Balogh Zsolt György

AZ INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSA

Nemzeti Közszolgálati Egyetem,

Budapest

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

A kiadvány
a **KÖFOP-2.1.2-VEKOP-15- 2016-00001 „A jó kormányzást megalapozó közszolgálat-fejlesztés”** című projekt keretében készült el és jelent meg.

Szerző:
© Balogh Zsolt György PhD
egyetemi docens

A kézirat lezárva
2018. augusztus 1.

TARTALOMJEGYZÉK

1. AZ INFORMÁCIÓS TÁRSADALMAT ÉRŐ KIHÍVÁSOK ÉS FENYEGETÉSEK

A cégek és a közfeladatot ellátó szervek – informatikai biztonság szempontjából szinte mindegy, hogy állami, önkormányzati vagy egyéb fontos közfeladatot ellátó szervről van-e szó – hatalmas és egyre nagyobb mennyiségű adatot kezelnek. Ezek az adatok lehetnek személyes adatok, üzleti titkok, szabadalmak, egyéb védett ismeretek vagy közbiztonsági, bűnüldözési, bűnmegelőzési szempontból kritikus adatok.

A szervezetek biztonságos működése, mint láttuk, egyre nagyobb mértékben ki van téve – ki van szolgáltatva – az általuk kezelt adatvagyonnak. Számos területen a szervezet működése lényegében ellehetetlenül, ha az adatállományaihoz nem fér hozzá. Ennek a szervezet szűkebb értelemben vett határain messze túlterjedő következményei lehetnek. A 2018. április 8-án tartott országgyűlési választásokat a politikai eseményeken és a választás eredményén kívül az is emlékezetessé tette, hogy a Nemzeti Választási Iroda informatikai rendszere a választás délelőttjén összeomlott, és a szolgáltatás teljeskörű helyreállítására lényegében egy teljes hetet kellett várnia a választói közvéleménynek, az ország politizáló közönségének[1]. Egy informatikai rendszer szolgáltatási képessége, rendelkezésre állása tehát a körülmények szerencsétlen együttállása esetén egy egész ország közvéleményét, politikai helyzetét, akár stabilitását is közvetlenül befolyásoló tényezővé nőheti ki magát.

1.1 Adatszivárgás lehetősége

Adatszivárgásról beszélünk, ha tetszőleges kommunikációs csatornán keresztül üzleti értéket képviselő vagy magántermészetű adat jogosulatlanul hagyja el a vállalatot. A bizalmas információk védelméhez egyre kevésbé elégséges a klasszikus, fájlrendszerbeli jogosultságokon alapuló hozzáférés-ellenőrzés. A biztonsági kihívásokra válaszolva új szemléletmóddal, a hagyományos módszereknél sokkal tágabban értelmezve kell az adatok lehetséges szivárgási útvonalait felderíteni és az ellenintézkedéseket megtenni.

- A cég valamely adatkezelést végző munkatársa véletlenül rossz ablakba illeszti be a vágólapra másolt bizalmas céges adatot, és visszavonhatatlanul elküldi egy online fórumba, blogba vagy egy nem megfelelő e-mail címre.

1 Heti Világgazdaság (2018).

- Hasonló helyzetet eredményezhet, ha az adatfeldolgozó munkatársa otthonról is folytatni szeretné a munkát, ezért egy félkész ajánlatot külső levelezőszerverre küld, amelyet bárhonnan kényelmesen elér.
- Egy elbocsátott dolgozó távozása előtt kinyomtatja a cég teljes ügyféllistáját vagy más érzékeny adatállományát, majd azzal együtt távozik.
- Egy rosszindulatú alkalmazott a titkos üzleti adatokat USB-kulcsra, CD/DVD-re lementve elviszi, és átadja a konkurenciának.
- A munkavállaló elveszíti valamely olyan okos eszközét (telefonját, tabletjét, laptopját), amelyen bizalmas e-maileket, dokumentumokat tárolt.

1.2 Informatikai bűnözés

Néhány évtizeddel ezelőtt az információs rendszerekkel való visszaélés, a kommunikációs hálózatok megbénítása, adatok illegális megszerzése vagy megváltoztatása még sokkal inkább számított a tudományos-fantasztikus irodalom egyik népszerű témájának, mint valóságos társadalmi problémákra irányuló biztonságpolitikai, kriminológiai, kriminalisztikai és büntetőjogi vizsgálatok tárgyának. A helyzet viszonylag rövid idő alatt változott meg; ránk köszöntött az információs forradalom korszaka, és a fejlett világnak szembe kellett néznie azzal a cseppet sem kellemes ténnyel, hogy a társadalom nemcsak haszonélvezője a modern információs technika „áldásainak", hanem kiszolgáltatott is a mindennapokat egyre jobban átszövő adatfeldolgozó és adattovábbító rendszereknek.

Naponta tapasztalhatjuk, hogy ma már integrált adatfeldolgozó rendszerek működnek a pénzügyi és bankvilágban, a közigazgatásban, az egészségügyi intézményekben, az energiaszolgáltató ágazatokban és a közlekedésben is – a repülésirányítástól a hajóforgalom navigációs rendszerein keresztül a vasúti szállításig. Az iparban a számítógépes tervezés és termelésirányítás éppúgy a mindennapi munka része lett, mint ahogy természetes, magától értetődő ténynek tekintjük a hadászati fegyverrendszerek számítógépes vezérlését vagy a műholdon keresztül történő televíziós műsorszórást. Ezek a rendszerek, noha általában megbízhatóan működnek, mégis jól tudjuk – vagy személyes tapasztalatból, vagy legalább a sajtóból származó értesülések alapján –, hogy esetleges üzemzavaraik milyen súlyos, néha végzetes, nem ritkán sok embert érintő következményekkel járhatnak.

Mindennapjaink biztonsága és nyugalma egyre nagyobb mértékben függ a kommunikációs és számítástechnikai infrastruktúra működésének zavartalanságától. Ezért előtérbe került az információbiztonság, mely nemcsak azonosítja a szervezetek adatfeldolgozási folyamatainak gyenge pontjait, az ezeket fenyegető veszélyeket, hanem olyan védelmi intézkedéseket is kialakít, amelyek a fellépő kockázatok kezelése által az adatfeldolgozás folyamatosságát biztosítják összhangban a szervezet általános biztonsági és működési céljaival. A megfelelő és hatékony információbiztonsági megoldások kialakítása alapvetően fontos az adatfeldolgozó szervezet, és általában az egész IKT-ágazat, iránti társadalmi bizalom megteremtése szempontjából.

Bonyolult rendszerek biztonságos működését fenyegethetik természeti katasztrófák, műszaki üzemzavarok és akár társadalmi válságok is. Ez többé-kevésbé minden ember által létrehozott nagy bonyolultságú struktúrára igaz. Azt azonban nem kell és nem is szabad a társadalomnak eltűrnie, hogy az információs infrastruktúrát – rajta keresztül pedig számos fontos érdeket és értéket – vétkes emberi magatartás veszélyeztessen.

1.2.1 Az informatikai bűnözés alapvető jellemzői

Az informatikai bűnözéssel foglalkozó minden monográfia és tanulmány szinte kötelező módon tartalmaz egy hosszabb-rövidebb statisztikai adatsort vagy legalább becslést az ilyen deliktumok által össztársadalmi szinten okozott – illetve a jelentős mértékű látencia miatt inkább csak *okozni vélt* – károk nagyságáról. Az információs piac gyors bővülése s ezzel együtt a számítógépes bűncselekmények számának és kártételének emelkedése miatt ezek az adatok, illetve becslések – ha esetleg megbízhatónak fogadjuk is el őket – igen rövid idő alatt meghaladottá válnak.

Azt azonban nagy biztonsággal megállapítjuk, hogy az informatikai bűnözés által okozott károk volumene – minden olyan országban, ahol ennek regisztrálásával egyáltalán foglalkoznak – évről évre növekedést mutat. A becslések alapján jellemzőnek tartják, hogy míg az összbűnözésen belül a számítógépes bűncselekmények aránya viszonylag alacsony, az általuk okozott károk nagysága lényegesen meghaladja az egy-egy bűncselekményre eső károk átlagos volumenét.

Fel kell tehát lépni mind a technikai, mind a jogi – köztük a büntetőjogi – védelem eszközeivel is az információs korszak sajátos bűnözési jelensége és új típusú alvilága ellen. Néhány év alatt szinte a semmiből teremtődött meg az információs társadalomnak az a szubkultúrája, amely illegális tevékenysége – esetleg sajátos „önmegvalósítása" – közegének tekinti a társadalomnak a számítástechnikával kapcsolatba kerülő szinte minden alrendszerét.

A számítógéppel kapcsolatos deviáns magatartásoknak viszonylag rövid idő alatt számos formája alakult ki, melyek kellően alapos tanulmányozásával, leírásával, osztályozásával mindeddig adósak maradtak a bűnügyi tudományok. Nem kis részben az elméleti munka hiányosságainak köszönhető, hogy a számítástechnikusok „boszorkányos praktikáit" legfeljebb szent borzadállyal figyelő közvéleménnyel együtt a bűnüldözésben szakmailag érintett jogászok túlnyomó része is kénytelen a napi sajtó szenzációs híradásaiból tájékozódni. Így gyakran ők sem képesek feldolgozni az új, hol utópisztikusan, hol groteszkül hangzó fogalmakat, s aligha tudják helyre tenni azokat a minduntalan felröppenő fantasztikus történeteket, melyek a NASA, az Egyesült Államok Védelmi Minisztériuma vagy a NATO számítógépeit feltörő ügyes kamaszokról vagy zseniális kisdiákokról szólnak.

Az informatikai bűnözés eleinte méltatlanul elhanyagolt területnek számított a bűnüldözésben. Érdekes tény, hogy a *Scotland Yard* kötelékén belül már 1971-ben felállították a *Computer Crime Unit*-ot (CCU), ez az „egység" azonban 1985-ig mindössze egyetlen (!) tisztből állt[2]. Az informatikai bűnözés fokozódó fenyegetését és az információs rendszerek sebezhetőségét észlelve ekkor négy főre növelték az állomány létszámát, amely azonban – tekintve, hogy a Scotland Yard egész Nagy-Britannia területén mozgósítható – még mindig nem képezett jelentős erőt.

Az informatikai bűnözéssel az 1950-es évek vége, az 1960-as évek eleje óta foglalkozik érdemben a büntetőjog-tudomány. Abban már a kezdetektől fogva gyakorlatilag egységes volt a jogászok véleménye, hogy a számítógép ellen vagy a számítógép segítségével más értékek ellen elkövetett támadásokra a büntetőjognak válaszolnia kell. A szakmai közvé-

2 Wasik, M. (1991), 46.

leményt inkább az osztotta meg, hogy milyen módon reagáljon a jog ezekre az újonnan jelentkező deviáns magatartásokra.

Az informatikai bűnözés mint kriminológiai jelenség legfontosabb jellegzetességei a gyorsaság, a magas látencia, a nemzetköziség és az intellektuális jelleg[3].

1.3 Az informatikai bűncselekmények osztályozása

Az informatikai bűnözés gyűjtőfogalom, amelybe sokféle cselekménytípus tartozik. Ezek megismeréséhez és megértéséhez elengedhetetlen az egyes magatartások alapos tartalmi feltárása és közös ismérvek alapján csoportokba való besorolása. Ez elemi előfeltétele az egyes társadalomra veszélyes magatartások büntetőjogi kriminalizálásának is.

A számítógépes bűncselekmények osztályozására tett egyes korai kísérletek számítástechnikai fogalmakon vagy az adatfeldolgozási folyamat egyes szakaszainak jellegzetességein alapultak. Többek között megkülönböztettek hardver, illetve szoftver elleni bűncselekményeket, valamint az input vagy az output adatok illegális megváltoztatásával, meghamisításával járó visszaéléseket. H. *Cornwall* osztályozása például nem az informatikai bűnözés egészét, csak annak egy részterületét, az *adatbűncselekményeket*, vagyis az adatokkal kapcsolatos törvénysértő manipulációkat és az adatok illegális megszerzését érinti. Ezeket három csoportba sorolja; úgymint *adatcsalás* (data fraud), *adatkikémlelés* (data spying) és *adatlopás* (data theft).

Ugyancsak gyakran hivatkoznak a szakirodalomban két igen általános kategóriára:

1. *számítógép mint célpont* ellen elkövetett bűncselekményekre (computer-as-target-crimes) és
2. *a számítógép mint eszköz* segítségével elkövetett bűncselekményekre (computer-as-tool-crimes).

Az újabb osztályozások a visszaélések által veszélyeztetett értékek és érdekek alapján állapítják meg a számítógépes bűncselekmények csoportjait, ami által többet árulnak el a cselekmények társadalmi veszélyességéről.

1.4 Jellemző elkövetési módok

A számítógépes bűncselekmények elkövetési módjai, technikái mind a jogi, mind az informatikai irodalomban sajátos elnevezésekkel szerepelnek. Ezek a fogalmak a számítástechnikai szaknyelvből, gyakran pedig ennek átszűrt változatából, egy különleges szubkultúrát hordozó szlengből származnak. A humoros, sőt nem ritkán groteszk, hangzású kifejezések valódi jelentése általában magyarázatra szorul. A következőkben néhány jellegzetes elkövetési technikát ismertetünk.

3 Balogh Zsolt György (1998), 261.

1.4.1 Hacking

1.4.1.1 A hacking jelentésváltozásai

Első felbukkanása óta a *„hacking"* kifejezés lényeges jelentésmódosuláson ment át. Az 1960-as években a hacking a számítástechnika iránti elkötelezettséget jelentette és olyan kiemelkedő programozói jártasságot, ami a leggyorsabb, legjobb, legkifinomultabb programok írását tette lehetővé. A korai *hacker*ek a számítástechnika megszállott művelői, tehetséges, kreatív, jól képzett programozók voltak, akik általában egyetemeken és kutatóintézetekben, például az *MIT (Massachusetts Institute of Technology)* laboratóriumaiban kísérleteztek az akkoriban a legmagasabb technikai színvonalat képviselő számítógépekkel. Kis létszámú szakmai közösségüket már-már legendás szakmai tudás, a beavatottak összetartása és elzárkózása, egy sajátos, romantikus életforma jellemezte[4].

Ezzel szemben a hacking ma azt jelenti, hogy valamely illetéktelen személy a tulajdonos, illetve a rendszergazda kifejezett vagy hallgatólagos engedélye és tudomása nélkül fér hozzá egy számítógéphez vagy számítógéprendszerhez és ezáltal a rajta tárolt adatokhoz, programokhoz. Ez általában a rendszer biztonsági rendszabályainak kijátszásával vagy a technikai védelem „feltörésével" történik. Az ilyen tevékenységet folytató személyeket nevezzük ma hackereknek.

A hajdani hacker-romantika nem múlt el nyomtalanul; visszfénye ma is él. Valószínűleg ennek tulajdonítható, hogy egyes szerzők élesen megkülönböztetik a jó szándékúnak tartott, az adatokat csak a kihívás, a szellemi csemege kedvéért kifürkésző hackereket és a számítógépes rendszerekhez jogosulatlanul hozzáférni törekvő, valóban ártó szándékú crackereket. A *Hálózati értelmező szótár* c. kiadvány például így fogalmaz:

„Hacker: olyan technofil ember, aki a szoftverek és a hardvereszközök működésének minél alaposabb megismerését, teljesítményük maximális kihasználását, a számítógépes és telekommunikációs rendszerek gyenge pontjainak felderítését, és nehéz programozási feladatok megoldását élvezi; tevékenysége célja nem a (szándékos) károkozás, szemben a crackerrel."[5]

1.4.1.2 A hacking jogi értelmezése

A jog azonban – legalábbis ma – nem ismeri el ezt a különbségtételt. Azokban az országokban, ahol büntetik a rendszerek jogosulatlan felhasználását, az adatokhoz való illegális hozzáférést, ezt a magatartást hackingnek nevezik. A betyárromantikára kevésbé fogékony szerzők rá is mutatnak, hogy a fent említett „ártatlan" hackerek is okozhatnak – talán valóban nem szándékosan – súlyos károkat a számítógépes adatfeldolgozásban.

A rendszerhez való hozzáférés, a jogosulatlan belépés általában távolról, a hacker saját vagy hivatali, munkahelyi számítógépéről történik kommunikációs hálózatokon keresztül. A hacker tevékenysége általában olyan kód megszerzésére, illetve visszafejtésére irányul, amely a legális belépést és a rendszer szolgáltatásainak használatát biztosítja.

4 Clough, B.–Mungo, P. (1992), 34.
5 Drótos László (1999), 37.

Mint számítógépes visszaélés, a hacking egyike a legjellegzetesebb és legelterjedtebb elkövetési technikáknak. Valójában tipikus *eszközcselekmény*, mely sok esetben csak a megfelelő feltételeket biztosítja más bűncselekményekhez, például gépidő- és szolgáltatáslopáshoz, számítógépes szabotázshoz, szerzői vagy személyiségi jogokat sértő deliktumokhoz. A hacking nem ritkán zsarolással kapcsolódik össze. Ez történik akkor, ha a hacker szabotázs – pl. vírus bejuttatása, adatok törlése – vagy egyéb számítógép segítségével elkövethető deliktum kilátásba helyezésével anyagi „ellenszolgáltatást" próbál kizsarolni a rendszer üzemeltetőjétől.

A nemzetközi gyakorlatot tekintve találkozhatunk ma már olyan törvényekkel is, melyek – miként az angol *Computer Misuse Act* – a hackinget önálló bűncselekményként szankcionálják. Eszerint a hacking alapvető tényállási elemei az alábbiak:

– az elkövető szándékosan arra használ egy számítógépet, hogy hozzáférést biztosítson magának olyan adatokhoz vagy programokhoz, melyeket ugyanazon vagy másik számítógépen tárolnak;
– az elkövető részéről a hozzáférés jogosulatlan;
– a tettes az elkövetés időpontjában mindezekkel tisztában van.

A hacker cselekménye tehát a gépen tárolt adatokra, illetve programokra, ezek megismerésére, megszerzésére vagy felhasználására irányul. A hacking mint bűncselekmény kulcsmozzanata a hozzáférés jogosultsága, illetve jogosulatlansága. Jogosult személy az, akit a *hozzáférés ellenőrzésére* kineveztek (rendszergazda) vagy akinek ilyen személytől származó engedélye van. A számítógéphez, illetve az adatokhoz, programokhoz való hozzáférés akkor tekintendő jogosulatlannak, ha az illető személy az előbbi feltételeknek nem felel meg. Munkahelyi, hivatali körülmények között az alkalmazottak, felhasználók számára egészen világossá kell tenni, hogy mely programok és adatok azok, amelyekre hozzáférési joguk kiterjed.

1.4.1.3 A hacker legjobb barátja: könnyen kihasználható biztonsági rések az elterjedt rendszerekben

A mai hackerek legtöbbje nem tartozik az információs és kommunikációs rendszerek működésének részleteit aprólékosan ismerő, nagyon magas szintű szakértelemmel rendelkező és kreatívan gondolkodó technikai zseni szűk csoportjába. A legtöbben a szoftverekben lappangó, mások által feltárt, az internetes fórumokon nyilvánosságra hozott biztonsági réseket használják ki, és lényegében szabványosra csiszolt behatolási megoldásokat alkalmaznak.

A szabványos megoldásokkal operáló hackereknek kezére játszik a nagy rendszerek tehetetlensége, a tömeges elterjedésből fakadó lassú reakcióideje. Hiába ismert ugyanis egy biztonsági kockázat valamely operációs rendszerben vagy hardverkomponensben, ha felhasználók millióinak kezében van a sérülékenységet hordozó eszköz, és hiába a hamar elkészülő és hozzáférhetővé váló hibajavító kód, ha a felhasználók nem frissítik a rendszereiket. A felhasználóknak szóló minden figyelemfelhívás, propaganda ellenére a hackerek, illetve az általuk elszabadított kártékony programok jó eséllyel indulnak, ha megfertőzhető, védtelen rendszert vagy felhasználót keresnek. A digitális járványokat okozó kártékony kódok és károkozó magatartások éppen úgy tudnak elterjedni, mint egy valamely betegség ellen nem immunizált populációban a kórokozó mikroorganizmusok.

1.4.2 Vírusok

A computervírus fogalma néhány év alatt az információs rendszerek fölött állandóan fenyegetően lebegő „sorscsapás” szinonimájává vált. Az elnevezés egyike a számítástechnika legszemléletesebb, legszellemesebb kifejezéseinek. A számítógépvírus ugyanis nem más, mint egy olyan program, amelynek legfőbb funkciója, hogy megfelelő célpontokat kiválasztva és hozzájuk kapcsolódva önnön kódját, lényegében saját magát terjessze. Viselkedése valóban emlékeztet az élőlényeket megtámadó, az élő sejtekben szaporodó vírusokéra.

A vírus metaforája – szemléletességével együtt – kissé talán megtévesztő is. Bár a biológiai vírusokhoz hasonlóan a számítógépvírusok is lappangva terjednek s „szaporodás” közben akár „mutációkon” mehetnek át, keletkezésük módja egészen különböző. A biológiai vírusok az evolúció során fejlődtek ki, s további alakulásukat, terjedésüket az ember csak közvetett módon, korlátozottan képes ellenőrzése alá vonni. A számítógépvírusok ezzel szemben egyszerűen csak programok, s így emberi alkotások. Keletkezésük és terjedésük egyaránt elképzelhetetlen aktív emberi cselekvés nélkül. Számítógépről számítógépre való áthurcolásuk, vagyis a „fertőzés” valamilyen fizikai adathordozó – például floppy lemez, vagy a számítógép-hálózatokat összekötő kábelrendszer – segítségével történik.

A számítógépvírus célpontjai elsősorban a futtatható programok bináris kódjait tartalmazó fájlok. Minden megfertőzött fájl vírusként viselkedik a továbbiakban, így a fertőzés tovább terjed. Egyes vírusfajták – ezeket *boot vírusoknak* nevezzük – a mágneslemezek szintén bináris kódot tartalmazó ún. „boot szektorába” hatolnak be, s innen kiindulva fertőzik tovább a lemezen lévő fájlokat. Ezek a vírusok azért különösen veszélyesek, mert amikor a számítógép dolgozni kezd egy lemezzel, akkor először mindig a boot szektor tartalmát olvassa ki. Ha ezen a helyen vírus van, akkor minden lemezkezeléssel járó további művelet egyúttal a vírust is szaporítja.

A vírusok „felfedezése” az *önreprodukáló és -javító programok* (self-replicating programs) fejlesztésére irányuló kutatásokban gyökerezik. A kiváló magyar matematikus, a számítástechnika egyik úttörőjeként tisztelt *Neumann* János már 1948-ban előre jelezte olyan programok írásának lehetőségét, amelyek képesek önmaguk reprodukálására[6]. Neumann ezeket az elektronikus környezetben létrejött mesterséges „élőlényeket” *automatá*knak nevezte. Rámutatott arra is, hogy az „automaták” reprodukciója igen gyors és egyszerű lehet.

Sok évvel – a számítástechnika történetét tekintve korszakokkal – Neumann munkássága után Fred *Cohen*, a University of South California végzős hallgatója, ugyancsak foglalkozott ezzel a témával[7]. 1985-ben fejezte be az önreprodukáló programokról szóló disszertációját. Írásában ő nevezte először ezen a ma már jól ismert néven a „computervírusokat”. Cohen egyúttal azt is jelezte, hogy a vírusok adatok módosítására és megsemmisítésére is alkalmasak lehetnek, így komolyan fenyegetik a számítástechnikai rendszerek biztonságát.

Ez a jóslat azok közé tartozik, amely valóban maradéktalanul teljesül is. A vírusok létezésére, létrehozatalukra és az ellenük való küzdelemre sajátos szubkultúra épült rá. Vírusfejlesztők és antivírusprogramok készítői vívják csendes és vértelen háborújukat számítógépeken és a világot átszövő hálózatokon. A vírusok „áldozatai” többnyire tájékozatlan,

6 Clough, B.–Mungo P. (1992), 75.
7 Clough, B.–Mungo P. (1992), 78.

óvatlan vagy egyszerűen csak balszerencsés felhasználók, akik nem tudnak eleget a vírusok veszélyeiről és az ellenük való védekezés lehetőségeiről, vagy könnyelműen bíznak abban, hogy őket majd elkerüli ez a kellemetlenség.

A vírusok részei általában a *mag*, az *aktivátor* és az *örökítő*. Az örökítő biztosítja a víruskód önreprodukálását, azaz a másolat hozzáfűződését a megfertőzhető fájlhoz.

Az aktivátor valamely logikai feltétel vizsgálatát végző programrész. A feltétel teljesülése váltja ki a magban rögzített utasítás-sorozat végrehajtását. A feltétel igen változatos lehet; valamely időpont, naptári nap elérkezte; az adott gépen az első fájl „fertőződésétől" számított megadott időtartam letelte; a gépen lévő összes fájlok valamely hányadának „fertőződése" stb. A feltételek olyanok, hogy teljesülésük, vagyis a vírus aktívvá válása véletlenszerűen, felkészületlenül érje a felhasználót.

