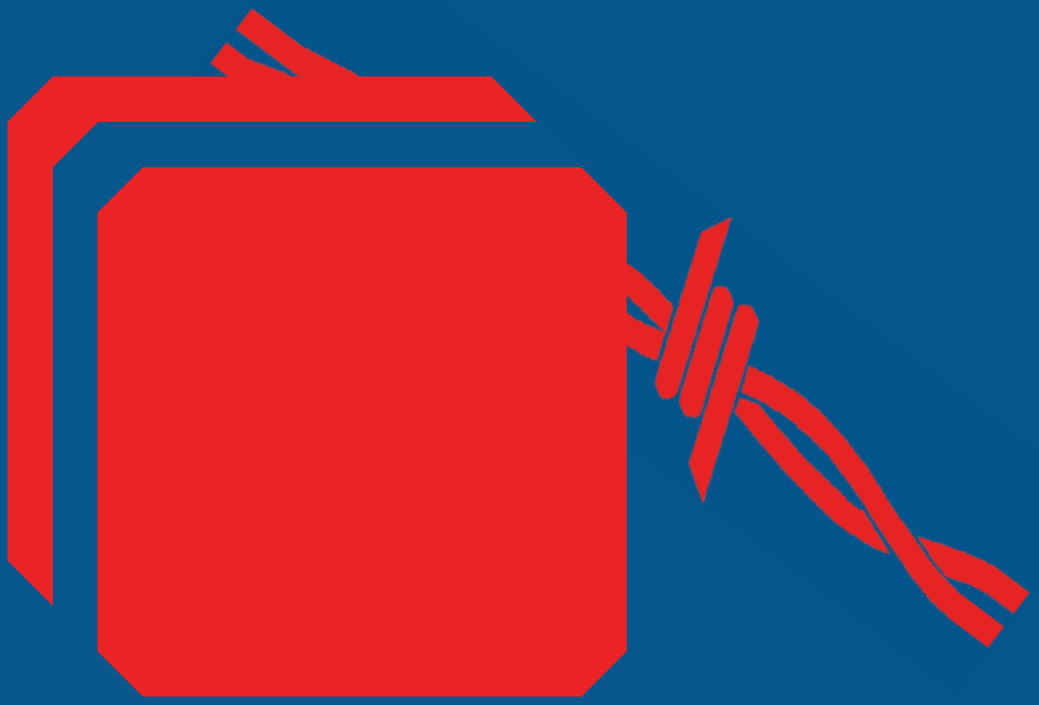
Virág Csaba

Gyakorlati felhasználói tanácsok az alapszintű IT biztonság eléréséhez



Nemzeti
Közszolgálati
Egyetem

Virág Csaba

GYAKORLATI FELHASZNÁLÓI TANÁCSOK AZ ALAPSZINTŰ IT BIZTONSÁG ELÉRÉSÉHEZ

Nemzeti Közszolgálati Egyetem ❖ Budapest

A kiadvány a KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése” című projekt keretében készült el és jelent meg.

Szerző:
Virág Csaba

Szakmai lektor:
Dr. Krasznay Csaba

Olvasószerkesztők:
Kotró Szimonetta, Stránglí Szandra

Kézirat lezárásának dátuma:
2017. november 6.

TARTALOM

1. BEVEZETÉS A KIBERBIZTONSÁGBA 7
1.1. Az információ- és kibertudatosság jelentősége 7
1.2. Az információ-technológiai fejlődés bemutatása 8
1.3. Magánélet és munkahely 9
1.4. Szabályzói és technikai háttér 9
1.5. A többszintű információbiztonság-tudatosság szerepe 9

2. A KIBERTÉR SZABÁLYOZOTTSÁGA 11
2.1. EU-s szabályozás (NIS, GDPR) 11
2.1.1. Hálózati és Informatikai rendszerek védelme (NIS) 12
2.1.2. EU adatvédelmi szabályozás (GDPR) 13
2.2. Hazai szabályozás 14
2.3. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) legfontosabb elemei 15
2.3.1. A szervezet vezetőjének a feladata és felelőssége 15
2.3.2. Az elektronikus információs rendszer biztonságáért felelős személy feladata és felelőssége 16
2.3.3. A NEIH feladata és felelőssége 16
2.3.4. Az információbiztonsági felügyelő 16
2.3.5. A Nemzeti Biztonsági Felügyelet feladata és kötelessége 17
2.3.6. Kormányzati eseménykezelő központ 17
2.3.7. Nemzeti Kiberbiztonsági Koordinációs Tanács 17

3. KIBERFENYEGETETTSÉG 19
3.1. Nem tudod megvédeni azt, amit nem értesz 19
3.2. Válaszd a biztonságot! 19
3.3. Támadó motivációk 20
3.4. Kiber-fizikai Rendszerek (CPS) 21
3.5. Dolgok Internete (IoT) 22
3.6. Támadási technikák összefüggései 22
3.7. Saját eszköz 24
3.8. Közösségi média 24
3.9. Terrorizmus 25
3.10. Belső fenyegetettség 25
3.11. Szabályzatok és szabályzók 26

4. BIZTONSÁGBAN A HÁLÓZATON 27
4.1. A biztonságos viselkedés általános bemutatása 27
4.2. Biztonságtudatos viselkedés kialakításának szempontjai és módszerei 27
4.2.1. Munka és privát élet 27
4.2.2. Adatbiztonság, személyes biztonság 27
4.2.3. Megfelelő viselkedés, megjelenés a közösségi térben 28
4.2.4. Jelszavak és azonosítók 29
4.2.5. Nyilvános hálózat 30
4.2.6. Titkosítás 30
4.2.7. Felhasználók 30
4.2.8. Biztonsági mentések 31
4.2.9. Kiberhigiénikus viselkedés 31

5. EMELT SZINTŰ KIBERTUDATOSSÁG 33
5.1. Stratégiák, Egyezmények 33
5.1.1. Nemzeti Kiberbiztonsági Stratégia 33
5.1.2. Budapesti Konvenció 35
5.1.3. Digitális Jólét Program 35
5.1.4. Stratégia alkotás az EU-ban 35
5.2. MULTINACIONÁLIS SZERVEZETEK 38
5.2.1. NATO 38
5.2.2. Európai Biztonsági és Együttműködési Szervezet (EBESZ) 38
5.2.3. Global Forum on Cyber Expertise (GFCE) 38
5.2.4. International Telecommunication Union (ITU) 38
5.2.5. Nemzetközi jog 38
5.3. Szabványok és minősítések 39
5.4. People Process Technology - PPT 40

ÖSSZEGZÉS 43

JOGSZABÁLYTÁR 44

IRODALOMJEGYZÉK 45

1. BEVEZETÉS A KIBERBIZTONSÁGBA

1.1. Az információ- és kibertudatosság jelentősége

2016 október 21-én[1] nagyságrendileg másfél millió webkamera és otthoni router elérhetetlenné tette több millció ember számára az internet bizonyos szegmensét azáltal, hogy megtámadták az internet egyik gerincét adó DNS[2] szervereket. A történelemben ez volt az első olyan elsöprő erejű támadás, amely elsősorban otthoni használatban lévő eszközöket használt fel és nem a klasszikus értelemben vett számítógépeket.

A támadás kivitelezéséhez szükséges eszközök fölötti irányítás átvételéhez nem volt szükség különösebb hozzáértésre: elég volt az olcsó webkamerák használati utasításából kiolvasni a gyári hozzáféréseket, majd az interneten csatlakozott kamerákat keresni. Az emberek többsége nem tudja a mai napig, hogy az általa megvásárolt pénztárcabarát eszköz ilyen célra is használható és hogy egyáltalán, képes az interneten támadást végrehajtani. Fenti példa mutatja igazán, hogy képes.

Manapság már nem arról beszélünk, hogy egy-egy eszközben számítógép van, hanem arról, hogy egy-egy számítógép milyen funkciót tölt be: van amelyik körül karosszéria van és vezetjük, van amelyik az időt mutatja, van amelyikkel telefonálni is lehet, van amelyik pénzt ad ki, van amelyik áramot termel és még sorolhatnánk. Csak önmagában egy átlagos mai autóban több mint 100 darab számítógép összehangolt munkájára van szükség ahhoz, hogy működhessen. Lenyomjuk a gázpedált, a számítógép gyorsít, vált, indexel, emeli a fordulatszámot, ellenőrzi az abroncsnyomást, kipörgést, stb. Egy repülő gyakorlatilag egy számítógépes hálózat, amelynek szárnya van, egy atomerőmű pedig nukleáris hasadást felügyelő informatikai rendszer.

Számítógépeket hordunk magunkon, ezen eszközökkel halmozzuk el a lakásunkat, adatokat gyűjtünk, számítógépet utasítunk és hajtatunk végre feladatokat. Az utcán számítógépekkel vagyunk körülvéve, szenzorok figyelik, merre haladunk, milyen sebességgel, világítson-e a lámpa, váltson, befizettük-e az autópályadíjat, az autók kommunikálnak egymással. Okos otthonokban élünk, mindenről adatot gyűjtünk és mindent mindennel összekötünk. Egy globálisan összekötött, számítógépesített hálózatban élünk.

Olyan mértékű automatizmusban éljük világunkat, hogy észre sem vesszük azt. 2017-ben, amikor ez a tananyag készült, már természetesnek tűnik, hogy a legtöbb dolog működtetéséhez számítógépek által vezérelt megoldásokat alkalmazunk és ezen eszközök többsége valahogyan kapcsolatban áll, vagy összekapcsolható egy másik számítógéppel. Az ipari innováció csodálatos oldala ez, amelyet hajt a felhasználói igény, a gyártói költség- és hatékonyságoptimalizálás és az új technológiák biztosította felhasználási lehetőségek. Viszont a biztonság idáig nem volt képes ilyen gyorsan fejlődni.

A kihívások és fenyegetettségek nem állnak meg a kibertér határánál, hanem kihatással vannak a minket körül ölelő fizikai világunkra. Onlineintézzük banki ügyeinket, közigazgatással kapcsolatos feladatokat és teendőket intézünk online, közösségi médiákat használunk, foglalunk, vásárolunk, eseményeket szervezünk. A fizikai életben kialakult gyakorlata van a védelemnek, zárak, ajtók, kerítések és egyéb védelmi rendszerek megtestesülésében. Virtuális térben ez azonban még mindig formálódik.

---

1 https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

2 https://techterms.com/definition/dns

A fent említett digitalizáció és a mindannyiunkat körülölelő technológiai fejlődések miatt is létfontosságú, hogy magunknak tudatosítsuk és rögzítsük, illetve megtanuljuk azokat az alapvető normatívákat és viselkedési mintákat, amelyekkel biztonságban tudunk létezni a virtuális világban is. Ennek a tudásnak és képességnek megszerzésének a legalapvetőbb eszköze a felhasználók információbiztonsági tudatosságának kialakítása, és annak folyamatos fejlesztése, a technológiai fejlettség fokának megfelelő szinten tartása.

Az egyéni felhasználók információbiztonsági tudatossági szintje az egyéni felhasználó közösségére és az általa képviselt szervezet számára is kritikus. Fontos érzékelni, hogy milyen kihívásokkal szembesül a társadalom és ezekre képes-e sikeres válaszokat adni. Ezen lehetséges válaszok túlmutatnak az egyénen, átívelnek a kiberbiztonság teljes területén: a képzésektől a törvényalkotásig, a megfelelő szervezeti kultúra és struktúra kialakításán át a geopolitikai helyzet stratégiai szemléletű kommunikációján keresztül a felsővezetőségi szemléletig és elkötelezettségig.

Jelen tananyag a fenti kérdésekre ad választ és vezeti be a résztvevőt a kiberbiztonság összetett világába, ismerteti meg az alapszintű tudnivalókkal.

1.2. Az információ-technológiai fejlődés bemutatása

Az internet, mint technológia az elmúlt 50 évben alakult ki. Alapvető célja a kommunikáció biztosítása távoli lokációk között elosztott hálózatban, azaz ne csak egy központra korlátozódjon a működtetése, hanem több központ is tudjon működni, ami így a fenntartható működést tudja biztosítani. A legelső e-mailt 1971-ben küldték, a legelső weboldalt 1990-ben indították, a Facebook, Twitter, Google pedig a késői ’90-es és a korai 2000-es évek termékei.

A legelső ismert kibertámadás, a Morris féreg1989-ben jelent meg. Ez az egy féreg az akkori internet jelentős részét elérhetetlené tette túlterheléses támadás révén (DoS). Az akkori hálózaton összesen elérhető számítógépek száma tízezres nagyságrendre becsülhető. Ekkor az internet már 20 éves volt,1989-ben jelent meg az első betárcsázós internetszolgáltatás, amelyet a civil és üzleti szféra is elérhetett (de még egy évet várni kellett az első HTML (web)oldalra és még egyet a world-wide-web bemutatkozására).

2017-ben a hálózatra kapcsolódó eszközök számát 28,4 milliárd darabra becsülik, ez a szám várhatóan 2020-ra meghaladja az 50 milliárdot.[3] Az internethez 3,26 milliárd ember fért hozzá 2015. év végével és 2017-es évben az internetes adatforgalom önmagában egyedül meghaladja majd várhatóan az összes korábbi évek adatforgalmát.[4]

Bár az adatforgalom és a felhasználók száma folyamatosan növekszik, a technológia mégis korlátot szab a biztonságos működtetésnek. Az internet alapját kiszolgáló technológiák, folyamatok, eszközök és protokollok az elmúlt években fundamentálisan nem tudtak változni, szinte minden új tömegesen elérhető technológia támogatja a régi rendszerek és protokollok működését. Ez magában hordozza a múltból eredő technológiai sérülékenységeket és ezek kiküszöbölésének nehézségeit.

Mint az élet olyan sok területén, az interneten is működik az aránytalanság elve, a szolgáltatások jelentős részét az interneten összesen elérhető eszközök kisebbik része biztosítja. Elég azonban csak az okostelefonokra vagy a számítógépeken található alkalmazásokra és programokra gondolni: egy átlagos felhasználó a készülék kapacitásának és tudásának kevesebb mint 20%-át használja.

Ez az aránytalanság az internetes hálózat biztonságára is igaz. Elegendő az internetes infrastruktúra 20%-át hatékonyan megtámadni ahhoz, hogy 80%-os elérhetetlenséget lehessen okozni. Gondoljunk bele, hogy milyen hatással van a világra, ha például a Google összes szolgáltatása elérhetetlenné válik.

---

3 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

4 https://hostingfacts.com/internet-facts-stats-2016/

1.3. Magánélet és munkahely

A technológiai fejlődés miatt napjainkban a munkahelyi- és a magánélet egyre inkább összemosódik az elérhetőség tekintetében. Hányan tekintenek munkaidőn kívül a munkahelyi levelezésükre, vagy végeznek el egy-egy feladatot számítógépük segítségével? Ahogyan a munkahelyi technológia beszivárog az emberek magánéletébe, úgy szivárog be a munkahelyre a magánélet technológiája. Emberek magukkal viszik az okostelefonjaikat és igénylik, hogy a munkahelyi wifit[5] használhassák.

Ezen összefonódás miatt a rendszerek keresztfertőződésének kockázata is megjelent, hiszen létezik egy olyan szürke szektor a szervezeti informatikában, amire a rendszergazdák és üzemeltetők nem látnak rá, a másik oldalról pedig sok ember használja magáncélra a szervezeti infrastruktúrát. Ami régen az volt, hogy céges költségen postáztak az alkalmazottak, az ma már munkahelyen történő közösségi média használat, privát felhőalkalmazások használata, illetve az úgynevezett árnyékinformatikai eszközök és szolgáltatások összessége.

Ezen árnyékinformatikának nevezett terület az, ahol összemosódik a hivatali/vállalati élet és a privátszféra. Ezen összemosódás okozhat adatvesztést, kártékony kód beszivárgást mind a szervezeti, mind pedig a magán informatikai eszközökbe és hálózatokba. A szétválasztás további jelentőségéről a későbbiekben még szó esik.

