személyt – az adatgazdát – széleskörű rendelkezési joggal ruházta fel. A szabályozás egyaránt kiterjed az elektronikus adatkezelésekre és a manuális, tehát papíralapú adatkezelésekre. A szabályozásban megjelentek a nemzetközi dokumentumok, amelyek közül az egyik, ugyan nem kötelező érvényű, de számos máig is fontos alapelvet tartalmazó szabályt külön ki kell emelni.
- *MDM rendszerek:* a legelterjedtebb okoseszközök – az okostelefonok – már évek óta jelen vannak a szervezetek életében, és okoznak fejtörést az információbiztonsággal foglalkozó szakemberek számára. Éppen ezért a piacon egyre több eszköz és megoldás jelenik meg az okostelefonok technikai oldalról működtetett kontrolljának a megvalósítására. Ezeket összefoglaló néven MDM, azaz *mobile device management* rendszereknek nevezik. A különböző gyártók különböző megoldásokat kínálnak a szervezet méretének, céljainak és eszközparkjának a függvényében. Mivel ezek a megoldások is folyamatosan fejlődnek és változnak, a következőkben csak néhány jellemző gondolatot összegzünk, hogy mire is alkalmasak ezek a rendszerek. Egy szervezet saját megoldásának keresése során mindenképpen célszerű, ha tájékozódik a piacon aktuálisan fellehető megoldásokról, hiszen ezekben jelentős eltérések lehetnek, mind a technikai megoldást, mind pedig az árakat illetően. Az MDM rendszerek általában alkalmasak a mobileszközök és a rajtuk tárolt információk és alkalmazások, illetve a rajtuk folyó kommunikációs folyamatok központi, távoli védelmére és flottában történő menedzselésére, amely így nem csak egységesen, de viszonylag könnyen meg is valósítható. Az MDM fő funkciói között megtalálható az üzembe helyezés, amely alkalmassá teszi a készüléket a beszerzését követően annak üzembe helyezésére, cégprofil kialakítására és a device management rendszerhez való távoli csatlakoztatására.
- *Megelőzés:* olyan hatás bekövetkezésének az elkerülése, amelyet egy fenyegetés okozhat.
- *Megfelelő tájékoztatás:* az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

- *Minősített adat* (korábbi elnevezése államtitok vagy szolgálati titok): olyan, minősítéssel védhető közérdek körébe tartozó információ, amelyről a minősítésre jogszabályban felhatalmazott személy megfelelő eljárásban megállapította, hogy az adat érvényességi időn belüli nyilvánosságra hozatala vagy illetéktelen személy részére hozzáférhetővé tétele veszélyeztetné Magyarország biztonságát. A Szigorúan titkos, a Titkos, a Bizalmas és a Korlátozott terjesztésű jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása vagy nyilvánosságra hozatala bűncselekmény. A minősítéssel védeni kívánt közérdek lehet Magyarország szuverenitása és alkotmányos rendje; honvédelmi, nemzetbiztonsági, bűnüldözési és bűnmegelőzési tevékenysége; igazságszolgáltatási, központi pénzügyi és gazdasági tevékenysége; külügyi és nemzetközi kapcsolatai; valamint az állami szervei illetéktelen külső befolyástól mentes működésének a biztosítása.
- *OECD irányelvek:* a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Tanácsa által elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvek, amelyek 1980. szeptember 23-án léptek életbe.
- *Okostelefon (smartphone):* fejlett, gyakran PC-szerű funkcionalitást nyújtó mobiltelefon.
- *„Okos város" (smart city):* egy komplex stratégia, a benne foglalt célkitűzések és a meglévő eszközök, fejlesztések és infrastruktúrák összehangolását és egymást szolgáló tervezését jelenti a fenntarthatóság és hatékonyság jegyében.
- *OSINT (Open Source Intelligence):* nyílt forrású információgyűjtés a hírszerzés. Ez a katonai felderítés egyik információ- és adatszerző tevékenysége, amely során az információt nyílt adatokból gyűjtik.
- *NAIH – Nemzeti Adatvédelmi és Információszabadság Hatóság:* az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, amelynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének a felügyelete.
- *Nemzeti adatvagyon:* a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.
- *NMHH:* Nemzeti Média és Hírközlési Hatóság.
- *NTG:* Nemzeti Távközlési Gerinchálózat
- *PreDeCo (Preventive-Detective-Corrective) elve:* a védelmi feladatok közé sorolja a megelőzést, a korai figyelmeztetést, az észlelést, a reagálást és az eseménykezelést.
- *Ransomware:* olyan *malware*, amely valamilyen fenyegetéssel megpróbál pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszi a számítógépet vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, amelynek a hatására visszaállítja az eredeti állapotot.
- *Reagálás:* a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére és a további károk mérséklésére tett intézkedés.
- *Rendelkezésre állás elve:* annak a biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
- *Rootolás:* olyan eljárás, amelynek folyamán az androidos telefonon a felhaszáló root userré/superuserré válik, vagyis egy olyan felhasználóvá, akinek teljes hozzáférése van minden utasításhoz és fájlhoz az operációs rendszerben.
- *Rövidülő életciklus:* a legtöbb használati cikkünkre igaz, hogy a tervezett felhasználási idejük egyre rövidül, mind technikailag, mind erkölcsileg sokkal hamarabb elavulnak. Terméktípustól függően 1-3 évente a gyártók újabb típusokkal és fejlettebb tudású eszközökkel rukkolnak elő, ezzel teszik elavulttá az egy, esetleg két generációval korábban kiadott készülékeiket. A rövidülő életciklus és a folyamatos újítási kényszer azonban nem csak az eszközök gyártóit terheli, hanem a szoftverek készítőit is.