A mag a vírus „cselekvő" része. Ez ugyancsak igen változatosan működhet. Az teszi olyan sokoldalúvá a vírusokat, hogy a magot alkotó program lényegében bármilyen utasításokat tartalmazhat. A vírusíró szándéka szerint egy vírus lehet *ártalmatlan* vagy *romboló* hatású.

Az ártalmatlan vírusok magja vagy üres – az ilyen vírus csak szaporodik –, vagy csak olyan utasításokat tartalmaz, melyek nem okoznak jelentősebb károkat a számítógépen tárolt adatokban, programokban. Egy ilyen vírus legfeljebb megváltoztatja a gép kimeneti vagy bemeneti perifériáinak működését, ezzel zavarva a felhasználó munkáját. Tipikus „tünet" a képernyőn megjelenő tréfás, obszcén, esetleg trágár üzenet, ábra, a karakterek összekeveredése, a gép hangszórójából szóló dallam, a billentyűzet leblokkolása. Sok fájlt megfertőzve, vagyis a háttértárakon elszaporodva az ártalmatlan vírusok is jelentős mértékben csökkenthetik a felhasználható tárterület nagyságát, komolyabb adatvesztést azonban nem okoznak. A megfelelő vírusirtó és -immunizáló program lényegében kockázat és veszteség nélkül megszabadítja a gépet és a felhasználót ezektől a kellemetlenkedőktől.

Egészen más a helyzet a romboló vírusokkal. Ezeknek a magja olyan utasításokat tartalmaz, amelyek érzékeny veszteséget, esetenként akár jelentős kárt is okozhatnak a felhasználónak. Ezek a károk és veszteségek általában adatok, illetve programok, tehát a szoftver megsemmisülésében, nem pedig a hardver megrongálódásában állnak. A romboló vírusok tipikus hatásai az alábbiak:

- valamely könyvtár vagy akár az egész merevlemez tartalmának törlése,
- a merevlemez formázása,
- a lemez ún. *partíciós táblájának* törlése, ami után magának a felhasználónak kell majd formáznia a lemezt és az egész rendszert újratelepíteni,
- adatok – jellemzően e-mail-címek, bizalmas rendszerekhez hozzáférést biztosító felhasználói nevek és jelszavak – megszerzése.

Ezek a műveletek igen durva beavatkozást jelentenek, mely után a rendszer eredeti állapotának helyreállítása hosszú időt vehet igénybe. Nem ritka az sem, hogy a vírus támadása folytán olyan adatok semmisülnek meg, melyek nem pótolhatók. A romboló vírusokkal szabotázs jellegű bűncselekmények is megvalósíthatók.

1.4.3 DoS és DDoS támadás

A szolgáltatásmegtagadással járó hálózati szolgáltatás kiesések lényege, hogy egy vagy több támadó a kliensek számára elérhetetlenné tesz olyan szolgáltatásokat, amelyeket a felhasználók el szeretnének érni. Ezeket nevezzük *Denial of Service* [DoS] támadásoknak. Amennyiben több támadó vesz részt a támadásban, azt jellemzően a támadó eszköz- – speciálisan erre a célra létrehozott szoftver- – együttes, koordinált futtatásával hajtják végre. Ez a *Distributed Denial of Service* [DDoS] támadás lényege.

A hálózati szolgáltatások azért válhatnak elérhetetlenné, mert a hálózaton keresztül küldött kérések nem jutnak el a szerverig vagy a szerver nem tudja azokat feldolgozni. Az okok között szerepelhet az elégtelen sávszélesség, egy köztes hálózati eszköz vagy a szerver időszakos túlterhelése, illetve a szerveren futó valamely szoftver – webkiszolgáló, adatbázis-kezelő, webes alkalmazás – összeomlása és leállása. A hálózati szinten végrehajtott támadást az teszi lehetővé, hogy az internet alapvető protokollcsaládjának, a TCP/IP-nek az alapja a szerver és a kliens közötti kommunikációs csatorna (TCP socket) felépítése. Ennek során az ún. TCP háromutas kézfogás (three-way handshake) játszódik le. De mi történik, ha a kliens sohasem küldi el a harmadik lépést jelentő TCP-csomagot? A létrejött sockethez mind a szerver, mind a köztes hálózati eszközök egy része erőforrásokat köt le, elsősorban memóriaterületet és processzoridőt. Ezek csak akkor szabadulnak fel, ha lejár a beállított várakozási idő (time out), és a szerver felszabadítja az erőforrásokat.

A kliensek – akár a támadók – és a szerver között helyezkedik el az internet infrastruktúrája, továbbá a szerver IP-címét biztosító internetszolgáltató routere(i), a szervert üzemeltető cég vagy szervezet ezenfelül jó esetben tűzfalat is üzemeltet. Ezek bármelyikét érintheti a szolgáltatásmegtagadási támadás és szűk keresztmetszetté válhatnak. A támadó azt az elvet alkalmazza, hogy az alap- vagy az alkalmazás-rétegbeli valamelyik protokoll elárasztja a szerverek túlterhelését okozó kérésekkel.

Elméletileg is tökéletes védelem jelenleg nem áll rendelkezésre, mivel a gyakorlatban csak a sikeres támadáshoz a támadó számára szükséges erőforrásigényt növelhetjük. Néhány lehetőség azonban mégis van. A védekezés kézenfekvő módja a rendelkezésre álló erőforrások növelése vagy a félig nyitott TCP/IP-kapcsolatok esetén érvényes várakozási idő csökkentése lehet. A kérések forráscímének blokkolása is egy beszámítható lehetőség. A szerverről a gyanúsnak ítélt IP-címek egy rövid időre kitilthatók. Problémák a gyanús tevékenység definiálásával és a kitiltás idejével lehetnek. A gyakorlatban ilyenkor normális tevékenységet folytató IP-című eszközök is kitiltódhatnak, ha „túl sokszor” próbálnak a szerverhez csatlakozni egy adott időintervallumban. Emiatt szokott a tiltás rövid ideig élni. Kellően felkészült, intelligens támadó ellen azonban ez a gyakorlatban nem megfelelő megoldás, mivel az IP-csomagokban található forrás IP-cím hamisítható.

Elosztott védekezés is kialakítható kellően nagy rendelkezésre álló erőforrások felhasználásával. Ha a kiszolgáló a kliensek felől érkező forgalmat egy nagyszámú speciális hálózati eszközből álló „felhőn” irányítja keresztül, továbbá a felhő elemei egyenként képesek a támadások észlelésére és a védekezésre, a támadó dolga nagyságrendileg nehezíthető. Így ugyanis a támadónak már az egész felhőt kell kiiktatni a kis számú router, tűzfal és szerver helyett, hogy a támadás sikeres legyen. Ilyen védelmi infrastruktúrát nyilván nem gazdaságos mindenhol üzemeltetni, léteznek azonban olyan szolgáltatók (Verizon Terremark, Verisign, CloudFlare, Incapsula), ahol ilyen biztonságos környezetet tudnak nyújtani.

1.4.4 Zombi számítógép, zombi hálózat; BotNet

A zombi számítógép olyan számítógép, amelyet különböző vírusokkal és trójai szoftverekkel irányítása alá vesz egy hacker. A számítógép erőforrásait ezután a saját céljára, sokszor DDoS támadások megszervezésére, kivitelezésére használja. Az ilyen távolról, titokban irányított gépeket használják kéretlen reklámüzenetek – ún. spamek – tömeges kiküldésére is.

A megfertőzött és különböző programokkal eltérített, a saját befolyásuk alá helyezett számítógépeket a hackerek úgynevezett botnetekbe rendezik. A név a *spam-robot* kifejezés rövidüléseként született meg. Egy-egy botnet több száz, sőt több ezer számítógépet tömörít eggyé, egy összehangolt támadásban pedig elérhetetlenné tehetik az internetes szervereket, illetve akár illegális tartalom is elhelyezhető rajtuk.

A számítógépes botneteket általában spamterjesztésre vagy túlterheléses támadások kivitelezésére adják bérbe a gazdáik, a mobilos zombi hálózatok azonban ennél nagyobb veszélyeket is rejthetnek. Egyrészt a mobileszközökön a felhasználók sokszor több és érzékenyebb személyes információt tárolnak, mint az asztali számítógépükön, másrészt a telefonszámla megterhelésével közvetlenül a felhasználó pénzéhez férhetnek hozzá a vírusok írói. Ráadásul a mobilvírusok elleni védekezés még egyáltalán nem kiforrott technológia. A gondos felhasználó jól teszi, ha nem tölt le a mobiltelefonjára gyanús, ellenőrizetlen forrásból származó alkalmazásokat.

1.5 Sértettek

A tapasztalatok alapján úgy tűnik, hogy a társadalom egyetlen szektora, csoportja, alrendszere sem érezheti magát védettnek attól a fenyegetéstől, amit a számítógépes bűncselekmények jelentenek. Tipikusan cégek, gazdálkodó – gyakran pénzügyi – szervezetek és hatóságok, hivatalok a visszaélések sértettjei.

Kutatások alapján a kriminológia már hosszú ideje bizonyítottnak tekinti, hogy az áldozattá válásban a sértettnek is viszonylag nagy a szerepe. Nincs ez másként a fehérgalléros bűnözés esetében sem, és okkal tételezhetjük fel, hogy a számítógépes bűnözés sem kivétel a szabály alól. A *viktimológia* (áldozattan) azonban eddig jobbára az egyének, természetes személyek sérelmére elkövetett bűncselekményekre – illetve ezek áldozataira – koncentrálta a figyelmét, ezért még viszonylag keveset tudunk a szervezetek bűncselekmény sértettjévé válásának körülményeiről, jellemzőiről.

A bűnügyi statisztika szerint a gazdálkodó szervezetek és hivatalok sérelmére elkövetett számítógépes visszaéléseknek az okozott kár nagysága alapján legsúlyosabb csoportjait a vagyon elleni bűncselekmények, az adatok megszerzésére irányuló deliktumok és a szolgáltatáslopások alkotják.

A vagyon elleni számítógépes bűncselekmények között két fő típust különböztethetünk meg. Egyes cselekmények során az elkövető adatok vagy programok manipulálásával vagyoni előny megszerzésére, illetve a sértettnek vagyoni hátrány okozására törekszik. A második típus jellegzetes magatartásai bizonyos zsarolásszerű cselekmények. Ekkor a sértett általában arról szóló értesítést kap, hogy számítógépes információs rendszerébe „valaki” romboló hatású programot – vírust, logikai vagy időzített bombát – juttatott, s a tettes csak meghatározott összegű anyagi ellenszolgáltatás fejében hajlandó ennek hatástalanítására.

Az adatok megszerzésére irányuló cselekmények, vagyis az illegális *adatlecsapolások* a közvetlen vagy követett vagyoni károkozáson kívül még egy figyelemre méltó sajátossággal rendelkeznek. Ha ugyanis a cselekmény az adatkezelőnél tárolt személyes adatok megszerzésével valósul meg, az nemcsak az adatkezelő érdekeit sérti, hanem valamennyi érintettét is, akinek személyes adatai a törvényes céltól eltérően kerülhetnek felhasználásra.

Az adatfeldolgozó rendszerek relatív védtelensége is szerepet játszik e bűncselekmények elkövethetőségében. Ezeket ugyanis eredetileg nem visszaélések kizárására, hanem könnyű kezelhetőségre és szabad hozzáférhetőségre tervezték. Nemcsak ez a technikai sajátosság játszik azonban a számítógépes bűncselekmények elkövetőinek kezére.

A tettesek dolgát gyakran megkönnyíti a sértettek gondatlansága, illetve nem kellő tájékozottsága is. Ma az a tipikusnak mondható helyzet – és nemcsak Magyarországon van így –, hogy hivatalokban, hatóságoknál egyszerű IBM PC-ken a Microsoft Windows valamelyik verziójának felügyelete alatt – vagyis átlagos technikai védelmi szint mellett, egyszerűen hozzáférhető módon – tárolnak és kezelnek személyes és a hivatali működéshez kapcsolódó egyéb adatokat. Ezen adatok nem kis része különleges személyes adat – például az egészségügyi intézmények esetében a betegekkel kapcsolatos adatok –, amelyek kezelését fokozott gondossággal kellene végezni. Tájékozatlan jóhiszeműségükben a felhasználók gyakran nem is gondolnak arra, hogy az adatokat és magát a feldolgozó rendszert megfelelő biztonsági rendszabályok és megoldások alkalmazásával védjék az illegális hozzáférés és a visszaélések ellen.

1.6 Vállalati rendszerek biztonsága

A cégvilág naponta szembesül az informatikai bűnözés jelenségével, következményeivel. A bankok, egyéb pénzügyi szolgáltató intézmények és az informatikai vállalkozások különösen ki vannak téve a számítógépes és hálózati támadásoknak. A vállalatok számos módon védekeznek, s valójában azoknak a biztonsági protokolloknak a nagy része, melyeket ma a közszféra informatikai biztonságának szavatolására alkalmaznak, a vállalati kultúrában született meg és vált először iparági gyakorlattá, majd ténylegesen is előírt, követendő szabvánnyá.

Van arra is példa, hogy egy nagyvállalat komolyan felveszi a harcot az informatikai támadások ellen, és lényegében saját ellenerőt fejleszt ki. Erre természetesen csak a legnagyobb gazdasági erejű szereplők képesek.

1.6.1 Microsoft Cybercrime Center

Például 2013 őszén Redmondban, a Microsoft főhadiszállásán felavatták a cég *Cybercrime Center* névre hallgató új központját[8], ahol az online alvilággal próbálják felvenni a harcot. A központban százan fognak dolgozni, a nagyon magasan képzett programozók és hálózati specialisták mellett erős jogi csapat is hadba száll majd, akiknek az lesz a feladatuk, hogy a hackereket, online kémeket, a vírusok íróit, botnetek építőit, illetve azok megbízóit meg tudják szorongatni más országok hatóságaival együttműködve.

8 Index (2013).

A központban külön egység foglalkozik majd a szerzői jogsértésekkel (magyarul az illegális letöltőközpontokkal), illetve a gyerekpornográfia terjesztőivel. Utóbbiakat a PhotoDNA nevű képelemző technológia fogja segíteni. Egy másik fontos irány, amiben úttörő szeretne lenni a Microsoft specialistáinak csapata, a SitePrint kezdeményezés, aminek célja az internetes szervezett bűnözés feltérképezése, az egyes internetes maffiacsoportok közötti kapcsolatrendszerek felderítése.

1.6.2 Biztonsági rés az ATM-ek operációs rendszerében

A Las Vegas-i Black Hat hackerkonferencián Barnaby Jack, a seattle-i IOActive biztonságtechnikai cég specialistája bemutatta azokat a módszereket, amikkel bankjegykiadó automatákat lehet kifosztani. A hacker évekig dolgozott az ATM-ek szoftveres és hardveres sebezhetőségeinek megtalálásán, és csak akkor mutatta be ezeket a nagyközönségnek, amikor a figyelmeztetése nyomán és az útmutatása alapján az automaták gyártói már befoltozták ezeket a biztonsági réseket[9].

Barnaby a kutatást úgy végezte, hogy vásárolt két ATM-et a neten a legnagyobb gyártóktól, a Tritontól és a Tranaxtól, majd olyan sérülékenységeket keresett a szoftverükben, amin át hozzáférhet a fájlrendszerükhöz. A Tranaxnál ezt sikerült a gép menüjén keresztül megoldania, majd az ATM rendszerén futó Windows CE-ből kinyerni a pénzkiadást felügyelő szoftvert. A Tritonnál hardveres megoldáshoz kellett folyamodni: kiderült, hogy bár a gép erősen páncélozott, az alaplap, amin az egészet irányító miniszámítógép van, egy, az internetről tíz dollárért beszerezhető kulccsal nyitható ajtó mögött van.

A hacker ezután írt két olyan vírust, amik betelepülnek az ATM-ek rendszerébe, és a megfelelően preparált kártyát vagy billentyűkombinációt érzékelve átadja a vezérlést a hackernek. A Tritonra a konferencián távolról egy modem segítségével jelentkezett be Barnaby, és egy gombnyomásra az automatában levő összes pénzt kiszórta a pódiumra.

Az ATM-eket eddig a kifinomult hackermódszerek helyett más trükkökkel fosztogatták a bűnözők: ilyen volt például az, amikor az automatára rászereltek egy plusz kamerát, ami rögzítette a PIN-kódok lenyomását, a gépet pedig úgy preparálták, hogy az lenyelje a kártyát és a csalók által felszerelt rekeszbe dobja, ne az automata gyomrába.

1.6.3 A Unix, Linux, Mac OS X rendszerek egyik kritikus sebezhetősége

2014 szeptemberében sokkolta az internetet az azóta *Shellshock Bash-bug*[10] néven emlegetett kritikus sebezhetőség. Ebben az esetben nem tipikus bugról, szoftverhibáról van szó, hanem csak egy nem dokumentált, elfelejtett funkcióról.

9 Index (2010).
10 Laza Bálint (2014).

Egy biztonságtechnikai szempontból át nem gondolt fejlesztés miatt a rosszindulatú támadók távolról belenyúlhatnak gépekbe, a webszerverektől a routereken át a gépekhez csatlakozó programok mind kihasználható felületet kínálnak a hibának, amivel a támadó mindenféle azonosítás, kulcs, jelszó, felhasználónév nélkül futtathat káros kódokat.

A Bash egy úgynevezett shell, egy parancsértelmező, amivel szöveges parancsokat lehet kiadni Unix(-alapú) és Linux rendszereken, tipikusan akár távolról is. Azonban ennél is többet tud: feldolgozóként is működhet webszerverek scriptjeihez. A Bash a nyolcvanas évek óta létezik és rendkívül népszerű. Vannak más alternatívák is, viszont a Bash alapértelmezett a legtöbb Linux és Mac OS X operációs rendszeren. A szervereken, különböző hálózati kiszolgáló eszközökön valójában a Unix és a Linux valamelyik változata a legnépszerűbb operációs rendszer.

Egészen a 4.3-as – a hiba felfedezése előtti – verzióig minden korábbi Bash érintett, ami azt jelenti, hogy az elmúlt nagyjából 25 év összes kiadása. A Bash-bug igazából nem is hiba. Egyszerűen arról van szó, hogy a modult 25 évvel ezelőtt tervezték. Akkor még alig internetezett valaki, a biztonsággal nem igazán foglalkoztak. A most kihasználható hiba pedig valójában tervezett, egyszerűen nem dokumentálták rendesen, így mindenki elfelejtette. Akkoriban nem számított, a mostani környezetben viszont már könnyen kihasználható.

2 AZ EURÓPAI UNIÓ INFORMATIKAI BIZTONSÁGI POLITIKÁJA ÉS KERETRENDSZERE

Miközben a társadalmunk egyre elképzelhetetlenebb internet vagy mobileszközök nélkül, és a gazdaság is egyre nagyobb részben támaszkodik digitális infrastruktúrákra, ez a rengeteg pozitívummal járó átalakulás egyben a biztonsági kockázatok megnövekedését is magával hozta. A sajtó naponta ad hírt tömeges adatszivárgásról, hálózati szolgáltatások blokkolásáról, hekkelésről, adatlopásokól, azt pedig akár bárki személyesen megtapasztalhatja, hogy a privát wifi hálózatok sincsenek biztonságban.

Az egy-egy céget érő, vagy a felhasználók adatait fenyegető, veszélyek mellett szaporodnak a kritikus infrastruktúra ellen hadműveletként végrehajtott támadások is, melyek akár egész országok nagy rendszereinek működőképességét áshatják alá. A nagy publicitást kapott első ilyen akciók között volt a botnettel végrehajtott Észtország elleni átfogó kibertámadás[11] 2007-ben. Többek között üzemzavart jelentettek a hírközlési szolgáltatók, és elérhetetlenné váltak az elektronikus banki szolgáltatások, megbénultak a készpénzkiadó automaták, s mindez egy olyan informatikától erősen függő országban, amely a pénzügyi tranzakciók 90%-át már akkor is interneten hajtotta végre. Ezzel a szabotázsművelettel kapcsolatban komolyan szóba került a nemzetközi agresszió, illetve agresszor fogalmának alkalmazása és a NATO szerződés 5. cikkelyének alkalmazása.

Hasonlóan brutális kibertámadás érte Ukrajnát 2015 végén, aminek a következménye az ország energiaellátásában bekövetkező széleskörű és tovaterjedő zavar lett[12]. Az elemzők mindkét incidens mögött orosz hackerek tevékenységét, sőt, tulajdonképpen Oroszország szervezett kiberhadviselési műveleteit látják.

Természetesen még rengeteg további példát fel lehetne sorolni, a következtetés azonban így is érthető. A világgazdaság, a közigazgatás, a politikai és társadalmi intézmények egyre nagyobb mértékben rá vannak szorulva az informatikai infrastruktúra eszközeire és szolgáltatásaira, s emiatt nyilvánvalóan kiszolgáltatottjaivá is váltak e szolgáltatások és rendszerek megbízható működésének. A sebezhetőség, a fenyegetettség is világossá vált mára, és erről az erősödő hangulatról is számos forrásból meggyőződhetünk.

Nemzetközi szervezetek nyugtalanító hangulatú jelentései emelik ki, hogy milyen várakozások lengik be az információs társadalmakat és gazdaságokat. A World Economic Forum 2018. januári jelentése például a kibertámadás és az adathamisítás, adatlopás bekövetkezési

11 Joshua Davis (2017).
12 Kim Zetter (2016).

kockázatát a világot fenyegető veszélyek között a *harmadik* és a *negyedik* helyre[13] teszi, olyan egyéb veszélyforrások között, mint a szélsőséges időjárási események, természeti katasztrófák, az éghajlatváltozás és a menekültválság.

A veszélyekkel együtt fokozódik a tudatosság is. Erről tanúskodik a PwC egyik idei jelentése[14] is, mely felmérésekkel igazolja, hogy a cégvezetők között jelentős mértékben növekedett az adatbiztonság, adatvédelem iránti felelősségérzet és cselekvési készség. A jelentés főbb megállapításait az alábbiak szerint foglalhatjuk össze:

- A vállaltvezetők számára ma már elengedhetetlen a felkészült és tudatos cselekvés az informatikai biztonság és az adatvédelem területén is.
- A digitális átállással járó kockázatok kezelése létfontosságú kérdéssé vált a vállalatok számára.
- Az adatvédelmi szabályok a személyes adatok kezelésének bizalmasságán kívül az adatok felhasználásának mikéntjére helyezik a hangsúlyt.
- A fejlett hitelesítési technológia bizalomépítő jelentőségű.
- Még az ipari titánoknak is meg kell erősíteniük a vezetői szintű szerepvállalást.
- Az EU-n kívüli vállalatnak is fontolóra kell venniük vezető adatvédelmi tisztviselő felvételét.
- A kérdést eddig hanyagul kezelő vállalkozásoknak most majd több munkát kell fektetniük az informatikai rendszerekkel kapcsolatos kockázatok kezelésébe.
- A fogyasztók a felelősségteljes innovációra és az adatok tisztességes, átlátható és felelősségteljes felhasználására fognak szavazni a pénztárcájukkal.

Kétség nem férhet hozzá, hogy az informatikai biztonság terén egyre nagyobb szükségünk van összehangolt stratégiára és a gyakorlatban is hasznos szabályozásra. Ezt a felismerést az EU döntéshozatali mechanizmusa is magáévá tette, s ennek megfelelő cselekvési programokat dolgozott ki, melyek mára tényleges, számonkérhető, kikényszeríthető jogi szabályozássá vált.

Az összehangolt, közös EU-s fellépés azért is indokolt, mert nemcsak a szolgáltatások nyúlnak át ma már az országhatárokon, de egy-egy hálózat- vagy információbiztonsági incidens is kihathat az egész Unióra.

13 World Economic Forum (2018), Figures I, IV. pp. 3., 6.
14 PricewaterhouseCoopers (2018).

2.1 Az EU információs társadalom politikája

Az EU információs társadalommal kapcsolatos politikájának kezdő lépéseit, az ezekhez vezető döntési folyamat első megnyilatkozásait nem célunk teljes részletességében feltárni és bemutatni. Csupán a témánk szempontjából legfontosabb elemeire fogunk röviden utalni.

2.1.1 Az informatikai biztonság iránti igény a Bangemann-jelentésben

A híres Bangemann-jelentés, amelyet az Európa Tanács 1994. évi korfui tanácskozásán fogadott el, az európai információs társadalom kialakításának első jelentős stratégiai dokumentuma. Piacbarát intézkedések elfogadásával látja elérhetőnek a célt, hogy az EU az információs technológiák jogi, gazdasági és társadalmi kihasználásával megerősítse helyzetét a világpiac vezető gazdasági térségei között. Ebből a nézőpontból irányozza elő az Európai Unió tagországainak fejlesztési és együttműködési teendőit az információs társadalom kialakítása érdekében.