1.4. Szabályzói és technikai háttér

A technológia gyorsabban fejlődik, mint a szabályzói háttér. A piaci igények kiszolgálása és a technológiai fejlődés sebessége nem csak a digitalizáció terén gyorsabb, mint a törvényhozói és szabályozói háttér, hanem az élet más területein is. Ez egyrészt lehetőséget ad a technológiai innovációnak és a lehetőségek kitárásának, ugyanakkor mind a biztonsági megfeleltetést, mind pedig az új veszélyek és kockázatok elleni védekezést elnehezíti, a kár bekövetkeztekor történő felelősségre vonásról nem is beszélve.

A technológia és a szabályzók közötti széles szakadék, mely ma tátong, sajnos rengeteg esetben a felhasználóra hárítja a felelősséget. Míg az élet más területein, mint például az építészet, törvényi előírások vannak a tervezéstől kezdve a kivitelezésen át az üzemeltetésig mindenre, addig ez sajnos az informatikában még csak csírájában van jelen. Szoftvergyártókat még nem vontak felelősségre tervezési hiba eredményeképp kiszivárgott adatok miatt és a közeljövőben ez nem is látszik, hogy megváltozna.

Ugyanakkor számos olyan törekvés van, amely részben jogi, illetve minőségi megfeleltetéssel igyekszik a megbízhatóságot és a biztonságot elősegíteni, ilyen az EU adatvédelmi szabályozása vagy a hazai *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: információbiztonsági törvény, Ibtv)*

1.5. A többszintű információbiztonság-tudatosság szerepe

Minden szervezet több szintből áll, legyen ez egy vállalkozás vagy egy állami hivatal. A biztonság egy rendszer és ennek a rendszernek a részei az emberek is. Az emberek a biztonság szó hallatán gyakran konkrét támadásokra és védekezési formákra gondolnak, ám a dolog nem ilyen egyszerű. A biztonság minden esetben egy rendszer része, ami mindig bonyolultabb, mint az egyes alkotóelemei. Mindentől függetlenül a biztonságot mindig a tágabb rendszer kontextusában célszerű elemezni és egyben fejleszteni.

Az adott szervezeti szinteknek és szerepköröknek megfelelő oktatás és tréning szükséges ahhoz, hogy a rendszer alkotóelemei megfelelő biztonságot tudjanak adni. A szervezet egészének értenie

[5] https://prohardver.hu/tudastar/wi-fi_direct.html

szükséges az információbiztonsági alapokat, ugyanakkor döntéshozatali szinten fontos stratégiai háttértudással és szemlélettel is rendelkeznie, míg egy IT fejlesztői pozícióban pedig a technológiai biztonság megteremtése és megtartása a szempont.

Ezen szerepkörök összehangolt képzése és működése szükséges egy adott incidens megelőzéséhez vagy az incidens gyors csillapítására, esetleg elhárítására. A biztonság kompromisszummal jár, abszolút biztonság nem létezik. Az életben vannak bizonyos kockázatok, és mindig kompromisszumra van szükség. Ezekről a kompromisszumokról mi magunk dönthetünk, legyen az személyes, üzleti, állami vagy más jellegű. A biztonságra nem lehet úgy rákérdezni, hogy: „Hatékony-e ez a biztonsági intézkedés?" Sokkal jobb úgy kérdezni: „Ez vajon jó kompromisszum?" Ennek tükrében fontos vizsgálni a minket körül ölelő világot.

2. A KIBERTÉR SZABÁLYOZOTTSÁGA

2.1. EU-s szabályozás (NIS, GDPR)

Az Európai Unió évek óta dolgozik azon, hogy megerősítse a kontinens kiberbiztonságát. Az okok érthetőek, hiszen évről évre egyre több a fenyegetés, egyre gyakoribbak a támadások. A személyes adatok védelmére hozott EU adatvédelmi szabályozás (GDPR- Global Data Protection Regulation) után a legfontosabb európai szolgáltatások védelmére hivatott NIS-irányelv (Network and Information System) is hatályba lépett 2016-ban. Ezen rendeletek az EU egészére vonatkoznak és céljuk, hogy egységben is és nemzetállami szinten is fejlessze és erősítse a kiberbiztonságot.

Az informatikai megoldások terjedésével és felfutásával egyidőben, a 2000-es évek során több országban az infokommunikációs rendszerek megfigyelésére és a felhasználók információs szabadságának korlátozására a nemzetbiztonságért felelős szervek jogosultságot kaptak. Ezen szervek a törvény által felhatalmazva lehallgatással megfigyelhetik az elektronikus levélváltásokat, telefonhívásokat, nyomon követhetik az internetforgalmat, jelszavakhoz férhetnek hozzá.

Az Európai Unióban is az amerikai 2001. szeptember 11-ei események indították el az információbiztonsági törekvéseket, ekkor vált mindenki számára nyilvánvalóvá és kézzelfoghatóvá az információs társadalom nagyfokú sebezhetősége. Az Európai Bizottság 2004. október 20-án adott ki egy közleményt „*A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben"*[6] címmel. Ez a dokumentum elsőként tesz említést a lehetséges kibertámadásokról, és azok következményeiről.

2005. november 17-én adta ki az Unió az úgy nevezett *Zöld Könyvet*, amely bemutatja a kritikus infrastruktúrák védelmére vonatkozó program (European Programme for Critical Infrastructure Protection- EPCIP) végrehajtási lehetőségeit. Célja, hogy a kritikus infrastruktúrák számára egyforma és megfelelő védelmi szintet biztosítson, minimálisra csökkentse a gyenge pontjait.

A következő mérföldkő 2009-ben jött, amikor az Európai Bizottság közleményt adott ki kiemelve, hogy az EU a hatékonyság növelése és az elkerülhető párhuzamosan azonos munkavégzés elkerülése érdekében nemcsak közösségi és nemzeti szinten kívánja elősegíteni a védelmet, hanem együtt kíván működni más nemzetközi szervezetekkel is. A 2010-ben kiadott *Európai Digitális Menetrend* szignifikáns eleme az EU kibervédelmi politikájának. A Menetrend II. fejezetének egyik fő kérdésköre a bizalom és a biztonság kérdése. A biztonsági stratégiájában az elektronikus levelek, internetes csalások, a személyazonosság-lopások, stb. kockázatként jelennek meg.

Az EU kiberbiztonsági törekvésének következő lényeges állomása a 2013-ban kiadott stratégia, melynek címe: „*Európai Unió Kiberbiztonsági Stratégiája*: *nyílt, biztonságos és megbízható kibertér"*. Ez a stratégia foglalja össze, hogyan lehetne a leghatékonyabban megelőzni és elhárítani az infokommunikációs rendszerek sérülékenységeit.

A dokumentumban meghatározott konkrét intézkedések célja növelni az információs rendszerek védelmi képességét a kibertérben történő támadásokkal szemben. Ezen célok megvalósításának lépcsői a lentebb taglalt rendeletek és szabályzók.

Az EU információbiztonsági rendje napjainkban két fő pillérre épül. Az egyik a tagországok adatkezelését közös nevezőre hozó általános adatvédelmi rendelet, a GDPR . Ez az európai állampolgárok

[6] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al33260

személyes adatait védi minden eddiginél alaposabban, és egységes működési keretet biztosít az ezeket az adatokat kezelő cégeknek, 2017 május végén lépett hatályba.

A másik jelentős pillér a 2017 augusztus elején életbe lépő, a hálózati és információs rendszerek biztonságáról szóló irányelv, vagyis a NIS . Ez az első uniós szintű kiberbiztonsági szabályozás, amely célja, hogy segítsen megelőzni az európai infrastruktúra elleni kibertámadásokat.

A rendelkezések céljai közös nevezőre hozni a tagállamok kibervédelmét, meghatározni egy közös biztonsági minimumot, és ehhez közös eszköztárat – intézményi rendszert, szabályozást – adni a tagállamok kezébe, azaz egyfajta EU-s standardizáció megalkotása.

2.1.1. Hálózati és Informatikai rendszerek védelme (NIS)

A NIS nem általános szabályozás, hanem két konkrét csoportra vonatkozik, azokra, amelyeknek a megtámadása a legérzékenyebben érinti a társadalmat.

Az egyik ilyen halmaz az **alapvető szolgáltatást nyújtó szolgáltatóké**: digitális infrastruktúrák, energiacégek, ivóvízellátók, közlekedési vállalatok, egészségügyi szolgáltatók, banki szolgáltatások, pénzügyi piaci infrastruktúrák, azaz kritikus rendszerek tartoznak bele. Az ide sorolandók pontos körét a tagállamok maguk határozzák meg az alapján, hogy az adott szervezet szolgáltatása alapvető-e a társadalom vagy a gazdaság számára, ennek a szolgáltatásnak a biztosítása függ-e hálózati és információs rendszerektől, illetve egy kiberbiztonsági incidens jelentős zavart okozna-e a szolgáltatásban.

A másik érintett csoportba azok a **digitális szolgáltatásokat nyújtó szolgáltatók** tartoznak, amelyek ugyan nem nélkülözhetetlen, de fontos társadalmi hatású szolgáltatásokat kínálnak: az online piacterek, a keresőszolgáltatások és a felhőszolgáltatók. Fontos, hogy azokra a szolgáltatókra is vonatkozik a NIS, amelyek az EU-n kívüliek, de itt is szolgáltatnak, tehát például az amerikai Amazon-ra vagy Google-re, vagy a Brexit után a brit cégekre.

Mindkét csoportnak meg kell felelnie két fontos szempontnak: egyrészt a kockázatokkal arányos mértékű hálózat- és rendszerbiztonságot kell garantálniuk, másrészt kötelező jelleggel szűkös határidőn belül be kell jelenteniük az illetékes nemzeti hatóságnak, ha jelentős biztonsági incidens éri őket. A kritikus infrastruktúra szolgáltatók esetében viszont nagyobb a szigor, az ő esetükben a tagállamok hatóságai ellenőrizhetik, hogy milyen biztonsági lépéseket terveznek, és hogy ezeket megfelelően átültetik-e a gyakorlatba is.

A NIS alapján a tagországoknak ki kell dolgozniuk egy nemzeti hálózat- és információbiztonsági stratégiát, valamint ki kell jelölniük egy nemzeti hatóságot, amely felügyeli a NIS átültetését és végrehajtását. Ezt a feladatot Magyarországon a **Nemzeti Elektronikus Információbiztonsági Hatóság** (NEIH) látja el.

Ezzel párhuzamosan ki kell jelölniük egy vagy több gyors reagálású kibervédelmi csapatot, azaz CSIRT-et (Computer Security Incident Response Team) vagy más néven CERT-et (Computer Emergency Response Team).

Szektoronként szükséges meghatározni, pontosan milyen kritériumok alapján számít egy-egy cég az irányelv hatálya alá, és ezután a konkrét cégeket is ki kell jelölni. Erre a 21 hónapos átültetés után még további 6 hónapja lesz a hatóságnak.

EU-s szinten pedig létre kell hozni a kiberbiztonsági csapatok együttműködését koordináló CSIRT-hálózatot, illetve a nemzeti hatóságok együttműködését segítő Együttműködési Csoportot is. Mindkét szervezet felállítására fél éve van az EU-nak – vagyis a tagállamoknak közösen – de érezhetően gyorsan akarnak haladni, ezért ezeket már el is kezdték előkészíteni a tagállamok.

Az irányelv előírja egy európai CSIRT-hálózat létrehozását is, ez hivatott hatékonyabbá tenni az együttműködést, ha például egy több tagországban is szolgáltatást nyújtó céget ér támadás. A különböző országbeli CSIRT-ek között már eddig is volt valamiféle együttműködés, közvetlenül és különböző CSIRT-szervezeteken keresztül is. Ezek viszont önkéntes szerveződések voltak, és a különböző szervezetekbe más-más tagok, más-más feltételek szerint kerültek be.

A NIS alapján tagállamonként csak egy CSIRT kötelező, de akár szektoronként egy-egy is felállítható. Magyarországon[7] már most is több ilyen eseménykezelő csoport működik: a kormányzati rendszerek védelmében a **GovCERT**-é a központi szerep, de emellett a Honvédelmi Minisztériumnál működik egy külön **MilCERT** is, a kritikus infrastruktúrákért, pedig a belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságának a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (**LRLIBEK**) a felelős. A kormányzati szektoron kívül pedig az önkéntes alapon szerveződő **HunCERT** az internetszolgáltatók, a **NIIF CSIRT** pedig az oktatási-kutatási-közgyűjteményi intézmények eseménykezelését látja el.

A szabályozás részleteinek a kidolgozására az Európai Bizottság létrehozott egy szakértői csoportot még 2017. májusban. Ennek magyar részről a **Nemzeti Kibervédelmi Intézet** (NKI) a tagja, és általában is az egész kiberbiztonsági szervezkedésben ők képviselik az országot.

Szervezeti szinten pedig már 2016 ősszel felállt egy egységes kiberbiztonsági intézményrendszer, középpontban a Nemzeti Kibervédelmi Intézettel (NKI). Ez foglalja magában a NIS felügyeletét is ellátó Nemzeti Elektronikus Információbiztonsági Hatóságot (NEIH) és a Kormányzati Eseménykezelő Központot (GovCERT) is, amely Magyarországon a NIS által előírt központi CSIRT szerepét látja el.

2.1.2. EU adatvédelmi szabályozás (GDPR)

A GDPR rendelet minden tagországra egységesen érvényes és az EU-n kívüli országok cégeire is vonatkozik, ha azok EU-s magánszemélyek vagy cégek adatait kezelik. Azaz ezeknek a cégeknek is szigorú szabályoknak kell megfelelniük, cserébe azonos feltételekkel indulnak az európai piacon.

A GDPR alappillére, hogy az adatkezelő cégektől minél nagyobb fokú átláthatóságot és elszámoltathatóságot követel meg, nagyobb nyomatékot kap, hogy a teljes adatkezelési folyamatnak transzparensnek kell lennie. Központi elem a gyakorlatban nehezen megfogható, beépített adatvédelem *(Privacy by Design és Privacy by Default)* nevű alapelv. A beépített adatvédelem szerint az adatbiztonságnak már az adatkezelési eljárások kidolgozásakor fontos szempontnak kell lennie, nem lehet puszta utógondolat. Az adatbiztonság az alapértelmezés, az adatkezelésnek átláthatónak és felhasználó-központúnak, az adatvédelemnek proaktívnak kell lennie, és az adat teljes életciklusát fel kell ölelnie, vagyis a teljes folyamatnak része kell, hogy legyen: bármilyen technológia vagy belső szabályozás fejlesztésekor vagy bevezetésekor már a tervezés fázisában szem előtt kell tartani. Egy szervezet csak annyi és olyan adatot kezeljen, amilyet és amennyit szükséges, és csak addig, amíg szükség van rá, az adatkezelés jogszerűségét igazolnia szükséges.

Az adatkezeléshez világos hozzájárulás szükséges, 16 éven aluli gyerekek esetében a szülőtől is. Minden felhasználónak joga lesz a személyes adatai igazolható töröltetéséhez, ha már nem kívánja használni az adott szolgáltatást. Az adathordozhatóság GDPR szerinti szabályozása szerint, ezentúl olyan formában szükséges átadni az adatokat, hogy azt egy másik szolgálatóhoz mindenféle módosítás nélkül át lehessen vinni.

A GDPR rendelet is tartalmazza az értesülés jogát adatvédelmi incidenseknél, azaz, ha a felhasználó adatait érintő biztonsági esemény következik be, a cégeknek ezentúl ezt közzé kell tenniük, illetve kötelezően értesíteniük kell az őket felügyelő adatvédelmi hatóságot is.

A rendelet ugyan egységes, de a végrehajtás továbbra is a helyi hatóság, vagyis Magyarországon a **Nemzeti Adatvédelmi és Információszabadság Hatóság** (NAIH) feladata.

A GDPR elsődlegesen a gazdasági oldalról igyekszik szabályozni a piacot és megteremteni az egységes technikai biztonság feltételeit. A GDPR által előírt büntetési tétel maximum egy cég árbevételének 4 százaléka, a rendelet pontosan leírja, hogy milyen esetben és mekkora cégnek mennyi bírság szabható ki arányosan.