- *Sértetlenség elve:* az adat tartalma és tulajdonságai megegyezik az adattal szemben felállított követelményekkel, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz az eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek az a tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme a rendeltetésének megfelelően használható.
- *Sérülékenység:* az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.
- *Sérülékenységvizsgálat:* az elektronikus információs rendszerek gyenge pontjainak (biztonsági réseknek) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.
- *SIGINT (Signals Intelligence):* rádióelektronikai felderítés – a hírszerzésnek egy fajtája, amely az ellenséges rádióforgalmazás (radar, távközlés, telemetria, IT) elfogása és elemzése alapján jut információhoz.
- *Social engineering:* az emberi tényező kihasználható tulajdonságaira és az emberi hiszékenységre építő támadási forma – olyan technikák és módszerek összessége, amely az emberek befolyásolására és manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését.
- *Súlyos biztonsági esemény:* olyan informatikai esemény, amelynek a bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek közvetlen veszélybe kerülhetnek, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, illetve alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.
- *Számítógépes eseménykezelő központ:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik (európai használatban: CSIRT [Computer Security Incident Response Team], amerikai használatban: CERT)
- *Számítógépes féreg:* egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá, illetve válnak a részeivé, addig a férgeknek nincs szükségük gazdaprogramra, hanem önállóan fejtik ki működésüket.
- *Személyes adat:* bármely meghatározott, azonosított vagy azonosítható természetes személlyel *(érintett)* kapcsolatba hozható adat és az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi ezt a minőségét, amíg a kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
- *Személyes adattal való visszaélés vétsége:* az követi el, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével, haszonszerzési célból vagy jelentős érdeksérelmet okozva, jogosulatlanul vagy a céltól eltérően személyes adatot kezel vagy az adatok biztonságát szolgáló intézkedést elmulasztja, vagy az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget és ezzel más vagy mások érdekeit jelentősen sérti.
- *Személyes adatok statisztikai célra történő felhasználása:* ebben az esetben érvényesül a célhoz kötöttség elve. A normaszöveg ilyenkor azt is rögzíti, hogy a statisztikai célra felvett, átvett vagy feldolgozott személyes adatok – eltérő törvényi rendelkezésnek hiányában – csak statisztikai célra kezelhetők, azzal, hogy a Központi Statisztikai Hivatal egyedi azonosításra alkalmas módon a kötelező adatkezelés keretében kezelt személyes adatokat átveheti és a törvényben meghatározottak szerint kezelheti.