Figyelemre méltó, hogy a szerkesztők már ekkor, az első lépések megtételekor is gondolnak a szükséges kiberbiztonsági stratégia kialakítására, ugyanis az irat az informatikai biztonság megteremtése, a tranzakciók biztonságos és hiteles lebonyolítása érdekében szükséges lépéseket is felvázolja.

Az *Elektronikus védelem (encryption), jogvédelem és biztonság* című fejezet szerint „az elektronikus védelem különösen fontos a távkereskedelemben, amely abszolút garanciákat igényel olyan területeken, mint az aláírások és a szöveg integritása, visszavonhatatlan időpont és dátum pecsételés és nemzetközi jogi elismerés".

A nemzetközi összefogás mellőzhetetlenségére is rámutatnak: „a rendszer megoldására nemzeti szinten adott válasz egészen biztosan nem lesz kielégítő, mivel a hírközlés túlnyúlik a nemzeti határokon és a belső piac alapelvei tiltják az olyan intézkedéseket, mint a dekóder berendezések importjának tilalma".

A szükséges fejlesztések és a szabályozási környezet kialakítását nagyon sürgős feladatnak tekintik, s a jelentést szövegező bizottság „javasolja az elektronikus és jogi védelem, továbbá a biztonság kérdésével összefüggő munkák felgyorsítását európai szinten".

A mából visszatekintve sajátosnak tekinthető szempontot is felvet a Jelentés, mikor a biztonsági intézkedések és rendszabályok miatti kényelmetlenségtől tartva arra figyelmeztet, hogy „az elektronikus védelem megnövekedett alkalmazása és az egyedi elektronikus rendszerek kifejlesztése növeli azok számát, akik elfordulnak a rendszerbe való becsatlakozástól a fizetés vagy a titoktartási kötelezettségek elkerülésére".

A tények és fejlemények ismeretében ma már elég nagy biztonsággal kijelenthetjük, hogy ezek az aggodalmak megalapozatlannak bizonyultak. Az informatikai biztonság iránti igény érzékelhetően növekszik, és ma sokkal inkább bizalomerősítő, mint elrettentő hatását látjuk. Ettől az apró melléfogástól eltekintve a jelentés ma is érvényes üzeneteket és célokat fogalmaz meg az európai információs társadalom fejlesztése iránt elkötelezett érdekeltek számára.

Bangemann-jelentés 1994-es elfogadását követő évtizedek európai közösségi dokumentumai jelentős részben újra és újra – természetesen nagyobb részletességgel és

kidolgozottabb tartalommal – megismételték az eredeti célkitűzéseket. Így egyebek mellett az informatikai biztonság szabályozása, az ezzel kapcsolatos szolgáltatási, ellenőrzési és szabványosítási témák is többször előkerültek. Ennek következtében a témára vonatkozó szabályozási anyag egyre érettebbé, az intézményrendszer pedig differenciáltabbá válik.

2.1.2 Az Európai Digitális Menetrend

A jelenleg irányadó európai uniós stratégiai dokumentumban, az Európai Digitális Menetrendben is kitüntetett figyelem irányult a kibernetikai biztonság kérdésére. A fogyasztóbarát egységes digitális piac megteremtésének céljához jól illeszkedik a biztonságos digitális környezet garantálása. **A számítógépes bűnözés terjedése miatt emberekben erős bizalmatlanság él a hálózatokkal kapcsolatban.** Az európai polgárok nem szívesen használják az online alkalmazásokat, mert nem érzik úgy, hogy teljes mértékben megbízhatnának az internetben. Ezért továbbá növelni kell a digitális szolgáltatásokba vetett bizalmat[1] és támogatni kell a távközlési szolgáltatások egységes piacának megerősödését.

A tisztességes, nyílt és biztonságos digitális környezet biztosítása érdekében az Európai Unió az alábbi elvekre építette a digitális egységes piaci stratégiát:

- a fogyasztók és vállalatok könnyebb hozzáférése a digitális termékekhez és szolgáltatásokhoz Európa-szerte;
- megfelelő körülmények teremtése a digitális hálózatok és szolgáltatások számára, hogy felvirágozzanak, és maximalizálják a digitális gazdaság növekedési potenciálját.

Ennek gyakorlatba ültetése során megtörtént az új adatvédelmi szabályozási keretek kidolgozása, a kiberbiztonsági szabályok reformját célzó jogalkotási munka, beleértve a biztonsági tanúsítást is.

A Digitális Menetrend céljai közé tartozik a digitális gazdaság növekedési potenciáljának maximalizálása, a digitális készségek és a magas teljesítményű számítástechnika előmozdítása, az ipar és a szolgáltatások digitalizálása, a mesterséges intelligencia fejlesztése, valamint a közszolgáltatások korszerűsítése révén.

A kezdeményezés kiterjed a számítógépes támadások elleni gyorsreagálású európai rendszer létrehozására, ennek részeként a kiberbiztonsági vészhelyzeteket kezelő csoportok hálózatának kialakítására, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepének megerősítésére.

2.2 Nyílt, megbízható és biztonságos kibertér. Az EU kiberbiztonsági stratégiája

A Digitális Menetrend keretében készült el az Európai Unió kiberbiztonsági stratégiája 2013-ban. A legfontosabb célkitűzést már a dokumentum alcíme is világosan kifejezi: *Nyílt, megbízható és biztonságos kibertér.*

1 Tóth András (2017), 17.

A dokumentum a kiberbiztonsággal kapcsolatban meghatározza a közösség számára iránymutatásként szolgáló alapelveket és ezekhez stratégiai prioritásokat rendel. Ezek együttesen jelölik ki az Európai Unió számra a kiberbiztonság terén követendő cselekvés stratégiai kereteit.

Az alapelvek[2] a következőkben foglalják össze azt a közös jövőképet, amit az információs társadalom kialakítása és fejlesztése terén az Unió követni kíván:

- Az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális világra, mint a fizikai világra.
- Ugyanazok a törvények és normák vonatkoznak a kibertérre, mint amelyek mindennapjaink más területein is érvényesek.
- Az alapvető jogok, a szólásszabadság, a személyes adatok és a magánélet védelme.
- Mindenki számára biztosított hozzáférés.
- Demokratikus és hatékony, számos érdekelt fél bevonásával történő irányítás.
- A biztonság közös felelősség.

A fenti elvekhez pedig öt stratégiai prioritás kapcsolódik, amelyek a hosszú távú célok érdekében a fenntartható és biztonságos digitális környezetet megteremtik:

- A kibertámadásokkal szembeni ellenálló képesség elérése.
- A számítástechnikai bűnözés drasztikus csökkentése.
- Kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (kbvp) tekintetében.
- Kiberbiztonsági ipari és technológiai erőforrások kifejlesztése.
- Összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása.

2.3 A szabályozási keretek és az intézményrendszer főbb elemei

Jelenleg az Unió informatikai biztonsági szabályozási keretrendszerét az alábbi fő elemek alkotják:

- A 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.
- Az 526/2013/EU rendelet az európai uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről.
- A GDPR, azaz a 2016/679 rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelvhatályon kívül helyezéséről.
- A 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

2 EU kiberbiztonsági stratégia.

A szabályozási csomag elemein kívül a kiberbiztonsági infrastruktúra lényeges elemei a megfelelő reagálásra képes alábbi operatív szervezetek. Az infrastruktúra kétszintű hierarchiába szervezve – uniós és tagállami szinten – látja el az informatikai biztonság fenntartásához szükséges és ehhez kapcsolódóan a közösségi koordináció feladatait.

Az Unió szintjén a következő szervezetek a legfontosabbak:

2.3.1 ENISA

Az ENISA (European Union Agency for Network and Information Security), azaz az Európai Hálózat- és Információbiztonsági Ügynökség a közösség informatikai biztonsági műveleteit és fejlesztési politikáját koordináló központi operatív szerv. Az Ügynökség székhelye Heraklion, Kréta szigetén, Görögországban. Emellett Athénban is fenntart egy operatív irodát.

Az ügynökséget eredetileg a 460/2004/EK rendelettel alapították meg. Ez a jogszabály mára hatályát vesztette; helyét az európai uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) szóló 526/2013/EU rendelet vette át.

Az ENISA aktívan hozzájárul az Unióban a magas szintű hálózati és információbiztonsági (NIS) infrastruktúra és szolgáltatások kiépítéséhez. Az Ügynökség szorosan együttműködik a tagállamokkal és a magánszektorral, számukra tanácsokat és megoldásokat dolgoz ki. Ez magában foglalja a páneurópai kiberbiztonsági gyakorlatokat, a nemzeti Cyber Security stratégiák fejlesztését, a CSIRT-k együttműködését és kapacitásépítését, valamint tanulmányokat a felhőalapú szolgáltatások biztonságos alkalmazásáról. Foglalkozik továbbá az adatvédelem kérdéseivel, a magánélet védelmét erősítő technológiákkal és a magánélet védelmével a feltörekvő technológiák, az elektronikus személyazonosítási rendszerek használata és fejlesztése terén. A digitális aláírás és az egyéb bizalmi szolgáltatások sérülékenységeinek vizsgálatán túl továbbá fontos szerepet tölt be a kibertérben érzékelhető fenyegetések és sérülékenységek azonosítása, feltérképezése és az ellenük való védekezés módjának kidolgozása terén.

Az ENISA továbbá hozzájárul az EU hálózati és információbiztonsággal kapcsolatos politikájának megvalósulását, a vonatkozó jogszabályok érvényre juttatását és a szabályozási keretrendszer továbbfejlesztését szolgáló tevékenységekhez.

2.3.2 CERT-EU (Computer Emergency Response Team)

A CERT-EU-t egy évnyi – sikeresnek ítélt – kísérleti előkészítő időszak után hozták létre az EU intézményei mint a közösség állandó számítógépes vészhelyzeti reagáló csoportját. Tevékenységét az EU intézményeire, ügynökségeire és testületeire vonatkozóan fejti ki, de ezenfelül részt vállal a tagállamokkal folytatott informatikai biztonsági együttműködésben is. A csapat az EU legfontosabb intézményei (az Európai Bizottság, a Tanács Főtitkársága, az Európai Parlament, a Régiók Bizottsága, a Gazdasági és Szociális Bizottság) IT-biztonsági szakembereiből áll. Szorosan együttműködik a tagállamokban és azokon kívül más CERT-ekkel, valamint a szakosodott informatikai biztonsági vállalatokkal. A CERT-EU fokozatosan bővíti szolgáltatásait az alapítók igényei szerint és a szakterület követelményei alapján, figyelembe véve a rendelkezésre álló kompetenciákat, forrásokat és a jelentkező kihívásokat.

2.3.3 Tagállami szervek

A tagállami CERT vagy CSIRT a tagállami szinten jelentkező információbiztonsági feladatok ellátásának központi szerve. Ennek révén kapcsolódik a tagállam a közösségi együttműködési rendszerbe és vesz részt a közösségi feladatok ellátásában. Magyarországon ezt a szerepet a *Nemzetbiztonsági Szakszolgálat* részeként működő *Nemzeti Kibervédelmi Intézet* látja el.

A Nemzeti Kibervédelmi Intézet (NKI) alárendeltségében működő *Kormányzati Eseménykezelő Központ* látja el az operatív kiberbiztonsági tevékenységet. Feladata a kibertérből érkező támadásokkal és fenyegetettségekkel szembeni fellépés, a közvetlen incidenskezelés. Az NKI e szerven keresztül tart fenn kapcsolatot a szakterületi és vállalati információbiztonsági incidenskezelő központokkal.

Szintén az NKI szervezeti rendszerében működik a *Nemzeti Elektronikus Információbiztonsági Hatóság*, mely az információbiztonságról szóló 2013. évi L. törvénnyel és végrehajtási rendeletével összhangban a kapcsolódó hatósági feladatokat látja el. Tevékenységi körébe tartozik az ügyfelek regisztrációja, az Ibtv. szerinti informatikai biztonsági osztályokba történő besorolások hatósági ellenőrzése, a magyar interneten észlelt biztonsági incidensekről szóló bejelentések fogadása és kezelése, magyar joghatóság alatt álló szervezet külföldön végeztett adatkezelésének engedélyezése.

2.4 A kritikus infrastruktúra védelme

Az úgynevezett ECI irányelv, azaz az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv az első volt az európai infrastruktúrák sérülékenységeinek azonosítására és ezek kivédésére irányuló szabályozás körében. Az irányelv elsősorban az energetikai rendszerekre és a közlekedési hálózatokra koncentrál.

Az *energetikai szektorban* a kritikus infrastruktúra elemei lehetnek az alábbiak:

- Villamosenergia-ipar
  - Villamosenergia-termelésre és -továbbításra szolgáló infrastruktúrák és létesítmények a villamosenergia-ellátás tekintetében.
- Olajipar
  - Olaj termelése, finomítása, feldolgozása, tárolása és vezetékes szállítása.
- Gáz
  - Gáz termelése, finomítása, feldolgozása, tárolása és vezetékes szállítása.
  - LNG-terminálok.

A *közlekedési ágazatban* a következő rendszerelemek minősülhetnek kritikus infrastruktúrának:

- közúti közlekedés,
- vasúti közlekedés,
- légi közlekedés,
- belföldi vízi közlekedés,
- óceáni és rövid távú tengeri hajózás és kikötők.

Alapelvként azt rögzíti, hogy ezek védelme elsősorban a tagállamok és a tulajdonosok[3] felelőssége és feladata. A szabályozás alapegysége is a *tagállami kritikus infrastruktúra*, vagyis a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban. Az irányelv azonban nem elsősorban ezekre, hanem az *európai kritikus infrastruktúra* elemeire koncentrál.

Ezek azok az egyes tagállamokban található olyan kritikus infrastruktúrák vagy elemei, amelyek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra. A hatás jelentőségét horizontális kritériumok alapján kell értékelni. Ide tartoznak azok a hatások is, amelyek az egyéb típusú infrastruktúrákkal fennálló, ágazatokon átnyúló kölcsönös függőségből erednek.

A Közösségben számos olyan kritikus infrastruktúra van, amelyek működési zavara vagy megsemmisítése több tagállamban is komoly következményekkel járna. Ilyen következmények lehetnek az összekapcsolt infrastruktúrák közötti interdependenciából fakadó, a határokon átnyúló, több ágazatot érintő hatások. Az ilyen kritikus infrastruktúra-elemeket a tagállamok közös eljárással azonosítják és jelölik ki, és a rájuk vonatkozó biztonsági követelményeket is közös minimumszabályok alapján határozzák meg. A kritikus infrastruktúrák védelme területén a tagállamok közötti kétoldalú együttműködési rendszerek jól megalapozott és hatékony eszközt jelentenek a határokon átnyúló kritikus infrastruktúrák kezelésében. Az EPCIP-nek ilyen együttműködésre kell épülnie.

2.5 A hálózati és információs rendszerek biztonsága

A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelv az EIC irányelv hatályán kívül eső, gyakorlatilag azonban egyre magasabb értéket képviselő és fokozódó kockázatoknak kitett hálózati és kommunikációs infrastruktúra védelme érdekében alakít ki egységes európai szabályozási kereteket. A szabályozás részben átfedi az EIC irányelv hatókörét, amennyiben az energetika és a közlekedés nagy alrendszerei mindkét irányelv védelme alatt állnak.

A szabályozás alapvetően különbséget tesz az *alapvető szolgáltatásokat nyújtó szereplők* és a *digitális szolgáltatók* között.

2.5.1 Alapvető szolgáltatások

Az alapvető szolgáltatásokat nyújtó szereplőket hét ágazatba és ezek néhány alágazatába sorolja a szabályozás.

- Energia
    - Villamosenergia-ipar
    - Olajipar

3 Tóth András (2017), 21.

    - Gáz
- Közlekedés
    - Légi közlekedés
    - Vasúti közlekedés
    - Vízi közlekedés
    - Közúti közlekedés
- Banki szolgáltatások
- Pénzügyi piaci infrastruktúrák
- Egészségügy
- Ivóvízellátás és -elosztás
- Digitális infrastruktúra

2.5.2 Digitális szolgáltatások

A hatálya alá tartozó digitális szolgáltatások körét három pontban határozza meg az irányelv:

- Online piactér
- Online keresőprogram
- Felhőlapú számítástechnikai szolgáltatás

Ez utóbbiak körében szokás szerint megkülönböztethetjük az infrastruktúra-, a platform- és a szoftver-szolgáltatásokat az alábbiak szerint:

    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (SaaS)

2.5.3 Az elvárt védelmi intézkedések

A szabályozás leglényegesebb követelménye a megfelelő nemzeti stratégia kidolgozása a védett rendszerek biztonságos üzemeltetése érdekében, továbbá az együttműködés. Ez a kötelezettség fennáll az adott rendszerelemek működtetői és a nemzeti biztonsági hatóságok között, valamint a jelentősebb, több országot érintő biztonsági események tekintetében a tagállamok között is.

Az *alapvető szolgáltatásokat nyújtó szereplők* megfelelő és arányos műszaki és szervezési intézkedéseket tesznek a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. Az intézkedések kidolgozása során tekintettel kell lenni a tudomány és a technika állására és a felmerülő kockázatok nagyságára. Elsősorban a biztonsági események megelőzésére és azok hatásainak csökkentésére kell törekedni, hogy csökkenthető legyen a szolgáltatások kieséséből eredő tovagyűrűző kár.

3 A MAGYAR KIBERTÉR VÉDETT ELEMEI

A hazai informatikai biztonsági rendszer alapvető célja az, hogy megteremtse és hosszú távon garantálja Magyarország nemzetbiztonsági érdekeinek, létfontosságú rendszereinek sértetlenségét, biztonságát, rendelkezésre állását az információs társadalom viszonyai között és a globális, valamint hazai kibertérben felmerülő sokféle fenyegetéssel és kockázattal szemben.

A *globális kibertér* fogalma alatt értjük a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét.

Ettől megkülönböztetjük – mint a globális rendszer alrendszerét – a magyar kiberteret, mely a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne.

Az ország kiberbiztonsági stratégiájával összhangban számos olyan jogszabály született, illetve módosult az elmúlt években, melyek az információs rendszerek biztonságát és a bennük tárolt, feldolgozott adatok védelmét szolgálják. Ebben a fejezetben ennek a szabályozási anyagnak azokat a legfontosabb darabjait tekintjük át, amelyek a védett információs rendszerek szektorális elemeire vonatkoznak, majd a következő fejezetekben kifejezetten az elektronikus információs rendszerek biztonságára vonatkozó szabályozás legfontosabb pillérjét képező informatikai biztonsági törvényt és végrehajtási rendeletét ismertetjük.

3.1 Magyarország kiberbiztonsági stratégiája

Magyarország nemzeti kiberbiztonsági stratégiáját az 1139/2013. (III. 21.) Korm. határozattal fogadta el a Kormány.

3.1.1 A stratégia céljai

A stratégia célja, hogy 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.

3.1.1.1 Szabad és biztonságos kibertér

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.

3.1.1.2 A gazdaság és társadalom szabad tevékenységének védelme

Célja továbbá a nemzetgazdaság és a 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.

3.1.1.3 Fenyegetések megelőzése, kivédése, kezelése

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.

A stratégia támaszkodik az Európa Tanács 2001-ben Budapesten elfogadott számítógépes bűnözés elleni egyezményének elveire („Convention on Cybercrime”), mely nemzetközi egyezményt referenciaként hivatkozzák és 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.

3.1.2 Magyarország kiberbiztonsági környezete

A stratégia megállapítja, hogy a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.

A kibertérben megjelenő, különböző forrásból származó fenyegetések megnövekedett száma és ezek nagyságrendekkel megnövekedett következményei jelzik, hogy az elmúlt évtizedben nagy gyorsasággal nőtt azon állami és nem állami felhasználók száma és hatékonysága, akik a kiberteret kritikus adatok, információk illegális megszerzésére, valamint a kommunikációs és informatikai rendszerekben történő károkozásra használják. Elektronikus információs rendszereinkre, illetve azokon keresztül létfontosságú rendszereink és létesítményeink működésére jelent fenyegetést a hadviselés új formája, az információs hadviselés, ami által a modern hadviselés egyik legfontosabb színtere a kibertér lett. A külső károkozások mellett további kockázatot jelent, hogy a kibertér alkotóelemeiként szolgáló

informatikai és hírközlési rendszerek üzembiztonsági szabályozása sem kellően rendezett. A dinamikusan megjelenő új technológiák, mint például az informatikai felhő vagy a mobilinternet, újabb biztonsági kockázatok folyamatos kialakulásához vezetnek. Jelen stratégia egyik fő célja annak a döntéshozó politikai és szakmai figyelemnek és képességnek a kiépítése, mely rugalmasan reagálva lehetővé teszi a belátható jövőben a technológiai fejlődésből fakadó új kiberbiztonsági problémák kezelését.

A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

Ezek a gondolatok már jól érzékelhetően vetítik előre a stratégiaalkotást követő évek új jogszabályait, melyek az elektronikus kereskedelmi és elektronikus közigazgatási szolgáltatásokat fejlesztve az informatikai biztonságot is erősíteni kívánják.

3.1.3 Magyarország kiberbiztonsági értékrendje, jövőképe, céljai

3.1.3.1 Nemzeti szuverenitás védelme a kibertérben

Magyarország szuverenitásának védelme a magyar kibertérben is nemzeti érdek; a magyar kibertér szabad, demokratikus jogállami és biztonságos működését alapvető értéknek és érdeknek tekinti. Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével, összehangolt tevékenységével valósul meg.

3.1.3.2 Együttműködés a hasonló kiberbiztonsági célokat valló országokkal és egyéb szereplőkkel

Magyarország a globális kibertér minden Magyarországgal hasonló értékrendet valló állami és nem állami szereplőjével kölcsönös bizalmon alapuló együttműködés kialakítását és fenntartását célozza meg, továbbá szövetségi és nemzetközi kapcsolati rendszerén, különösen az EU és a NATO, továbbá az Európai Biztonsági és Együttműködési Szervezet (EBESZ), az ENSZ, az Európa Tanács és más nemzetközi szervezeti tagságán keresztül törekszik a globális kibertér szabad és biztonságos használatának szavatolására. Magyarország tudatában van annak, hogy a kibertérben megjelenő fenyegetések és támadások elérhetnek egy olyan szintet, ami szövetségesi együttműködést tehet szükségessé, ezért kiemelten fontosnak tartja, hogy a kiberbiztonság kérdése bekerült a NATO Alapító Okmányának 5. cikkelye alá tartozó kollektív védelem körébe. E szövetségesi nemzetközi együttműködésben Magyarország saját biztonsága miatt is érdekelt. Magyarország különös figyelemmel tekint a közép- és kelet-európai régióra, melynek kiberbiztonságát regionális együttműködések keretében tovább erősíthetőnek látja.

3.1.3.3 Innováció és biztonság a jövő érdekében

A stratégia szerint Magyarországnak a jelen és a jövő kihívásaihoz igazodva arra kell törekednie, hogy a magyar kibertér nyújtson biztonságos és megbízható környezetet:

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

3.2 A nemzeti adatvagyon

3.2.1 A nemzeti adatvagyon fokozott védelméről szóló törvény jelentősége

A *nemzeti adatvagyon* a 2010. évi CLVII. törvény értelmező rendelkezései szerint a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.

A nemzeti adatvagyon fogalmi köre azon adatfajtákra terjed ki, amelyek integritásának és hozzáférhetőségének védelméhez kiemelt közérdek fűződik, vagy azt az adatalanyok alapjogainak védelme indokolja.

A nemzeti adatvagyon-törvény legfontosabb rendeltetése az volt, hogy számos adatkezeléssel kapcsolatos jogszabályt módosított, kiegészített. Rendelkezései beépültek az

- elektronikus hírközlési törvénybe (2003. évi C. törvény),
- az azóta már hatályát vesztett Art.-be, és az elektronikus közszolgáltatásokról szóló törvénybe (2009. évi LX. tv.),
- a régi Btk.-ba.

A sok hatályon kívül helyezés láttán joggal tehetjük fel a kérdést, hogy van-e egyáltalán jelentősége ennek a törvénynek. Nos, kimondhatjuk, hogy van, mert a rendelkezések sorrarendre átkerültek a régiek helyébe lépő új jogszabályokba.

Például a kicsit cifra nevű „*a nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény*” tényállása még a régi Btk.-ban jelent meg a nemzeti adatvagyontörvény nyomán, de lényegében azonos tartalommal megtaláljuk az új Btk.-ban is.

3.2.2 A törvény célja

A törvény célja, hogy a kezelt adatok jellegére és a nyilvántartások alapján végzett állami feladatok fontosságára tekintettel kiemelt jelentőségű állami nyilvántartások védelmét biztosítsa egyfelől annak előírásával, hogy a jövőben e nyilvántartásokkal kapcsolatban adatfeldolgozói tevékenységet is csak az állami szférába tartozó, ily módon az adatkezelő által

közvetlenül ellenőrizhető szervezet láthasson el, másfelől az ilyen nyilvántartások jogszerű felhasználását akadályozó cselekmények büntetőjogi szankcionálásával.