---

[7] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500185.KOR

A GDPR alapján – és ebben az új rendelet követi a korábbi irányelvet – harmadik országba csak akkor lehet európai adatokat továbbítani, ha a célországban is megfelelő szintű védelem biztosított ezeknek az adatoknak. Annak a biztosítására és igazolására, hogy egy-egy célországban megvan ez a védelem, több lehetőség is adott, de meghatározóan három megoldás a jellemző:

- A Bizottság kimondja ezt egy megfelelőségi határozatban. Ilyen jelenleg 11 nem EU-s terület esetében létezik Svájctól Izraelen keresztül Új-Zélandig – és ilyen volt a 2016 novemberben hatályon kívül helyezett Safe Harbour egyezmény is, amely az Amerikába történő adattovábbításra vonatkozott.
- Egyes cégek adatkezelési gyakorlatát is ítélheti megfelelőnek az Európai Bizottság, amelyhez többféle modellszerződést is kidolgoztak. Olyan általános szerződési feltételekről van szó, amelyek vállalásával egy cég biztosíthatja magának az EU által elvárt szintű adatbiztonságot. Ennek a megoldásnak a hátránya, hogy kevésbé rugalmas és ha egy cég sok országban működtet lányvállalatot, megnövekedhet a külön-külön megkötendő szerződések adminisztratív terhe.
- A harmadik tipikus megoldás a kötelező érvényű vállalati szabályok (BCR) bevezetése. Ez a belső céges adatkezelési szabályzat a cégcsoporton belüli adattovábbítást teszi lehetővé különböző országok között. Egy BCR-t minden érintett tagállam hatóságának jóvá kell hagynia, ami után az EU-ban egy kijelölt nemzeti hatóság felügyelete alá fog tartozni a teljes cégcsoport.

2.2. Hazai szabályozás

Magyarország a világon élenjáróként, az elsők között alkotta meg *2013. évi L. törvényt (t, Ibtv.)*, mely a következő bevezetőt tartalmazza: „A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága."

Viszont a fentebb taglalt NIS és GDPR szabályozások új feladatokat is hoznak, hiszen a hazai szabályozások a piaci szereplőkre nem vonatkoznak és a NIS alá tartozó szektorokból is csak néhánynál léteznek IT-biztonsággal foglalkozó előírások. Ezen kívül várható a hazai szabályozás 2018-2019-ben történő jelentős átalakítása, tekintettel az EU-s rendelkezésekre.

Az *Ibtv.* – valamint a *Nemzeti Kiberbiztonsági Stratégiáról* szóló 1139/2013. (III. 21.) Kormányhatározat– nyomán hazánkban 2013-tól kezdődően törvényi előírás és 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.

A létfontosságú infrastruktúra védelmére vonatkozó jogszabályok 2008-2013 között léptek hatályba. Ezek olyan létfontosságú fizikai és információs-technológiai berendezések és -hálózatok, szolgáltatások és eszközök védelmét érintik, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a kormányok hatékony működései szempontjából.

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló, fentebb már említett Kormányhatározata meghatározza Magyarország kibertérre vonatkozó értékrendjét, jövőképét és céljait, és előrevetette a dinamikusan változó kibertér igényeihez és az ez által generált feladatokhoz alkalmazkodni képes kormányzati képességeket biztosító kormányzati struktúra kiépítését.

A stratégia gyakorlati megvalósulását hivatott biztosítani a fentebb többször említett Ibtv. A törvény felállítja a szükséges intézményrendszert a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága alapfeltételei megteremtéséhez.

Az intézményrendszer része a Nemzeti Biztonsági Felügyelet szakhatósági feladata, amely keretében a biztonsági incidensek megelőzését, a sérülékenységek és hibás működési beállítások felkutatását végzi, továbbá javaslatot tesz azok elhárítására, valamint közreműködik a biztonsági incidensek műszaki vizsgálatában.

Az Ibtv. és végrehajtási rendeletei létrehozták a NEIH-et és szakhatósági feladatok ellátásával ruházták fel az elektronikus információbiztonság területén. A Hatóság legfőbb feladata, hogy felügyelje a költségvetési szervek információtechnológiai, adatkezelő- és feldolgozó tevékenységét és az információtechnológiai fejlesztési projektekben az információbiztonsági követelmények teljesülését. Továbbá engedélyezi az érintett szervezetek által az Európai Unió tagállamaiban történő elektronikus információs rendszer üzemeltetését és ellenőrzi az érintett szervezetek által az Európai Unió tagállamain kívül történő elektronikus információs rendszerüzemeltetést.

Ennek érdekében a törvény kötelezettséget állapít meg a szervezetek számára, kiemelten a szervezet vezetője, az elektronikus információs rendszer biztonságáért felelős személy számára.

Magyarországon több rendelet/törvény is foglalkozik az adatvédelemmel illetve a számítógépes rendszerekkel, itt most azokat a főbb pontokat van lehetőség bemutatni, amelyek a közigazgatás szempontjából érdekesek lehetnek:

- **2013. évi L. törvény** az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
- **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.
- **2012. évi CLXVI. törvény** a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

2.3. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) legfontosabb elemei

2.3.1. A szervezet vezetőjének a feladata és felelőssége

Az Ibtv.) 7. § 3. és 5. bekezdése alapján a szervezet vezetője jóváhagyja az adott szervezet biztonsági osztályba sorolását és felel a jogszabályoknak való megfelelőségéért, az adatok teljességéért és időszerűségéért. A szervezet vezetője továbbá indokolt esetben magasabb vagy alacsonyabb biztonsági osztályt is megállapíthat.

Az Ibtv. 11. § szerint a szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről. A védelem biztosítása magában foglalja:

- a jogszabályokban megfogalmazott követelmények teljesülésének a biztosítását,
- az elektronikus információs rendszer biztonságáért felelős személy kinevezését vagy megbízását, aki azonos lehet a Mavtv. (2009. évi CLV. törvény a minősített adat védelméről) szerinti biztonsági vezetővel,
- az információs rendszerekre vonatkozó informatikai biztonságpolitika és informatikai biztonsági szabályzat kiadását; az informatikai biztonsági stratégiának a meghatározását,
- annak a meghatározását, hogy a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra milyen szabályok vonatkoznak,
- gondoskodást az információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai Információbiztonsági ismereteinek szinten tartásáról, továbbá a biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatásáról,

- annak biztosítását, hogy a rendszer eseményei nyomon követhetőek legyenek,
- biztonsági esemény bekövetkezésekor a rendelkezésre álló erőforrások tükrében, a gyors és hatékony reagálást,
- hogy amennyiben a szervezet az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- hogy amennyiben a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatást,
- a rendszer védelme érdekében egyéb szükséges intézkedések elvégzését.

A szervezet vezetőjének a felelősségét befolyásolja az, ha jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

2.3.2. Az elektronikus információs rendszer biztonságáért felelős személy feladata és felelőssége

Az elektronikus információs rendszer biztonságáért felelős személy az Ibtv. 13. § alapján az alábbi feladatokkal és felelősséggel rendelkezik:

- feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést,
- felel a szervezetnél elforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.

Az elektronikus információs rendszer biztonságáért felelős személy a közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban jogosult tájékoztatást kérni, megfelelőség alátámasztásához szükséges adatokat, illetve a rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot bekérni.

2.3.3. A NEIH feladata és felelőssége

A Nemzeti Elektronikus Információbiztonsági Hatóság az Ibtv. 14.§ alapján ellátja a törvény hatálya alá eső elektronikus információs rendszerek biztonságának a felügyeletét. Az informatikáért felelős miniszter által vezetett minisztérium szervezeti keretébe került beágyazásra a Hatóság, amely önálló feladat- és hatáskörrel rendelkezik.

Az Ibtv. 16. § szerint a Hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek.

2.3.4. Az információbiztonsági felügyelő

Információbiztonsági felügyelő kirendelésére akkor van lehetőség, ha adott költségvetési szerv felszólítás és a felügyelő szerv közreműködése ellenére a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti. Ezt az Ibtv. 16.§ tartalmazza.

2.3.5. A Nemzeti Biztonsági Felügyelet feladata és kötelessége

Az Ibtv. 18.§ alapján nemzeti szakhatóságként a Nemzeti Biztonsági Felügyelet került kijelölésre. A Felügyelet két fő tevékenységi köre a sérülékenységvizsgálatok és a biztonsági események műszaki vizsgálatának elvégzése.

Az alábbi tevékenységeket a Felügyelet végezheti:

- éves ellenőrzési terv alapján, és az Ibtv. szerinti biztonsági szintbe és osztályba sorolás ellenőrzéseként szakhatóságként a hatóság megkeresésére, továbbá egyedi esetekben a hatóság felkérésére az érintett szervezet vezetőjét előzetesen tájékoztatva sérülékenységvizsgálatot, valamint biztonsági események adatainak műszaki vizsgálatát végzi, valamint
- a szervezet felkérésére sérülékenységvizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi.

A szakhatóság a feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó intézkedési tervről a vizsgálat lezárását követően haladéktalanul tájékoztatja a vizsgált szervezet vezetőjét és a hatóságot.

2.3.6. Kormányzati eseménykezelő központ

A kormányzati eseménykezelő központ feladatait az Ibtv. 19-20. § szabályozza. A központ a törvényben foglalt biztonsági események kezelésére lett létrehozva és a katasztrófák elleni védekezésért felelős miniszter irányítása alá́ helyezték.

2.3.7. Nemzeti Kiberbiztonsági Koordinációs Tanács

A kormányzati koordináció biztosítására került létrehozásra a Nemzeti Kiberbiztonsági Koordinációs Tanács, amely a Miniszterelnökséget vezető államtitkár vezetése alatt áll, akinek a munkáját a Miniszterelnökség által delegált kiberkoordinátor támogatja.

A Tanács az Ibtv. 21. § feladatszabása alapján:

- összehangolja a törvény hatálya alá́ tartozó szervezetek együttműködését a kiberbiztonsággal összefüggő feladatok ellátásában,
- elősegíti a kiberbiztonság szabályozását, valamint a kiberbiztonság ágazati munkacsoportjainak munkáját,
- támogatja a nem kormányzati szereplőkkel való együttműködésnek keretet biztosító́ Nemzeti Kiberbiztonsági Fórum (a továbbiakban: Fórum) munkáját,
- támogatja a források hatékony felhasználását,
- figyelemmel kíséri Magyarország Nemzeti Kiberbiztonsági Stratégiájának végrehajtását és erről jelentést tesz a Nemzetbiztonsági Kabinetnek,
- elősegíti a kiberbiztonságot érintő́ egységes magyar kormányzati álláspont kialakítását és hozzájárul Magyarország nemzetközi politikai képviseletéhez.

A Tanács munkáját az általa felkért szakmai, illetve nem kormányzati gazdasági vezetőkből álló Nemzeti Kiberbiztonsági Fórum (továbbiakban: Fórum) és az ágazati kormányzati és nem kormányzati együttműködést biztosító kiberbiztonsági munkacsoportok segítik javaslattételi joggal és véleményezési lehetőséggel.

3. KIBERFENYEGETETTSÉG

3.1. Nem tudod megvédeni azt, amit nem értesz

Az információs társadalom felé való haladás folyamán úgy látszik, hogy a társadalom és a világ két részre szakadt. Az egyik – kisebbik része – érti a technológiát, amit használ, a másik – a nagyobbik része – pedig megmarad felhasználói szinten, aki nem is próbálja megérteni a mögöttes összefüggéseket. Ezt a jelenséget nevezik digitális szakadéknak, digitális tudásollónak. Utópisztikusnak tűnhet, de a kevésbé tudatos rétegek felemelése és támogatása ezen a téren az egész világ közös érdeke.

Annak érdekében, hogy a tudatosítás megvalósulhasson, több szinten is változtatásra van szükség. Egyrészről a felhasználókban meg kell, hogy legyen az igény a tudásra és a mögöttes folyamatok megértésére, egyúttal biztosítani szükséges a hozzáférést ehhez a tudáshoz képzések és oktatások által. Az embereket érdekelnie kell a saját maguk biztonsága és a magánéletük védelme. Minél több eszköz csatlakozik az internetre, minél inkább gépek és algoritmusok hozzák meg az emberek helyett a döntéseket, annál inkább tisztába kell kerülni azzal, hogy mi a mögöttes technológia, hiszen szó szerint: az életünk múlhat rajta.

3.2. Válaszd a biztonságot!

Az adatvédelem és az egyéni kiberbiztonság nem arról szól, hogy az embernek rejtegetni valója van. Arról szól, hogy az ember irányíthatja, hogy hogyan mutatja ezt meg a világnak, arról, hogy van egy publikus arca az embernek, de mellette lehet privát gondolata és cselekedete. A személyes méltóságról, a személyes méltósághoz való jogról beszélünk

Mindenki gyűjt adatot. Cégek, akiknek a szolgáltatásait az emberek használják, emberek, akik – digitális – kapcsolatban állnak egymással, mi magunk a saját emlékeinkről, a fontosnak tartott dolgainkról. Ezeket a digitális adatokat általában hálózatokon keresztül osztjuk meg. Ezekre a hálózatokra pedig az emberek többsége egyre inkább - a kényelem jegyében - vezeték nélkül csatlakozik.

A kibertérben egy támadás kockázata felbecsülhetetlen. Egy ellopott adat lehet az adott időpillanatban jelentéktelen értékű és okozhat óriási kárt évekkel később. A kibertámadások nagy része alacsony költséggel és kiszámítható bevétellel kivitelezhető. Elég egy darab laptop internet eléréssel és tönkre lehet tenni egy személyt vagy egy egész vállalatot. A közelmúltban élő példák erre a *Panama papírok (ahol offshore cégek bizalmas iratai kerültek ki)*[8], *Hacking Team (ahol egy kifejezetten titkosszolgálatokat kiszolgáló hacker céget törtek fel)* [9] vagy *Ashley Madison (a világ legnagyobb társkereseő szolgáltatójának felhasználóinak levelezései és adatai kerültek nyílvánosságra)*[10] incidensek. A kiberbűnözés forgalma 2013-ban elérte a háromezer milliárd amerikai dollárt. Ez több mint a világ marihuána, kokain és heroin forgalma együttvéve[11]. Ebből is látszik, hogy egy rendkívül nyereséges üzletágról van szó.

---

8 https://hu.wikipedia.org/wiki/Panama-akták

9 https://en.wikipedia.org/wiki/Hacking_Team#Data_Breach

10 https://en.wikipedia.org/wiki/Ashley_Madison#Data_breach

11 https://www.tripwire.com/state-of-security/regulatory-compliance/pci/cybercrime-is-now-more-profitable-than-the-drug-trade/

A kiberbűnözés részben azért is tud rendkívül költséghatékonyan működni, mert a felhasználók többsége gyári alapbeállításokat használ, mert nem érti a mögöttes összefüggéseket, nem tart be alapvető biztonsági intézkedéseket és mellőzi a külső szakértői segítséget. Egyszer megírt kóddal több millió eszköz támadható egy kattintással.

Szerencsére ma már egyre több internetes cikk foglalkozik a kibervédelemmel és biztonsággal, viszont ez emberek többsége egyszerűen nem mer nekiállni saját maga beállítani megfelelő biztonsági szintet az eszközein, fizetni ezért nem akar . Ezen a gondolkodásmódon mindenféleképpen szükséges változtatni, tudatosítás és akár céges, akár kormányzat és szolgáltatók által finanszírozott oktatások által.

A jogi szabályozások csak bizonyos szintig képesek a szolgáltatókat és szoftvergyártókat felelősségteljes működésre és szolgáltatásra kényszeríteni. Rövid- és középtávon a felhasználói tudatosítás és oktatás által lehet előremutató eredményt és változást elérni, hiszen fontos, hogy a felhasználó is értse, hogy mi történik körülötte, hogyan működik a világ, ami őt körülveszi. Hiába vezeti valaki a világ legbiztonságosabb autóját, ha nem köti be magát, a védelmirendszer nem fogja tudni megvédeni.