- *Személyes adatok tudományos kutatás során történő kezelése:* ebben az esetben fokozottan érvényesül a célhoz kötöttség elve. A normaszöveg rögzíti, hogy a tudományos kutatás céljára felvett személyes adat csak tudományos kutatás céljára használható fel. A tudományos kutatást végző szerv vagy személy személyes adatot csak akkor hozhat nyilvánosságra, ha ahhoz az érintett hozzájárult, vagy az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges. Ez esetben a személyes adat érintettel való kapcsolata megállapításának a lehetőségét ki kell zárni azzal, hogy a végleges kizárásig (lehetetlenné tételig) külön kell tárolni azokat az adatokat, amelyek a meghatározott vagy meghatározható természetes személy azonosítására alkalmasak.
- *Szervezet:* az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető.
- *Szoftver:* az információs rendszerek másik egyértelmű eleme (a *hardver* mellett), amely alatt a legszűkebb értelemben az információtechnológiai berendezéseket működtető programokat értjük. A jelen technikai szinten, amikor hétköznapi körülmények között az azonos hardverkiépítésű eszközök a legtöbb esetben a szoftvereknek köszönhetően a legkülönbözőbb feladatokra válnak alkalmassá, kijelenthető, hogy a szoftverek sokfélesége biztosítja az eszközeink sokféle feladatra való alkalmasságát. Az „okos” eszközök esetén szintén ilyen módon működnek, vagyis a különféle szoftverek a legkülönbözőbb tulajdonságokat biztosítanak nekik. Ebből adódóan fontos, hogy kellő alapossággal mérjük fel mind a szoftvereket, mind azok verzióit.
- *Szolgáltatás-megtagadásos támadás:* az informatikai szolgáltatás teljes vagy részleges megbénítása vagy a helyes működési módjától való eltérítése. Egy meghatározott alkalmazás vagy operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassulhat, elérhetetlenné válhat, esetleg össze is omolhat. A támadás lényege, hogy lehetőség szerint megakadályozza a célgép elérését.
- *Tablet:* hordozható számítógép, amelyet leginkább tartalomfogyasztásra fejlesztettek ki.
- *Teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.
- *Tiltakozás:* az érintett nyilatkozata, amelyben személyes adatainak kezelését kifogásolja és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.
- *Tiltott adatszerzés bűntette:* az elkövető a személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot jogosulatlan módon akarja megismerni. Ezeknek az adatoknak a jogosulatlan megszerzése megvalósulhat más lakásának, egyéb helyiségének vagy az azokhoz tartozó bekerített helynek a titokban való átkutatásával; az ott történteknek technikai eszköz alkalmazásával való megfigyelésével, rögzítésével; más közlést tartalmazó zárt küldeményének felbontásával vagy megszerzésével és tartalmának technikai eszközzel való rögzítésével; illetve elektronikus hírközlő hálózat útján másnak továbbított vagy azon tárolt adat kifürkészésével és az észleltek technikai eszközzel való rögzítésével.
- *Trójai progam:* egy olyan *malware*-program, amely nem magát próbálja lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az ún. hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz.
- *Uniós adatvédelmi irányelv:* az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad

áramlásáról. Ez az Európai Unió 1995. október 24-én született általános adatvédelmi irányelve, amely – többek között – létrehozta az ún. 29-es Adatvédelmi Munkacsoportot.

- *URBACT:* olyan, tapasztalatcserét és tanulást támogató program, amely segíti az európai fenntartható városfejlesztést. A program képessé teszi a városokat arra, hogy a főbb városi kihívásokra közösen megoldásokat dolgozzanak ki és az egyre komplexebb társadalmi változásokkal szembesülve a központi szerepüket megerősítsék. Az új, fenntartható gyakorlati megoldások integrált megközelítéssel adnak válaszokat a társadalmi, gazdasági és környezeti folyamatokra. A legjobb gyakorlati példákat és tapasztalatokat a programban résztvevő partnervárosok Európa-szerte megosztják egymással, a várospolitikában, várostervezésben érintett szakemberekkel és minden olyan érdeklődővel, aki elkötelezett a szűkebb vagy tágabb városi lakó- és munkakörnyezete felé.
- *Üzemeltető:* az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszernek vagy annak a részeinek a működtetését végzi és a működésért felelős.
- *Vírus:* olyan rosszindulatú program, amely képes sokszorosítani és terjeszteni magát, az egyik gépről a másikra. Ugyanez a féregre is igaz, azzal a különbséggel, hogy a vírus általában „befúrja" magát egy futtatható fájlba, hogy teljesítse a célját.
- *Zártcélú elektronikus információs rendszer:* a nemzetbiztonsági, honvédelmi, rendészeti és diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az erre a célra létrehozott szervezet és technika működését szolgálja.
- *Zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

JOGSZABÁLYTÁR

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945
- A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=133022.240462
- A minősített adat védelméről szóló 2009. évi CLV. törvény http://njt.hu/cgi_bin/njt_doc.cgi?-docid=126195.323131
- A szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=143166.323488
- A Büntető Törvénykönyvről szóló 2012. évi C. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=152383.328747
- Polgári Törvénykönyvről szóló 2013. évi V. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=159096.323415
- Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=57566.323251
- Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény http://njt.hu/cgi_bin/njt_doc.cgi?docid=193173.316584
- Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845
- A „Digitális Nemzet Fejlesztési Program” megvalósításáról szóló 1631/2014. (XI. 6.) Korm. határozat http://njt.hu/cgi_bin/njt_doc.cgi?docid=172387.275675283
- A „Digitális Nemzet Fejlesztési Program” településközpontú kísérleti alprogramjának megvalósításához szükséges források biztosításáról szóló 1854/2014. (XII. 30.) Korm. határozat http://njt.hu/cgi_bin/njt_doc.cgi?docid=173503.328348
- Az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér című közös közleménye http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=hu
- Az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32014R0910&from=HU

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Császár-Biró Anna

Tördelőszerkesztő:
Vörösss Ferenc

ISBN 978-963-498-490-0 (elektronikus)