A nemzeti adatvagyon körébe tartozó adatállományok tekintetében a törvény az *adatkezeléssel megbízható jogalanyok* körét *szűkítheti*, vagy az adatfeldolgozással való megbízás lehetőségét az adott adatkezelő meghatározott adatállománya részéről *teljesen kizárhatja*. A törvény előírja továbbá, hogy abban az esetben, ha az ágazati törvény az adatfeldolgozók lehetséges körét szűkíti, az adatkezelő csak a kormányrendeletben az általa kezelt nyilvántartás vonatkozásában megjelölt jogalannyal vagy jogalanyokkal köthet adatfeldolgozási szerződést.

A törvény annak érdekében, hogy a nemzeti adatvagyon körébe tartozó nyilvántartások adatállományának kellő védelme biztosított legyen, előírja, hogy ezekkel kapcsolatban az adatfeldolgozással megbízott szerv vagy szervezet adatfeldolgozási műveletet – így különösen az adatok tárolását – csak Magyarország területén végezhet.

3.2.3 Az elektronikus kormányzati szolgáltatásokat támogató nyilvántartások

A modern elektronikus kormányzati és közszolgáltatási szolgáltatások – és általában az államszervezet – működésében az elektronikus nyilvántartások mellőzhetetlenül fontos szerepet töltenek be. A szabályozás által érintett nyilvántartások informatikai rendszerekben létező adatbázisok, virtuális térben vezetett nyilvántartások, ezért e nyilvántartások esetében sajátos szabályok alkalmazása szükséges. Ezeket tartalmazza az általános megfogalmazás szintjén a törvény. A törvény rögzíti továbbá, hogy ha adatfeldolgozó igénybevétele kötelező, akkor az elektronikus adatfeldolgozás ellenértékének biztosítására az elektronikus kormányzati szolgáltatások infrastrukturális megvalósíthatóságának és üzemeltetésének biztosításáért felelős miniszter *közszolgáltatási szerződést köt* az adatfeldolgozóval. Az adatkezelő és az adatfeldolgozó jogai, kötelességei és felelősségi viszonyai ebben az esetben is az általános törvényi előírások – tehát az Infotv. szabályai – szerint alakulnak.

3.2.4 Büntetőjogi védelem a kiemelten fontos nyilvántartásoknak

A törvény egyes, az állam működésének szempontjából kiemelkedően fontos nyilvántartásokban kezelt adatok feldolgozását csak állami szerv vagy kizárólagos állami tulajdonban lévő gazdálkodó szervezet számára teszi lehetővé. Az ebbe a körbe tartozó nyilvántartásokban kezelt adatokhoz való folyamatos hozzáférés biztosítása az adatkezelő számára a közigazgatás folyamatos és zavartalan működésének biztosítása szempontjából olyan közérdek, amelynek megsértése indokolttá teszi a büntetőjogi szankcionálást. Erre tekintettel a törvény a Büntető Törvénykönyvet új tényállással egészítette ki.

A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény tényállása alapján három évig terjedő szabadságvesztéssel büntetendő, aki a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatnak az adatkezelő részére történő *hozzáférését* vagy az adatkezelés körébe tartozó *művelet elvégzését akadályozza vagy lehetetlenné teszi*. A tényállás minősített esetként azonosítja a jelentős érdeksérelem okozását. Ebben az esetben a cselekmény öt évig terjedő szabadságvesztéssel büntetendő.

A régi Btk.-ban még megvolt, az újból hiányzik az az értelmező rendelkezés, amely a nemzeti adatvagyon körébe tartozó állami nyilvántartást definiálná. Ez esetleg a jelenlegi törvény Btk. alkalmazása során értelmezési bizonytalanságra vezethet. Eredetileg azt a nyilvántartást kellett ez alatt érteni, amelyben adat feldolgozását törvény alapján kizárólag állami szerv vagy kizárólagos állami tulajdonban lévő gazdálkodó szervezet végezheti, függetlenül attól, hogy az adatfeldolgozást ténylegesen ilyen szerv látja-e el.

3.3 Bizalmi szolgáltatások

3.3.1 A jelenlegi szabályozási keretek kialakulása

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény lényegében az eIDAS-rendelet alapján született, és az EU közösségi szabályozását jelentős részben megismételve rendelkezik a bizalmi szolgáltatásokról. Az Európai Unióban az elektronikus aláírásokról korábban az 1999/93/EK irányelv rendelkezett. A legtöbb tagállamban ez alapján született meg a saját nemzeti törvényi szabályozás az e-aláírásokra. Magyarországon ez volt az elektronikus aláírásról szóló 2001. évi XXXV. törvény (a továbbiakban: Eatv.).

Az irányelvet 2014-ben váltotta fel az eIDAS-rendelet, azaz a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU rendelet. Ennek nyomán, az eIDAS-rendelet jobb alkalmazhatósága, a magyar jogrendszerbe való könnyebb illeszkedése érdekében alkotta meg az Országgyűlés az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvényt (E-ügyintézési törvény).

Ezek a rendelkezések léptek a magyar jogrendszerben az Eatv. helyébe.

A bizalmi szolgáltatások kulcsfontosságú szerepet töltenek be az információs társadalom adatfeldolgozó rendszereinek és különböző online szolgáltatásainak biztonságos üzemeltetésében. Ezek a bizalmi szolgáltatások az eIDAS-rendelet 3. cikk 16. pontja szerint olyan rendszerint ellenszolgáltatás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:

a) elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
b) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
c) elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése.

Ennek fokozatos hatálybalépése által folyamatosan történt meg a rendeleti szintű részletszabályok elfogadása és a jogharmonizáció. A tagállamoknak hatályon kívül kell helyezniük e-aláírás szabályozásuk nagy részét, mivel a rendelet szövege és a végrehajtási szabályok közvetlen belső jogi hatállyal bírnak és kötelezően alkalmazandók.

Az eIDAS-rendelet főbb újdonságai:

- A felügyeleti szervek nagyobb mértékben vannak együttműködésre kötelezve egymással és az Európai Bizottsággal.

- Az e-azonosítási rendszerek terén együttműködési kötelezettség jelenik meg: ez tartalmilag a többi tagállam e-azonosítási megoldásainak kötelező vizsgálata, és sikeres vizsgálat után kényszerű elfogadása. Ezáltal a valamely tagállam bejelentett, megfelelő (alacsony, jelentős vagy magas) biztonsági szintű e-azonosítási megoldását használó természetes vagy nem természetes személy képes lesz másik tagállam elektronikus szolgáltatásaihoz hozzáférni, határokon átívelő módon.

3.3.2 Az implementációval kapcsolatos megfontolások

A rendeleti formából és a kiterjedt hatályos magyar elektronikus aláírási szabályozásból következően az átültetést meghatározó feladat a deregulációs kötelezettség, másrészről azonban be kell azonosítani azokat a rendelkezéseket is, amelyekre az eIDAS-rendelet végrehajtása miatt van szükség. Az eIDAS-rendeletben kifejezetten előírt, a tagállamra ruházott kötelező végrehajtási jogalkotás terjedelme igen szűk, ugyanakkor jelentős az olyan szabályok köre, amelyre azért van szükség, hogy a kötelezően alkalmazandó uniós szabályok hatékonyan alkalmazhatóak legyenek.

A fentiekre tekintettel a bizalmi szolgáltatásokról szóló törvény a korábbi elektronikus aláírásról szóló törvény rendelkezései és a kialakult hatósági gyakorlat megőrzésére törekszik úgy, hogy egyúttal e rendszert hozzáillessze az eIDAS-rendelet szerkezetéhez és fogalmaihoz.

A szakirodalom már kritikával illette a törvénynek azt a sajátos fogyatékosságát, hogy nem vette át a korábbi Eat. 4 § (1) bekezdésének „hídszabályát", amely szerint a fokozott biztonságú elektronikus aláírások kielégítik az írásba foglaltság törvényi követelményeit. „Ebből fakadóan most előfordulhat, hogy egyazon elektronikus dokumentum jogi minősítése eltér attól függően, hogy közigazgatási hatósági eljárás, polgári per, avagy munkajogi vita rendezése során használják fel azt."[1]

A törvény szerkezetét illetően először a valamennyi bizalmi szolgáltatásra vonatkozó általános feltételeket rögzíti (beleértve a tanúsítványt kibocsátó bizalmi szolgáltatásokra vonatkozó olyan közös szabályokat is, amelyek nem kifejezetten az aláírás vagy bélyegző létrehozással kapcsolatosak, hasonlóan az eIDAS-rendelet 24. cikkéhez). Ezen fejezetben találhatóak a szolgáltatás nyújtásának megkezdésével, a szolgáltatási szerződéssel és a tanúsítványokkal összefüggő ellenőrzéssel kapcsolatos kötelezettségek, valamint a bizalmi szolgáltatás keretében kibocsátott tanúsítványok ideiglenes felfüggesztésével és visszavonásával kapcsolatos szabályok.

Ezt követően egy külön fejezetben olvashatóak a bizalmi szolgáltatás nyújtásának befejezésével kapcsolatos szabályok, amelyeket a bizalmi szolgáltatókat terhelő adatszolgáltatási kötelezettségek és a felügyeleti szabályok fejezete követ. Ez utóbbi fejezet jelöli ki az eljáró hatóságot (a Nemzeti Média- és Hírközlési Hatóságot), amelynek eljárására az általános közigazgatási rendtartás irányadó. Ez a fejezet tartalmazza a nem megfelelés esetén alkalmazható jogkövetkezményeket és az alkalmazható bírságok mértékét is.

1 Szádeczky–Szőke–Zámbó (2017), 4.

3.3.3 Általános háttérszabályok az elektronikusan hiteles iratok átalakítására

A törvény pótolta azt a hiányosságot, hogy korábban nem volt általános háttérszabály az elektronikus úton hitelesített iratok hiteles papíralapú kiadmánnyá történő átalakíthatóságáról.

Ennek orvoslása céljából – abban az esetben, ha jogszabály bizonyos körben nem rendelkezik másképp – az egyéb megoldásoktól (központilag kijelölt hitelesítő, iratérvényességi nyilvántartás) függetlenítve a törvény kimondja, hogy a közfeladatot ellátó szerv által kiállított hiteles elektronikus iratról a kiállító szerv vagy jogutódja – tehát csak saját maga – hiteles papíralapú másolatot állíthat ki, megfelelő záradék felvezetésével.

A törvény háttérszabályt ad arra az esetre is, hogy ha az akarategység szempontjából lényeges egy okirat több fél általi hiteles aláírása, melyik kiadmány minősül hitelesnek, ha az egyik fél elektronikus aláírást kíván használni, a másik fél pedig hagyományosan ír alá (a törvény értelmében az elektronikusan kiadmányozott iratról készült, záradékkal hitelesített papíralapú másolaton a másik fél aláírásával hitelesített irat).

3.3.4 A bizalmi szolgáltatások uniós rendszere

Az online szolgáltatásoknál használt elektronikus azonosítás körében az eIDAS-rendelet a tagállami önkéntesség és a kölcsönös elismerés elvére építi a szabályozást. Azaz egy tagállam szabadon eldöntheti, hogy a tagállamban használt valamely elektronikus azonosítási rendszerét bejelenti-e a Bizottságnak, de ha bejelenti, akkor ezt a rendszerét (adott biztonsági szinten belül) minden más tagállam is köteles elismerni, aki már tett ilyen bejelentést. Pontosabban ez az elismerés csak azon közigazgatási szervek által nyújtott szolgáltatások online elérésére terjed ki, amelyek a tagállamon belül a bejelentett rendszert használják. E körben tehát a tagállami szabályozási szabadság a rendeleti szabályozási szint ellenére is alapvetően érintetlen marad.

Az eIDAS-rendelet másik eszköze a bizalmi szolgáltatások uniós kerete. Itt az elektronikus aláírások kapcsán már kialakult egyes szolgáltatástípusok alapján határozzák meg az általánosabb „bizalmi szolgáltatás” fogalomkörét, és az ilyen szolgáltatások felügyeletének uniós rendjét, beleértve a minősített és nem minősített szolgáltatások közötti különbségtételt is. Az eIDAS-rendelet tételesen nevesít néhány bizalmi szolgáltatást is, és egyes bizalmi szolgáltatásokhoz uniós szinten joghatásokat is rendel (pl. a *minősített elektronikus aláírás* a saját kezű aláírással azonos joghatású, *minősített időbélyegző* esetében vélelmezni kell a feltüntetett dátum és időpont pontosságát és a hozzá kapcsolt adatok sértetlenségét stb.). Az azonosítástól eltérően azonban a bizalmi szolgáltatások uniós kerete jelentősen meghatározza a hazai szabályozási mozgásteret is.

3.4 Az elektronikus aláírás szabályozása és jogi alkalmazása

Az elektronikus aláírás szabályozási kereteit nemzetközi és hazai jogszabályok együttesen alkotják. Az Európai Unió 1999. december 13-án bocsátotta ki az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló 1999/93/EK irányelvet. A tagállamok ennek alapján dolgozták ki saját belső nemzeti szabályozásukat.

Az irányelv állást foglal néhány lényeges kérdésben. Így biztosítja, hogy a kulcsfontosságú hitelesítés-szolgáltatást nyújthatja állami szerv, illetve természetes vagy jogi személy, amennyiben ez utóbbit a nemzeti jognak megfelelően hozták létre. Elvárja ugyanakkor, hogy a tagállamok gondoskodjanak olyan akkreditációs rendszer kialakításáról, amely a szolgáltatók minőségi és törvényességi kritériumoknak való megfelelését felügyeli.

Az irányelv hozzájárul az elektronikus aláírások közösségen belüli alkalmazásához és jogi elismeréséhez. Az elektronikus hitelesítési módszerek általános elfogadásának támogatása érdekében biztosítani kell, hogy az elektronikus aláírásokat minden tagállamban bizonyítékként lehessen felhasználni a bírósági eljárásokban, ugyanakkor az irányelv nem sérti a bizonyítékok szabad bírói mérlegelésére vonatkozó nemzeti szabályokat. Ezen túlmenően a nemzeti jog határozza meg, hogy a jog mely területein lehet elektronikus dokumentumokat és elektronikus aláírást alkalmazni. A hitelesítés-szolgáltatókra vonatkozó felelősségi szabályokat ugyancsak a nemzeti jog állapítja meg.

A hazai szabályozás gerincét a bizalmi szolgáltatásokról szóló törvény, a polgári perrendtartásról szóló törvény (Pp.) vonatkozó szakaszai, valamint a Polgári törvénykönyvnek (Ptk.) a jognyilatkozatokról – különösen az írásbeli alakhoz kötött nyilatkozatok érvényességéről – szóló rendelkezései alkotják. A polgári jogot érintő lezajlott jelentős jogalkotási munkálatokra is tekintettel kell lenni, így ahol szükséges, figyelembe vesszük a régi Ptk. [1959. évi IV. törvény] és az új Ptk. [2013. évi V. törvény] felfogása közötti különbségeket is.

3.4.1 Alapfogalmak

A törvény értelmében *elektronikus dokumentum* az elektronikus eszköz útján értelmezhető adategyüttes, azaz nemcsak **írott dokumentum**, hanem **állókép, mozgókép, hangfelvétel stb.** is lehet elektronikus dokumentum (természetesen digitális formátum esetén), vagy akár szoftver is, és így ezek elektronikus aláírása is elképzelhető.

Az *elektronikus aláírás* a törvény szerint (az elektronikusan aláírt) elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.

Az *aláírás-létrehozó adat* olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.

Aláírás-ellenőrző adat olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás-létrehozó eszköz olyan hardver-, illetve szoftver-eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláíró az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult.

A törvény három különböző biztonsági szintű elektronikus aláírást különböztet meg: (1) az egyszerű elektronikus aláírást, (2) a fokozott biztonságú elektronikus aláírást és (3) a minősített elektronikus aláírást.

3.4.2 Egyszerű elektronikus aláírás

Egyszerű elektronikus aláírás, amelyhez különösebb joghatások nem kapcsolódnak. Ilyen pl. az e-mail vagy a dokumentum végére begépelt név.

Ez nem alkalmas arra, hogy a dokumentum szerzőjének személyéről vagy a dokumentum tartalmáról hiteles információt szolgáltasson.

3.4.3 Fokozott biztonságú elektronikus aláírás

Fokozott biztonságú elektronikus aláírás: olyan elektronikus aláírás, amely

a) alkalmas az aláíró azonosítására,
b) egyedülállóan az aláíróhoz köthető,
c) olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak, és
d) a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető.

A törvény tehát funkcionális követelményeket támaszt az aláírással szemben, és nem szól e követelmények technikai, eljárási és szervezeti megvalósításáról. Mindazok a technikai, eljárási és szervezeti megoldások felhasználhatók, amelyek kielégítik a fokozott biztonságú elektronikus aláírással szembeni követelményeket.

Lényegében az első részben vázolt technikai folyamatok eredményeként létrejövő elektronikus aláírás ezeket a követelményeket teljesíti.

3.4.4 Minősített elektronikus aláírás

Minősített elektronikus aláírás: olyan – fokozott biztonságú – elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

A minősített elektronikus aláírás esetében tehát nem az aláírás funkciói, hanem annak biztonsági feltételei változnak. A funkciók azonosak, hiszen ez a fokozott biztonságú elektronikus aláírás egyik fajtája.

Minősített elektronikus aláírás elhelyezéséhez szükséges eszközöket csak a Nemzeti Média- és Hírközlési Hatóság által minősített hitelesítés-szolgáltatóként nyilvántartásba vett szervezet bocsáthat ki, s csak ilyen szolgáltató használhatja tevékenységével kapcsolatban a „minősített” jelzőt.

3.4.4.1 Minősített elektronikus aláírást létrehozó eszközök

Az eIDAS-rendelet II. számú melléklete a *minősített elektronikus aláírást létrehozó eszközökkel* szemben szigorú követelményeket támaszt. Eszerint az eszköz megfelelő technikai és eljárási megoldásokkal biztosítja, hogy

a) az elektronikus aláírás létrehozásához használt adat bizalmassága ésszerű mértékben biztosítva legyen;
b) az elektronikus aláírás létrehozásához használt adat gyakorlatilag csak egyszer jöhessen létre;
c) az elektronikus aláírás létrehozásához használt adatok kikövetkeztethetősége ésszerű mértékig kizárható legyen, az elektronikus aláírás pedig megbízhatóan védve legyen a jelenleg rendelkezésre álló technológiákkal elkövetett hamisítás ellen;
d) az elektronikus aláírás létrehozásához használt adatot a jogszerűen aláíró személy megbízható védelemmel tudja ellátni a mások általi felhasználás ellen.

A második követelmény teljesítése általában az eszköz jó minőségű véletlenszám-generátorán múlik, amely az egyedi magánkulcsot generálja, és magát a kulcsot nem lehet kinyerni az eszköz belsejéből. Ez megfelel annak az alapvető elgondolásnak, hogy ez egy személyre szabott eszköz, amelyet az aláíró saját maga kontrollál. A harmadik követelmény úgy teljesül, ha az eszköz csak megfelelő kriptográfiai algoritmusokkal hajlandó használni a magánkulcsot.

Az eszköznek nem szabad az aláírandó elektronikus dokumentumot az aláírás elhelyezéséhez szükséges mértéken felül módosítania, illetőleg nem akadályozhatja meg azt, hogy az aláíró a dokumentumot az aláírási elhelyezése előtt megjelenítse. Az eszköz tehát például a szükséges mértékben kiegészítheti a dokumentumot, de nem cserélheti le egy másik dokumentum lenyomatára.

Ilyennek kizárólag az az aláíróeszköz és egyéb elektronikus aláírási termék tekinthető, amely rendelkezik az NMHH által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolással. E feltétel meglétét az NMHH az aláíróeszköz, illetve a szolgáltató nyilvántartásba vételével egyidejűleg, illetve azt követően is ellenőrzi.

Az EU-ban nyilvántartásba vett tanúsító szervezetek általában csak akkor állítanak ki ilyen igazolást, ha az adott eszköz rendelkezik valamely mértékadó nemzetközi tanúsítással. A minősített elektronikus aláírást létrehozó eszközök általában intelligens kártyák, de ez nem kötelező feltétel; USB-stick is betölthet ilyen szerepet.

3.4.4.2 A minősített tanúsítvány

A minősített tanúsítvány igazolja, hogy a magánkulcshoz tartozó nyilvános kulcs kinek a birtokában van. Ilyen tanúsítványt a hitelesítés-szolgáltató kizárólag személyes regisztráció alapján bocsát ki, és ha a magánkulcs illetéktelen személy befolyása alá került, haladéktalanul visszavonja. A minősített hitelesítés-szolgáltató anyagi felelősséget vállal a tanúsítvánnyal okozott károkért, és felelősségbiztosítással is rendelkezik.

A minősített tanúsítványok a következő elemeket tartalmazzák:

a) annak megjelölését, hogy a tanúsítvány minősített tanúsítvány,
b) a hitelesítés-szolgáltató és székhelyének (ország-) azonosítóját,
c) az aláíró nevét vagy egy álnevet, ennek jelzésével,
d) az aláírónak külön jogszabályban, illetve a szolgáltatási szabályzatban, illetőleg az általános szerződési feltételekben meghatározott speciális jellemzőit, a tanúsítvány szándékolt felhasználásától függően,
e) azt az aláírás-ellenőrző adatot, amely az aláíró által birtokolt aláírást készítő adatnak felel meg,
f) a tanúsítvány érvényességi idejének kezdetét és végét, valamint azt az időtartamot, ameddig a hitelesítés-szolgáltató a feladatot a tanúsítvány vonatkozásában ellátja,
g) a tanúsítvány azonosító kódját,
h) az adott tanúsítványt kibocsátó hitelesítés-szolgáltató fokozott biztonságú elektronikus aláírását,
i) a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
j) a tanúsítvány felhasználásának korlátait,
k) más személy (szervezet) képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt személy (szervezet) adatait.

3.5 A hitelesítés-szolgáltató szerepe és jogállása

3.5.1 Hitelesítés

A hitelesítés az az eljárás, amelynek során a hitelesítő a kriptográfiai kulcspárt – vagy egyéb aláírás-létrehozó és -ellenőrző eszközt – biztonságosan hozzárendeli egy meghatározott és azonosított személyhez. A hozzárendelésről kiállított igazolás a tanúsítvány. Elektronikus aláírás esetén a hitelesítést az ún. hitelesítés-szolgáltató végzi.

Hitelesítésre a saját kezű aláírás vonatkozásában is szükség van: léteznie kell egy olyan dokumentumnak, amely a saját kezű aláírást külső fél által hitelesítetten az aláíróhoz, annak arcképéhez rendeli. A személyi okmány egyrészt az arckép feltüntetésével azonosítja az okmány tulajdonosát, másrészt az okmányon szereplő aláírást is hozzárendeli az okmány tulajdonosához. Az azonosítás és a hozzárendelés hitelességét, harmadik személy általi kétségbevonhatatlanságát az okmány (igazolvány) kiállítójának egyértelmű megbízhatósága adja. (Más esetben pl. az aláírásnak tanúk, közjegyző vagy ügyvéd általi hitelesítése során a tanúk, a közjegyző vagy az ügyvéd aláírása bizonyítja azt, hogy az aláírás valóban az aláírótól származik.)

Az elektronikus aláírás hitelesítésével kapcsolatban egységesen az a szabályozási megoldás alakult ki, hogy a hitelesítés nem (állami) hatósági feladat, hanem piaci szolgáltatás, a hitelesítők nem közigazgatási szervek, hanem vállalkozások. A hitelesítés-szolgáltató „megbízható harmadik félként” bekapcsolódik a felek közötti jogviszonyba: az aláíró által fizetett díj ellenében tanúsítja az aláíró személyazonosságát, és ezért felelősséggel tartozik.

A hitelesítés során a hitelesítés-szolgáltató azonosítja az igénylő személyét (gyakorlatilag személyes megjelenés útján, személyazonosító igazolvánnyal azonosítja) és ez alapján tanúsítványt bocsát ki. A hitelesítés-szolgáltató felelős azért, hogy a tanúsítvány a valóságnak megfelelő adatokat tartalmazzon.

3.5.2 A hitelesítés-szolgáltató jogállása

3.5.2.1 Szolgáltatási jogosultság

Mivel a hitelesítésszolgáltatást végző vállalkozásokra a jogalkotó igen komoly bizalmi feladatot ruház, ezért velük szemben egyúttal átfogó, a szolgáltatás biztonsági szintje szerint differenciált szervezeti és működési szabályokat állapít meg.

Fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatásokat a meghatározott pénzügyi követelmények teljesítése esetén bármely belföldi lakóhelyű vagy belföldön tartózkodási hellyel rendelkező természetes személy, illetve belföldi székhelyű (telephelyű) jogi személy vagy jogi személyiség nélküli szervezet nyújthat. A szolgáltatásnyújtás bejelentési kötelezettséghez kötött, amit a szolgáltató legkésőbb a szolgáltatás elindítása előtt 30 nappal a Nemzeti Média- és Hírközlési Hatóság felé köteles teljesíteni.