3.3. Támadó motivációk

Miért van annyi kibertámadás? Legegyszerűbb magyarázat talán az, hogy azért, mert nehéz megakadályozni, hogy ne legyen. A kibertérben és a fizikai világunkban lévő motivációk azonosak: aki a fizikai világban társadalmilag kártékony, az a kibertérben is az lesz. A különbség a hatástöbbszörözésben rejlik. Sokkal nehezebb fizikailag betörni találomra valahova, amit valószínűleg őriznek és védenek, és nem lehet tudni, hogy mi van bent, mint találomra, automatizált folyamatokkal számítógépes rendszereket támadni, amik maguktól megkeresik a sérülékenységet és kivonják az értékes adatokat. Ez utóbbi egyedül, egy darab laptoppal a világ bármely pontjáról kivitelezhető, míg az előbbi nem. Ráadásul a fizikai világban a lebukás esélye nagyobb és a törvénykezési folyamat kevésbé akadályozott, mint a kibertérben, ahol tipikusan nemzetek közötti összefogásra van szükség és annak a képességére, hogy megállapítható legyen, hogy az adott pillanatban ki ült a számítógép előtt.

A kérdés ettől még fennáll: miért támadnak a támadók? Néha egyértelmű: pénzért, haszonért. De néha az egyértelműnek tűnő eset valójában csak egy fedőakció egy másik motiváció elfedésére.

Általánosságban a következő motivációkat különböztetjük meg:

- **Kémkedés:** Tipikusan állami és nagyobb üzleti szereplők által történik, ún. APT[12] csoportok (csapatok) bevonásával. A kémkedés elsődleges célja, hogy minél tovább legyenek a rendszerben észrevétlenül. Lebukás után nem ritka, hogy más támadási vektorral újra visszaszivárognak. A kémkedés motiválta támadás felderítéssel kezdődik, ahol a rendszer gyenge pontjait keresik a támadók, amely akár egy megfelelő hozzáféréssel rendelkező alkalmazott is lehet. A rendszerhez történő hozzáférés után vertikálisan és horizontálisan is mozognak, minél magasabb szintű hozzáférést célozva. Megfelelő hozzáféréssel pedig már hozzáférhető a céges adatvagyon és adattár. Ha a támadók ügyesek, akkor olyan hátsó kapukat tudnak elhelyezni a rendszerbe, amikkel bármikor ki-be léphetnek, akár lebukás nélkül.
- **Profit:** Ez talán a legegyértelműbb motiváció. A különböző bankkártyalopásoktól kezdve, a kiszivárgott adatbázisokból húzható hasznon át a zsarolóvírusokig[13] sok minden ide tartozik.
- **Politika:** Politikai motivációjú támadás lehet egy ideológiai vagy hacktivista csoport (pl. Anonymous[14]) által elkövetett támadás vagy az állami szereplők által megrendelt támadások.

[12] http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

[13] A zsarolóvírus olyan rosszindulatú szoftver, amely képes titkosítani az információkat a megfertőzött számítógépeken, vagy akár egész hálózatokon is. A tevékenység mögött üzleti érdek áll. A titkosítás addig nem kerül feloldásra, amíg a felhasználó ki nem fizeti a hackerek által megszabott váltságdíjat. Gyakran előfordul, hogy a fájlok titkosításának feloldásához használt kulcsokat akkor sem adják ki, ha a felhasználó fizet.

[14] http://anonofficial.com

Egyre több állam rendelkezik nem csak kibervédelmi, hanem kibertámadó képességgel is. Ezen államilag finanszírozott támadások célja a kémkedésen át, a szabotázson keresztül, a kártevésig sokáig terjedhet.

- **Szabotázs:** Egyre gyakrabban jelennek meg hírek, amelyek valamilyen kritikus infrastruktúra elem megtámadásáról szólnak: vízellátó- vagy áramelosztó-, esetleg légiforgalmi irányítási rendszerek vagy egyéb kritikus infrastruktúra elemek ellen. Több szempont is felmerül az ilyen támadásoknál: hatékonyság csökkentése, zsarolás vagy csak képességfitogtatás. Ilyen támadás érte a közelmúltban Ukrajna villamosenergia hálózatát, vagy 2010-ben az iráni urándúsítót.
- **Zsarolás:** Míg egy zsarolóvírus vagy DDoS[15] támadás is lehet zsarolási eszköz, ennél kifinomultabb az, amikor az áldozatot kompromittáló anyag kiszivárogtatásával zsarolják a támadók és cserébe hozzáférést kell biztosítani a saját vagy vállalati rendszerhez, esetleg egyéb utasítást kell végrehajtania.
- **Önigazolás:** Azon támadók tartoznak ebbe a csoportba, akik a hírnévért teszik, amit csinálnak, bár néha politikai vagy társadalmilag hasznos cselekedetnek álcázzák a hírnév utáni vágyukat. Az ő fő célpontjuk gyakorlatilag minden, aminél a lehetőséget meg lehet ragadni. Aztán büszkén dicsekednek, hogy ők voltak.
- **Bosszú:** Egy exalkalmazott, aki rossz viszonyban távozott, a tipikus megtestesítője a bosszúálló támadónak. Lehet, hogy még megvannak a céges hozzáférései, vagy vannak nála értékes céges dokumentumok, adatok. Bár nem klasszikus értelembe vett kibertámadás, de a hírnévnek jelentősen árt, ha egy elégedetlen ügyfél, több más ügyféllel összefogva a közösségi médián lejáratja az adott szervezetet. Bosszúállás kategóriába tartozik még a Magyarországon nem elterjedt úgynevezett „swatting”, amikor is egy megadott címre illegális küldemény érkezik (pl. drog) és az átvétel pillanatára a különleges alakulatot kihívják. Ezzel egyidőben a sajtó is értesítésre kerül és élő közvetítéssel, illetve a közösségi média adta lehetőségekkel maximalizálható a reputációs (azaz hírnévben keletkező) kár.
- **Trollok:** Végül, de nem utolsósorban említsük meg a trollokat. Ők azért támadnak, mert megtehetik, mert kedvük van hozzá és valami vélt vagy valós problémájuk van valakivel. Ők azok, akik internetes fórumokon csak a hecc kedvéért piszkálják a többieket, csak itt konkrét támadásokat intéznek, hogy ellehetetlenítsék a célzott rendszert.

3.4. Kiber-fizikai Rendszerek (CPS)

A kiber-fizikai rendszerek (CPS) a fizikai világ és a digitális világ közötti kölcsönhatást hozzák létre. A technológia révén a járművek például képesek lehetnek az egymás közötti kommunikációra, továbbá az olyan külső környezetből érkező ingerek felismerésére, mint amilyen egy gyalogos közeledése is. A kiber-fizikai rendszerek egy olyan világot hoznak létre, amelyekben a szoftverek és a hardverek integrált rendszerekké olvadnak össze és minden össze van kötve egymással. Ilyen rendszereket már most is számos ágazatban alkalmaznak, például az iparban, ahol elvárás, hogy a valós idejű adatgyűjtéssel jelentős mértékben növelni lehessen a különböző létesítmények hatékonyságát. A kiber-fizikai rendszereknek köszönhetően csökkenthető lehet például a balesetek száma, de alkalmazásuk egyre elterjedtebb lesz a jövőben az ipar, az energiaellátás vagy például az egészségügy területén is.

[15] A szolgáltatásmegtagadásos támadás egy meghatározott alkalmazás, 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 lényege, hogy lehetőség szerint megakadályozza a célgép elérését.

3.5. Dolgok Internete (IoT)

Régen elmúltak azok a boldog idők, amikor a kiberbűnözés nagyjából annyit jelentett, hogy a kiberbűnözők bankszámlákat törtek fel és hitelkártya adatokat loptak. Erről a változásról jelentősen tehet a dolgok internete (internet of things, IoT). A kiberbűnözés eddig többnyire kétdimenziós térben, a számítógép képernyőjén zajlott, és kizárólag a digitális létünket, adatainkat kockáztathattuk. De ahogy a számítógépek megváltoznak, úgy fog megváltozni az élet is; épp olyan veszélybe kerülhet, mint az adatok.

A kiberbűnözés a harmadik dimenzióba lépett, már nemcsak adatok vannak veszélyben, hanem életek is.

A különböző otthoni vagy ipari szenzorok adatainak ismeretében ki lehet ismerni egy felhasználó viselkedését, mikor van otthon, mit szokott csinálni. Az adatok manipulációjával pedig anyagi károkat, illetve életre veszélyes cselekedetet lehet elkövetni. Az interneten elérhető olyan keresőmotor, ami kifejezetten az internetre csatlakozott IoT eszközök keresésére szolgál.[16]

Az orvosi eszközök is egyre okosabbak és ezáltal egyre sebezhetőbbek. A testbe ültethető defibrillátorok, az okosított inzulinadagolók és a wifis pacemakerek is tudnak csatlakozni az internethez, okoseszközökhöz. Jelenleg egy Hewlett-Packard tanulmány[17] szerint az okoseszközök 70 százaléka feltörhető és egy kütyünek átlagosan 25 sebezhető pontja van.

2015 júliusában egy szoftverhiba miatt közel egymilliárd Android eszköz vált sebezhetővé; ehhez elég volt egy fertőzött SMS-t megnyitni. A Stagefright[18] nevű hibajelenség az egész telefont a támadó kezébe adta: a tartózkodási helyünket, a bankszámlaadatainkat, a telefon tartalmát, és a mikrofon vagy a kamera fölött is átvehették az irányítást.

Végül pedig egy kis statisztika:

Elemzők 2020-ra 200-250 milliárd[19] csatlakoztatott eszközt várnak, ez a világ lakosságállományára kivetítve fejenként kb. 26 db okoseszköz. Az autók[20] 90%-a internet csatlakozással készül majd 2020-ra. Jelenleg a csatlakoztatott eszközök 90%-a[21] gyűjt személyes információt (is) és ezen adatok titkosítatlan üzenetként közlekednek a hálózaton. A tömegekben elérhető eszközök közel 70%-a tartalmaz valamilyen sérülékenységet.

3.6. Támadási technikák összefüggései

Általánosságban kijelenthető, hogy nincs feltörhetetlen rendszer és egy adott rendszer – illetve az általa tárolt információ – többféleképpen is kompromittálható. Ez történhet egy jól kivitelezett támadáson keresztül vagy egyszerűen egy adott szoftver vagy hardver hibájából kifolyólag is, a humán tényezőről nem is beszélve.

Az informatikai rendszereket érő kockázatok a fenyegetések és képességek széles spektrumából táplálkoznak. Maga a kár mértéke (a hatás) három dologból tevődik össze: a **lehetőségből**, amit a rendszer biztosít, a **képességből**, amivel a támadó rendelkezik és a lehetőséget ki tudja aknázni és a **támadás motivációjából**.

Bár a támadók rendelkezhetnek a motivációval és a képességgel, mégis szükségük van a lehetőségre, hogy sikeres támadást tudjanak kivitelezni. A motivációjukat és a képességeiket nem tudjuk

16 www.shodan.io
17 http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WcATbK2B3dQ
18 https://www.androidcentral.com/stagefright
19 https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
20 http://www.techradar.com/news/car-tech/90-of-new-cars-to-be-network-connected-by-2020-1123712
21 https://www.techdirt.com/articles/20150211/10134429988/cars-are-delivering-tons-driving-data-to-manufacturers-with-minimal-security-even-less-transparency.shtml

befolyásolni, de a saját és szervezeti kitettségünket igen. Ehhez fontos megérteni a támadások alapvető működését és kivitelezéseit.

Alapvetően kétféle támadás különböztethető meg:

- **Célzott támadás:** Célzott támadás esetén a támadó kifejezetten az adott szervezetet támadja. A támadás előkészítése hónapokig/évekig is tarthat, hogy a támadó kódot megfelelően tudják bejuttatni. A célzott támadások tipikusan sokkal károsabbak, mint a nem célzottak, hiszen ebben az esetben testreszabott támadó kódok kerülnek felhasználásra. Célzott támadások során (a teljesség igénye nélkül) használhatnak:
  - **Spear-phising** – célzott adathalász e-mailek, amelyek rosszindulatú kódot vagy hivatkozást tartalmaznak.
  - **Botnet telepítése** – a célgépet zombihálózathoz csatolják, hogy azon keresztül támadjanak más rendszereket.
  - **Szállítói lánc támadása** – a beszállítói lánc ellehetetlenítésével akadályozzák a szervezet munkavégzését.
  - **Social engineering** – gyakorlatilag az emberi jóhiszeműséget kihasználó támadás, amikor is nem technikai eszközökkel, hanem az ember bizalmába férkőzve nyer ki a támadó információt vagy veszi rá az áldozatot valamilyen cselekedetre.
- **Nem célzott támadás:** A nem célzott támadások válogatás nélkül támadnak mindent és mindenkit. Nem törődnek azzal, hogy ki vagy mi lesz az áldozat, nagy számok törvénye alapján előbb vagy utóbb biztosan beletalálnak sérülékeny rendszerbe, vagy hiszékeny emberbe. Ahhoz, hogy célba érjenek, az internet nyitottságát használják ki, a következő technikákkal:
  - **Phising** (Adathalászat) – nagy mennyiségű e-mail kiküldése érzékeny adatok gyűjtésére (pl. banki információ) vagy hamis oldalakra való tovább terelésre.**Watering hole** (kb. lesből vadászat) – hamis weboldal felállítása, hogy a megtévesztett felhasználó megadja adatait. **Ransomware** (zsarolóvírus) – előbb a támadó kód titkosítja az adattárolót, majd a támadó pénzért cserébe megadja a feloldó kulcsot. **Scanning** (feltérképezés) – az internet széles spektrumába történő egyidejű támadás.

A támadások motivációja és technikája ugyan eltérhet, de egy általános lépés-mintázat megfigyelhető a kivitelezésükben:

1. Felderítés – Itt történik a célpont általános megismerése és felmérése, az elérhető információk összegyűjtése és a támadási vektor, illetve stratégia megalkotása az elemzésből valószínűsíthető sérülékenységek kiaknázására. A támadók mindenféle elérhető információt összegeznek ebben a fázisban: technikai információk a rendszerekről, személyes információk az alkalmazottakról (Facebook, LinkedIn, stb.). Az általános információgyűjtést kiegészítheti a Social Engineering típusú tevékenység is.

2. Csomagküldés – A vélt vagy valós sérülékenységet támadó (adat)csomag eljuttatása a sérülékenységhez, például:

- fertőzött USB osztogatása kereskedelmi rendezvényeken,
- fertőzött csatolmányt vagy URL-t tartalmazó e-mailek küldése,
- a szervezet online szolgáltatásainak feltörése,
- hamis weboldal felállítása az alkalmazottak vagy ügyfelek megtévesztésére.

A támadó célja a legjobb eszköz megtalálása és annak kivitelezése.

3. Betörés – A sérülékenység kihasználása, valamilyen hozzáférés megszerzése. A kár mértéke azon múlik, hogy a támadó milyen sérülékenységet talált és használ ki. Lehetőséget kaphat például:

- a rendszer irányítását befolyásolni,
- az összes online fiókot elérni,
- teljes irányítása alá vonni a felhasználó számítógépét, tabletjét vagy telefonját.

Ha ezek megtörténnek, a támadónak lehetősége van az áldozat nevében cselekedni (személyiséglopás) és az általa hozzáférhető rendszerekhez hozzáférni.

4. Kiaknázás – a rendszerben a támadó a szándékának megfelelően elkezd tevékenykedni, akár hosszútávra berendezkedni. Az úgynevezett APT (Advanced Persistent Threat) típusú támadásoknál a támadó célja nem a károkozás, hanem az, hogy minél hosszabb ideig felderítetlenül hozzáférhessen az áldozat rendszeréhez és onnan információt kinyerhessen, esetleg döntést befolyásolhasson vagy idővel folyamatokat és rendszereket károsíthasson. Egy felhasználói fiók irányításának átvétele már általában ehhez hozzásegíti a támadót, ha pedig egy rendszergazda fiókja felett sikerül az irányítást átvenni, az garantált siker. Ez utóbbinál már telepítési jogköre is lesz a támadónak és így észrevétlenül tud elhelyezni kártékony kódokat. Miután elérte a célját, a támadó eltüntetheti a nyomait a rendszerből vagy eladhatja a hozzáférést másnak.

Néhány támadó pedig csak zajt és kárt akar okozni és ennek megfelelően fognak viselkedni, illetve cselekedni.