A minősített szolgáltatások nyújtása a nagy fokú személyi, szakmai, műszaki és pénzügyi megbízhatóságnak az NMHH által lefolytatott minősítési eljárás során történő igazolásához kötött. Minősített szolgáltatást az a szolgáltató végezhet, amelyik

a) igazolja, hogy a természetes személy, illetőleg a jogi személy vagy jogi személyiséggel nem rendelkező szervezet vezető tisztségviselője, illetőleg vezetője és alkalmazottai büntetlen előéletűek,
b) igazolja, hogy a természetes személy, a jogi személy vagy jogi személyiséggel nem rendelkező szervezet vezető tisztségviselője, illetőleg vezetője vagy alkalmazottja a jogszabályban meghatározott szakképesítéssel rendelkezik,
c) rendelkezik a tevékenység biztonságos folytatásához szükséges pénzügyi háttérrel és felelősségbiztosítással,
d) biztosítja a tevékenység végzéséhez szükséges, jogszabályokban meghatározott szervezeti, biztonsági, eljárási, tájékoztatási követelményeket.

Amennyiben a minősítés során bebizonyosodik, hogy a szolgáltató megfelel a jogszabályokban foglalt követelményeknek, az NMHH a hitelesítés-szolgáltatót, mint minősített tanúsítvány kibocsátására jogosult hitelesítés-szolgáltatót, nyilvántartásba veszi. A szolgáltató köteles a működésében bekövetkező változást bejelenteni, és a változással érintett körülményekre vonatkozóan a minősítést újra el kell végezni.

3.6 A tanúsítvány

3.6.1 A tanúsítvány fogalma

A tanúsítvány a hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot (nyilvános kulcsot) egy meghatározott személyhez kapcsolja, és igazolja e kapcsolat fennállást, az aláíró személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági, hivatali jelleget is.

A tanúsítvány gyakorlatilag a hitelesítésszolgáltató elektronikus aláírásával ellátott elektronikus dokumentum, amely tartalmazza az aláíró aláírásellenőrző adatát – tehát a nyilvános kulcsát – és egyéb, az aláíróra, a hitelesítésszolgáltatóra és a felhasználás feltételeire vonatkozó információkat.

A tanúsítvány kiállítható az aláíró által meghatározott álnévre is. Ebben az esetben a tanúsítvány azt igazolja, hogy az aláírás az álnév tulajdonosától származik. Tényleges személyazonosságot ez esetben nem igazol. A tanúsítvány kiállítható továbbá olyan céllal is, hogy az az aláírót más személy vagy szervezet *képviseletében* történő aláírásra jogosítsa fel.

3.6.2 Az attribútum-tanúsítvány

Mivel a gyakorlatban nemcsak az aláíró személyazonosságának, hanem egyéb alanyi minőségének is jelentősége van, esetenként az elektronikus aláírásnak ezeket a tulajdonságokat is meg kell jelenítenie. Az aláíró ilyen megkülönböztető ismérve lehet az, hogy természetes személyként vagy valamely jogi személy képviseletében jár el és használja fel, bocsátja ki az aláírásával ellátott dokumentumot. Ekként lehet tehát valamely szervezet tagja, munkatársa, gazdálkodó szervezet képviselője, valamely áru vagy szolgáltatás vásárlója, előfizetője, illetve valamely hivatásrend keretében eljáró személy – különösen ügyvéd vagy közjegyző.

Természetes és egyszerű megoldásként kínálkozik, hogy az aláíró speciális szerepeivel összefüggő tulajdonságokat – attribútumokat – az aláíró tanúsítványt kibocsátó hitelesítés-szolgáltató tüntesse fel a tanúsítványban. Ez az opció azonban bizonyos hátrányokkal is együtt jár. Azzal például, hogy ettől fogva mindenki, aki az aláíró tanúsítványt kezeli, egyúttal minden olyan személyes adatról is tudomást szerezhet, amely nem tartozik az érdekkörébe. További jelentős gyakorlati hátrány, hogy ezt követően minden olyan adatnak a megváltozása, amely a tanúsítványban szerepel, egyúttal a tanúsítvány visszavonásával és új tanúsítvány létrehozásának, kibocsátásának a szükségességével jár együtt, ami természetesen jelentősen megnöveli az elektronikus ügyintézéssel kapcsolatos tranzakciós költségeket.

A fenti gyakorlati nehézségek kiküszöbölésére szolgáló technológiai fejlesztés az attribútum-tanúsítvány. Ennek felhasználása során az aláíró egyes speciális ügyköreihez kapcsolódó tulajdonságokat a hitelesítés-szolgáltató helyett a megfelelő attribútumot kezelő partner igazolja. Ezek az adatok pedig a tanúsítványban nem kerülnek feltüntetésre, hanem csupán az attribútummal kapcsolatos igazolásokat kell a tanúsítványhoz csatolni. A tanúsítvánnyal könnyen összekapcsolható, szabványos formátumú, számítógéppel feldolgozható dokumentumként létrehozott igazolást *attribútum-tanúsítványnak* nevezzük.

Attól függően, hogy egy hitelesítés-szolgáltató milyen információkat, valamint hol és hogyan tüntet fel valakinek a tanúsítványában, az illető jogosultságai más és más módon állapíthatóak meg a tanúsítvány alapján. A szabványosításnak különösen nagy jelentősége van, ugyanis együttműködési, kompatibilitási problémákhoz vezet az, ha a hitelesítés-szolgáltató az egyes információkat a szabványtól eltérően tünteti fel az ügyfél számára kiadott tanúsítványban. Ilyenkor előfordulhat, hogy egy személyazonosítási rendszer nem ismeri fel és nem engedi be az egyébként megfelelő jogosultsággal rendelkező felhasználót, vagy nem az őt megillető jogosultságokat engedélyezi számára, illetve ennek az ellenkezője is megtörténhet, hogy ugyanis jogosulatlan felhasználót enged be.

3.6.3 Érvényességi idő

Biztonsági okokból a tanúsítvány érvényességi ideje nem korlátlan. A jogalkotó általános korlátozást a minősített tanúsítványokkal kapcsolatban állapít meg, amelyek érvényességi ideje nem haladhatja meg az aláírás-ellenőrző adathoz kapcsolható aláírás-létrehozó

eszközzel összefüggésben meghatározott érvényességi időt, de legfeljebb a kibocsátástól számított két évet.

3.7 Időbélyegzés

Egyes esetekben nem csak a dokumentum változatlansága, a küldő fél azonosított személye, hanem a dokumentum keletkezésének vagy módosulásának időpontja is fontos lehet. Ennek megállapítására alkalmas az időbélyegző-szolgáltatás. Az időbélyegző nem tartalmaz információt az aláíró személyére vonatkozóan, hanem az adott dokumentum adott időpontbeli tartalmát igazolja.

A törvény szerint az időbélyegző elektronikusan aláírt elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikusan aláírt elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett.

Előfordul a gyakorlatban az is, hogy elektronikus aláírással nem rendelkező, műszaki biztonsági jelentőségű elektronikus dokumentumokra kérnek időbélyeget a felhasználók annak későbbi bizonyítása érdekében, hogy a bélyegzés időpontjában a dokumentum már létezett. Ilyen dokumentumok lehetnek jellemzően a hálózati kiszolgáló számítógépek naplóállományai (log-file).

3.8 Személyes adatok védelme

Az informatikai biztonság környezetéről és jogi szabályozásáról aligha beszélhetünk a személyes adat fogalmának és szerepének tárgyalása nélkül. Illusztrációként említhetjük, hogy az Ibtv. és végrehajtási rendelete ötfokozatú skálán sorolja be biztonsági osztályokba az elektronikus információs rendszereket, s ennek a nómenklatúrának is az egyik kulcskritériuma az a körülmény, hogy a vizsgált rendszerben személyes adatokat – illetve azokat is – dolgoznak-e fel.

Tekintsük át tehát a személyes adatok védelmének alapvető intézményeit.

3.8.1 Az információs önrendelkezési jog

Az adatvédelem fogalma a személyes adatok védelméhez való jogra vonatkozik – bár főként az amerikai szakirodalomban elfogadott és széles körben használatos a tradicionális magánszféra-védelem (*privacy protection*), vagy még pontosabban az információs *privacy* vagy személyes *privacy* kifejezés is. Ennek információs oldala az egyénre vonatkozó információk feletti ellenőrzés jogának garantálása, az adatvédelem nyelvére lefordítva ez nem más, mint az információs önrendelkezési jog. A magánszféra védelmével való összefüggést

több nemzetközi jogi dokumentum is deklarálja, így a 95/46/EK[2] és a 2002/58/EK irányelv[3] 1. cikke egyértelműen meghatározza az adatvédelmi irányelvekbe foglalt szabályok végső célját: védeni a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében. A szoros kapcsolódás mellett azonban fontos megjegyezni, hogy a magánszféra védelmével nem teljesen azonos az adatvédelem, elég, ha csak arra gondolunk, hogy számos személyes adat nem tartozik a szorosan vett magánélethez. Erre tekintettel alapos megfontolások szólnak az adatvédelem jogi önállóságának megjelenítése mellett.

Az adatvédelem „olyan jogi védelem, amely az egyének magánszférájának védelmét célozza az egyénnel kapcsolatba hozható adatok (személyes adatok) kezelésére vonatkozó szabályok előírásával".

A fogalmi alapvetés körében ki kell térni az adatvédelem – adatbiztonság – informatikai biztonság kifejezésekre is. Az adatvédelem nem az adat, hanem a mögötte álló adatalany védelmét hivatott jogi eszközökkel biztosítani. A személyes adatok tényleges védelmére, adminisztratív, fizikai és logikai biztonságának megteremtésére az adatvédelmi szabályozásban az adatbiztonság kifejezés használatos, amelynek célja a személyes adatok védelme a véletlen vagy jogellenes megsemmisülés, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése ellen.[4] Az adatbiztonsági szabályok által garantált védelem eszerint mind az informatikai eszközökkel végzett, mind a manuális adatkezelésekre kiterjed.

3.8.2 Adatvédelem és információbiztonság

Ezzel szemben az informatikai biztonság „az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos". Az informatikai biztonság tehát nem csak a személyes adatok, hanem az információs rendszerben tárolt bármely adat technikai védelmét magában foglalja, ugyanakkor ez nem korlátozódhat kizárólag az informatikai eszközökre (kriptográfiai megoldások, tűzfal stb.), hanem kiterjed az informatikai infrastruktúra fizikai védelmére is. Az informatikai biztonsági követelményeknek való megfelelés így az ezen eszközökkel kezelt személyes adatok biztonságát is szolgálják. Az informatikai biztonság tárgya azonban minden esetben az informatikai rendszer védelme, így a manuálisan kezelt adatok adatbiztonsági kérdései kívül esnek a hatókörén.

2011. július 11-én az Országgyűlés elfogadta az *információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény*t, azaz közismert nevén az Infotv.-t. A jogszabály 2012. január 1-én lépett hatályba, és így felváltotta az adatvédelem és információszabadság 1992 óta hatályban volt szabályozását: a személyes adatok vé-

2 Az Európai Parlament és Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.

3 Az Európai Parlament és a Tanács 2002. július 12-i 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről.

4 95/46/EK irányelv 17. cikk (1) bekezdés.

delméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényt. Az Infotv. egyike azoknak a sarkalatos törvényeknek, amelyek az új Alaptörvény elfogadása kapcsán készültek 2011 folyamán.

3.8.3 A személyes adat fogalma

Az Infotv. külön határozza meg az érintett fogalmát, amely a 3. § 1. pontja szerint bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy. A *személyes adat* pedig az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek."[5] Ez egyértelmű elmozdulás a személyes adatok abszolút értelmezésétől a relatív értelmezés felé.

3.8.3.1 Anonim adatok

Külön megfontolásra érdemes az anonimizálás problémája, vagyis az a művelet, melynek során az adatkezelő eltávolítja az adatbázisból azokat az azonosító adatokat, amelyek – legalábbis első közelítés szerint – a leíró adatok megszemélyesítéséhez, egy konkrét személyhez rendeléséhez szükségesek. Egyes esetekben, például statisztikai célú adatkezelés során az adatkezelő ezen a módon tesz eleget személyiségvédelmi kötelezettségének. Ha azonban egy adatbázisból eltávolítjuk az alanyok nevét és – ha van ilyen – azonosító számát, az még nem jelenti azt, hogy valóban megnyugtató módon elvégeztük az anonimizálást. Ha ugyanis kellően sok további adattal rendelkezik az adatkezelő, akkor ezek megfelelő csoportosításával, következtetések levonásával számtalan alternatív módot találhat az érintettek azonosítására.

Az anonimizálás elvégzése kellő felkészültséget, szakmai jártasságot, átgondoltságot és privacy-tudatos hozzáállást kíván ugyanis az adatkezelőtől. Ezek nélkül illuzórikussá válhat az anonimizáláson alapuló adatvédelem. Meggyőzően bizonyítja ezt a tételt az egészségügyi és társadalombiztosítási adatok kezelése körében *Alexin Zoltán* 2014-ben megjelent tanulmánya.[6]

3.8.3.2 A személyes adat abszolút és relatív értelmezése

A személyes adat abszolút és relatív értelmezésének középpontjában az adat és az érintett közötti kapcsolat helyreállíthatóságának, azaz az érintett közvetett azonosíthatóságának kérdése áll. A (szélsőségesen) *abszolút értelmezés* szerint személyes adatnak minősül egy adat, ha az adat és a személy közötti kapcsolat *elvileg* megteremthető. Amennyiben tehát az érintett akár több különböző adatkezelőnél lévő adatok segítségével, több lépésben, kü-

5 Infotv. 4. § (3).
6 Alexin (2014), 40-41.

lönböző technikai eljárásokkal, de végül is azonosítható, akkor – függetlenül attól, hogy az adott adatkezelőnek van-e tényleges vagy jogszerű lehetősége erre – az adatot személyes adatnak kell tekinteni. Ez az értelmezés a személyes adat fogalmát igen tágra szabja.

A *relatív értelmezés* szerint egy adat személyes adat jellegét az adatkezelő szempontjából kell vizsgálni: amennyiben az *adatkezelő ténylegesen nem képes* az általa kezelt adatokat az érintetthez kötni, úgy az adat e vonatkozásban (ezen adatkezelőnél) nem minősül személyes adatnak.

A hazai adatvédelmi biztosi gyakorlat – kisebb kilengésekkel – az abszolút értelmezés mellett foglalt állást: „minden olyan adat személyes adat, amely természetes személlyel kapcsolatba hozható […] tekintet nélkül arra, hogy a kapcsolat csak több lépésben építhető fel, illetve arra, hogy a kapcsolat megteremtésére valamely adatkezelő önmagában nem képes".[7] A kódolt „adatok annál az adatkezelőnél is személyes adatnak minősülnek, amelynek informatikai rendszere nem alkalmas azok értelmezésére".[8] Az uralkodó abszolút értelmezést azonban – néhol ellentmondást is tartalmazó állásfoglalásokkal – a rendszámok személyes adat jellegének elemzése kapcsán az adatvédelmi biztos többször is megtöri.

A személyes adat relatív értelmezése felé történő elmozdulás, és az új, érdekmérlegelésen alapuló jogalap együttesen – bár sok esetben életszerűbb és könnyebben betartható szabályozást eredményez – egyértelműen az adatvédelmi szabályozás „lazítását", illetve hatályának jelentős szűkítését eredményezi. Utóbbi kapcsán kiemelendő, hogy például egy vagyonvédelmi vagy közterületi kamerarendszert működtető adatkezelő vagy egy elektronikus kereskedelmi szolgáltatást kínáló tartalomszolgáltató gyakran nem rendelkezik azokkal a technikai feltételekkel, amelyek segítségével az általa kezelt adatokat: képfelvételeket, IP-címeket és hozzá tartozó böngészési szokásokat – amelyek a hatályos szabályozás alapján személyes adatnak minősülnek – képes lenne konkrét személyhez kapcsolni. Ugyan mindkét területen alkalmazandók ágazati szabályok is, de igen furcsa helyzet állhat elő, ha az adatvédelmi törvény rendelkezéseit nem, de az ágazati törvények adatvédelmi szabályait alkalmazni kell például ezen adatkezelésekre, különös tekintettel arra, hogy az ágazati törvények is „személyes adatok" kezeléséről szólnak, a személyes adat fogalmát viszont az (új) Avtv. a korábbiakhoz képest szűkebben határozza meg.

3.8.4 Az adatkezelés jogalapja

Az Infotv. talán legjelentősebb újdonsága az adatkezelési jogalapok bővítése. A korábbi adatvédelmi törvény kizárólag két esetben tette lehetővé a személyes adatok kezelését: ha ehhez az érintett hozzájárult vagy ha ezt törvény, illetve törvény felhatalmazása alapján, az abban meghatározott körben helyi önkormányzat rendelete elrendelte.

7 Jóri (2005), 163.
8 Jóri (2005), 111.

3.8.4.1 Az érdekmérlegelésen alapuló adatkezelés

A GDPR 6. cikkének f) pontja szerint személyes adatok kezelhetők többek között abban az esetben, ha az adatkezelés az adatkezelő vagy az adatokat megkapó harmadik fél vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendű az érintettnek a magánélet tiszteletben tartásához való joga. Az érdekmérlegelés jelentősen kitágítja a jogszerű adatkezelések körét, és egyúttal szükségszerűen bizonytalanabbá is teszi azok határait. A hozzájárulás és a törvényi felhatalmazás az érintett számára elvileg minden esetben előzetesen ellenőrizhetővé és átláthatóvá teszi az adatkezelés feltételeit. Ehhez képest az érdekmérlegelés akár az érintett tudta nélkül is alapot adhat a személyes adatok kezeléséhez, és minden esetben csak utólag, alapvetően szubjektív szempontok alapján dönthető el, hogy az adatkezelő valóban helyesen mérlegelte-e a szemben álló érdekeket, azaz jogszerű volt-e az adatkezelés. A felmerülő viták eldöntése a jogalkalmazóra is nagyobb felelősséget ró.

Mindezzel együtt az érdekmérlegelés, mint adatkezelési jogalap, megjelenése rugalmasságot hoz a szabályozásba, és világos helyzetet teremt számos, korábban jogsértő, de jogkövetkezmény nélkül maradó adatkezelés számára. Ilyen jogsértések állhattak elő többek között a munkáltató adatkezelési gyakorlatában, amikor pontosan meghatározott jogalap nélkül ellenőrizte a munkavállalók tevékenységét, a munkáltatók, oktatási intézmények által az intézményben dolgozók, tanulók részére nyújtott távközlési szolgáltatásokhoz kapcsolódó adatkezeléseknél, az oknyomozó újságíró tevékenységében, amikor valamely ügy felderítése kifejezetten az érintett akarata ellenére történik, vagy éppen a szerződés megszűnését követően az elévülési időn belül a szerződésből eredő károk érvényesítéséhez kapcsolódóan. Sőt számos, formálisan jogsértő adatkezelés jogi helyzetét tisztázhatja a rendelkezés olyan kötelező adatkezelések esetében, amelyek törvényi feltételeit – a korábbi és az új szabályozás egyaránt szigorú és részletes előírása ellenére – a jogalkotó nem határozta meg kellő pontossággal.

A törvényi feltétel megfogalmazása során a jogalkotó feltehetően hangsúlyozni akarta a hozzájáruláson alapuló adatkezelés elsőbbségét, amit azonban éppen a másik érdekmérlegelési jogalap von kétségbe. Az eredetitől eltérő célból történő adatkezelés, bár az irányelvi rendelkezés kétségtelenül magában foglalja e lehetőséget – sőt akár a hozzájárulás beszerzésének lehetetlensége is értelmezhető úgy, hogy az magában foglalja ezt az esetet is –, mégis jelentős kockázat az információs önrendelkezési jog szempontjából. Az érintett ebben az esetben ugyanis éppen arra számíthat, hogy az adatkezelő a birtokában lévő adatok kezelését nem folytatja. A célhoz kötöttséget, mint az Alkotmánybíróság által az információs önrendelkezési jog legfontosabb garanciájaként meghatározott adatkezelési korlátot, e rendelkezés kiüresíti, a célhoz kötöttség megsértésének bizonyítása legalábbis szinte lehetetlenné válik. Másrészről viszont a jogalkalmazói gyakorlat olyan értelmezést is kialakíthat, amely szerint az érdekmérlegelés egyik legfontosabb szempontja az adatkezelés célja, így akár gyakorlati szempontból fel is értékelődhet a célhoz kötöttség elve.

3.8.4.2 Az érintett tiltakozási joga

Új tartalmat nyer viszont az érintett tiltakozási joga, ami ilyen adatkezelések esetén is lehetőséget biztosít a kifogásolt adatkezelés megszűntetésének kezdeményezésére. Korábban ez a jogintézmény az érintett adattörlési joga mellett önálló jelentőséggel nem rendelkezett, most azonban olyan esetekben is lehetővé teszi az adatkezelés megszüntetését, amikor az érintett a törlési jogával nem élhet. Ugyanakkor nem egyértelmű az érintett tájékoztatásának szabályozása. Az adatkezelőt terhelő proaktív tájékoztatási kötelezettség nélkül az érintett tudomást sem szerez az adatkezelés tényéről. A törvény szerint az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező.[9] Az érdekmérlegelésen alapuló adatkezelés szigorúan értelmezve egyik esetnek sem felel meg, ebből következően a tájékoztatási kötelezettség sem terjed ki rá. Mivel azonban formálisan természetesen maga a törvény teszi lehetővé az adatkezelő számára, hogy a megfelelő feltételek teljesülése esetén kezelje a személyes adatokat, ezért a fenti rendelkezés értelmezhető úgy is, hogy az adatkezelő az érdekmérlegelésen alapuló adatkezelés megkezdése előtt is köteles tájékoztatni az érintettet. Az információs önrendelkezési jog érvényesülését kizárólag az utóbbi értelmezés garantálja.

Az adatkezelések számos területén felmerülő nehézségeket orvosol az érdekmérlegelés, mint adatkezelési jogalap, megjelenése a hazai szabályozásban. Ez azonban olyan mély beavatkozás az információs önrendelkezései jog korábban kialakult értelmezésébe, amely megköveteli a jogalkotótól, hogy az érintetteket védő többletgaranciákkal korlátozza az adatkezelők mozgásterét. A szabályozással kapcsolatos egyik kifogásunk, hogy az továbbra sem követi teljes egészében a közösségi jogi rendelkezéseket – amelyek számonkérésére irányuló eljárás azonban az Európai Unió szervei részéről korábban sem indult –, másrészt az érintetteket védő garanciák nem kellően átgondoltak. A kapcsolódó jogalkalmazói gyakorlattól függően így elképzelhető, hogy a jelenlegi adatvédelmi koncepció az új szabályozási környezetben nagyrészt változatlan marad, de ugyanígy az is, hogy az adatkezelők a korábbiakhoz képest lényegesen nagyobb mozgástérhez, az érintettek pedig lényegesen kisebb védelemhez jutnak.

3.8.5 Az adatvédelmi hatóság

Az Infotv. átalakította az adatvédelem – és mellette az információszabadság – törvényességi felügyeleti rendszerét. Ennek lényege, hogy – megtartva több adatvédelmi biztosi jogosítványt – új hatósági jogkörökkel és bírságolási joggal kiegészülve felügyeleti hatóság jön létre, amelynek elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi ki. Az új hatóság 2012. január 1-i felállítása miatt az adatvédelmi biztos intézménye az utolsóként hivatalban volt adatvédelmi biztos mandátumának félidejénél megszűnt.

9 Infotv. 20. § (1).

3.8.5.1 A hatóság jogállása

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) autonóm államigazgatási szerv, amelynek elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi. A kinevezés módja a korábbi modellhez képest egyértelmű visszalépés: az Országgyűlés kétharmadának szavazatával megválasztott adatvédelmi biztoshoz képest a hatóság elnöke kevésbé lehet független tisztség. A hatóságnak ráadásul jelentős részben azt a hatalmi ágat kell ellenőriznie, amelynek vezetőjétől a kinevezése ered: a közérdekű adatok nyilvánossága és a titokfelügyelet kapcsán szinte kizárólag, de a személyes adatok kezelésével kapcsolatban is gyakorta kell a hatóságnak az állami szervekkel (azon belül is a végrehajtó apparátussal) szemben – akár határozattal – fellépnie. E fellépéshez nagyobb legitimációt és „bátorságot" biztosítana az Országgyűlés minősített többsége általi megválasztás. A hatóság tényleges súlyát nagymértékben meghatározza majd a hatóság vezetőjének személye és szerepfelfogása.