Fontos megemlíteni, hogy 2017-ben már megjelentek azok, a bűnözők által is használt támadó kódok, amelyek már nem igényelnek emberi beavatkozást, hanem maguktól képesek a rendszerekben kártékonyan tevékenykedni. Ezen támadó kódok első közismert képviselője az úgynevezett WannaCry és NotPetya zsarolóvírusok voltak, amelyek technikai alapját a CIA-tól ellopott és közzé tett kiberfegyverek adták. Mindkettő kód több százezer rendszert érintett a világon, súlyos anyagi károkat és működési fennakadásokat okozva.

3.7. Saját eszköz

Manapság teljesen elfogadott, hogy a munkaidejükben az emberek a saját eszközeiken dolgoznak, vagy a munkaeszközeiket magáncélra is használják. Ilyen az, amikor megnézzük a privát levelezésünket a munkaeszközön, vagy a munkahelyi e-mail beállításra kerül a privát tulajdonú telefonon. Ez a fajta általános viselkedés megnehezíti a munka és a magánélet elkülönítését és egyre inkább mossa össze a határokat a munka és a magánélet között, annak összes előnyével és hátrányával együtt.

Legnagyobb kockázat, hogy nem lehet felügyelni a munkavállaló saját eszközét a szervezeti hálózaton, hiszen a munkavállalók nem engedik át – teljesen érthetően – az eszköz felügyeletét a szervezeti informatikusoknak. A helyzet kicsit könnyebb a cég által biztosított eszközök esetében, ott gyakran kikötés szokott lenni a privát használat tiltása, illetve a felügyeleti jog tudatosítása a felhasználóban (azaz a munkáltató bármikor belenézhet az eszközbe, a fájlokba, stb.).

Ugyanakkor a piaci szervezetek 85%-a megengedi a saját eszközök használatát és függetlenül attól, hogy szabályozva van vagy nincs, az alkalmazottak 67%-a használja saját eszközét munkacélokra. Ezen eszközök használata szervezeti hálózaton lehetőséget teremthet adatszivárgásra vagy fertőzésre. Elég csak egy elhagyott mobileszközre gondolni, amiből a megtaláló ki tud nyerni érzékeny üzleti adatokat, hozzáféréseket vagy a nevünkben tud kommunikálni.

3.8. Közösségi média

Önmagában a közösségi média használata nem jelent kockázatot. A közösségi média felületeken viszont általában az emberek megosztják az életük egy-egy részét, egy kicsit kieresztik a feszültséget és egyfajta bizalmi felületként kezelik, ahol az ismerőseikkel közös élményeket osztanak meg. Az olyan oldalakon, mint a Facebook vagy Twitter, sokkal nagyobb eséllyel „szólja el" magát az ember óvatlanul.

A közösségi médiában megosztott információk pedig könnyen felhasználhatók az ember vagy a szervezet ellen. Sokszor a támadók a közösségi média oldalakon kezdik a felderítést a célpontjukkal kapcsolatban, onnan szerzik azt az információt, ami alapján a social engineering támadásukat felépítik. Elég pusztán egy poszt arról, hogy az ember milyen szakmai konferenciára megy és utána már kaphat is egy adathalász levelet megfelelő témával és adathalász oldalra mutató linkkel. Míg a hirtelen meghalt nigériai herceg öröksége vagy egy holland lottónyeremény témája a legtöbb embernél gyanút

kelt, addig egy megfelelő tartalommal összeállított, legitimnek tűnő e-mail át szokott jutni a technikai és emberi védelmi szinteken.

Az ilyen típusú adatgyűjtéstől természetesen a szakmai közösségi portál, a LinkedIn sem mentes, azzal a különbséggel, hogy az emberek itt előszeretettel mutatják meg szakmai kompetenciájukat, hátterüket és érdeklődési körüket. Ezen információk birtokában szintén meg lehet célozni az egyént, vagy a szervezetet magát kártékony kóddal, zsarolóvírussal.

Az internet eléréssel rendelkező felnőttek 52%-a, az összes aktív internetfelhasználónak pedig 70%-a használ közösségi oldalt[22]. A 18-29 évesek között ez az arány 90%. Súlyosbítja a helyzetet, hogy a felhasználók 75%-a ugyanazt a jelszót használja a közösségi oldalon, mint az e-mail fiókjánál. És mivel a többség szeret ismerkedni és minél több ismerőst tudni a közösségi felületen, ezért a felhasználók 40%-a elfogad ismeretlentől is meghívást. Az már csak pusztán érdekesség – de nem meglepő -, hogy az Egyesült Államokban a lebukott betörők 78%-a nyilatkozott arról, hogy közösségi oldalon felderítést végez a célpont kiválasztásnál[23,24].

3.9. Terrorizmus

A terrorizmus lényege a rémületkeltés, néha egy politikai cél előmozdítása érdekében, néha pedig puszta gyűlöletből. A terroristák eszközeiről és módszereiről napi szinten lehet az újságokban olvasni, amiről viszont kevés szó esik, hogy mi is a valós céljuk a terroristáknak.

Nem azok az emberek a valódi célpontok, akiket a terroristák megölnek; ők csupán a „járulékos veszteség". Nem a repülők, vonatok, piacok vagy buszok felrobbantása a cél; ez csupán „taktikai művelet". A terrorizmus valódi célja a túlélő többiek: az a több milliárd ember, akiket nem ölnek meg, de ezekkel a gyilkos cselekedetekkel megfélemlítenek. A terrorizmus valódi lényege nem maga a cselekmény, hanem az arra adott reakciók.

A digitális világ, mint az az élet más területein is látható, a terrorizmusban is hozott változásokat. Itt lehet a kommunikációs csatornákra vagy az internet sötétebb bugyraiban elérhető információmennyiségre gondolni. Sajnos az informatikai rendszerek sérülékenysége nem csak a bűnözök, hanem a terroristák fantáziáját is mozgatja, hiszen alacsony költségvetéssel, relatív biztonságban nagy kárt lehet okozni a világ bármely pontján.

A kiberbiztonsági és a védelmi szakma már régóta számol annak veszélyével, hogy egy pontosan kivitelezett(például egy erőmű, egy gát vagy a repülésirányítás elleni) informatikai támadás akár halálos következményekkel is járhat. A terrorizmus a kiberteret jelenleg elsősorban anyagi haszonszerzésre, toborzásra és propaganda terjesztésre használja, illetve a támadások előkészítésére és[25] koordinálására. Részben az ismert kockázat az oka annak, hogy a magyar és az európai szabályozók igyekeznek olyan jogi környezetet teremteni, amelyben a létfontosságú rendszerelemek, a kritikus infrastruktúrák üzemeltetőit kötelezik információbiztonsági védelem kiépítésére (lásd NIS, GDPR).

3.10. Belső fenyegetettség

2015-ben a vállalatok 73 százalékánál történt belső információbiztonsági incidens és ezek többsége a munkavállalók óvatlansága miatt következett be egy Kaspersky Lab tanulmány szerint.

---

22 http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

23 https://www.bitdefender.com/news/bitdefender-finds-exposed-social-media-credentials-often-provide-access-to-email-accounts-1682.html

24 http://www.brokerlink.ca/blog/social-media-security/

25 https://usa.kaspersky.com/about/press-releases/2015_the-threat-within-3-out-of-4-companies-affected-by-internal-information-security-incidents

A 26 országban 5500 informatikai szakember bevonásával készült felmérés kimutatta, hogy a vállalati informatikai infrastruktúra fejlődésével új sebezhetőségi pontok jönnek létre és ezáltal növekszik a rendszer fenyegetettsége is. A helyzetet az is súlyosbítja, hogy nem minden munkavállaló képes lépést tartani a változó informatikai környezet kihívásaival. Ezáltal a szervezetek tehát nem csak külső, hanem belső fenyegetettségnek is ki vannak téve.

A vizsgálat megállapítása szerint a vállalatok 21 százalékánál történt olyan, az üzleti eredményt is érintő adatvesztés, ami kifejezetten belső kockázati tényezőnek volt tulajdonítható.

Egy másik statisztika szerint az összes adatszivárgás 47%-a belső kockázati tényező miatt történt, ennek 50%-a (tehát az összes adatszivárgás közel 25%-a) szándékos károkozás volt.

A legegyszerűbb megközelítésben kétfelé lehet bontani a belső fenyegetettséget: **gondatlanságból elkövetett** és **szándékos károkozásra.**

Gondatlanság lehet, amikor az alkalmazottak mobil készülékeit elveszítik vagy ellopják. Gondatlanság elől hagyni a jelszavakat az asztalokon, vagy nem lezárni a számítógépet, amikor az ember otthagyja az asztalát. De ide tartozik az is, amikor céges adatokat privát e-mail címre elküldi magának az alkalmazott, pusztán jó szándékból (mondjuk mert hétvégén dolgozni akar rajta).

Szándékos károkozás önmagáért beszél. Mindenki ismer olyan esetet, amikor valaki ellopta a cég adatbázisát, vagy módosított valamit az informatikai rendszerben a saját javára. Ide sorolhatók a nemtörődömségből eredő károk is, amikor valaki lustaságból, felelőtlenségből vagy figyelmetlenségből sem tartja be a szabályzatokat és előírásokat.

3.11. Szabályzatok és szabályzók

Többször is esett már szó a szervezeti szabályzatokról. A szervezeti szabályzatok – mint a nevük is mutatja – a szervezet működését szabályozzák. Teszik ezt részben törvényi megfeleltetésből, részben tanúsítási megfontolásból vagy pusztán a működés szabályozhatósága végett. A szabályzatok felelnek azért, hogy az adott szervezet dolgozói tisztában legyenek az elvárt viselkedéssel, munkavégzési módszerrel, adatok kezelésével, váratlan esemény bekövetkeztekor szükséges teendőkkel, stb. Ahogyan például a tűzvédelmet, úgy az informatikai biztonságot is szabályozni szükséges. A kormányzati, illetve önkormányzati szektorban fontos kiemelni a törvény szerinti szervezeti- és osztály besorolásokat, amelyekről a biztonsági vezető köteles tájékoztatni az alkalmazottakat.

4. BIZTONSÁGBAN A HÁLÓZATON

4.1. A biztonságos viselkedés általános bemutatása

Az internet elterjedése és az internet elérését lehetővé tevő infokommunikációs szolgáltatások átalakították életvitelünket, szokásainkat. Az internet segítségével szervezzük meg tevékenységeinket, programjainkat a munkában, az üzleti- és a privát szférában, ügyeinket, de még vásárlásainkat is mindinkább online intézzük. Bármikor, bárhol, akár utazás közben is kapcsolatban lehetünk másokkal.

Az online kapcsolattartás minden formája elérhető a mobiltelefonálásra használt eszközökön is, különösen az egyes élethelyzetekre kifejlesztett alkalmazások segítségével. A digitális kompetencia általános szükségletté, alapkövetelménnyé vált.

Miként a valós, ún. „offline" világban, úgy az interneten is találkozhatunk veszélyekkel, és tudatosan fel is kell készülnünk az azokkal szembeni megfelelő védekezésre. Az eddigi fejezetekben ezt a mögöttes hátteret taglaltuk. Fontos, felismerni és tudatosítani, hogy a biztonság mindig a kompromisszumok tükrében értelmezhető, viszont a kibertérben a veszély sokszor láthatatlan formában van jelen.

4.2. Biztonságtudatos viselkedés kialakításának szempontjai és módszerei

4.2.1. Munka és privát élet

Ahogyan ez fentebb is kifejtésre került, a munka és a privát élet digitális értelemben vett szétválasztása egyre nehezebb. Biztonsági szempontból viszont mindenképpen törekedni szükséges rá. Ugyanakkor az itt megfogalmazott tanácsok és jó gyakorlatok mind a munkahelyi, mind pedig a magánéletben használhatóak.

Ha lehetséges, digitális szempontból ne keveredjen a magánélet és a munka. Ne kerüljenek letöltésre vagy továbbításra munkahelyi adatok, anyagok személyes használatú eszközre, hiszen ezáltal az adatok védelméért való felelősség terhe is a felhasználóra száll, annak összes jogi és pénzügyi kötelezettségeivel. A munkahelyi, illetve szervezeti szabályzatok megléte és ismerete biztosíthatja a biztonságos távoli munkát, akár saját eszközről is, de erről mindenképpen a szervezetnél kijelölt biztonsági felelőstől szükséges tájékoztatást kérni.

4.2.2. Adatbiztonság, személyes biztonság

Az internetezésre használt eszköz biztonsági beállításainak megfelelő megválasztásával, friss, biztonságos szoftverekkel, az eszköz használatához, az internetes műveletek elvégzéséhez, weboldalakra történő bejelentkezésekhez használt jelszavak gondos megválasztásával és gyakori változtatásával megakadályozható, hogy az adott hivatkozásokra való kattintással elért weboldalakon az eszköz vírussal fertőződjön és támadásnak legyen kitéve.

Fontos, hogy az interneten különösen érvényes az „először elolvasni, átgondolni, aztán kattintani” elv. A felhasználási feltételek és a jogosultság engedélyezések előtt célszerű felmérni az applikáció vagy a szolgáltatás használatával járó esetleges veszélyeket.

A közösségi oldalakon a megfelelő biztonsági beállításokkal lehet megelőzni, hogy a nevünkben posztoljanak, illetve, hogy még gondatlanságból, figyelmetlenségből se tegyünk közzé olyan tartalmat, ami később bajt okozhat. Tartózkodjunk a saját, illetve mások aktuális, vagy gyakori tartózkodási helyének beazonosítását lehetővé tevő információ közzétételétől. Privát képeket, illetve csoportképeket az érintettek megkérdezése nélkül ne tegyünk közzé, egyúttal javasolt olyan képek feltöltése és megosztása, amelyek nem tartalmaznak GPS koordinátákat.

A chat programok esetén szintén ajánlatosfokozott óvatossággal eljárni és megismerni a személyes adatkezelésre vonatkozó tájékoztatásokat. Az ilyenformán nyert információ alapján tudja a felhasználó eldönteni, hogy az alkalmazás vagy szolgáltatás használatával tulajdonképpen mihez is járul hozzá és milyen adatokat oszt meg magáról és azokkal az adatokkal mi történhet.

Fogadjuk el tényként, hogy az interneten nincsenek titkok és minden szolgáltató a felhasználói adatokból próbál megélni. Ezáltal előfordulhat, hogy a felhasználó által kitörölt posztok, képek és tartalmak valójában nem kerülnek törlésre, így javasolt csak olyan tartalmak megosztása akár emailen, akár chat programon keresztül, ami nem tartalmaz kényes információt.

Az irodai asztalon javasolt rendet tartani, jelszavakat nem elöl hagyni és az érzékeny adatokat tartalmazó anyagokat pedig elzárni.

4.2.3. Megfelelő viselkedés, megjelenés a közösségi térben

Fogadjuk el és toleráljuk, hogy sokan szenzációsnak, közérdekűnek, bájosnak, viccesnek vélt tartalmakat, valamihez való csatlakozásra, segítségnyújtásra, közreműködésre buzdító vagy elvekkel, meggyőződéssel, elhivatottsággal kapcsolatos információt keresnek, illetve terjesztenek. Ugyanakkor mérlegeljük ezeknek az életszerűségét is. A Facebook nem fizet „like” darabszám után (ez elolvasható a feltételei között), illetve senki nem fog ingyen mobiltelefonokat osztogatni azért, mert valaki válaszol 3 kérdésre egy felugró ablakban. Legjobb védekezés, ha elfogadjuk, hogy – ahogyan a fizikai valóságunkban is – ha valami túl jónak tűnik, akkor az általában nem valóságos .

Javasolt kerülni a számunkra érdektelen, vagy zavaró közléseket, megosztásokat. A hírfolyamot tisztítsuk meg a nem kívánt tartalmaktól, a játékfelkérésektől, eseményértesítésektől. Válasszuk meg, kivel ismerkedünk, csevegünk. Ameddig valakivel nem találkoztunk személyesen, addig nem tudhatjuk, hogy ő tényleg az, akinek állítja magát. Amit még fontos megérteni, hogy sosem lehetünk abban biztosak, hogy tényleg csak annyian olvasunk egy chat üzenetet vagy e-mailt, ahány embernek mi elküldtük azt.Újfent: kerüljük a kényes tartalmak megosztását titkosítatlan üzenetekben, chatprogramokon keresztül.