A szervezetrendszerrel kapcsolatban több rendelkezés is biztosítja a formális függetlenséget. Az elnök megbízása meglehetősen hosszú időre, kilenc évre szól, és a visszahívás feltételei korlátozottak és pontosan körülhatároltak. Az újraválaszthatóság lehetősége ugyanakkor nagymértékben rontja a hosszú kinevezési idő függetlenséget erősítő hatását. A törvény az elnökjelölttel szemben részletes összeférhetetlenségi szabályokat és szakmai követelményeket határoz meg, melyek nem különböznek lényegesen a hatályos, adatvédelmi biztosra vonatkozó szabályoktól.[1]

A hatóság függetlenségével kapcsolatban a magyar szabályozás mellett releváns rendelkezéseket tartalmaz a GDPR is, amelynek 51. cikk (1) bekezdése előírja, hogy minden tagállamnak rendelkeznie kell arról, hogy a rendelet alkalmazásának ellenőrzésére egy vagy több független nemzeti felügyeleti hatóságot kell létrehozni. Ezek a hatóságok a rájuk ruházott feladatok gyakorlása során teljes függetlenségben járnak el. Valójában a GDPR előtt már az EU adatvédelmi irányelve is tartalmazott hasonló előírást.

1 Infotv. 40. § (1)–(2). Az új szabályozás 10 év helyett 5 év szakmai tapasztalattal is megelégszik.

4 AZ INFORMATIKAI BIZTONSÁG KERETSZABÁLYOZÁSA MAGYARORSZÁGON

Mint a bevezetőben már megállapítottuk, a modern társadalom, és annak minden alrendszere, szervezete és polgára, kiszolgáltatottá vált a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett információs infrastruktúrának. Az elektronikus információs rendszerek nélkülözhetetlenné váltak a társadalom egésze számára, mert az állam működése, a különböző szolgáltatások megvalósítása és igénybevétele már nehezen volna fenntartható e rendszerek nélkül. Már önmagukban ezeknek az információs rendszereknek a kiesése is katasztrófahelyzetet idézhet elő. Információs rendszereink és hálózataink – azok közül is elsősorban azok, amelyek működése elengedhetetlen a társadalom és a gazdaság zavartalan működéséhez – egyre gyakrabban szembesülnek az igen sokféle forrásból származó biztonsági fenyegetéssel. A szándékos károkozások olyan formái, mint a különböző hackercsoportok számítógépvírusokkal történő vagy az információs rendszer leállására vezető ún. szolgáltatásmegtagadást eredményező támadásai egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. Folyamatosan növekvő fenyegetést jelent sérülékeny információs rendszereinkre a hadviselés egy új formája, amelyet kiberműveleteknek (angolul: cyber operations) neveznek, de még inkább a békeidőkben is állandóan fenyegető terrorizmus számítógépes változata, a kiberterrorizmus. A különböző információs infrastruktúrák, eszközök és szolgáltatások bármelyikének megsemmisülése vagy sérülése a társadalom széles rétegeit érintheti. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell.

A magyar kibertér védelmének, sértetlenségének keretrendszerét az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény teremti meg. A továbbiakban ennek a kerettörvénynek a rendszerét és legfontosabb rendelkezéseit tekintjük át.

Bizonyos közigazgatási informatikai rendszerek biztonságát korábban az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet szabályozta, amely 2012 áprilisában hatályon kívül helyezésre került, így jelenleg nincsen olyan jogszabály, amely egységes biztonsági követelményeket szabna az elektronikus információk védelmével kapcsolatban.

A minősített adatok és az ezeket kezelő elektronikus információs rendszerek védelme a minősített adatok védelméről szóló 2009. évi CLV. törvényben és a végrehajtására kiadott rendeletekben szabályozásra került.

A nemzet szempontjából fontos, a minősített adatok körébe nem tartozó, de a kezelt adatok jellegére és a nyilvántartások alapján végzett állami feladatok fontosságára tekintettel kiemelt jelentőségű állami nyilvántartások védelmének biztosítását a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény szolgálja.

A törvény hatálya kiterjed a létfontosságú infrastruktúrákra is, melynek alapvető rendelkezéseit a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény tartalmazza.

A törvény tudatosan használja az információbiztonság, információs rendszer kifejezések előtt az „elektronikus" jelzőt. Az információbiztonság ugyanis a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ezzel szemben az elektronikus információs rendszerek biztonsága csak az elektronikus információs rendszerekben szereplő adatok és az azokat kezelő rendszer védelmét jelenti. A törvény pedig az elektronikus információs rendszerekben tárolt, kezelt információk védelmét célozza az azokat kezelő szervezetek tudatos biztonságának növelésén keresztül.

Az elektronikus információs rendszerek védelme egy igen széles körű információvédelem része, amely önállóan is működtethető. A NATO *Security within the North Atlantic Treaty Organisation* direktívája szerinti elektronikus információvédelmen (INFOSEC) kívül az információvédelem többi részét (személyi védelem, dokumentumvédelem, fizikai védelem, elhárítás/hírszerzés) is magában foglalja, de csak az elektronikus információs rendszer vonatkozásában.

Az elektronikus információs rendszerek értelmezése az informatikai, a kommunikációs és az egyéb elektronikus rendszerek konvergenciájára épül. Az információs társadalomhoz és a médiához kötődő iparágak konvergenciájáról az Európai Bizottság *i2010: európai információs társadalom a növekedésért és a foglalkoztatásért* című [COM(2003) 784.] közleménye az európai audiovizuális politika szabályozásának jövőjére vonatkozóan megállapítja: „Az információs társadalom és a média területén működő szolgáltatások, hálózatok és eszközök digitális konvergenciája végre mindennapjaink valóságává válik".

A törvény egy preventív szabályozási környezetnek az alapjait kívánja megteremteni, amely ténylegesen a megelőzést helyezi előtérbe és ezen keresztül a biztonsági problémák kialakulásának mérséklését és az előforduló biztonsági események számának csökkentését, illetve tudatos kezelését célozza.

4.1 Egyes alapfogalmak

A törvény által alkalmazott alapfogalmakat a 2. § értelmező rendelkezései definiálják. Ezek közül a teljesség igénye nélkül a legfontosabbakat emeljük csak ki.

4.1.1 Az elektronikus információs rendszer és annak biztonsága

A törvény tárgyi hatályát meghatározó legalapvetőbb fogalom az *elektronikus információs rendszer,* amely

- az adatok, információk kezelésére használt eszközök, eljárások, valamint az ezeket kezelő személyek együttese, ezen belül

  - a számítástechnikai rendszerek és hálózatok;
  - a helyhez kötött, mobil és egyéb rádiófrekvenciás,
  - műholdas elektronikus hírközlési hálózatok, szolgáltatások;
  - rádiós vagy műholdas navigáció;
  - az automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek);
- fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

Eszközök alatt a környezeti infrastruktúrát, a hardvert, a hálózatot, és az adathordozókat, eljárások alatt a szabályozást, a szoftvert és a kapcsolódó folyamatokat is érteni kell.

Az *elektronikus információs rendszer biztonsága* pedig természetesen a törvény legalapvetőbb célját határozza meg úgy, mint az elektronikus információs rendszer *olyan állapota*, amelyben annak védelme az elektronikus információs rendszerben

- kezelt adatok
  - bizalmassága,
  - sértetlensége és
  - rendelkezésre állása,
- valamint az elektronikus információs rendszer elemeinek
  - sértetlensége és
  - rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

E definíció teljes mélységében való értelmezéséhez ide kell idéznünk a bizalmasság, a sértetlenség és a rendelkezésre állás fogalmait is. A jogalkotó mindezeket szintén az elektronikus információs rendszer fogalmához köti. Eszerint tehát:

4.1.2 A bizalmasság

A *bizalmasság* az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt

- csak az arra jogosultak és
- csak a jogosultságuk szintje szerint
  - ismerhetik meg,
  - használhatják fel, illetve
  - rendelkezhetnek a felhasználásáról.

4.1.3 A sértetlenség

A *sértetlenség* ezzel szemben kettős természetű.
Egyfelől ugyanis az adat tulajdonsága, amely szerint

- az adat tartalma és tulajdonságai az elvárttal megegyeznek,
- ideértve a bizonyosságot abban, hogy az
  - az elvárt forrásból származik (hitelesség) és
  - a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát).

A sértetlenség eleme továbbá az *elektronikus információs rendszer elemeinek azon tulajdonsága*, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

4.1.4 A rendelkezésre állás

A *rendelkezésre állás* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

4.1.5 A fenyegetés

A fenyegetés olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.

4.1.6 Védelmi intézkedések csoportjai

A törvény a védelmi intézkedéseknek három fő csoportját jelöli ki. Ezek az adminisztratív, a fizikai és a logikai védelmet jelentik.

Az *adminisztratív védelmi intézkedések* keretében az adatkezelő a védelem érdekében szervezési, szabályozási, ellenőrzési intézkedéseket hoz, továbbá a védelemre vonatkozó oktatást folytat.

A *fizikai védelem* a fizikai térben megvalósuló fenyegetések elleni védelmet jelenti, amelynek fontosabb részei

- természeti csapás elleni védelem,
- mechanikai védelem,
- elektronikai jelzőrendszer,
- élőerős védelem,
- beléptető rendszer,
- megfigyelő rendszer,
- tápáramellátás,
- sugárzott és vezetett zavarvédelem,
- klimatizálás,
- tűzvédelem.

Végül tekintsük a *logikai védelem* körét, mely az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelmet jelenti. Ez a definíció meglehetősen rövid összefoglalását adja annak a rendkívül összetett, sok tényezőből felépülő, igen magas szakmai jártasságot kívánó rezsimnek, amely az információs társadalom szolgáltatásait és infrastruktúráját a kibertérben fenyegető informatikai támadások és egyéb szoftverekkel megvalósított visszaélések, illetve a mindezen rendszerekben lappangó technológiai kockázatok ellen biztosítja.

4.1.7 A biztonsági esemény

Ha az elektronikus információs rendszer biztonsága sérül, azt a helyzetet biztonsági eseménynek nevezzük. A *biztonsági esemény* valójában olyan

- nem kívánt vagy nem várt
- egyedi esemény vagy eseménysorozat, amely
- az elektronikus információs rendszerben *kedvezőtlen változást* vagy egy
- *előzőleg ismeretlen helyzetet* idéz elő, és amelynek
- hatására az elektronikus információs rendszer által hordozott információ
    - bizalmassága,
    - sértetlensége,
    - hitelessége,
    - funkcionalitása vagy
    - rendelkezésre állása elvész, illetve megsérül.

4.1.8 A biztonsági osztály és a besorolás

A biztonsági események kiküszöbölése, illetve előállásuk során a rendszer megfelelő reagálása azon alapul, hogy az adott elektronikus információs rendszer milyen biztonsági osztályba tartozik. A törvény hatálya alá tartozó valamennyi elektronikus információs rendszerre nézve a rendszer üzemeltetője meg kell, hogy határozza a rendszer *biztonsági osztályát,* azaz a *rendszer védelmének elvárt erősségét*.

A besorolási fokozatok és a hozzájuk rendelt értékelési szempontok, valamint elvárt intézkedések a feladatok számonkérhetőségét, a rendszer transzparenciáját szolgálják. A biztonsági osztályba történő besorolás az elektronikus információs rendszer védelme elvárt erősségének meghatározása, mely a felmerülő kockázatok alapján történik.

4.1.9 A biztonsági szint és a besorolás

Míg a biztonsági osztály normatív kategória és szervek, adatkezelők csoportjaira vonatkozóan állapít meg elvárásokat, a *biztonsági szint* konkrét információs rendszerre és annak üzemeltetőjére vonatkozik.

A *biztonsági szint* megmutatja a szervezet felkészültségét a törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok ellátására.

Ezzel összhangban történik meg a *biztonsági szintbe való besorolás*, melynek során meghatározásra kerül a szervezet felkészültsége a törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

A gyakorlatban előfordulhat, gyakran elő is fordul, hogy a szervezet, illetve az adatkezelő rendszer felkészültsége – biztonsági szintje – elmarad a kockázatokkal arányosan megállapított biztonsági fokozat által támasztott elvárásoktól. Az elvárásoknak megfelelő felkészültségi szint megközelítésére, elérésére a törvény és a végrehajtási rendelete átlátható és számonkérhető fejlesztési irányokat jelöl ki.

4.2 A törvény hatálya

Minden jogszabály egyik legkritikusabb része a hatály kijelölésére vonatkozó rendelkezés. Ugyanis ez jelöli ki a további szabályok alkalmazási kereteit, meghatározva azon személyeknek, szervezeteknek – jogalanyoknak – a körét, és azoknak a magatartásoknak, jogviszonyoknak a halmazát, amelyek vonatkozásában a jogszabály jogokat és kötelezettségeket fog megállapítani.

Az informatikai biztonsági törvény személyi hatálya igen tág, és lényegében még túl is terjed a törvény címében megjelölt „állami és önkormányzati" szervek szűken értelmezett körén, ugyanis egyéb közfeladatot ellátó szerveket is a személyi hatálya alá von, tekintet nélkül arra, hogy milyen jogi jelleggel rendelkeznek, tehát közhatalmat gyakorló állami és/vagy önkormányzati szervekről van-e szó, vagy a tevékenység jellege folytán – bár nem állami – de kritikus infrastruktúrába tartozó vagy létfontosságú feladatot végző szervről. Ez utóbbi olyan jogalany is lehet, amely a szó szűkebb értelmében maganjogi jogalany, és gazdasági társaság formájában működik.

Ilyen jogalany lehet egy bank, közműszolgáltató vállalat, jelentősebb élelmiszeripari vállalat, hírközlési szolgáltató cég és még számos polgári jogi vállalkozás, amely jelentőségénél fogva a létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló törvény alapján mint európai vagy nemzeti létfontosságú rendszerelemet kijelöltek.

4.2.1 A hatályra vonatkozó általános rendelkezések

Eszerint a személyi hatály az alkotmányos rend fenntartása szempontjából kiemelt fontosságú közszolgálati szervek adatait kezelő szervezetek és a nemzeti adatvagyont kezelő szervezetek mellett az európai és nemzeti létfontosságú információs rendszerek, rendszerelemek közé tartozó szervezetekre is kiterjed.

Az érintett szervek felsorolásának alapját a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény, a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény, az ügyészségről szóló 2011. évi CLXIII. törvény és a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról szóló 2010. évi CXXVI. törvény képezi. A Kormány és a kormánybizottságok nem kerülnek a törvény személyi hatálya alá, mivel önálló szervezetrendszerrel nem rendelkező testületként gyakorolják feladataikat és önálló elektronikus információs rendszerekkel nem rendelkeznek.

A tárgyi hatály a kiemelt fontosságú közszolgálati szervek adatait és a nemzeti adatvagyont kezelő szervezetek, valamint az európai és nemzeti létfontosságú információs infrastruktúrák elektronikus információs rendszereinek védelmére vonatkozik.

Ez a személyi és tárgyi hatály kellően széles körű ahhoz, hogy Magyarország kibervédelme szempontjából minden, az állam működése szempontjából lényeges elektronikus információs rendszer védelmére kitérjen.

A törvény az egységes szabályozási környezet kialakítása érdekében rendelkezik a más törvényekkel való összhangról. Ennek értelmében a minősített adatok vonatkozásában e törvény rendelkezéseit a minősített adat védelméről szóló 2009. évi CLV. törvényben foglalt eltérésekkel kell alkalmazni.

A törvény kifejezetten elkülöníti a rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek, a Katonai Nemzetbiztonsági Szolgálat és a Magyar Honvédség zárt célú elektronikus információs rendszereit, a külpolitikáért felelős miniszter diplomáciai információs célokra használt zárt célú elektronikus információs rendszereit, a Miniszterelnök irányítása alá tartozó Információs Hivatal, valamint a Nemzeti Adó- és Vámhivatal állami költségvetési bevételek biztosítását támogató elektronikus információs rendszereit. Ezeknek az esetében is kötelező a megfelelő biztonság kialakítása és fenntartása, de a rendszerek fokozott védelme érdekében a hatósági és eseménykezelési feladatok az irányítást ellátó miniszter felelősségi körén belül maradnak, így nem nő azok köre, akik ezen érzékeny rendszereket, azok védelmi megoldásait megismerhetik, vagy akár annak védelmét felülbírálhatnák.

4.2.2 A személyi (szervi) hatály különös rendelkezései

A törvény hatálya tehát kiterjed az alábbi kritériumoknak megfelelő szervezetekre:

- Kiemelt jelentőséggel rendelkező és a nemzeti adatvagyon kezelését ellátó szervezetek.
- A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói elektronikus információs rendszerei.
- Európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek.
- A személyi hatály alá tartozó szervek és a számukra adatkezelést végző szervek elektronikus információs rendszereinek védelme.

A törvény 2. § (1) bekezdése nevesítve is felsorolja a legfontosabb olyan szerveket, melyekre a rendelkezéseket alkalmazni kell. Ezek tehát sorrendben:

- a központi közigazgatási szervek,
- a Köztársasági Elnöki Hivatal,
- az Országgyűlés Hivatala,
- az Alkotmánybíróság Hivatala,
- az Országos Bírósági Hivatal és a bíróságok,
- az ügyészségek,
- az Alapvető Jogok Biztosának Hivatala,
- az Állami Számvevőszék,
- a Magyar Nemzeti Bank,
- a fővárosi és megyei kormányhivatalok,
- a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalai, a hatósági igazgatási társulások,
- a Magyar Honvédség.

Nem lehet nem észrevenni, hogy a személyi hatály *nem terjed ki (!)* a Kormányra és a kormánybizottságokra, továbbá az önkormányzatok képviselő-testületeire, annak bizottságaira és a közgyűlésre. Arra nézve sajnos nem tartalmaz semmiféle utalást a törvény, hogy miért és milyen jogpolitikai célok, érdekek miatt alakult úgy, hogy éppen ezek a szervek nem esnek a törvény hatálya alá.

A személyi hatály további speciális rendelkezéseiként, illetve következményeként a törvényt alkalmazni kell az alábbi szervek, szervezetek elektronikus információs rendszereinek vonatkozásában:

- a Földmérési és Távérzékelési Intézetre és a földhivatalokra mint az ingatlan-nyilvántartás, a földhasználati nyilvántartás és egyéb földmérési és térképészeti nyilvántartás adatfeldolgozóira;
- az Országos Nyugdíjbiztosítási Főigazgatóság (ONYF) mint a nyugdíjbiztosítási nyilvántartás adatkezelőjére;
- a Nemzeti Egészségbiztosítási Alapkezelő (NEAK; korábban OEP) mint az egészségbiztosítási nyilvántartás adatkezelőjére;
- az MH Geoinformációs Szolgálat és a HM Térképészeti Közhasznú Nonprofit Kft.-re, a közepes és kisméretarányú állami topográfiai térképek adatfeldolgozása tekintetében;
- a Pillér Pénzügyi és Számítástechnikai Kft-re, a Nemzeti Adó- és Vámhivatal által kezelt adó- és vámhatósági adatok nyilvántartásának adatfeldolgozása tekintetében;
- a Nemzeti Infokommunikációs Szolgáltató Zrt.-re, a Foglalkoztatási és Szociális Adatbázis, a kulturális örökségvédelmi nyilvántartás elektronikus adatfeldolgozása tekintetében.

4.2.3 A tárgyi hatály különös rendelkezései

Ugyancsak a hatályra vonatkozó különös szabályok között említhetjük, hogy a törvényt alkalmazni kell a valamikor KEK KH (Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala), jelenleg a Belügyminisztérium illetékes államtikársága által kezelt alábbi nyilvántartások elektronikus információs rendszereire:

- a polgárok személyi adatainak és lakcímének nyilvántartására;
- a központi idegenrendészeti nyilvántartásra;
- az egyéni vállalkozók nyilvántartására;
- a központi útiokmány-nyilvántartásra;
- a közúti közlekedési nyilvántartásra;
- a Magyar igazolvány és a Magyar hozzátartozói igazolvány
- tulajdonosainak nyilvántartására;
- a szabálysértési nyilvántartási rendszerre;
- a bűnügyi nyilvántartási rendszerre;
- a Nemzeti Rehabilitációs és Szociális Hivatalnak az egységes
- szociális nyilvántartására és az egységes örökbefogadási nyilvántartásra.

Mint létfontosságú rendszerekre és létesítményekre, az ezek azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján az

- energetikai,
- közlekedési,
- agrárgazdasági,
- egészségügyi,
- pénzügyi,
- ipari,
- infokommunikációs,

- vízügyi,
- kormányzati,
- közbiztonsági

ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

Ez utóbbi kör tényleges szereplőinek megállapítása bizonyos tág diszkrecionális hatáskört rendel a besorolásban illetékes hatóságokhoz.

4.2.4 Adatkezelés Magyarország területén, illetve más EU-tagállam területén

A törvény arra való tekintettel, hogy napjainkban fontos kérdés az adatok külső szolgáltatónál történő tárolása, illetve az elektronikus információs rendszerek kiszervezése általánosan elfogadott gyakorlattá vált – s ezzel a kérdéssel már a nemzeti adatvagyon törvény is foglalkozik –, korlátozza az adatvagyon Magyarország területén kívüli kezelését. Ez a tilalom nem terjedhet ki azonban a Magyar Honvédségre és a külképviseletekre, mert ezek számára szükséges lehet, hogy külföldön elérhessék adataikat, elektronikus információs rendszereiket.

A létfontosságú információs infrastruktúrákhoz olyan intézmények tartozhatnak, a már említett pénzintézeteken, hírközlési szolgáltatókon kívül, amelyek esetében a csak Magyarország területén belül engedélyezett adatkezelés súlyos költségkihatásokkal járhat. Itt az adatok Európai Unión belüli kezelésének kényszere elégséges korlátozás, mert az uniós és az uniós országok nemzeti szabályozása megfelelő védelmet és ellenőrizhetőséget biztosít.

Mivel a nemzeti adatvagyon eleme része lehet a létfontosságú információs infrastruktúráknak, de kötelezően nem az, ezért a törvény szerinti szigorító kivétel a csak hazai kezelésre vonatkozik.

Az adatok külső szolgáltatónál történő tárolása, illetve az elektronikus információs rendszerek kiszervezése miatt került a törvénybe az a kényszer, hogy amennyiben nem Magyarországon bejegyzett cég végzi az adatok kezelését, akkor legyen elérhető kapcsolattartó személy, illetve ez a személy folyamatosan (24/7) legyen felkérhető, utasítható a törvény végrehajtásával kapcsolatban, és akár a felelősségre vonásra is sor kerülhessen.

4.2.5 Auditálás, minőségi tanúsítványok figyelembevétele

A nemzeti adatvagyont kezelő szervezetek, illetve a létfontosságú rendszerelemként számításba vehető szervezetek egy része komoly munkával és jelentős költségekkel auditáltatta szervezetét az informatikai biztonságirányítási rendszerről szóló nemzetközi ISO/IEC 27001 szabvány szerint, illetve a nemzetközi egyezménnyel elfogadott Common Criteria vagy a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma szerint minősített informatikai eszközöket, vagy más szabványok vagy ajánlások alapján tanúsított rendszerelemeket használ. Ezek a minősítések garanciát szolgáltatnak a tudatos eljárásokra, így – és a jog-

biztonság megőrzését is szem előtt tartva – ezen tanúsítványokat a hatóság az eljárása során figyelembe veszi.

4.3 Az elektronikus információbiztonsági követelmények

4.3.1 Az elektronikus információs rendszerek biztonsági osztályokba sorolása

A védelemnek költséghatékonynak kell lennie, azaz csak a lehetséges veszteségek és károk nagyságrendjével arányosan indokolt a védelemre költeni. Ennek érdekében meg kell állapítani, hogy az adott elektronikus információs rendszer, illetve az abban kezelt adatok a bizalmasságának, a sértetlenségének vagy a rendelkezésre állásának elvesztése külön-külön milyen nagyságrendű károkat okoz. A nagyságrend megállapítása elégséges, mert egyrészt a pontos értéket nehéz, hosszadalmas és költséges meghatározni, másrészt a nagyságrend ismerete már elég ahhoz, hogy a védelemre történő ráfordítások értéke meghatározható legyen. Mivel az osztályba sorolást külön el kell végezni a bizalmassági, sértetlenségi és rendelkezésre állási szempontok szerint is, így minden egyes elektronikus információs rendszerre számos kombinációban állíthatók be a műszaki védelmi intézkedések. Ez biztosítja a kockázatarányos és költséghatékony műszaki védelmet. A biztonsági osztályozás részletszabályainak meghatározására a törvény végrehajtási rendeletében kerül sor.

Ilyen biztonsági osztályozás és a hozzátartozó követelmények részletes szabályait a törvény *végrehajtási rendelete*, „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről” szóló 41/2015. (VII. 15.) BM rendelet tartalmazza. A rendeletben alkalmazott besorolási kritériumokkal az alábbiakban részletesen is foglalkozunk.

A szervezet vezetőjének a felelőssége, hogy az elektronikus információs rendszerek osztályba sorolását elvégezzék. Mivel a kockázatok folyamatosan változnak, ezért az osztályba sorolást rendszeresen frissíteni kell. Ez az elvárás biztosítja azt, hogy a biztonság ne egy statikus, egyszer kialakított állapot legyen, hanem a szervezetnek folyamatosan figyelemmel kelljen kísérnie a rá vonatkozó kockázatokat, azaz legyen egy kockázatkezelési folyamata. A mérvadó információbiztonsági szabványok és ajánlások kivétel nélkül ezt a lépést tekintik a legalapvetőbb elvárásnak a biztonság megteremtéséhez.

Az elektronikus információs rendszerek biztonsági osztályának és a szervezetek biztonsági szintjének elérési követelményei a fokozatosság elvére épülnek. Az adott osztály és szint elérése a szervezet feladat- és hatáskörének függvénye, amelyek biztosítják, hogy a szervezet a feladatellátásával, a közigazgatási szervezetrendszerben elfoglalt helyével, piaci szerepével, valamint elektronikus információs rendszereinek jelentőségével, állapotával arányosan kerüljön kialakításra.

4.3.2 A biztonsági osztályok

Tekintsük most sorjában az egyes biztonsági osztályokba való besorolásra vonatkozó kritériumok rendszerét. A besorolás alapját a bekövetkező kár mértéke alapján határozzuk meg, melyet a rendelet a

- jelentéktelen,
- csekély,
- közepes,
- nagy,
- kiemelkedően nagy

fogalmaival ad meg, és az alábbiak szerint rendszerezi azokat.

4.3.2.1 Az 1. biztonsági osztály

Az 1. biztonsági osztály esetében csak *jelentéktelen* káresemény következhet be, mivel

- az elektronikus információs rendszer nem kezel jogszabályok által védett (pl. személyes) adatot;
- nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen.

4.3.2.2 A 2. biztonsági osztály

A 2. biztonsági osztály esetében *csekély* káresemény következhet be, mivel

- személyes adat sérülhet;
- az érintett szervezet üzlet- vagy ügymenete szempontjából csekély értékű és/vagy csak belső (intézményi) szabályzóval védett adat vagy elektronikus információs rendszer sérülhet;
- a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.

4.3.2.3 A 3. biztonsági osztály

A 3. biztonsági osztály esetében *közepes* káresemény következhet be, mivel

- különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;
- az érintett szervezet üzlet- vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet;
- a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.

4.3.2.4 A 4. biztonsági osztály

A 4. biztonsági osztály esetében *nagy* káresemény következhet be, mivel

- különleges személyes adat nagy mennyiségben sérülhet;
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
- az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet;
- a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében vagy vezetésében személyi felelősségre vonást kell alkalmazni;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.

4.3.2.5 Az 5. biztonsági osztály

Az 5. biztonsági osztály esetében *kiemelkedően nagy* káresemény következhet be, mivel

- különleges személyes adat kiemelten nagy mennyiségben sérülhet;
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
- a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
- a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt, jogok sérülhetnek;
- az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

4.4 Információbiztonsági irányítási rendszer kialakítása

A megelőzés alapját képező, kockázatokkal arányos, költséghatékony védelem kialakításának egyik nemzetközileg elfogadott eszköze az információbiztonsági irányítási rendszer kialakítása a szervezetnél. Ez biztosítja, hogy az alapvető biztonsági követelmények meghatározása egy magas absztrakciós szinten is megtörténjen. A szervezeti biztonság megteremtése azért is fontos, mert bevezetésének költsége elenyésző (elsősorban szabályozási feladatokat határoz meg), mégis jelentősen növeli az információbiztonság szintjét. Eszerint minden érintett szervezetnek kötelessége rendszerszinten kezelnie az információbiztonságot.

4.4.1 Biztonsági szintekbe történő besorolás. A legmagasabb elvárt biztonság követelménye

A törvény egyik fontos követelménye az, hogy a szervezetnek azt a biztonsági szintet kell elérnie az információbiztonsági irányítási rendszerében, amely megegyezik az általa kezelt elektronikus információs rendszerek közül a *legmagasabb biztonsági osztállyal*.

Azaz, ha pl. nemzeti adatvagyon elemet kezelő rendszere van a szervezetnek, a legmagasabb érettségi szintet kell elérnie, vagy ha pl. egy központi államigazgatási szerv olyan elektronikus információs rendszert kezel, melyben az információk bizalmassági besorolása 2., sértetlenségi besorolása 3., rendelkezésre állási besorolása pedig 1., akkor a szervezeti biztonsági szintjét 3. szintre kell hoznia. Ha ennél a szervezetnél minden érték 2., a szervezeti biztonsági szintje akkor is 3., hiszen a törvény 9. § (2) bekezdés *b)* pontja eszerint rendelkezik.

A 7–9. és a 10–11. §-ok együttes alkalmazása költséghatékony megoldás, mert nem a szervezet egészénél egységesen, azonos biztonsági osztályba sorolva kell az elektronikus információs rendszerek védelmét megvalósítani, hanem ez rendszerenként eltérő lehet. A szervezet biztonsági szintjének elérése viszont garantálja, hogy az információbiztonsági irányítási rendszer a legmagasabb kockázatok által elvárt legyen.

A szervezeti biztonsági szintet ugyan az általa kezelt elektronikus információs rendszer besorolása határozza meg, de ennek a biztonsági szintnek az elérése jól tervezhető módon, kellő időráfordítással valósítandó meg. A szervezet vezetője kezdetben besorolja a szervezetet az aktuális érettségi szintre, majd kétévente köteles egy szintet lépni a skálán mindaddig, amíg eléri az elvárt szintet. Pl. egy olyan központi államigazgatási szervnél, ahol nincsen jelen az információbiztonsági szabályozás, akár 4 év is rendelkezésre áll a követelmények teljesítéséhez.

4.4.2 Besorolástól független vezetői feladatok

A törvény a 11–12. §-okban az érintett szervezetek vezetőinek legfontosabb, a szervezet besorolási szintjétől és az elektronikus információs rendszer besorolási osztályától független feladatait és felelősségeit határozzák meg. Ezek a feladatok elsősorban adminisztratív feladatok, amelyek arra vonatkoznak, hogy a szükséges szinten és a szükséges mélységben legyen szabályozva az elektronikus információs rendszerek biztonsága, és annak nevesített felelőse legyen a szervezetnél. A szervezet köteles biztonsági stratégiát és informatikai biztonsági szabályzatot készíteni, utóbbiak része lehet a biztonságpolitika is. A szakmai irányítást ellátó miniszter által meghatározott ágazati informatikai biztonságpolitika és ágazati informatikai biztonsági stratégia keretében szabályzat-minták és iránymutatások kiadására is sor kerülhet.

A szervezet vezetőjének felelősségét nem csökkenti, ha az elektronikus információs rendszer kiszervezésre kerül, függetlenül attól, hogy a közreműködőkkel kötött szerződésben köteles a törvényi rendelkezések kötelező alkalmazását előírni.

Az előírások között a folyamatos oktatás, képzés kötelezettségének rögzítése egy, a technikai fejlődés következtében gyorsan változó területnek való megfelelés miatt szükséges.

A szervezet vezetője köteles együttműködni a hatósággal, így lehetőség nyílik arra, hogy a védelmi tevékenységben szükséges kapcsolattartás és információcsere megvalósulhasson. Ezen információcsere egyik legfontosabb esete a törvényben külön nevesítésre került: a szervezet vezetője köteles a bekövetkezett biztonsági eseményeket a hatóság, a Nemzeti Biztonsági Felügyelet és a biztonsági események kezelésére vonatkozó feladatokat ellátó kormányzati eseménykezelő központ tudomására hozni. Ez is hozzájárul az országos szintű kibervédelmi rendszer kialakításához, mely összhangban van az Európai Unió tervezett kibervédelmi intézkedéseivel.

4.4.3 Információbiztonsági felelős

Az elektronikus információs rendszert használó, üzemeltető szerv vezetője gondoskodni tartozik a biztonsági feladatok ellátásáért kellő szakértelemmel rendelkező, felelősséggel tartozó személy kiválasztásáról, megbízásáról. A törvény ugyanis előírja, hogy a szervezeteknek legyen olyan munkatársa az elektronikus információs rendszer biztonságáért felelős személyében, aki képes az elektronikus információs rendszerek védelmének feladatait összefogni, koordinálni. Hatásköre mindenre ki kell, hogy terjedjen az elektronikus információs rendszerek védelme kapcsán, ugyanakkor felelőssége oszthatatlan. Az információs rendszer biztonságáért felelős személy alapfeladatainak meghatározására a szervezet besorolási szintjétől és az elektronikus információs rendszer besorolási osztályától függetlenül, általánosságban került sor.

A törvény nagy hangsúlyt helyez a felhasználói tudatosság növelésére, melynek révén elérhető, hogy maguk az érintettek is körültekintően védjék adataik biztonságát, megértve a kérdés jelentőségét. Ennek érdekében a törvény hatálya alá tartozó szervezetek munkatársainak, kiemelten az elektronikus információs rendszer biztonságáért felelős személyeknek a törvény kötelező képzésen való részvételt ír elő.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 77. § (1) bekezdés *a)* pontjában foglaltakra figyelemmel a Kormány rendeletben állapítja meg azokat a munkaköröket, amelyek – a 2. számú melléklet 18. pontja alapján – fontos és bizalmas munkakörnek minősülnek, illetve e munkakörök tekintetében meghatározza a biztonsági ellenőrzések szintjét. Azon kormányzati szándékhoz igazodva, amely szerint a jövőben kiemelt figyelmet kell fordítani arra, hogy az állami szereplők számára informatikai szolgáltatást nyújtó személyek vagy szervezetek esetén az informatikai felelősök nemzetbiztonsági ellenőrzése megtörténjen, a jövőben az elektronikus információs rendszer biztonságáért felelős személy esetében is felmerülhet ilyen irányú igény.

4.4.4 A megelőzéstől az eseménykezelésig

A törvény egyik legfontosabb eleme az alapvető elektronikus információbiztonsági követelmények meghatározása. Az ebben a körben használt fogalmakat az informatikai szakma már régóta használja ugyan, de azok törvényi szinten, általános követelményként történő megfogalmazása olyan előrelépést jelent az elektronikus információs rendszerek biztonsága területén, ami önmagában mérföldköve lehetne az elmúlt időszak ez irányú szabályozási törekvéseinek.

A törvény az elektronikus információs rendszerek biztonságának általános követelményeit, az elektronikus információs rendszerek biztonságának definíciójából levezetve, úgy határozza meg, hogy a védelem minden lehetséges módja (logikai, fizikai és adminisztratív védelem) a tervezéstől a megvalósításig felhasználásra kerüljön. A védelem olyan legyen, hogy lehetőleg kerülje el a fenyegetések bekövetkezését, de ha ez nem lehetséges, akkor erről annak bekövetkezése előtt az érintettek szerezzenek tudomást. Az elektronikus információs rendszerek esetében különösen fontos a biztonsági események bekövetkeztének azonnali észlelése, hogy arra mielőbb reagálhasson a szervezet vezetése. A biztonsági esemény bekövetkezése után kiemelt szerepet kap a gyakran incidenskezelésnek is nevezett biztonsági események kezelése. Ennek során a bekövetkezett biztonsági események hiteles dokumentálása, a bekövetkezett károk következményeinek a kezelése, a biztonsági eseményeket kiváltó okok kivizsgálása és a felelősségek megállapítása, a szükséges felelősségre vonás után a szabályozás javításával, a védelmi intézkedések kiegészítésével vagy megerősítésével és az érintettek oktatásával, a tudatosság képzésével gondoskodni kell arról, hogy az adott biztonsági események bekövetkezésének esélye kisebb legyen és az ezáltal okozott kár is csökkenjen.

Az információ biztonságának érdekében a

- megelőzés,
- korai figyelmeztetés,
- észlelés,
- reagálás,
- eseménykezelés

láncolat követésével a törvény előírja a lehetséges biztonsági események megelőzését, a bekövetkezett biztonsági események kezelését.

Eszerint a(z)

- *megelőzés* nem más, mint a fenyegetés hatásának elkerülése (Ibtv. 1. § 36. pont),
- *korai figyelmeztetés* a várható fenyegetésről szóló időben kiadott jelzés, ami lehetővé teszi a hatékony védelmi intézkedések megtételét (Ibtv. 1. § 32. pont),
- **észlelés** a biztonsági esemény bekövetkezésének felismerése (Ibtv. 1. § 17. pont),
- *reagálás* pedig az esemény következményeinek megakadályozása, késleltetése, valamint a károk mérséklése (Ibtv. 1. § 37. pont).

A láncolat kiemelt mozzanata a biztonsági esemény kezelése, amely magában foglalja az elektronikus információs rendszerben bekövetkezett biztonsági esemény

- dokumentálását,
- következményeinek felszámolását,
- a biztonsági esemény bekövetkezése okainak és felelőseinek megállapítását, továbbá
- a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet.

A törvény elfogadja azt a nézetet, hogy a védelem tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze vagy szinten tartsa azt az állapotot, amit biztonságnak nevezünk. A biztonság a védett rendszer olyan állapota, amelyben annak

védelme az összes számításba vehető fenyegetést figyelembe veszi, a rendszer valamennyi elemére kiterjed, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul és annak költségei hosszútávon arányosak a fenyegetések által okozható károkkal.

A biztonság nagyon sok részletet jelent, ugyanakkor egy és oszthatatlan. Ezt az egy és oszthatatlan biztonságot a védelmi tevékenységek (folyamatok) részterületein keresztül lehet megvalósítani. Az információbiztonság alapvető feladatai a megelőzés és a korai figyelmeztetés, az észlelés, a reagálás és a biztonsági események kezelése. A korai figyelmeztetés előírásként történő meghatározása nem figyelmeztető rendszer kiépítésére, hanem a szervezet aktív cselekvési képességére vonatkozik, az észlelés folyamatának azon része, amely más szervezettől érkező figyelmeztetések azonosítására és feldolgozására utal. A biztonság tervezése, kialakítása során e feladatok mindegyikére kellő hangsúlyt kell fektetni ahhoz, hogy a védelem elérje célját.

4.5 Az elektronikus információs rendszerek biztonságának felügyelete

A jogalkotó gondoskodik az elektronikus információs rendszerek biztonsági felügyeletének országos szervezeti infrastruktúrájáról is. A törvény szerint létrejön ugyanis az informatikáért felelős miniszter irányítása alatt, a minisztérium szervezeti keretében önálló feladattal és hatósági jogkörrel rendelkező szervezeti egység (a továbbiakban: hatóság), amely az információbiztonsággal kapcsolatos nyilvántartásokat vezeti, illetve ellenőrzi a törvény betartását.

Létrehozásának indoka, hogy szükség van egy olyan hatóságra, amely képes ellenőrizni a törvényben foglaltakat és az azokhoz kapcsolódó követelmények megvalósulását. Ennek keretében a hatóság jogosult szankciót alkalmazni azokban az esetekben, amikor a szervezetnél az elektronikus információs rendszert veszélyeztető informatikai állapot alakul ki. Nem közigazgatási szervek esetében bírságolási joga van.

A hatóság közigazgatási szervek esetében információbiztonsági felügyelőt nevezhet ki. Az információbiztonsági felügyelő jogosult a szervezet által meghozott védelmi intézkedéseket véleményezni, adott esetben az intézkedéssel szemben kifogással élhet. A fenyegetés elhárítása érdekében intézkedéseket, eljárásokat javasolhat. Ezzel a jogkörrel a törvényben foglaltak megvalósítása jelentősen hatékonyabban történhet meg.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 77. § (1) bekezdés *a)* pontjában foglaltakra figyelemmel a Kormány rendeletben állapítja meg azokat a munkaköröket, amelyek – a 2. számú melléklet 18. pontja alapján – fontos és bizalmas munkakörnek minősülnek, illetve e munkakörök tekintetében meghatározza a biztonsági ellenőrzések szintjét. Az információbiztonsági felügyelő esetében ezért indokolt a munkakörnek az e felhatalmazás szerinti kormányrendeletben történő megjelenítése.

4.5.1 A Nemzeti Biztonsági Felügyelet

A Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) feladatainak rendszere:

- Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény szabályai szerinti szakhatóságként közreműködik az osztályba sorolás és a biztonsági szint megha-

tározására, a hatósághoz érkező bejelentések kivizsgálására vonatkozó, a hatóság által lefolytatott eljárásban, valamint a hatóság éves ellenőrzési terv alapján végzett ellenőrző tevékenységében.

- A szervezet felkérésére az ellenőrzési tervtől függetlenül is végezhet sérülékenységvizsgálatot, feltárva ez által a biztonsági esemény bekövetkezését megelőzően az esetleges sérülékenységeket, hiányosságokat, költséghatékonnyá téve ez által a megelőzést.
- Saját hatáskörben hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervezhet, valamint a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviseli Magyarországot.

A hatóság és az NBF közötti feladatmegosztás leképezi a kormányzaton belüli feladatmeghatározást, melynek értelmében az informatikai terület ellenőrzése az informatikáért felelős miniszter feladat- és hatáskörébe, míg a szélesebb értelemben vett információbiztonság az e-közigazgatásért és a minősített adatok védelmének szakmai felügyeletéért felelős miniszter feladatkörébe tartozik.

4.5.2 Nemzeti Kibervédelmi Intézet

A törvény 2015-ben hatályba lépett módosítása eredményeként 2015. október 1-jétől a Nemzetbiztonsági Szakszolgálat irányítása alatt több új szervezet alakult. Ekkor jött létre a *Nemzeti Kibervédelmi Intézet*, amely szakfeladatok ellátására magában foglalja a következő szervezeteket:

- Kormányzati Eseménykezelő Központot (GovCERT-Hungary),
- Nemzeti Elektronikus Információbiztonsági Hatóság,
- E-biztonsági Intelligencia Központ (NBF-CDMA).

A Nemzeti Kibervédelmi Intézet az elektronikus információs rendszerek teljes információbiztonsági életciklusára vonatkozóan feladatkörrel rendelkezik: nyomon tudja követni és segíteni tudja annak alakulását, tervezési szakaszait, a szabályozást, az ellenőrzést, valamint az incidenskezelést egyaránt.

A Nemzeti Kibervédelmi Intézet (továbbiakban: NKI) szervezetén belül három szakmai terület került kialakításra:

- a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó incidenskezelési szakterület (GovCERT = Kormányzati Eseménykezelő Központ);
- a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH);
- a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási és sérülékenység-vizsgálati szakterület.

4.5.2.1 A Kormányzati Eseménykezelő Központ (GovCERT-Hungary)

A törvény létrehozta Kormányzati Eseménykezelő Központot (GovCERT-Hungary), mint a magyar kormányzat információmegosztó és incidenskezelő szervezetét.

A Kormányzati Eseménykezelő Központ a magyar és a nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra-védelmi szervezetek felé mint az országon belüli koordinációs szervezet végzi az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, továbbá közzéteszi a felismert és publikált szoftver-sérülékenységeket.

A Központ a szolgáltatásait (preventív információmegosztás és operatív incidenskezelés) a kormányzati szervezetek és önkormányzatok részére nyújtja. A Központnak kiemelt szerepe van a nemzetgazdaság és az állami működőképesség szempontjából kritikus fontosságú informatikai rendszerek védelmében, ezzel összefüggésben a nemzetközi szervezeteknél Magyarország képviseletében és a hálózatbiztonság tudatosításában egyaránt.

A Kormányzati Eseménykezelő Központ speciális feladata az állami és önkormányzati szervek munkatársainak felkészítése az internet minél tudatosabb és biztonságosabb használatára, szemléletformáló kampányok, tudatosító előadások formájában.

4.5.2.2 Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH)

A NEIH az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. Amennyiben a szervezet a hatósággal nem működik együtt, úgy – költségvetési szerv esetében – a hatóságnak joga van kirendelni ún. információbiztonsági felügyelőt, míg nem költségvetési szerv esetén bírság kiszabására is lehetősége van.

A hatóság ellenőrző funkciója erőteljes támogató funkcióval is bír, ugyanis jogosult a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában véleményezni és ellenőrizni az információbiztonsági követelmények megtartását. Az információtechnológiai fejlesztések elektronikus információbiztonsága szempontjából kiemelt fontosságú, hogy a vonatkozó előírások a rendszerek teljes életciklusa alatt következetesen és maradéktalanul megvalósításra kerüljenek és a fejlesztések eredményeként önmagukban is teljes, továbbá a meglévő rendszerekhez funkcionálisan és biztonsági aspektusból is harmonikusan és költséghatékonyan illeszkedő rendszerelemek, rendszerek épüljenek ki.

4.5.2.3 Biztonságirányítás és sérülékenység-vizsgálat

Míg az NKI egyes szakterületei kívülről támogatják az állami és önkormányzati szerveket abban, hogy saját rendszereik védelmét ellássák, és ennek keretében kialakítsák saját ún. információbiztonsági irányítási rendszerüket (röviden: biztonságirányítási rendszer), addig a biztonságirányítási szakterület ezt a feladatot tevőlegesen is végzi – részint az NKI biztonsági felügyeletére bízott, kiemelt kormányzati rendszerek esetében, részint pedig szakmai támogatást nyújtva a hatósági szakterület részére.

A sérülékenység-vizsgálat célja az esetleges biztonsági események bekövetkeztét megelőzően az elektronikus információs rendszer gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása. A sérülékenység-vizsgálat végrehajtása során a vizsgálat alá vont elektronikus információs rendszerben a GovCERT felkutatja többek között a potenciális szoftverhibákat, gyenge jelszavakat, hibás beállításokat, amelyeket egy támadó képes lenne kihasználni és ezeken

keresztül kárt okozni a rendszerben. Ez a tevékenység együtt jár azzal, hogy a vizsgálatot végzők pontos, mélyreható ismeretekkel rendelkeznek az adott elektronikus rendszerről.

A törvény szerint a zárt célú elektronikus információs rendszerek, az állami és önkormányzati szervek létfontosságú rendszerelemeinek elektronikus információs rendszerei, valamint a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek vonatkozásában kizárólag a GovCERT végezhet sérülékenység-vizsgálatot. A fenti körbe nem tartozó állami rendszerek esetében pedig a törvény (Ibtv.) lehetővé teszi magas szintű szakmai és biztonsági elvárásoknak megfelelő gazdálkodó szervek számára is a sérülékenység-vizsgálat lefolytatását.

A sérülékenység-vizsgálat eredményeként elkészítésre kerülő vizsgálati jelentésben a GovCERT minden esetben javaslatot tesz az azonosított sérülékenységek kijavítására is.

4.6 Oktatás, képzés és a kapcsolódó kutatás-fejlesztési tevékenység

A törvény 23. §-a tulajdonképpen a Nemzeti Közszolgálati Egyetem kizárólagos kompetenciájába utalja azon szakamberek kiképzésének feladatát és felelősségét, akik a törvény hatálya alá rendelt szervezeteknél az elektronikus információs rendszerek vonatkozásában az informatikai biztonsági vezetői feladatokat megfelelő szakképesítés birtokában elláthatják.

Ez kétségtelenül hatalmas feladat az NKE számára, hiszen az érintett szervezetek számát, méretét és feladatkörét figyelembe véve több ezer – óvatos becslés szerint is 8000-10 000 – közötti számban kell megfelelő szakembereket viszonylag rövid idő, mindössze néhány év alatt felkészíteni igényes és nagy szakértelmet kívánó feladatok ellátására, s a természetes fluktuáció ellensúlyozására folyamatosan képezni az említett szakemberek új és új generációit.

A törvény alapvető célja az elektronikus információs rendszer biztonságáért felelős személy kötelező információbiztonsági képzésének előírása. A hazai felsőoktatási környezetben az információbiztonság területén jelenleg ilyen kötelező jellegű, intézményesített vezetőképzés nincs. A mérnök, a programozó és a gazdasági informatikus alap- és mesterszakokon különböző műszaki jellegű oktatások vannak, amelyek között a Budapesti Műszaki Egyetemen és az Óbudai Egyetemen informatikai biztonsági szakirányú képzést is tartanak. A Nemzeti Közszolgálati Egyetemen a nemzetbiztonsági képzés keretén belül oktatnak informatikai védelmet. Akkreditált felnőttképzés e téren a Nemzetközi Technológiai Közhasznú Kft. (Puskás Alapítvány) informatikai biztonsági felelős képzése, amely alapvetően az időközben hatályon kívül helyezett, az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet követelményeihez igazodik. A törvényben előírt követelményeknek megfelelő képzés és a vezetőképzés erősítése érdekében mindezekre figyelemmel szükséges egy új átfogó képzési struktúra kialakítása.

Az információbiztonsági tudatosság növelése érdekében a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kara javaslatot tesz a képzési követelményekre, és részt vesz a törvény hatálya alá tartozó személyek kötelező oktatásában. Ez biztosítja, hogy az érintettek magas színvonalú képzésben részesüljenek.