Elsődlegesen az érintettek védelmében, de saját jól felfogott érdekünkben is indokolt kerülni a hozzátartozóinkkal, a munkáltatónkkal, illetve bárki mással kapcsolatos bizalmas, nyilvánvalóan nem közérdekű kommunikációt, a rájuk vonatkozó adatok, fényképek megosztását, az őket érintő tartalmakhoz való folyamatos hozzászólást.

Végül, de nem utolsósorban, tudva, hogy az általunk közzétett képekkel, közlésekkel, megosztásokkal akaratlanul is egyfajta képet festünk magunkról, fel kell mérnünk, milyennek látszunk mások szemében az online világban.

Ismeretlen feladótól vagy akár ismerőstől jövő üzenetben lévő fájlra csak akkor kattintsunk, ha teljesen biztosak vagyunk benne, hogy nekünk volt szánva az üzenet és nem gyanús. Amennyiben a legkisebb gyanú is felmerül, mindenképpen szóljunk egy hozzáértőnek – vállalati informatikának például – mielőtt kattintunk. Ha ismerős nevében jön az üzenet vagy a csatolmány akkor akár kattintás nélkül javasolt felhívni vagy egy megerősítő emailben megkérdezni, hogy tényleg nekünk lett-e szánva az üzenet.

Ebbe a kategóriába tartoznak még az úgynevezett rövid URL-ek pl.: goo.gl/kjsksj. Az ilyen rövid URL-lel az a probléma, hogy nem lehet tudni, hova mutat és kattintás nélkül nem tudjuk felmérni a kockázatot.

4.2.4. Jelszavak és azonosítók

Az interneten jelenleg általában email cím és jelszó párossal azonosítjuk magunkat. Ez mindaddig jól működik, ameddig a felhasználók:

- változatos és biztonságos jelszavakat használnak,
- szolgáltatásonként más jelszavakat használnak,
- nem osztják meg a jelszavaikat,
- és a szolgáltatók biztonságosan tárolják az ügyféladatokat, jelszavakat.

Nézzük sorban:

Mitől biztonságos egy jelszó? Legalább 16 karakter hosszú, tartalmaz kisbetűt, nagybetűt, számot és speciális karaktereket. Ez alapján az: „ANagyZoldAlmafa_2017” egy biztonságos jelszó kellene hogy legyen, de mégsem az. A támadók előszeretettel használnak szótár alapú jelszófeltöréseket, ahol egy számítógép egyesével kipróbál különböző variációkat. A „wDgM2Pq3c@W2hz6L” egy jó jelszó, viszont nehéz megjegyezni. Minden oldalhoz külön ilyen jelszót használni pedig a legtöbb ember számára nagy kihívás.

Kétféle elfogadott megközelítése van az erős jelszó felhasználó általi alkotásának. Mindkettő azon alapszik, hogy az emberi agy könnyebben meg tud jegyezni dolgokat, ha azokat tudja mihez kapcsolni. Az egyik megközelítés szerint a felhasználó gondoljon egy mondatra, könyvcímre, dalszövegre, amit ismer és amit meg tud jegyezni. Ezt a mondatot lehet utána átalakítani biztonságos jelszóvá. Az ismert népdalból „Debrecenbe kéne menni” például a következő több, mint 16 karakteres jelszót könnyen ki lehet alakítani: „*D€br3cenbE_ke’n€M3NN!*”. Mint látszik, bizonyos magánhangzók lecserélődtek speciális karakterekre, illetve számokra.

A másik megközelítés hasonló, pusztánott megmaradnak az eredeti szavak, amelyek közé beszúrhatók a speciális karakterek: „*Debrecenbe,ke’ne_menni!*”

A legegyszerűbb megoldás viszont a jelszótároló alkalmazások használata. Ezáltal a jelszavak lehetnek teljesen véletlenszerűek és megfelelő hosszúságúak továbbá megvalósítható az, hogy minden esetben más jelszót használjunk. Hátránya, hogy ha valaki hozzáfér a jelszótárolóhoz, akkor az összes jelszót megszerezheti. Ha ilyet használunk, ennek a jelszótárolónak mindenképpen hosszú és kellőképpen bonyolult jelszava kell, hogy legyen, illetve figyeljünk arra, hogy rendelkezzünk biztonsági mentéssel és a felhőben ne tároljunk jelszavakat, illetve ilyen jellegű biztonsági mentéseket.

Fontos azt is szem előtt tartani, hogy a jelszavaink a szolgáltatónál csak addig vannak biztonságban, ameddig a szolgáltató azt képes megvédeni. Bármelyik céget érheti bármikor kibertámadás, válhatadatlopás áldozatává, így már csak emiatt is érdemes a különböző szolgáltatásoknál különböző jelszavakat használni.

Kiegészítő megoldás még az úgy nevezett hitelesítő szolgáltatások használata, mint például a Google Authenticator vagy az Authy. Ezek a hitelesítő szolgáltatások egy ideiglenes kódot generálnak és így gyakorlatban nem szükséges jelszavakat használni, elég csak a mobiltelefon segítségével engedélyezni a belépést az adott szolgáltatásba (pl.: Gmail). A hitelesítő alkalmazások a „Felhasználók” alfejezetben leírt kétfaktoros hitelesítésnek is megfelelő alternatívái lehetnek.

4.2.5. Nyilvános hálózat

A nyilvános hálózatok potenciális veszélyeiről az átlagos felhasználó sok helyen tájékozódhat, mégis az emberek többsége mindenféle biztonsági megfontolások mellett is bátran használja. A hálózatok működéséből fakadóan az egy hálózaton lévő eszközök láthatják a hálózati forgalmat, azaz tudni lehet, hogy hány eszköz van a hálózaton, azok az eszközök mit csinálnak (pl. bankol, facebookozik, stb.) és megfelelő technikai feltételekkel és tudással az eszközök támadhatók illetve az általuk küldött vagy fogadott adatok manipulálhatóak, olvashatóak.

Ha egy mód van rá, kerüljük a publikus hálózatokat. reptereken, vendéglőkben, iskolákban, szállodákban elérhető publikus hálózatokat. Ha mégis használni kényszerülünk ilyet, akkor külön figyelmet kell szentelnünk arra, hogy érzékeny adatot ne küldjünk át rajta, ne bankoljunk, stb.

Ha mégis biztonságosan szeretnénk nyilvános hálózatot használni, akkor az úgynevezett VPN (Virtual Private Network) szolgáltatás segítségével, titkosított csatornán tudunk csatlakozni a megadott szolgáltatáshoz. VPN szolgáltatást tud biztosítani a munkahelyünk vagy magánemberként is választhatunk több szolgáltató kínálatából is. Az utóbbi esetében érdemes szem előtt tartani, hogy bizonyos szolgáltatók naplózzák a felhasználói tevékenységet, így bár a nyilvános interneten nem lehet látni az adatforgalmunk részleteit, a szolgáltató láthatja.

4.2.6. Titkosítás

Jelen tananyag keretei sajnos nem teszik lehetővé, hogy mélyebben elmerüljünk a titkosítás, valamint a rejtjelezés fogalmaiba és technikáiba. Alapszintű felhasználói szinten annyit érdemes megtenni, hogy ahol lehet, ott titkosított csatornán keresztül kommunikáljunk. Ilyen lehet a titkosított webes kapcsolat, azaz a *https*, vagy bizonyos *chatprogramok* által kínált titkosítás. Már önmagában az, hogy jelszavas védelemmel látunk el egy word dokumentumot, vagy jelszóval védett tömörített fájlba csomagoljuk és úgy küldjük el, sokat segít az adatvédelemben (még akkor is, ha képzettebb támadót ez csak hátráltat, de nem akadályoz meg).

Képzettebb felhasználók viszont megismerkedhetnek a PGP[26]-vel, amely üzenetek,fájlok aláírására és titkosítására használható megoldás.

4.2.7. Felhasználók

Javasolt az eszközökön a hagyományos felhasználó használata, azaz olyan felhasználói fiókkal történő mindennapi használat, amely nem rendelkezik rendszergazdai jogokkal, azaz nem telepíthet, nem engedélyezhet csak úgy folyamatokat. Ezáltal minden egyes alkalommal, ha egy program települni szeretne a rendszerre, az jelszót fog kérni és át lehet gondolni, hogy ez az alkalmazás vagy folyamat tényleg legitim-e.

Mind a munkahelyen, mind pedig az otthoni rendszereken csak a saját felhasználói fiókunkat használjuk érzékeny adatok megadására. Idegen eszközön ne lépjünk be netbankba, közösségi médiafiókunkba vagy egyéb érzékeny adatot tároló szolgáltatásba. Sosem tudhatjuk, hogy az idegen eszköz nem fertőzött-e (akár a tulajdonos tudta nélkül).

Ahol lehetőség van rá, használjunk úgynevezett kétfaktoros/kétlépcsős bejelentkezést. A legtöbb online szolgáltató ingyenesen biztosít ilyet. Ez esetben nem csak az email/jelszó párossal azonosítjuk magunkat a rendszerben, hanem még egy azonosításra szükség van, ami tipikusan SMS kódot vagy a korábban említett hitelesítő szolgáltató (Google Authenticator, Authy, stb.) használatát jelenti. Ezáltal nem elég csak a jelszavunkat ellopni, hanem a telefonunkra is szükség lesz.

[26] http://openpgp.org

Amennyiben új szolgáltatást vagy eszközt veszünk igénybe és lehetőség van a gyári vagy rendszer által biztosított jelszavak megváltoztatására, akkor azt tegyük meg.

4.2.8. Biztonsági mentések

Egyértelműnek tűnik, hogy a biztonsági mentések fontosak, mégis az emberek és szervezetek többsége nem rendelkezik vele. Szervezeti oldalról ez általában biztosított, hiszen a szervezeti informatikai részleg a biztonsági mentéseket – optimális esetben – rendszeresen elvégzi, így egy esetleges adatvesztés elkerülhető. Magánéletben az emberek többsége sajnos nem végez biztonsági mentéseket, pedig egy eszközmeghibásodás (vagy akár egy sikeres zsarolóvírus támadás) esetén helyreállíthatatlan károk keletkezhetnek: pótolhatatlan adatok (családi fényképek, levelek, stb.) vagy például az összes jelszó elveszhet, ami egy helyen volt tárolva.

4.2.9. Kiberhigiénikus viselkedés

Korlátlan ideig lehetne az előző listát folytatni, de a legfontosabb alapelv a gondolkodás és a megelőzés. E tekintetben a kibertér nagyon hasonlít a fizikai világunkra és az abban lévő veszélyekre, kórokozókra. Ahogyan a fizikai világunkban a viselkedésünk nagyban befolyásolja, hogy áldozatok leszünk-e vagy nem, ugyanúgy igaz ez a kibertérben történő viselkedésre is. Csak ameddig a fizikai létben a veszélyt többnyire lehetséges látni, addig a kibertérben a veszély gyakran nehezen érzékelhető az érzékszerveinkkel. Emiatt javasolt egy folyamatos készenléti tudatállapot elérése és az ennek megfelelő viselkedés az informatikai rendszerek használatakor.

Ahogyan a fizikai életünkben jelen van a napi higiénia, úgy szükséges az online életünkben is az ennek megfelelő rutin kialakítása. Ilyen lehet a védelmi rendszerek használata (vírusirtó, jelszókezelő alkalmazás, tűzfal, stb.), személyes adataink védelme, valamint a kritikus szemlélet az internetes ajánlatokkal szemben.

A kiberhigiéniai szemléletnek fontos aspektusa, hogy egyéni szinten történjen meg a napi rutin kialakítása, legyen egyfajta belső igény rá. A kiberhigiénikus viselkedés érdekében javasolt a napi hírfolyamokban a biztonságot érintő híreket is olvasni, tájékozódni. A kiberbiztonság, az adatvédelem mindenkit érint és nem csak az informatikusok feladata a védelem megalkotása. Egyéni törekvések és fejlődések nélkül nem fog a védelem kialakulni.

5. EMELT SZINTŰ KIBERTUDATOSSÁG

5.1. Stratégiák, Egyezmények

Az általános kibertudatosságon túl érdemes elmélyülni bizonyos törvényi, szabályozói és stratégiai összefüggésekben. Ezen összefüggések rávilágítanak a kibertér összefüggéseire és mélyebb betekintést adnak a folyamatok összetettségére.

Az információs rendszerek, a bennük előállított, tárolt, továbbított adatok, valamint a felhasználók által alkotott kibertér biztonsága érdekében szükséges, hogy nem csak az Európai Unió szintjén, de tagállami szinten is, így Magyarország is rendelkezzen azokkal a minimumképességekkel, amelyek biztosítani tudják a megfelelő szintű védelmet, és amelyek képessé teszik az országot a nemzetközi együttműködésekben való eredményes részvételre. A kapcsolódó, nemzeti szinten megvalósítandó feladatok legmagasabb szintű dokumentuma a Nemzeti Kiberbiztonsági Stratégia. A jelenlegi stratégiát 2013-ban fogadták el, így pusztán a „korát" tekintve egyáltalán nem számít elavult dokumentumnak még nemzetközi szinten sem.

5.1.1. Nemzeti Kiberbiztonsági Stratégia

A stratégia célja,hogy „az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján 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. A stratégia célja a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme a XXI. század meghatározóvá vált új közege, a kibertér létrejöttének következtében megváltozott nemzeti és nemzetközi környezetben. Célja továbbá a nemzetgazdaság és társadalom szabad tevékenységének védelme és biztonságának garantálása, az új technológiai innovációk biztonságos adaptálása a gazdaság növekedésének biztosítása érdekében, valamint nemzetközi együttműködések kialakítása ezen a téren a magyar nemzeti érdekek szerint. Jelen stratégia jelzi, hogy Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel vállalja és a magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét szabad, biztonságos és innovatív környezetté kívánja alakítani. A megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése.

Jelen stratégia Magyarország Alaptörvényében megfogalmazott alapértékek – szabadság, biztonság, jogállamiság, nemzetközi és európai együttműködés – leképezése egy külön biztonság-, és gazdaságpolitikai területre, az Alaptörvény 38.cikkéből levezetett, a nemzeti vagyon részét képező nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények kiberbiztonságának dokumentuma. A stratégia összhangban az 1035/2012. (II. 21.) Korm. határozattal elfogadott Magyarország Nemzeti Biztonsági Stratégiájával, abból kiindulva kifejti annak a kiberbiztonságról szóló 31. pontjában meghatározott törekvéseket és megfogalmazott kormányzati felelősséget. Gyökereiben a 2001-ben elfogadott Budapesti Konvencióig nyúlik vissza („Convention on Cybercrime"), mely

nemzetközi egyezmény napjainkban is referenciaként használt, nemzetközileg elfogadott alapelveket fogalmaz meg. A stratégia egyben igazodik az Európai Parlament által 2012. november 22-én elfogadott, „A kiberbiztonságról és védelemről szóló", 2012/2096 (INI) számú határozatában a tagállamok felé megfogalmazott ajánlásokhoz, valamint az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én „Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleményhez. A stratégia illeszkedik továbbá a NATO 2010 novemberében elfogadott Stratégiai Koncepciójához, a Szövetség 2011 júniusában elfogadott Kibervédelmi Politikájához és ennek végrehajtási tervéhez, valamint a 2010. november 19–20-ai lisszaboni és a 2012. május 20–21-ei chicagói NATO-csúcs dokumentumaiban megfogalmazott Szövetségi kibervédelmi elvekhez és célokhoz."[27]

Mint látszik a stratégia megfogalmazásában is, több olyan szervezet, rendelet, nemzetközi egyezmény is szerepel benne, amely megalapozta és amelyhez igazodik nem csak a magyar, hanem több EU-s illetve EU-n kívüli ország kiberstratégiája is.

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:

1. Kormányzati koordináció: a kormányon belüli, továbbá az állami, gazdasági, tudományos és civil szereplők közötti együttműködés koordinációjának elősegítése és a végrehajtás figyelemmel kísérése a Miniszterelnökség keretein belül létrehozott testület révén.
2. Együttműködés: olyan operatív együttműködési fórumok működtetése, amely a civil, a gazdasági és a tudományos területek képviselőinek részvételét biztosítja a kormányzati döntés-előkészítési folyamat során és lehetőséget nyújt arra, hogy ezen fórumok tagjai ajánlásokat és véleményt fogalmazzanak meg a kiberbiztonsági tevékenység fejlesztésére, folyamatos újítására.
3. Szakosított intézmények: egymással, valamint az adat- és titokvédelem területén hatósági feladatokat ellátó más szervezetekkel is együttműködő, speciális szakértelemmel és hatáskörrel rendelkező szervezetek általi feladatellátás a kibervédelem terén [pl. az európai kormányzati incidenskezelő csoport (European Governmental CERT Group) által akkreditált tagszervezetként működő kormányzati eseménykezelő központ és az egyes szakágazatok területén működtetett ágazati eseménykezelő központok].
4. Szabályozás: többszintű (törvényi, kormányrendeleti és miniszteri rendeleti szintű) jogalkotási tevékenység és együttműködési megállapodások a civil, a gazdasági és a tudományos terület szereplőivel.
5. Nemzetközi együttműködések: Magyarország aktív szerepének további erősítése az EU és a NATO keretein belül folyó kibervédelmi kezdeményezésekben, együttműködésben és kibervédelmi gyakorlatokban, valamint az ENSZ és az EBESZ kiberbiztonsági együttműködéseiben. Szerepvállalás a nemzeti/kormányzati és ágazati incidenskezelő központok európai, atlanti és globális szervezeteiben, az Európai Hálózati és Információ Biztonsági Ügynökségben, valamint az Európai Elektronikus Hírközlési Hatóságok Testületében.
6. Tudatosság: 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.
7. Oktatás, kutatás-fejlesztés: 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.

[27] http://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf

8. Gyermekvédelem: a Gyermekbarát Internet Európai Stratégiája célkitűzéseinek figyelembevételével 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.
9. Gazdasági szereplők motivációja: olyan intézkedések kidolgozása a gazdasági szereplők számára, amelyek a kiberbiztonság fokozását célozzák, így különösen az informatikai és hírközlési közbeszerzések kapcsán olyan kiberbiztonsági követelmények meghatározása, amelyek során a lehető legmagasabb szintű kiberbiztonsági védelem kialakítására ösztönzik a közbeszerzéseken résztvevő informatikai és hírközlési eszközgyártókat és szolgáltatókat.

5.1.2. Budapesti Konvenció

Az Európa Tanács 2001. november 23-án Budapesten fogadta el a „Számítástechnikai bűnözésről" szóló egyezményt. Az egyezmény 2004. július 1-jén lépett életbe, miután az Európa Tanács 5 tagállama – köztük hazánk – ratifikálta azt. 2011. október 1-ig az Európa Tanács 31 tagja és az Egyesült Államok ratifikálta az egyezményt.

Az egyezmény védeni kívánja a számítástechnikai rendszerek, hálózatok, adatok hozzáférhetőségének sérthetetlenségét, az ilyen rendszerek titkosságát; biztosítani a rendszerek, hálózatok, adatok visszaélésszerű használatának megelőzését. Az egyezmény bűncselekménnyé nyilvánítja az ilyen eseteket. Továbbá meghatározza a kiberbűnözés elleni hatékony fellépést lehetővé tevő felderítést, nyomozást és üldözést nemzeti és nemzetközi szinten biztosító jogköröket és rendelkezéseket.

5.1.3. Digitális Jólét Program

A magyar kormány 2015-ben fogadta el a Digitális Jólét Programot (DJP), azzal a célkitűzéssel, hogy a fejlesztési programok eredményeképpen a hazai IKT-szektor kiegyensúlyozottantudjon fejlődni, lehetőséget nyújtva a versenyképességnek, a fenntartható gazdasági növekedésnek, a foglalkoztatásnak és a társadalmi esélyegyenlőségnek az infokommunikációs eszközök és szolgáltatások segítségével. A DJP program az indulás óta továbbfejlődött, kiegészítő célok és stratégiák kerültek meghatározásra, illetve hatással van egyéb stratégiák kialakítására is (pl. oktatási stratégia).

5.1.4. Stratégia alkotás az EU-ban

Az Európai Bizottság, mint az Európai Unió döntés-előkészítő, végrehajtó, döntéshozó, ellenőrző és képviseleti szerve (az Európai Parlament és az Európai Unió Tanácsa mellett a három fő uniós kormányzati intézmény egyike) először 2001-ben, „Hálózat- és információbiztonság: javaslat egy európai politikai megközelítésre" című közleményében hívta fel a figyelmet a hálózat- és információbiztonság növekvő jelentőségére. Ezt 2006-ban követte a biztonságos információs társadalomra irányuló stratégia elfogadása, amelynek célja az európai hálózat- és információbiztonsági kultúra kialakítása volt. 2009-ben jelent meg a kritikus informatikai infrastruktúrák védelméről (CIIP) szóló bizottsági közlemény, amely Európa hálózati zavarokkal szembeni védelmével foglalkozott. Az Európai Bizottság mellett az Európai Unió Tanácsa – mely az Európai Parlamenttel együtt az Európai Unió törvényhozó szerve – is foglalkozott az információbiztonság kérdésével, amikor 2009-ben állásfoglalást adott „a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről".

Érzékelhető, hogy az Európai Unió bár felismerte az információbiztonság tárgykörének fontosságát, korábban csupán közlemények, állásfoglalások szintjén foglalkozott a témával. A megelőzés, észlelés és elhárítás terén megvalósítandó feladatokat általános és kötelező jelleggel előíró jogszabályok elfogadására uniós szinten akkor még nem került sor.

Az Európai Unió először az információs rendszerek elleni támadások szankcionálása tárgyában alkotott konkrét szabályokat. Az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat[28] célja a tagállami büntetőjogszabályok harmonizálása a tagállamok igazságügyi és egyéb hatóságai – így a rendőrség és egyéb bűnüldözési szakszolgálatok – közötti együttműködésének javítása érdekében.

A kerethatározat egy olyan uniós jogi eszköz, amely a tagállami jogi és a közigazgatási előírások harmonizálását szolgálja. A kerethatározatban megfogalmazott cél megvalósítása a tagállam számára kötelező feladat, de a végrehajtási formáját és eszközét a tagállamok szabadon választhatják meg (pl. a meglévő jogszabályaikat módosítják, vagy új jogszabályt alkotnak). Nem közvetlen hatályú, tehát a magánszemélyek a nemzeti vagy az európai bíróságok előtt közvetlenül nem hivatkozhatnak a kerethatározatban foglaltakra.

A kerethatározat alapvetően büntetőjogi megközelítést alkalmaz, rögzíti, hogy melyek azok a cselekmények, amelyek megvalósítását a tagállamoknak legalább jelentősebb bűncselekménynek kell minősíteniük, milyen szempontok mentén kell meghatározni a szankciókat, melyek a súlyosbító körülmények és miként alakul a jogi személyek felelőssége és szankcionálása. A Büntető Törvénykönyvről szóló 2012. évi C. törvény (továbbiakban: Btk.) 375. §-a és XLIII. fejezete ezen kerethatározatban foglaltakkal összhangban került megalkotásra.

További, az információbiztonság témaköréhez kapcsolódó szektorális szabályok megalkotására került sor az elektronikus hírközlés (2009/136/EK irányelv), a személyes adatok védelme (95/46/EK irányelv), az általános adatvédelem (a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló rendelet tervezete) és a létfontosságú rendszerelemek védelme (2008/114/EK irányelv) terén. Ezek az irányelvek olyan európai uniós jogi aktusok, amelyek az elérendő célok tekintetében kötelezik a tagállamokat, de az általános cél megvalósításának konkrét formáját, a megfelelő eljárásokat és eszközöket a tagállamok maguk választják meg.

A tagállamoknak kötelességük, hogy az irányelvben foglaltak meghatározott időn belül nemzeti jogszabályaikban meghatározásra kerüljenek, azaz jogszabályi szinten rögzíteni kell az előírásokat.

Az Európai Bizottság 2010 májusában mutatta be az Európai Digitális Menetrend című akciótervét, melynek célja a gazdasági fellendülés felgyorsítása és a fenntartható digitális jövő alapjainak megteremtése. A cselekvési terv hét kiemelt intézkedési területet határozott meg, melyek közül az egyik az internet iránti bizalom és a biztonság erősítése, figyelemmel arra, hogy a fent említett kerethatározatban foglaltak ellenére az információs rendszerek elleni támadások száma továbbra is nőtt. A Bizalom és biztonság intézkedési területen célként került meghatározásra:

1. a javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;
2. a 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;
3. a javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról;
4. a tudatosságnövelés, így többek között az internetes védelem iskolai oktatása;
5. egyebek mellett a gyermekbántalmazással, a személyazonosság-lopással és számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása;

[28] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:l33193

6. a magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten és azon kívül egyaránt.

Az Európai Bizottság felismerte, hogy a Digitális Menetrendben foglaltak érvényesítése érdekében a büntetőjogi aspektus vizsgálata és kiteljesítése mellett uniós érdek a kiberbiztonság kérdéskörének átfogó, stratégiai szintű áttekintése. Erre figyelemmel az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága 2013 februárjában közzétette közös közleményét „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" című uniós stratégiáról (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.) a 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 teljesítését célozza a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvjavaslat (továbbiakban: irányelvjavaslat). Az irányelvjavaslat előírja, hogy:

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 információmegosztás 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.

A korábbi fejezetekből látható, hogy ezen stratégiák milyen intézkedések és rendeletekhez vezettek, illetve alapvetően hogyan határozzák meg a következő évek EU-s és hazai kiberstratégiáját. A következő években várhatóan folytatódni fog az EU-s határok – mind fizikai, mind pedig digitális értelemben – történő lezárása olyan tekintetben, hogy egyfajta biztonságos kereskedelmi zóna kerül kialakításra, amelyen belül egységes biztonsági, megfelelőségi és törvényi keretek között lehet élni,kereskedni és jelentős hangsúly kerül a gazdasági szankcionálásra (pl.: GDPR büntetési mechanizmus).

5.2. MULTINACIONÁLIS SZERVEZETEK

Számos olyan multinacionális szervezet létezik, amely hatással van a magyar ésa nemzetközi stratégiákra, rendeletekre egyaránt. A legkézenfekvőbb ilyen nemzetközi szervezet, amely kihat a magyar jogszabályi környezetre az Európai Unió, de az EU mellett érdemes a következő szervezeteket is közelebbről megismerni:

5.2.1. NATO

A NATO avagy Észak-atlanti Szerződés Szervezete egy politikai és katonai szövetség, jelenleg 29 ország a tagja. Kiberbiztonság szempontjából kiemelt fontossággal bír a NATO CCD COE avagy a NATO Cooperative Cyber Defense Centre of Excellence, azaz a NATO kiberbiztonsági kiválósági központja, amely Tallinnban található. Ez a központ világszínvonalú technológiai, stratégiai, operatív és jogi fejlesztéseket végez. Ezen központnak támogatója (sponsoring nation) Magyarország is.

5.2.2. Európai Biztonsági és Együttműködési Szervezet (EBESZ)

A legátfogóbb páneurópai biztonsági szervezet, 57 résztvevő + 11 partner állammal. Az EBESZ az ENSZ Alapokmány VIII. fejezete által meghatározott regionális szervezet. Az európai biztonság és stabilitás megőrzése érdekében gyakorolt fő funkciói: a korai előrejelzés, a konfliktusmegelőzés, a válságkezelés és a válságok megoldását követő rehabilitáció.

A biztonságot átfogó és kooperatív módon kezeli, mivel a biztonság minden szektorával egységesen foglalkozik. 2014. november 7-én tartott egyeztetéseken már kiemelt hangsúlyt kapott a tagországok kibereseményekkel kapcsolatos információmegosztásának jelentősége.

5.2.3. Global Forum on Cyber Expertise (GFCE)

Olyan globális szervezet, amely elsődleges célja, hogy megteremtse a kormányok, vállalatok és nemzetközi szervezetek információcseréjének platformját, ezáltal elősegítve a legjobb gyakorlatok globális elterjedését, illetve elősegítse a kiberkapacitás fejlesztését.

5.2.4. International Telecommunication Union (ITU)

Az ENSZ telekommunikációs egyesülete. Globális rádióspektrumokat és műholdas keringtetésekkel kapcsolatos kiosztásokat végeznek, illetve olyan technikai szabványokat dolgoznak ki, amelyek biztosítják a hálózatok és a technológiák összekapcsolódását, valamint célja, hogy javuljon az információs és kommunikációs technológiákhoz való hozzáférés világszerte.

Emellett rendszeresen elkészítik az úgy nevezett Global Cybersecurity Index-et (GCI), amely azt méri, hogy a tagországok mennyire követik és implementálják az ITU globális kiberbiztonsági ajánlásait, kimutatva a fejlődési, illetve a fejlesztési lehetőségeket és hiányosságokat.

5.2.5. Nemzetközi jog

A kibertér szabályozottsága, mint a korábbiakból látszik, jelentősen eltér térségről térségre és országról országra, még az EU-n belül is. Ennek mélyebb megismerésére a fentebb említett ITU GCI nagyon jó eszköz, amely alapján rendszerezetten látszik a különböző országok értékelése.

Törekvések mégis vannak, hogy létrejöjjön egyfajta közös értelmezése a kibertér jogi aspektusának. Ezeket a javaslatokat, valamint gyakorlatokat dolgozták ki és összegezték a Tallinn Manual című munkában, amelynek kettő kötete is megjelent már.

Az első kötet a „*Tallinn Manual on the International Law Applicable to Cyber Warfare*", 2013-ban jelent meg, hiánypótló kiadványként a témában, a NATO CCD COE munkatársai munkássága által. Ennek frissített illetve kiegészített verziója a "*Tallinn Manual 2.0*", amely 2017-ben jelent meg. Míg az első könyv főleg a katonai szempontok alapján vizsgálta a jogot és a kibertámadásokra adható válaszokat, addig a második kiadás már egy általánosabb megközelítésben vizsgálja és értelmezi a kibertérből érkező eseményeket.

5.3. Szabványok és minősítések

Szabványosítás: „olyan tevékenység, amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen."[29]

A szabványosítás definíció szerint olyan tevékenység, amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen. Esetünkben az informatikai biztonsági kihívásokra adott válaszok optimalizálása a céljuk.

A szabványosítás feladata a szabványok kidolgozása, kibocsátása, és alkalmazása. A szabványosítás eredménye fokozza a termékek, eljárások, szolgáltatások rendeltetésszerű alkalmasságát, elhárítja a kereskedelem termékekkel, szolgáltatásokkal kapcsolatos technikai akadályait és elősegíti a technológiai együttműködést. Egységesíti például a rajzjeleket, a terminológiát, a vizsgálati módszereket és a betartandó követelményeket.

A szabványosításnak több szintje van, melyek közül a legmagasabb a nemzetközi szabványosítás, ebben bármely ország illetékes szervei részt vehetnek. Nemzetközi szintű szabványügyi szervek a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO), melynek hazánk 1947 óta tagja, a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, IEC) és a Nemzetközi Távközlési Unió (International Telecommunication Union, ITU), amely az ENSZ szakosított szerve.

A regionális szabványosítás olyan szabványosítás, amelyben a világ csak egy meghatározott földrajzi, politikai vagy gazdasági területéhez tartozó országok illetékes testületei vehetnek részt. Regionális szabványügyi szervek például az Európai Szabványügyi Bizottság (Comité Européen de Normalisation, CEN), Európai Elektrotechnikai Szabványügyi Bizottság (Comité Européen de Normalisation Electrotechnique, CENELEC) és az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute, ETSI).

A nemzeti szabványosítás egy meghatározott ország szintjén folyó szabványosítás. Nemzeti szabványügyi szervek például a Magyar Szabványügyi Testület (MSZT), British Standards Institution (BSI), Deutsches Institut für Normung e.V. (DIN), és az American National Standards Institute (ANSI).

Vállalati szabványosításról beszélhetünk, ha a gazdasági társaság a saját szervezetén belül érvényes, általában kötelező, többnyire termékhez kapcsolódó műszaki előírást készít és alkalmaz, biztosítja a nemzeti szabvány vállalati szintű végrehajtását. A vállalati szabványok betartását a beszállítótól is megkövetelhetik.