A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kara az elektronikus információs rendszerek biztonsága, a létfontosságú információs infrastruktúrák védelme,

a kibervédelem tekintetében a jövőben nemzeti és esetleges nemzetközi kutatóhelyként is részt vehet a szakterület kutatásában, fejlesztésében. E feladatokban való részvétellel az egyetemi oktatók-kutatók folyamatos gyakorlati ismereteket szereznek, illetve azokat karbantartják. Az oktatói-kutatói kapacitást a szükséges szakmai kidolgozó munkában költséghatékonyabban lehet felhasználni, mint külső cégeket igénybe venni erre a feladatra.

A törvény az oktatás, a fejlesztés és a gyakorlat kombinációjával egy magas szintű oktatási, kutatás-fejlesztési centrumot hoz létre az elektronikus információs rendszerek biztonságának területén.

A nemzetközi oktatási környezetben már számos akkreditált képzés elfogadott. Ezek közül a legelismertebbek közé tartozik:

- Az Information Systems Audit and Control Association (ISACA) nemzetközi szervezet Certified Information Security Manager (CISM) képzése, amelyet az USA Védelmi Minisztériuma is szakirányú képzésként ismer el és vezetői szintű ismereteket nyújt. A képzést Magyarországon felsőfokú oktatási intézményekben – külön megállapodás alapján –, az ISACA magyarországi szervezetének felügyeletével, hazai informatikai szakemberek külföldi tananyag és követelmények alapján tartják. A képzés eredményes elvégzését ANSI-ISO szabvány szerint akkreditált oklevél igazolja.
- Az International Information Systems Security Certification Consortium, Inc. Certified Information Systems Security Professional (CISSP) képzése az informatikai rendszerek technikai kérdéseinek biztonsági vonatkozásairól szól. A képzést Magyarországon a Budapesti Műszaki Egyetemen hazai informatikai szakemberek külföldi tananyag és követelmények alapján tartják. A képzés eredményes elvégzését ANSI-ISO szabvány szerint akkreditált oklevél igazolja.

Mindkét (CISM, CISSP) végzettség megszerzéséhez gyakorlati tapasztalatokat is igazolni kell, a képzések időtartama eltérő, a minősítések megtartásához éves szinten meghatározott kreditpontot kell elérni.

Nemzetközileg ismert és elfogadott még az EC-Council Certified Ethical Hacker és Certified Penetration Tester képzés, amely Magyarországon a NetAcademia Oktatóközpontnál végezhető el.

A képzések üzleti alapon, a hazai viszonylatokhoz képest nagyon drágán működnek, ezért célszerű a költséghatékonyabb és a nemzetközi oktatási környezettel összhangban álló – adott esetben a későbbiekben mesterképzés útján elismertethető – hazai képzést előnyben részesíteni, ami egyúttal a kutatási kapacitás fejlesztését is lehetővé teszi.

5 VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA A VHR. SZERINT

A védelmi intézkedések technikai részleteit, a biztonsági osztályokba, illetve a biztonsági szintekbe történő besoroláshoz szükséges útmutatásokat az Ibtv. végrehajtási rendelete tartalmazza igen részletesen.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, valamint a biztonsági osztályba és a biztonsági szintbe sorolási követelményekről szóló 41/2015. (VII. 15.) BM rendelet legfontosabb elemeit a négy melléklet tartalmazza.

Az 1. melléklet a biztonsági osztályba sorolás szempontjait adja meg. (Lásd: jelen fejezet 4.2 alpontja)

5.1 Biztonsági szintek megállapítása

A 2. mellékletben a szervezeti biztonsági szintek megállapításához találunk kritériumokat. Az 1. szint attribútumait önállóan határozza meg a rendelet, majd a felsőbb szinteken rendre az alábbi szinthez képest támaszt lépésről lépésre egyre magasabb elvárásokat.
Tekintsük most át ezt a rendszert:

5.1.1 Az 1. biztonsági szervezeti szint követelményei

Az ezen a szinten lévő szervezet személyes adatot nem kezel.

1. Az érintett szervezet az érintett személyi kör részére biztosítja a szervezeti vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasítását, belső rendelkezését, szabályozását vagy más, erre célra szolgáló dokumentumot (a továbbiakban együtt: szabályzat).
2. Az informatikai biztonsági szabályzat része a folyamatos kockázatelemzési eljárás, amely tartalmazza a beépített ellenőrzési pontokat.
3. Az informatikai biztonsági szabályzat vonatkozhat egész szervezetre és működési területére, vagy meghatározott vagyonelemre, vagy szervezeti egységre.
4. Az informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezetőnek kell jóváhagynia.
5. Az informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket.
6. Az informatikai biztonsági szabályzat be nem tartása jogkövetkezményt von maga után.

5.1.2 A 2. biztonsági szervezeti szint követelményei

Az érintett szervezet biztonsági szintje 2., ha a szervezet vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.

A 2. biztonsági szervezeti szint követelményei az 1. szinthez rendelt követelményeken túl:

1. Az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak.
2. Az eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét.
3. Az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében.
4. Az egyes folyamatokat szervezeti egységek vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel vagy szervezeti egységekkel.
5. A folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontrolltevékenység – ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét – megállapítható legyen.

5.1.3 A 3. biztonsági szervezeti szint követelményei

Az érintett szervezet biztonsági szintje 3., ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.

A 3. biztonsági szervezeti szint követelményei a 2. szinthez rendelt követelményeken túl:

1. Az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket.
2. A folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni.
3. A folyamatok nem alkalmazandók egyéni vagy eseti eljárásokra.
4. A folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult vezetőnek kell jóváhagynia.
5. A folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését.
6. A szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.

5.1.4 A 4. biztonsági szervezeti szint követelményei

Az érintett szervezet biztonsági szintje 4., ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.

A 4. biztonsági szervezeti szint követelményei a 3. szinthez rendelt követelményeken túl:

1. Az üzemeltetési vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét.
2. Tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint.
3. Azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges vagy bekövetkezett biztonsági esemény kezelését is.
4. Folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben vagy egészben történhetnek alvállalkozók vagy más, erre feljogosított vagy a szerv felett felügyelet gyakorló szerv bevonásával.
5. A szervezet folyamatba épített belső értékelései nem helyettesíthetőek.
6. A 3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk vagy riasztások alapján tesztelési eljárást vagy biztonsági ellenőrzést kell végezni.
7. A tesztelés értékelése alapján megállapított követelményeket – beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is – dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni.
8. Az egyedi kontrolleljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.

5.1.5 Az 5. biztonsági szervezeti szint követelményei

Az érintett szervezet biztonsági szintje 5., ha a szervezet vagy szervezeti egység a 4. szinthez rendelt jellemzőkön túl európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.

A 5. biztonsági szervezeti szint követelményei a 4. szinthez rendelt követelményeken túl:

- Biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését.
- Biztosítani kell a szabályzatok, tesztelési eljárások, biztonsági folyamatok folyamatos felülvizsgálatát és továbbfejlesztését.

- A szervezetnek rendelkeznie kell átfogó információbiztonsági programmal, amely szerves része a szervezet feladatellátásnak és biztosítja a személyi állomány biztonságtudatosságának növelését.
- A szervezet személyi állományának rendelkeznie kell információbiztonsági operatív képességgel és a feladat elvégzéséhez szükséges szaktudással.
- A biztonsági sérülékenységek felismerésének és kezelésének képességét a szervezet egésze tekintetében meg kell valósítani.
- A fenyegetettségek folyamatos újraértékelésével, a kontrollfolyamatok felülvizsgálatával nyomon kell követni információbiztonsági környezet változását.
- Az információbiztonságot érintő külső vagy belső környezeti változásokra figyelemmel további információbiztonsági alternatívákat kell meghatározni.
- A szervezetnek ki kell alakítania az információbiztonsági képesség- és állapotmérési és értékelési módszertanát, meg kell határozni annak mutatóit és 5.1.7. pont szerinti esetben aktualizálnia kell azt.

5.2 Besorolási útmutató

A Vhr. 3. melléklete táblázatos formában igen részletesen áttekinti és rendszerezi azokat az intézkedéstípusokat, amelyeket az egyes szinteken a megfelelő biztonsági besorolás teljesítése érdekében végre kell hatjani.

Az Ibtv. és a Vhr. logikáját követve az adminisztratív, a fizikai, majd a logikai védelmi intézkedésekre kerül sor. Kétségtelenül ez a Vhr. legfontosabb része. A táblázat természetesen igen tömör, és itt nincs mód az egyes intézkedések részleteiben történő kifejtésére. Az innen hiányzó magyarázatokat végül a Vhr. 4. mellékletében találjuk.

Adminisztratív védelmi intézkedések
Az adminisztratív védelmi intézkedések körében az alábbiak szerint 7 főcsoportot, majd azokon beül további intézkedéscsoportokat találunk. A főcsoportok tehát a következők:
1. Szervezeti szintű alapfeladatok
2. Kockázatelemzés
3. Tervezés
4. Rendszer és szolgáltatás beszerzése
5. Biztonsági elemzés
6. Emberi tényezőket figyelembe vevő biztonság
7. Tudatosság növelése és képzés
A főcsoportokon belül pedig részletes útmutatás szolgál a további intézkedések megtervezésére és dokumentálására.

1. Szervezeti szintű alapfeladatok	1. Informatikai biztonságpolitika 2. Informatikai biztonsági stratégia 3. Informatikai biztonsági szabályzat 4. Az elektronikus információs rendszerek biztonságáért felelős személy 5. Pénzügyi erőforrások biztosítása 6. Az intézkedési terv és mérföldkövei 7. Az elektronikus információs rendszerek nyilvántartása 8. A biztonsági teljesítmény mérése 9. Szervezeti szintű architektúra 10. Kockázatkezelési stratégia 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás 12. Tesztelés, képzés és felügyelet 13. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel
2. Kockázatelemzés	1. Kockázatelemzési eljárásrend 2. Biztonsági osztályba sorolás 3. Kockázatelemzés 4. Sérülékenység teszt 5. Felfedhető információk
3. Tervezés	1. Biztonságtervezési eljárásrend 2. Rendszerbiztonsági terv 3. Személyi biztonság 4. Információbiztonsági architektúra leírása

4. Rendszer és szolgáltatás beszerzése	1. Beszerzési eljárásrend 2. Erőforrásigény felmérése 3. A rendszer fejlesztési életciklusa 4. Beszerzések 5. Az elektronikus információs rendszerre vonatkozó dokumentáció 6. Biztonságtervezési elvek 7. Külső elektronikus információs rendszerek szolgáltatásai 8. Fejlesztői változáskövetés 9. Fejlesztői biztonsági tesztelés 10. A védelem szempontjainak érvényesítése a beszerzés során 11. Fejlesztési folyamat, szabványok és eszközök 12. Fejlesztői oktatás 13. Fejlesztői biztonsági architektúra és tervezés
5. Biztonsági elemzés	1. Biztonságelemzési eljárásrend 2. Biztonsági értékelések 3. Az elektronikus információs rendszer kapcsolódásai 4. Cselekvési terv 5. Folyamatos ellenőrzés 6. Belső rendszerkapcsolatok
6. Emberi tényezőket figyelembe vevő – személy – biztonság	1. Személybiztonsági eljárásrend 2. Munkakörök, feladatok biztonsági szempontú besorolása 3. A személyek ellenőrzése 4. Eljárás a jogviszony megszűnésekor 5. Az áthelyezések, átirányítások és kirendelések kezelése 6. Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények 7. Fegyelmi intézkedések
7. Tudatosság növelése és képzés	1. Képzési eljárásrend 2. Biztonságtudatosság képzés 3. Szerepkör vagy feladat alapú biztonsági képzés 4. A biztonsági képzésre vonatkozó dokumentációk

Fizikai és környezeti védelmi intézkedések

A fizikai védelem köre, bár ez is rendkívül szerteágazó, szinte szerénynek hat az adminisztratív, illetve, mint látni fogjuk, a logikai védelem differenciált eszközrendszere mellett. A fizikai védelem körében az alábbi feladatok biztosítása, illetve megoldása vár a rendszer üzemeltetőjére:

Fizikai és környezeti védelem egyes elemei	1. Fizikai belépési engedélyek 2. A fizikai belépés ellenőrzése 3. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz 4. A kimeneti eszközök hozzáférésének ellenőrzése 5. A fizikai hozzáférések felügyelete 6. A látogatók ellenőrzése 7. Áramellátó berendezések és kábelezés 8. Vészkikapcsolás 9. Tartalék áramellátás 10. Vészvilágítás 11. Tűzvédelem 12. Hőmérséklet és páratartalom ellenőrzés 13. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem 14. Be- és kiszállítás 15. Tartalék munkahelyszínek

Logikai védelmi intézkedések

A logikai védelmi intézkedések rendkívül kifinomultak és differenciáltak. Ezzel mintegy azt is kifejezik, milyen szerteágazó és sokféle kockázatokkal kell szembenézni egy elektronikus információs rendszer üzemeltetése során. A logikai védelmi intézkedések körében 10 főcsoportot, majd azokon beül további intézkedéscsoportokat különböztethetünk meg. A főcsoportok a következők:

1. konfigurációkezelés,
2. üzletmenet-, ügymenet-folytonosság tervezése,
3. karbantartás,
4. adathordozók védelme,
5. azonosítás és hitelesítés,
6. hozzáférés ellenőrzése,
7. rendszer- és információsértetlenség,
8. naplózás és az elszámoltathatóság,
9. rendszer- és kommunikációvédelem,
10. a biztonsági eseményekre történő reagálás.

A főcsoportokon belül pedig részletes útmutatás szolgál a további intézkedések megtervezésére és dokumentálására. Ezeket tekintjük át az alábbiakban.

Konfigurációkezelés	• Konfigurációkezelési eljárásrend • Alapkonfiguráció • A konfigurációváltozások felügyelete (változáskezelés) • Biztonsági hatásvizsgálat • A változtatásokra vonatkozó hozzáférés korlátozások • Konfigurációs beállítások • Legszűkebb funkcionalitás • Elektronikus információs rendszerelem leltár • Konfigurációkezelési terv • A szoftverhasználat korlátozásai • A felhasználó által telepített szoftverek

Üzletmenet-, ügymenet-folytonosság tervezése	• Üzletmenet-folytonosságra vonatkozó eljárásrend • Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre • A folyamatos működésre felkészítő képzés • Az üzletmenet-folytonossági terv tesztelése • Biztonsági tárolási helyszín • Tartalék feldolgozási helyszín • Infokommunikációs szolgáltatások • Az elektronikus információs rendszer mentései • Az elektronikus információs rendszer helyreállítása és újraindítása
Karbantartás	• Rendszer karbantartási eljárásrend • Rendszeres karbantartás • Karbantartási eszközök • Távoli karbantartás • Karbantartók • Időben történő javítás
Adathordozók védelme	• Adathordozók védelmére vonatkozó eljárásrend • Hozzáférés az adathordozókhoz • Adathordozók címkézése • Adathordozók tárolása • Adathordozók szállítása • Adathordozók törlése • Adathordozók használata
Azonosítás és hitelesítés	• Azonosítási és hitelesítési eljárásrend • Azonosítás és hitelesítés • Eszközök azonosítása és hitelesítése • Azonosító kezelés • A hitelesítésre szolgáló eszközök kezelése • A hitelesítésre szolgáló eszköz visszacsatolása • Azonosítás és hitelesítés (szervezeten kívüli felhasználók)
Hozzáférés ellenőrzése	• Hozzáférés ellenőrzési eljárásrend • Felhasználói fiókok kezelése • Hozzáférés ellenőrzés érvényesítése • Információáramlás ellenőrzés érvényesítése • A felelősségek szétválasztása • Legkisebb jogosultság elve • Sikertelen bejelentkezési kísérletek • A rendszerhasználat jelzése • Egyidejű munkaszakasz kezelés • A munkaszakasz zárolása • A munkaszakasz lezárása • Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek • Távoli hozzáférés • Vezeték nélküli hozzáférés • Mobileszközök hozzáférés ellenőrzése • Külső elektronikus információs rendszerek használata • Információmegosztás • Nyilvánosan elérhető tartalom

Rendszer- és információsértetlenség	• Rendszer- és információsértetlenségre vonatkozó eljárásrend • Hibajavítás • Kártékony kódok elleni védelem • Az elektronikus információs rendszer felügyelete • Biztonsági riasztások és tájékoztatások • A biztonsági funkcionalitás ellenőrzése • Szoftver- és információsértetlenség • Kéretlen üzenetek elleni védelem • Bemeneti információ ellenőrzés • Hibakezelés • A kimeneti információ kezelése és megőrzése • Memóriavédelem
Naplózás és az elszámoltathatóság	• Naplózási eljárásrend • Naplózható események • Naplóbejegyzések tartalma • Napló tárkapacitás • Naplózási hiba kezelése • Naplóvizsgálat és jelentéskészítés • Naplócsökkentés és jelentéskészítés • Időbélyegek • A naplóinformációk védelme • Letagadhatatlanság • A naplóbejegyzések megőrzése • Naplógenerálás
Rendszer- és kommunikációvédelem	• Rendszer- és kommunikációvédelmi eljárásrend • Alkalmazás szétválasztás • Biztonsági funkciók elkülönítése • Információmaradványok • Túlterhelés – szolgáltatásmegtagadás alapú támadás – eleni védelem • A határok védelme • Az adatátvitel bizalmassága • Az adatátvitel sértetlensége • A hálózati kapcsolat megszakítása • Kriptográfiai kulcs előállítása és kezelése • Kriptográfiai védelem • Együttműködésen alapuló számítástechnikai eszközök • Nyilvános kulcsú infrastruktúra tanúsítványok • Mobilkód korlátozása • Elektronikus információs rendszeren keresztüli hangátvitel (úgynevezett VoIP) • Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás) • Biztonságos név/cím feloldó szolgáltatás • Architektúra és tartalékok név/cím feloldási szolgáltatás esetén • Munkaszakasz hitelessége • Hibát követő ismert állapot • A maradvány információ védelme • A folyamatok elkülönítése

A biztonsági eseményekre történő reagálás	• Biztonsági eseménykezelési eljárásrend • Képzés a biztonsági események kezelésére • A biztonsági események kezelésének tesztelése • A biztonsági események kezelése • A biztonsági események figyelése • A biztonsági események jelentése • Segítségnyújtás a biztonsági események kezeléséhez • Biztonsági eseménykezelési terv

5.3 Záró megjegyzések

Az elektronikus információs rendszerek esetében ezek az absztrakt intézkedések és szabályok egyedi eltérésekkel alkalmazhatók. Ezeket az egyedi védelmi intézkedéseket a helyi viszonyok, értékek, a kezelt adatok köre és értéke alapján, az arányosság követelményét és elveit szem előtt tartva kell megkonstruálni.

Esetenként akár helyettesítő biztonsági intézkedéseknek minősülő eljárások és feltételek rögzítése is szükségessé válhat annak érdekében, hogy az Ibtv.-ben kialakított biztonsági rezsimet alkalmazni lehessen. Ezek a helyben, a fennálló viszonyokhoz igazított rendszabályok érinthetik:

- a működtetést, a környezetet,
- a fizikai infrastruktúrát,
- a nyilvános hozzáférést,
- a technológiát,
- a biztonsági politikát és a szabályozást,
- a biztonsági intézkedések fokozatosságát,
- a biztonsági célokat.

Az elektronikus információs rendszerek biztonságának, a tartós, folyamatos integritás megőrzésének és a reagálóképesség fejlesztésének legfontosabb kulcstényezője a tapasztalatok hasznosítása, a rendszer folyamatos fejlesztése, naprakészen tartása, a tanulságok levonása, a tapasztalatok kiértékelése. Ennek mellőzhetetlen előfeltétele a rendszeresség, a fegyelem, a hozzáértés és a pontos, naprakész, a valóságot helyesen tükröző dokumentáció.

6 IRODALOMJEGYZÉK

6.1 Szakirodalom

- Alexin Zoltán (2014): Does fair anonymization exist? *International Review of Law, Computers and Technology* 28., 21.
- Balogh Zsolt György (1998): *Jogi informatika.* Dialóg Campus, Pécs.
- Clough, B.–Mungo, P. (1992): *Approaching Zero. Data Crime and the Computer Underworld.* Faber and Faber, London.
- Drótos László (1999): *Hálózati értelmező szótár.* N.I.I.F., Budapest.
- Erdősi Péter Máté – Solymos Ákos (2017): IT biztonság közérthetően. NJSZT. http://njszt.hu/de/it-biztonsag-kozerthetoen [A letöltés ideje: 2018. január 11.]
- Jóri András (2005): *Adatvédelmi kézikönyv.* Osiris, Budapest.
- NHIT (Nemzeti Hírközlési és Informatikai Tanács) (2008): Égen-földön informatika. Az információs társadalom technológiai távlatai. Typotex, Budapest.
- Szádeczky Tamás–Szőke Gergely László–Zámbó Alexandra Erzsébet (2017): Titkosítás és jog – Gondolatok a titkosításhoz kapcsolódó jogi szabályozásról. *Infokommunikáció és Jog,* 68, 3.
- Tóth András (2017): Hálózati és információs rendszerek biztonsága európai szabályozásának alapjai. *Infokommunikáció és Jog*, 68,16.
- PricewaterhouseCoopers (2018): Revitalizing privacy and trust in a data-driven world. Key findings from The Global State of Information Security® Survey 2018 https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf [A letöltés ideje: 2018. május 16.]
- Wasik, M. (1991*): Crime and the Computer.* Clarendon Press, Oxford.
- World Economic Forum (2018): *The Global Risk Report 2018.* 13th edition. http://www3.weforum.org/docs/WEF_GRR18Report.pdf [A letöltés ideje: 2018. március 8.]

6.2 Sajtóanyagok

- Feledy Botond (2016): Javában zajlik a kiberháború Oroszországgal. https://index.hu/velemeny/2016/07/05/javaban_zajlik_a_kiberhaboru_oroszorszaggal/ [A letöltés ideje: 2018. április 21.]
- Heti Világgazdaság (2018): Egy hétbe telhet összekalapálni az NVI informatikai rendszerét. http://hvg.hu/itthon/20180410_nvi_informatikai_rendszer [A letöltés ideje: 2018. április 10.]
- Joshua Davis (2017): Hackers take down the most wired country in Europe. *Wired*. https://www.wired.com/2007/08/ff-estonia/ [A letöltés ideje: 2018. április 21.]
- Kim Zetter (2016): Inside the cunning, unprecedented hack of ukraine's power grid https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [A letöltés ideje: 2017. március 7.]

- Laza Bálint (2014): Az elmúlt 25 év legdurvább bugja. http://index.hu/tech/2014/09/30/az_elmult_25_ev_legdurvabb_bugja/ [A letöltés ideje: 2014.09.30.]
- Index (2010): Így kell ATM-et feltörni. http://index.hu/tech/biztonsag/2010/07/29/igy_kell_atm-et_feltorni/ [A letöltés ideje: 2010. július 29.]
- Index (2013): Innen harcol a Microsoft a hekkerek ellen http://index.hu/tech/2013/11/16/innen_harcol_a_microsoft_a_hekkerek_ellen/ [A letöltés ideje: 2013. november 16.]

6.3 EU-joganyagok

- Bangemann-jelentés. Európa és a globális információs társadalom. Az Európai Unió Tanácsának készült Bangemann-jelentés. A korfu-i európai csúcsértekezlet határozata. 1994. http://www.mek.iif.hu/porta/szint/muszaki/szamtech/wan/hatasok/bangemn.hun [A letöltés ideje: 2002. november 5.]
- **Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér /* JOIN/2013/01 final */**
- 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (ECI irányelv)
- 526/2013/EU rendelet az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről
- **910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről** (eIDAS-rendelet)
- COM(2015) 192 A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Európai digitális egységes piaci stratégia
- 2016/679 rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelvhatályon kívül helyezéséről (általános adatvédelmi rendelet)
- 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS irányelv)

6.4 Magyar jogszabályok

- 2003. évi C. tv. az elektronikus hírközlésről
- 2009. évi CLV. tv. a minősített adat védelméről
- 2010. évi CLVII. tv. a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Kritikus infrastruktúra tv.)
    - Melléklet tartalmazza a létfontosságú rendszerek felsorolását
    - Indoklás
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 2016. évi XXX. törvény a védelmi és biztonsági célú beszerzésekről
- 2016. évi CLXXXIX törvény a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok kölcsönös védelméről szóló egyezmény kihirdetéséről
- 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról (*Hatályon kívül!*)
- 85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól
- Kormányzati stratégiai irányításról szóló 38/2012.(III.12.) Korm. rendelet: kidolgozási szempontrendszer
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012.(II.21.) Korm. határozat 1. melléklet 31. pont
- 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
- 1139/2013. (II.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 12/2012. (III. 22.) BM utasítás a Belügyminisztérium Informatikai Stratégiájáról
- Magyary Program: Közigazgatási stratégiaalkotás

A Nemzeti Közszolgálati Egyetem kiadványa

Kiadó:
Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert dékán
Címe: 1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Zsoldos Sándor

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-106-0 (elektronikus)