Látható, hogy a szakmai kompetencia tekintetében a magasabb szinteken egy távközlési, egy elektrotechnikai és egy általános szabványügyi szerv került megalakításra. Az ilyen szervezetekben műszaki bizottságok (Technical Committee, TC) végzik az operatív munkát. Manapság a fent ismertetett

[29] http://www.tankonyvtar.hu/en/tartalom/tamop425/0019_1A_Egeszsegugyi_informatika/ch01s04.html

hierarchikus rend mellett sok esetben összetettebb a helyzet az informatikai szabványosítás területén és sok olyan szervezet készít de facto szabványokat, amelyek eddig nem végeztek ilyet.

A számítógéprendszerek és hálózatok eredő biztonságát az egyes építőelemek közül a leggyengébbnek a biztonsága határozza meg (leggyengébb láncszem elve). A szabványok alkalmazásának a legnagyobb előnye ezen gyengeségek kiküszöbölése azáltal, hogy minden elemet egyenlő szintre hoz. A szabványok nélküli biztonság-kialakítás lehetséges, de nem megbízható, hiszen nem lehet a szabványosságot, mint formális objektív mércét használni. Az informatikai biztonság megfelelőségének biztosítása más esetekben is szükséges lehet, mint például minőségirányítási rendszer bevezetése, megfeleltetés (compliance) vagy beszállítói audit esetén.

A szabványok alkalmazása a magyar jog szerint nem kötelező, de természetesen érdemes. Az egyenszilárdságú informatikai biztonság kialakításának ez a legcélszerűbb módja, viszont kötelező erő hiányában a megvalósítás nem várható el. A kérdés az, hogy hogyan lehet a szabványok jó technológiai szint-követését és jól definiáltságát a kötelező erővel rendelkező jogi követelményekkel összemérni.

A gyakorlatban az informatikai biztonsági szabványok az informatikai biztonságot szabályozó jogszabályokhoz hasonlóan nem egységesek.

A számítástechnika őskorában, az 1960-70-es években a kötegelt feldolgozású „mainframe" számítógépek esetében a külön szabványalkotás a jogi szabályozás megalkotásához hasonlóan nem volt szükséges, a hagyományos papíralapú titokvédelmi eljárások megfelelően működtek. A több felhasználós, erőforrásokat megosztó rendszerek támasztottak először új igényeket, amire válaszként 1970-ben szakértői jelentés készült „Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security" címmel. A dokumentum elemezte az új kockázatokat és javaslatot tett a bevezetendő intézkedésekre. 1972-ben jelent meg az egyik első követelményrendszer Computer Security Technology Planning Study, amelyet az Air Force Systems Command készített.

Azóta sok idő eltelt és a technológiai fejlődéssel a szabványok is fejlődtek, igyekezve lefedni a legújabb technikai megoldásokat és kockázatokat figyelembe véve a törvényi megfeleltetéseket. Kiberbiztonsági vonatkozásban általánosságban az amerikai NIST Cyber Security Framework, az ISO 27001, a Common Criteria szabványok a legelterjedtebbek, de természetesen iparági tevékenységtől függően más szabványok is előfordulnak.

5.4. People Process Technology - PPT

Az információ biztonságos kezelésének és védelmének feltétele és alapja az ún. információbiztonsági PPT modell mindhárom elemének, az ember(people), a szabályozás(policy/process) és a technológia(-technology) megfelelő, együttes kezelése. Az ember, szabályozás, és a technológia hármas felosztása a folyamatirányítási PPT modellre (People, Process, Technology) vezethető vissza. Az információbiztonság úgy értelmezi ezt a felosztást, hogy az információnak a három halmaz metszéspontjában szükséges elhelyezkedni a biztonságos állapot megteremtéséhez. Ez azt jelenti, hogy az alkalmazott technológiának összhangban kell lennie a bevezetett biztonsági intézkedésekkel és a felhasználók, üzemeltetők képességeivel, képzettségeivel, motiváltságaival.

Abban az esetben, ha ezen elemek közül bármely kezelése nem megfelelő, avagy nem megfelelő a menedzsment támogatása a helyes kezelés kialakításában, akkor az információ veszélynek van kitéve, azaz az információ biztonságos kezelése nagy valószínűség szerint sérül.

Egy információs rendszer folyamatos változásban van. Adott környezetben folyamatosan jelennek meg például új fejlesztések, ezáltal avulttá válhatnak a régi eszközök. Új beszerzésekkel további eszközök kerülnek a rendszerbe, ezzel tovább növelve annak heterogenitását, továbbá az alkalmazottak fluktuációja is elkerülhetetlen, mely szintén komoly kockázatot hordoz magában az újabb dolgozók információbiztonság-tudatosságának megfelelő szintre emelése időt vesz igénybe, és ez az időbeli delta sérülékenység-ablakot képez a rendszer védelmi képességeit csökkentve.

Az információ védelmére törekvő harmonikus együttállást folyamatosan gyengíti az összes halmaz egymástól történő eltávolodása. A két-két halmaz közti eltávolodások különböző kockázat növelő faktoroknak adhatnak teret. Ezen faktorok a szándék (ember a szabályozással szemben, illetve attól eltávolodva), a sebezhetőség (ember a technológiával szemben, illetve attól eltávolodva) és a lehetőség (szabályozás a technológiával szemben, illetve attól eltávolodva). A halmazok egymástól való eltávolodásának kezelése elengedhetetlen egy biztonságos rendszer fenntartásához.

Az esetleges kártékony szándék az ember és a szabályozás halmazok távolodásakor kap teret. A probléma alapja, hogy a biztonsági szint gyengül, ha a felhasználók és üzemeltetők nem tartják be a biztonsági házirendet vagy a vonatkozó, ilyen tartalmú dokumentumot -vagy nem is létezik ilyen házirend/szabályozás. Megoldás: a felsővezetésnek úgy kell kialakítania a mindenkor aktuális házirendet, hogy azt a rendelkezésre álló körülmények között a felhasználók be kell, hogy tudják tartani és ezzel párhuzamosan megfelelően motiváltak is legyenek e szabályozások irányában.

A felhasználók szándékának befolyásolására képes egy szervezet a három lehetséges kockázati faktor közül a legegyszerűbben és a legkisebb anyagi ráfordítást igénylően, információbiztonság-tudatosítás képzéseken keresztül hatást gyakorolni. Közvetett hatásként is bezárulhat az ember-szabályozás olló, a kártékony szándék számára nem hagyva lehetőséget, ez azonban csak a többi két probléma helyes kezelése mellett lehetséges.

A gyakorlatban a kártékony emberi szándék azért nem nyerhet teret a másik két probléma (sérülékenység, lehetőség) kezelésével, mert a támadónak túl nagy energia-befektetésre lenne szüksége ahhoz, hogy megérje számára kompromittálni a rendszert, például egy jelszavak és hozzáférések megszerzésére irányuló, de a szervezet felhasználóinak magas információbiztonság-tudatossága miatt sikertelen social engineering kampány esetén. (A sikertelen kampány ebben az esetben arra utal, hogy a szervezet dolgozói képesek felismerni a social engineering mögötti káros szándékot, és adott esetben nem adják ki a saját hozzáféréseiket jogosulatlan támadó számára, ezzel a jogosulatlan támadónak csak a technikai eszközökkel történő behatolás lehetőségét hagyva meg.).

A rendszerek információbiztonsági szintje gyengül akkor, ha az alkalmazott technológia nem képes támogatni az aktuális biztonsági házirendet, vagy más vonatkozó szabályozókat. Ha a technológia nem képes megvalósítani a házirendben támasztott követelményeket, hiába lesz megfelelő, erős szabályozás, az hamis biztonságtudatot eredményez a vezetésben. Problémát jelent ennek a fordítottja is, ha a házirend nem követi a technológiai lehetőségeket, melynek azonnali következményeként a jelentős, vagy megfelelő összegű biztonsági fejlesztések nem érik el a hatásukat (az alkalmazott információbiztonsági technológia drága, mégis hatástalan lesz). Megoldás: a felsővezetők számára szükséges világossá tenni azt, hogy a technológiai háttér fejlesztése és/vagy a szabályozók technológiához történő felzárkóztatása, a technológia és a szabályozók harmóniában tartása elengedhetetlen, különösen abban a tekintetben, hogy a szabályozóknak az alkalmazott technológiához igazítása töredék költségráfordítást igényel a szükséges technológiai fejlesztések jellemző költségigényével szemben

Az információ biztonsága szempontjából a legkritikusabb állapot az, ha a felhasználók, üzemeltetők képzettségi szintje nem alkalmas az aktuális, alkalmazott technológia kezelésére. Minél jobban távolodik a technológia fejlettségi szintje a kezelő személyzet felkészültségi szintjétől, a tudásolló annál nagyobbra nyílik, ezáltal egyre nagyobb lesz a megfelelő szakértelem hiányából adódó sérülékenységek mennyisége, melyek jogosulatlan, esetlegesen rosszindulatú felhasználók által kihasználhatók. Megoldás: a felhasználó, üzemeltető személyzet képzése, és megfelelően képzett szakemberek alkalmazása. Az alkalmazott információvédelmi technológia és azzal párhuzamosan a támadási technológiák, módszerek folyamatos fejlődése miatt elengedhetetlen a szakértők folyamatos vagy rendszeres továbbképzési lehetőségének megteremtése.

ÖSSZEGZÉS

Jelen tananyag kereteibe számtalan téma nem fért bele, illetve az itt taglalt témáknak is vannak még mélyebb rétegei, azonban aki aktívan érdeklődik a téma iránt, annak jó hír, hogy hazai szinten is egyre több képzési és tájékozódási lehetőség érhető el.

Szervezeti, illetve egyéni szinten a biztonságtudatosság megteremtése nem egyszerű feladat, de alapvető szükséglet. Az utóbbi két évtized során mind a szervezetek, mind pedig az egyének vonatkozásában a biztonság által felölelt terület növekvő tendenciát mutat, és egyre inkább lefed olyan területeket is, amelyeket korábban nem. A kiberbiztonság, mint ahogyan látszik, egy nagyon átfogó terület és az élet minden szintjén megjelenik, ahol informatikai eszközöket használnak.

A kiberbiztonsági kérdés és kihívás elsősorban nem technológiai , hanem emberi kérdés. Léteziktechnológiai összetevője is a biztonsági megoldásoknak, de alapvetően emberi probléma. Fontos, hogy közös problémaként közelítsünk a kérdéshez és ennek megfelelő hozzáállással kezeljük. A kibertudatos viselkedés és a személyes kiberhigiénia megteremtése nem választható, hanem kötelező eleme kell, hogy legyen életünknek, ezáltal megteremtve az információtechnológiai eszközök és lehetőségek biztonságos használatát.

JOGSZABÁLYTÁR

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
2010. évi XLIII. törvény a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról
1995. évi CXXV. törvény a nemzetbiztonsági szolgálatok működéséről
233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről
36/2013. (VII. 17.) BM rendelet a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
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.
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

IRODALOMJEGYZÉK

Ashford, Warwick: BlackHat 2015: RiskIQ Reports Huge Spike in Malvertising. ComputerWeekly.com, 2015. augusztus 4.
http://www.computerweekly.com/news/4500251077/BlackHat-2015-RiskIQ-reports-huge-spike-in-malvertising (utolsó letöltés: 2018. január 2.)
Deschartres, Solange: 7 Security Tips To Protect Your Mobile Workforce. Symantec Blog, 2014. június 30.
http://www.symantec.com/connect/blogs/7-security-tips-protect-your-mobile-workforce (utolsó letöltés: 2018. január 2.)
Graham, Robert: How Hackers Will Crack Your Password. InformationWeek DarkReading, 2009. január 21.
http://www.darkreading.com/risk/how-hackers-will-crack-your-password/d/d-id/1130217 (utolsó letöltés: 2018. január 2.)
Keller, Joy: How Businesses Stay Safe and Secure Using Social Media. Webroot, [s.d.].
http://www.webroot.com/us/en/business/resources/articles/social-media/how-businesses-stay-safe-and-secure-using-social-media (utolsó letöltés: 2018. január 2.)
Kjaersgaard, Morten: How You Can Get Infected via World Wide Web Exploits. Heimdal Security, 2015. március 3.
https://heimdalsecurity.com/blog/internet-browser-vulnerabilities/ (utolsó letöltés: 2018. január 2.)
LeVar Balttle, Sr.: Top 11 Security resolutions for the New Year. Webroot, 2015. december 29.
https://www.webroot.com/blog/2015/12/29/top-11-security-resolutions-for-the-new-year/ (utolsó letöltés: 2018. január 2.)
Needle, David: How a Security CEO Fell Prey to Scammers (Almost). RSA Conference, 2016. március 3.
http://www.rsaconference.com/blogs/security-ceo-scammers#sthash.egMiB2xW.dpuf (utolsó letöltés: 2018. január 2.)
Pinola, Melanie: The Top 10 Usernames and Passwords Hackers Try to Get into Remote Computers. Lifehackers, 2016. március 3.
http://lifehacker.com/the-top-10-usernames-and-passwords-hackers-try-to-get-i-1762638243 (utolsó letöltés: 2018. január 2.)
Siciliano, Robert: 11 Tips to Secure Mobile Devices and Client Data. Entrepreneur, 2015. június 11.
http://www.entrepreneur.com/article/246814 (utolsó letöltés: 2018. január 2.)
Svajcer, Vania: When Malware Goes Mobile: Causes, Outcomes and Cures. SophosLabs, 2015.
https://www.sophos.com/enus/medialibrary/Gated%20Assets/white%20papers/Sophos_Malware_Goes_Mobile.pdf (utolsó letöltés: 2018. január 2.)
Szádeczky Tamás: Információbiztonsági szabványok. Budapest: NKE, 2014.
https://www.tilb.sze.hu/tilb/targyak/NGB_TA0028_1/informaciobiztonsagi-szabvanyok.original.pdf (utolsó letöltés: 2018. január 2.)

*

HUNCERT – Szolgáltatók – Tudásbázis – Szabványok, ajánlások – Szabványok, kvázi szabványok, ipari szabványok – Magyar informatikai biztonsági szabványok
http://www.cert.hu/magyar-informatikai-biztonsagi-szabvanyok (utolsó letöltés: 2018. január 2.)
Lockheed Martin – What We Do – Aerospce & Defense – Cyber Solutions
http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html (utolsó letöltés: 2018. január 2.)
Subrananian, Latha & Liu, Jianhong & Winterdyk, John: Cyber-Terrorism and Cyber Security: A Global Perspective. 2016, október
https://www.researchgate.net/publication/308983209_Cyber-Terrorism_and_Cyber_Security_A_Global_Perspective (utolsó letöltés: 2018. január 2.)
This one chart explains why cybersecurity is so important. Business Insider, 2016. május 4.
www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3 (utolsó letöltés: 2018. január 2.)
***
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (utolsó letöltés: 2018. január 2.)
A Kormány 2012/2015. (XII. 29.) Korm. határozata az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról
http://www.magyarkozlony.hu/hivatalos-lapok/309ef8a8f595ea39b407b514a69963e2d9e000c1/dokumentumok/85daf8e78042dda-84e541bf5d8f46dd13b52545a/letoltes (utolsó letöltés: 2018. január 2.)
Anglia Ruskin University Library: Harvard System of Referencing Guide. 2008.
https://libweb.anglia.ac.uk/referencing/harvard.htm (utolsó letöltés: 2017. január 6.)
Bodó Attila Pál, Dr.: Információbiztonsági jogi ismeretek vezetőknek. Budapest: NKE, 2014.
http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10084/Inform%C3%A1ci%C3%B3biztons%C3%A1gi%20jogi%20ismeretek.pdf?sequence=1&isAllowed=y (utolsó letöltés: 2018. január 2.)
Nemzeti Infokommunikációs Stratégia 2014-2020. Az infokommunikációs szektor fejlesztési stratégiája, 2014.
http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (utolsó letöltés: 2018. január 2.)

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó: Nemzeti Közszolgálati Egyetem; Államtudományi és Közigazgatási Kar • 1083 Budapest, Üllői út 82. • Felelős kiadó: Prof. Dr. Kis Norbert Dékán • www.uni-nke.hu • Kiadói szerkesztők: Kotró Szimonetta, Stránglí Szandra • Tördelőszerkesztő: Bödecs László

ISBN 978-615-5057-78-6 (PDF)

A kiadvány a KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése” című projekt keretében készült el és jelent meg.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE