Incidensmenedzsment

Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára

BERZSENYI DÁNIEL – BODÓ ATTILA PÁL –
KAPITÁNY SÁNDOR – SÁGI GÁBOR –
SEBŐK VIKTÓRIA

Nemzeti Közszolgálati Egyetem, Budapest

A Nemzeti Közszolgálati Egyetem kiadványa

Szerzők:
Berzsenyi Dániel
Dr. Bodó Attila Pál
Kapitány Sándor
Sági Gábor
Sebők Viktória

Szakmai lektor:
Prof. Dr. Nemeslaki András

A hatályosítást 2022-ben végezte:
Mikula Fanni

A hatályosításért felelős szakmai szakértő:
Legárd Ildikó

A hatályosított kézirat lezásrásának dátuma:
2022. február 25.

Eredeti megjelenés éve:
2016

Kiadja:

Közigazgatási Továbbképzési Intézet

Felelős kiadó:
Prof. Dr. Kis Norbert
rektorhelyettes

TARTALOM

I. BERZSENYI DÁNIEL: A KIBERTÉR AKTUÁLIS NEMZETKÖZI BIZTONSÁGPOLITIKAI KIHÍVÁSAI

1. A kibertér fokozódó kihívásai

Napjainkban egyre szélesebb körben ismert és elfogadott tény, hogy korunk biztonságpolitikai kihívásai között kiemelkedő szerepet töltenek be a kibertérből érkező fenyegetések és veszélyek. Ennek legfőbb oka, hogy számuk folyamatos növekedésén túl, a mindennapi életünk egyre több területén fejtenek ki egyre jelentősebb hatást, vagyis a fenyegetési spektrum is dinamikusan növekszik. Miközben az információs társadalomban természetesnek vesszük, hogy a kibertérből elérhető adatok és információk folyamatos növekedést mutatnak, sokak számára kevésbé nyilvánvaló, hogy ezeknek a megfelelő szintű védelméről is gondoskodnunk kell. Tovább súlyosbítja a helyzetet, hogy az infokommunikációs technológia fejlődése következtében egyre több társadalmi folyamat zajlik a kibertérben, vagy annak felhasználásával, és a folyamatosan gyarapodó információkhoz egyre többféle módon és egyre többféle eszközzel férhetünk hozzá.

Korábban egy átlagos felhasználó számára a legnagyobb problémaként az jelentkezett, ha óvatlansága miatt számítógépe vírussal fertőződött meg, és ennek következtében kéretlen reklám üzeneteket kapott, vagy átmenetileg blokkolásra került a hálózati hozzáférése. Idővel azonban kialakult egy olyan alapvető biztonságtudatosság, aminek köszönhetően ma már a legtöbb számítógépes felhasználó számára egyértelmű, hogy a megfelelő célszoftverekkel (víruskereső, tűzfal) jelentős mértékben csökkenteni tudja a kockázatot. Azonban az elmúlt néhány évben gyökeresen átalakult a kiberbiztonság helyzete nemcsak az egyéni, de nemzeti, regionális és globális szinten egyaránt. A jelenleg is tartó átalakulás rendkívül gyorsan és komplex módon zajlik. A kibertérben elérhető szolgáltatások dinamikus bővülése, az okoseszközök rohamos elterjedése, a gyártók felelőtlensége, a rosszindulatú felhasználók és az általuk alkalmazott módszerek egyre növekvő száma, valamint a technológiai és tudástranszfer következtében mára egy átlagos felhasználó kitettsége sokszorosára nőtt a kibertérből érkező támadásokkal szemben. Napjainkban az imént említett célszoftverek, vagyis egy számítógépre telepített víruskereső és tűzfal kombináció az alapvető biztonság szavatolásához is kevés lehet, ha emellett nem gondoskodunk adataink, kommunikációs csatornáink és okoseszközeink védelméről, nem használunk megfelelő hosszúságú és bonyolultságú jelszavakat, többlépcsős azonosítási módszereket, és nem ismerjük fel időben az emberi hiszékenységen, illetve megtévesztésen alapuló támadásokat *(social engineering)*.

Az átlagos felhasználó jellemzően nincs tisztában azzal, hogy a kibertámadásokkal szembeni kitettsége mekkora mértéket ölt, és nem is lehet reális elvárás, hogy mindenki önmaga kiberbiztonsági szakembere legyen. Ugyanakkor a kiberbiztonsági tudatosság fejlesztésére és terjesztésére egyre jelentősebb igény mutatkozik, hiszen a kibertér sajátosságaiból fakadóan az egyén tájékozatlansága és felelőtlen felhasználói magatartása könnyedén megbéníthat egy egész szervezetet, de akár veszélyt jelenthet a nemzetbiztonságra is. A kibertérben nincsenek államhatárok, ahol ellenőrzést lehetne folytatni, az ott zajló események gyakran a másodperc tört része alatt következnek be, miközben hatásuk évekig eltarthat, a folyamatok attribútumainak bizonyító erejű meghatározása pedig a legtöbb esetben rendkívül bonyolult, sokszor lehetetlen. Szintén eltér a hagyományos (offline) világunk szabályszerűségeitől, hogy a kibertérben a nemzetállamok korántsem egyeduralkodók, a társadalom megannyi szereplője megtalálható, a multinacionális cégektől, a szervezett bűnözői és aktivista csoportokon át

egészen az egyéni felhasználóig. A kibertér említett jellemzői jól mutatják, milyen sokszínű és bizonyos tekintetben mennyire eltérő a virtuális világ a hagyományoshoz képest.

A kibertér sajátosságait figyelembe véve a nemzetállamok a világon mindenütt próbálnak a hagyományos területekkel foglalkozó nemzetközi együttműködésekhez hasonló szövetségeket létrehozni a kibertér biztonságának szavatolása érdekében. Ezek az együttműködési kezdeményezések elsősorban az elmúlt évek kiberbiztonsági trendjeinek köszönhetők, amelyek rádöbbentették a kormányokat arra, hogy önállóan nem képesek megvalósítani a kibertér biztonságos használatának alapvető feltételeit. A kibertérhez kapcsolódó nemzetközi együttműködések legtöbbször a szabályozatlanság problémájára próbálnak megoldást találni, de egyre több a kiberbűnözés elleni, határokon átnyúló összefogás, illetve a szellemi tulajdon védelmében és a kibertérben folytatott kémkedés ellen létrehozott multinacionális kooperáció. Magyarország több nemzetközi kiberbiztonsági kezdeményezésben is érintett, egyrészt az euroatlanti szövetségi rendszerhez kapcsolódó beágyazottsága, másfelől az önálló, illetve harmadik fél általi regionális kezdeményezések révén. Utóbbiak közül kiemelkedő a 2013 májusában Ausztria és Csehország kezdeményezésére létrehozott Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform – CECSP), melynek hazánk mellett Lengyelország és Szlovákia is tagja.

Annak érdekében, hogy egy szervezet különböző szintjein megjelenő kiberbiztonsági probléma kapcsán ne csak az aktuális kihívást lássuk, és adott esetben az akut elhárításon, illetve „tűzoltáson" túl hosszabb távú megoldást lehessen kidolgozni, érdemes egy pillanatfelvételt készítenünk azokról a nemzetközi kiberbiztonsági trendekről, amelyekre az előző bekezdésben már utaltunk. A biztonságpolitikai megközelítés egyik alapja, hogy egy incidens vagy konfliktus kialakulása számos tényezőre vezethető vissza. Ezeknek a tényezőknek a feltérképezésében és azonosításában jelentős szerepük van a körülöttünk zajló lokális, regionális és globális folyamatoknak, melyeknek értékelése és figyelemmel követése elengedhetetlen ahhoz, hogy a szükséges helyen és időben megfelelően felkészültek lehessünk. Az offline világunk hagyományos incidenseihez vezető út elemzése, az események monitorozása, illetve újabbak előrejelzése olyan tevékenységek, amelyek teljes mértékben alkalmazhatók a kibertérre vonatkozóan is, így a kiberbiztonsági problémák kezelhetőbbé válnak.

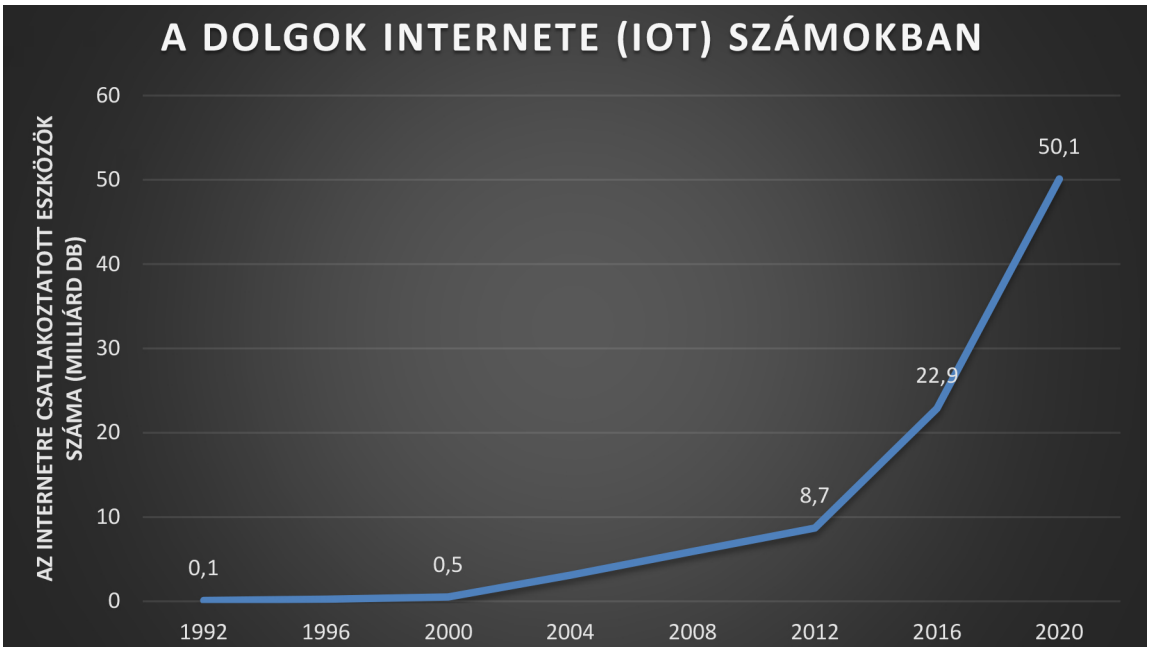
2. Biztonsági trendek a kibertérben

Amikor kiberbiztonsági kérdésekkel foglalkozunk, előbb vagy utóbb fontos szerepük lesz a kibertérben zajló folyamatoknak és trendeknek, illetve az ezeket számszerűsítő kimutatásoknak és statisztikai adatsoroknak. Például egy kiberbiztonsági incidens kapcsán az egyik elsőként felmerülő kérdés, hogy mennyi felhasználót vagy rendszert érint az adott eset. Annak érdekében, hogy tisztában legyünk az ember alkotta virtuális világ méretével, népességével és arányaival, ajánlott az aktuális trendeket áttekinteni. Számos forrás és adatsor található arra vonatkozóan, hány ember él a világon, és használja manapság az internetet, ugyanakkor az egyes földrajzi és gazdasági régiók között jelentős eltérések mutatkoznak több tekintetben is. Az egyik megbízható forrásnak számító Nemzetközi Távközlési Egyesület (International Telecommunication Union, továbbiakban: ITU) 2016 júniusában kiadott adatai szerint a világ lakosságának több mint fele továbbra sem fér hozzá az internethez. Ugyan az ITU szerint 2016 végére 3,9 milliárd főre csökkent azoknak a száma, akik nem használják a világhálót, regionális bontásban, például Afrikában, a lakosság 75 százaléka nem fér hozzá, miközben Európában ugyanez az arány csupán 21 százalék. Az adatok sajátos bemutatása az ENSZ Fenntartható Fejlődési Célkitűzéseihez köthető, ha azonban megfordítjuk a megközelítést, azonnal látható, hogy 47 százalékos lefedettség mellett, globális szinten majdnem minden második ember rendelkezik internet-hozzáféréssel. Európában a háztartások 84 százaléka csatlakozik az internethez, miközben a szélessávú mobil-előfizetések aránya meghaladja a 76 százalékot (ITU 2016). A 738 millió fős európai lakosságra (UN ESA 2015) vetítve ez több mint fél milliárd felhasználó. Tovább szűkítve a

vizsgálati kört, Magyarországon a rendszeres internethasználók aránya eléri a 72 százalékot (KSH 2016), ami több mint 7 millió felhasználó hazánkban.

Más megközelítésben érdemes elgondolkodni azon, mi történik az interneten, ha egyetlen szűk perc keresztmetszetét próbáljuk megvizsgálni. Egy 2016 nyarán megjelent felmérés szerint gigantikus méreteket ölt a különböző online tartalmak generálása. A kutatási eredményeket publikáló jelentés „tartalomsokknak" nevezi a jelenséget, aminek következtében a 2013-ban egy perc leforgása alatt elküldött e-mailek száma 182,9 millióról 2015-re 205,6 millióra nőtt. De hasonló adatokat mutat a legnépszerűbb internetes keresőmotor (Google) használata is. A 2013-as egy perc alatt indított 2,6 millió keresés 2015-re elérte a 3,1 milliót, míg a világelső közösségi oldalon (Facebook) közzétett posztok száma 2,5 millióról 3,3 millióra nőtt. Ennél is jelentősebb a változás a legnépszerűbb közösségi videomegosztó (YouTube) oldal esetében, ahol 2013-ban egy perc alatt még csak 100 órányi videótartalmat töltöttek fel a felhasználók, 2015-ben viszont már 400 órányit. Szignifikáns a különbség az egyik népszerű azonnali üzenetküldő (WhatsApp) alkalmazás esetében is, amelynek segítségével a felhasználók 2013-ban még 11,8 millió üzenetet küldtek egy perc leforgása alatt, 2015-ben viszont már 44,4 milliót.Az említett adatok azt mutatják, hogy jelentős és folyamatos növekedés mutatkozik mind a felhasználók számában, mind pedig a felhasználás mértékében. A kiberbiztonság jelentőségének megértéséhez további folyamatokat is feltétlenül figyelembe kell venni, melyek közül kettőt fontos kiemelni.

Mindennapi életünk során egyre több szálon kapcsolódunk a virtuális világhoz. Míg korábban elsősorban az asztali vagy hordozható számítógépünk segítségével kommunikáltunk az interneten keresztül, később pedig pénzügyi tranzakciók lebonyolítására vagy multimédiás tartalmak fogyasztására használtuk, ma már egyre több eszközünk kapcsolódik a kibertérhez, amelyek a legkülönbözőbb funkciókon keresztül képesek digitalizálni mindennapjainkat. Gondoljunk a manapság oly divatos okoseszközökre (telefonok, televíziók, karórák stb.), melyek mindegyike egy-egy újabb szálon kapcsol bennünket a világhálóhoz. Az okoseszközök által dominált virtuális világ angol elnevezése az *Internet of Things* (IoT), vagyis a dolgok internete, ami jóval túlmutat a ma elterjedt okoseszközök képességein és lehetőségein. A dolgok internete tulajdonképpen nem más, mint hálózatba kapcsolt eszközök, járművek, épületek és egyéb ember alkotta tárgyak, amelyek a beépített elektronikának, szoftvereknek és szenzoroknak köszönhetően képesek egymással kommunikálni a hálózati kapcsolataikon keresztül. Távoli eléréssel a hálózaton keresztül érzékelhetők és irányíthatók ezek az eszközök, aminek köszönhetően egyre inkább elmosódik a határ a fizikai és a virtuális világ között. Az ITU 2012-ben kiadott ajánlása értelmében az IoT nem más, mint az információs társadalom infrastruktúrája. (ITU 2012) Az előrejelzések alapján az IoT térnyerése következtében robbanásszerűen megnövekszik az internethez csatlakoztatott dolgok (eszközök) száma az elkövetkező néhány évben. Már most is közel 23 milliárd eszköz csatlakozik az internethez globális szinten, de ez a szám 2020-ra elérheti, sőt nagy valószínűséggel meg is haladja majd az 50 milliárdot. Ez azt jelenti a világ 7,4 milliárd lakójára nézve, hogy minden ember már ma is három különböző eszköz révén érhető el online.



1. ábra: Az internetre csatlakozó eszközök számának változása
Forrás: A szerző saját szerkesztése a CompTIA Projecting the 'Things' Behind the Internet of Things grafikonja alapján.[1]

A IoT térhódítása több szempontból is megállíthatatlannak tűnik. Az internetre csatlakoztatott eszközök száma már 2008-ban meghaladta a Föld népességének számát (Evans 2011), 2017-ben pedig az IoT-eszközök piaca nagyobb lesz, mint az asztali számítógépek, tabletek és telefonok piaca együtt. (Business Insider 2014) Ez számokban kifejezve azt jelenti, hogy a 2013-as 1,9 billió dolláros szintről 2020-ra az IoT-piac 7,1 billió dollárra nő. (Economist 2015) Hamarosan olyan hétköznapi használati tárgyaink és eszközeink is kapcsolatban lesznek a kibertérrel, mint az autónk, a háztartási eszközeink (hűtő, mosógép, sütő, kávéfőző stb.), vagy akár az otthonunk teljes gépészeti, elektromos és egyéb rendszerei. A trendekből kirajzolódó folyamatnak azonban van egy árnyoldala is, amivel ma még a kiberbiztonsági szakembereken kívül meglehetősen kevesen foglalkoznak. A legtöbb felhasználóban nem tudatosul, hogy az internetre kapcsolódó eszközök számának emelkedésével együtt növekszik az a támadási felület is, amin keresztül a rosszindulatú felhasználók károkat okozhatnak. Jó példa erre a világ egyik legjelentősebb kiberbiztonsági konferenciája a DefCon, ahol 2016-ban 21 gyártó 23 eszközében összesen 47 sérülékenységet mutattak be a résztvevők. (Mészáros 2016) Ugyanakkor a már jelenleg is kiterjedt támadási felület nagyságát jól szemlélteti egy 2015-ben megjelent tanulmány, amely azt vizsgálta, milyen szintű Magyarország kiberbiztonsági kitettsége az internethez csatlakozó ipari folyamatirányító rendszerek tekintetében, amelyek jellemzően erőművek vezérléséért, a közüzemi szolgáltatások működésért vagy éppen különféle gyártósorok üzemeltetéséért felelősek. Az erről szóló tanulmányban bemutatott 4 és fél óra alatt elvégzett mérés eredményei szerint 6100 olyan támadási pont volt található a kibertérben, amin keresztül a hazai szolgáltatások és infrastruktúrák működése megzavarható vagy leállítható lett volna, és milliós nagyságrendűre becsülhető azoknak a sérülékenységeknek a száma, amelyek kritikus infrastruktúrákat irányító rendszerekben találhatók. (Berzsenyi–Ványi 2015).

[1] Az eredeti grafikon elérhető: http://blogs-images.forbes.com/gilpress/files/2016/08/Slide2.jpg?width=960 (utolsó letöltés: 2016. november 4.)

A bemutatott példák és adatok a kiberbiztonsági trendeket csak nagy vonalakban ábrázolják, azonban a bevezetőben leírt dinamikus növekedést, a kibertér hódítását és a kihívások mindezzel párhuzamos fokozódását jól szemléltetik. Az egyre nagyobb kitettség következtében új szegmensek jönnek létre a különböző iparágakon belül; ilyen az egyelőre főként nagyvállalati környezetben terjedő kiberbiztosítás. Az egyik legújabb biztosítási piac lényege, hogy a vállalatok az egyre jobban elterjedő digitalizált folyamatok következtében a kibertérből érkező veszélyekkel és veszteségekkel szemben is szeretnének fedezetet. A kibertámadások személyre, iparágra, nemzetre való tekintet nélkül mindenkit fenyegetnek. Az összes kapcsolódó kihívás áttekintése jelen esetben a teljes tankönyv határain is nagyságrendekkel túlmutatna, így a rendelkezésre álló kereteken belül a legfontosabb és leginkább aktuális nemzetközi biztonságpolitikai vonatkozású kiberbiztonsági kihívások bemutatására kerül sor.

3. Lokális folyamatokat érintő kiberbiztonsági kihívások

Már az alfejezetcím olvasása közben felmerülhet a kérdés, hogyan eshet szó lokális folyamatokról egy alapvetően nemzetközi biztonságpolitikai kihívásokat tárgyaló fejezetben. A kérdés jogos, a válasz pedig egyszerű: a választások külföldi befolyásolásának tárgyalása révén. A fejlett nemzetek számára – választási rendszerüktől függetlenül – a demokratikus választás és annak külső behatás nélkül történő lebonyolítása az államiság egyik alapja. Az államok belügyeibe történő külső beavatkozás nem csak a demokratikus elvek mentén működő államok problémája. A 21. század első felének egyik legnagyobb kihívása minden ország számára, hogy a belső politikai folyamatait megóvja a külső befolyásolástól, ami nem új keletű a nemzetállamok között, régóta működik szabályozott és szabályozatlan keretek között egyaránt. Az újdonság a kibertér szerepének jelentős megnövekedésében rejlik. Az említett befolyásolásnak egy új dimenziója nyílik meg napjainkban, az Amerikai Egyesült Államokban lezajlott 2016-os választásokat követően, illetve a 2017-es francia választások közben. Nagy valószínűséggel az elkövetkező évek során nem lesz olyan választás, amit ne érintene valamilyen szinten egy kibertérből érkező kihívás. Legyen szó a választási adatok megváltoztatásáról, a választási kampányba történő beavatkozásról vagy a szemben álló felek politikai ellehetetlenítéséről, a legtöbb állam egyelőre csak keresi azokat a megoldásokat, amelyek a segítségével a kibertérből érkező kihívásokat minimalizálni lehetne a választásokkal összefüggésben.

Az Amerikai Egyesült Államokban lezajlott legutóbbi választások során a kibertérnek, illetve a kibertérből érkező fenyegetéseknek igen nagy jelentőséget tulajdonítottak az egész világon. Mivel az USA továbbra is a világ első számú katonai hatalma, szerte a világon nagy figyelemmel kísérték a választási kampányt és az azt megelőző eseményeket. Bár a mai napig több „kibertámadásként" emlegetett esemény bizonyítatlan, illetve a részletek ismeretlenek, a befolyásolásra utaló jelek mértéke akkora, hogy nem lehet őket figyelmen kívül hagyni. 2016. június közepén kerültek nyilvánosságra az első olyan információk, amelyek arra utaltak, hogy a választásokat is érintő kiberbiztonsági incidens történt a Demokrata Nemzeti Bizottságnál (Democratic National Committee, továbbiakban: DNC). Rövid időn belül a feltételezett tetteseket is bejelentették: ezek szerint az elkövetők az orosz kormányhoz köthető „Fancy Bear" illetve „Cozy Bear" néven ismert hackercsoportok. Néhány nappal később a Wikileaks portál mintegy 20 ezer DNC-hez köthető szerverről származó e-mailt hozott nyilvánosságra, amelyre válaszként az Amerikai Egyesült Államok Szövetségi Nyomozó Irodája (Federal Bureau of Investigation, továbbiakban: FBI) nyomozást indított. Néhány héttel később, 2016. augusztus közepén a DNC vezetőinek adatai kiszivárogtak, majd a nyár hátralevő része kölcsönös nyilatkozatháborúba fulladt az orosz fél, illetve a két amerikai elnökjelölt és stábjaik között. Már javában zajlott az amerikai elnökválasztási kampány, amikor újabb 58 ezer üzenet került nyilvánosságra a Wikileaks jóvoltából, egyenesen a demokrata jelölt kampányfőnökétől. 2016 őszére az amerikai hatóságok egybehangzóan Oroszországot nevezték meg a választások körül kialakult helyzet okozójaként, azonban a motiváció tekintetében bizonytalanság mutatkozik. Az elindított vizsgálatoknak

köszönhetően kiderült, hogy a DNC sorozatos hibákat követett el, és nem az elvárható módon reagált a kiberbiztonsági incidensekre; mindez értelemszerűen hozzájárulhatott a támadások sikeréhez. A választások körül kialakult botrány következtében végül az USA szankciókat vezet be Oroszországgal szemben, és 35 orosz diplomatát 72 órás határidővel kiutasítottak az országból. A titkosszolgálatok vizsgálati eredményei azt mutatják, hogy a választásokat közvetlenül nem befolyásolták, a szavazógépek és a szavazások lebonyolításához használt számítógépek nem kompromittálódtak.

A 2017-es franciaországi választások során is történt olyan, amely a választások kibertámadásokkal szembeni kitettségére hívja fel a figyelmet. 2017. április 25-én a Trend Micro nevű cég elemzői bejelentették, hogy bizonyítékokkal rendelkeznek arra vonatkozóan, hogy a francia elnökválasztási kampány egyik jelöltjét és stábját támadja a Fancy Bear (APT28) néven ismert hackercsoport. A támadás kapcsán kiadott jelentés szerint célzott adathalász e-maileket kaptak a kampánystáb tagjai, amelyek a politikai mozgalom honlapja helyett fertőző oldalakra irányították a felhasználókat. A támadók figyeltek arra is, hogy a használt weboldalaknak az eredeti oldalak címeihez hasonló neveket adjanak. Ezt követően május 6-án több ezer e-mail vált nyilvánosan elérhetővé az *En Marche!* mozgalom belső levelezőrendszeréből. A mozgalom közleménye szerint a kampánystáb egy kiterjedt és összehangolt hackertámadás áldozatává vált, aminek következtében számos belső információ került át a közösségi médiába. Az áldozatok külön kiemelték, hogy az eredeti dokumentumok fiktív elemekkel kibővítve terjednek a világhálón, így téve azokat még alkalmasabbá a megtévesztésre és a súlyos dezinformáció terjesztésére.

A választások befolyásolására irányuló kísérletek minden jel szerint a következő évek velejárói lesznek, ezért fontos lenne, hogy a problémával nemzetközi szinten foglalkozzanak az érintett felek. 2017-ben tartanak még egy Európai Uniós viszonylatban jelentősnek számító választást, Németországban, 2018-ban pedig Magyarországon is. Németország jelentős erőkkel készül a választások kibertámadásokkal szembeni védelmére; a német Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz, továbbiakban: BfV) vezetője nyíltan beszélt egy konferencián a befolyásolásról és az egyre agresszívabbá váló kiberkémkedési tevékenységről. A német hatóságok ellehetetlenítik, szükség esetén működésképtelenné teszik azokat a szervereket, amelyeknek az üzemeltetői, illetve tulajdonosai nem képesek garantálni, hogy azokat ne használják fel kibertámadásokhoz. (Rettmann 2017) Amennyiben a német választásokat valóban kibertámadás éri valamilyen formában, és a német hatóságok a bejelentésnek megfelelően járnak el, ez lehet az első olyan nyilvános eset, ahol egy állam proaktívan lép fel, és visszatámad (hackback) a kibertérben.

4. Regionális folyamatokat érintő kiberbiztonsági kihívások

Egyre jellemzőbb, hogy a konfliktusok által sújtott régiókban az egymással szemben álló felek a kibertérben is aktív tevékenységet folytatnak. A biztonságpolitikai elemzők az elsők között szokták említeni példaként a 2008-ban Oroszország és Grúzia között lezajlott fegyveres összecsapást, amelynek nemcsak előkészítése során, de a katonai műveletek ideje alatt és azt követően is jelentős szerep jutott a kibertérben folytatott műveleteknek. A fegyveres harcokhoz képest hetekkel korábban megindultak az elosztott szolgáltatásmegtagadással (Distributed Denial of Service, továbbiakban DDoS) járó támadások: számos honlap és szerver vált hosszabb-rövidebb időre elérhetetlenné, erősen akadozott a kommunikáció az érintett területeken. A támadók gyakorlatilag információs blokád alá vették Grúziát. 2008-ban a grúz kormány az oroszokat vádolta meg a támadások elkövetésével, azonban az orosz kormány szóvivője mindezt azzal hárította, hogy lehetnek olyan hazafias magánszemélyek Oroszországban, akik így nyilvánítják ki véleményüket. A Torontói Egyetem egyik szakértője az eseményeket követően azt nyilatkozta, hogy „méretét és a nemzetközi dimenziókat figyelembe véve mérföldkő a támadás". (Hart 2008) Korábbról valóban nem tudunk olyan példát felhozni, amikor egy reguláris erőkkel vívott küzdelmet az előkészítéstől a lezárást követő időszakig ilyen volumenű kibertevékenység kísért volna. Egy valami beigazolódott a 2008-as eseményeket követően is: a kibertámadások

olcsón és egyszerűen kivitelezhetők, néhány száz számítógép és pár képzett hacker elegendő ahhoz, hogy egy országot blokád alá vonjanak a kibertérben. Szintén jól kirajzolódott, hogy nem pusztán a kommunikáció megbénítása volt a támadók célja, hanem annak kontrollja is, vagyis ebben az esetben az orosz támadásokat előkészítő és segítő propaganda terjesztése. Bár jó esély van arra, hogy soha nem derül ki teljes bizonyossággal a támadók kiléte, a konfliktusok legalapvetőbb szabálya, hogy mind a támadó, mind a védekező fél egyértelműen azonosítsa a másik felet. A fegyveres konfliktusokat szabályozó hadijog mindezt részletesen kifejti. Azonban olyan időket élünk, amikor a felek azonosítása nemcsak a fizikai világban válik egyre nehézkesebbé, a gerilla hadviselés, illetve a terrorista módszerek elterjedése miatt, de – a kibertér sajátosságaiból fakadóan – azt is szinte lehetetlen meghatározni, hogy egy-egy kibertámadás mögött ki áll (egy másik nemzet, egy politikai csoportosulás vagy esetleg bűnszervezet). 2008 óta ez a terület szinte még érintetlen, nem igazán sikerült sem technikai, sem szabályozói oldalról olyan megoldásokat kidolgozni, amelyek a kibertámadások elkövetőinek felelősségre vonását és a bizonyítást elősegítené.

De nem feltétlenül kell egy konfliktusnak fegyveres összecsapássá eszkalálódnia ahhoz, hogy valamelyik fél kibertámadáshoz folyamodjon. Kiváló példa erre a 2007 tavaszán történt észtországi kiberkonfliktus, amelynek kirobbantásával szintén Oroszországot vádolták meg. A kibertérben végrehajtott műveleteket 2007. április 27-én az észt fővárosban, Tallinnban kitört zavargások előzték meg, melyek egy szovjet hősi emlékmű elköltöztetése miatt alakultak ki. Ebben az esetben is DDoS támadások játszották a főszerepet, melyek néhány nappal a tüntetéseket követően kezdődtek, és alapvetően észt kormányzati hivatalokat, minisztériumokat és a parlamentet vették célba. Ugyanakkor számos pénzügyi intézmény, telekommunikációs vállalat és médiacég szerverei is megbénultak. A kiválasztott célpontok, a támadások előkészítettsége és precíz végrehajtása, valamint mértékük egyaránt arra utalt, hogy átlagos hackereknél komolyabb erők állnak a háttérben, vagyis egy nemzetállam által támogatott támadásról volt szó, ami a tallinni események nyomán leginkább az oroszoknak állhatott érdekében. Bár a világsajtó az észt társadalomra nézve katasztrofálisnak mutatta az események következményeit, egy kis utánajárással hamar kiderül, hogy az átlagemberek életében korántsem okozott akkora fennakadást a támadássorozat, mint azt kívülállóként gondolnánk. Közel két hét alatt 128 túlterheléses támadást regisztráltak, melyek között volt, amelyik csak néhány óráig tartott, de volt, amelyik napokig, továbbá számtalan oldalt feltörtek, és módosítottak valamilyen oroszbarát tartalommal. Mivel Észtország ekkor már 4 éve a NATO tagja volt, viszonylag gyorsan felmerült a kérdés, hogy katonai akciónak minősíthető-e a kibertérben végrehajtott támadás, és ilyen esetben is érvénybe léptethető-e a NATO 5. cikkely szerinti segítségnyújtás a többi tagállam részéről. Akkoriban nem mutatkozott egyetértés ebben a kérdésben, így a NATO szakértői nem minősítették katonai támadásnak az esetet.

A 2015-ös ukrán konfliktus kapcsán azonban nem kérdés, hogy katonai műveletekről van szó. Az orosz fél érintettsége itt is jelentős, azonban Oroszország hivatalosan nem ismeri el, hogy katonai hírszerzőkön kívül komolyabb erőt alkalmazott volna egy másik állam területén. Bár 2015 végén az ukrán energetikai rendszer ellen elkövetett kibertámadások széles körben ismertté váltak, az Ukrajnában zajló fegyveres konfliktusról kevésbé köztudott, hogy a grúz esethez hasonlóan aktív kiberműveletek zajlottak a háttérben. Ezek a támadások – melyekért ismét Oroszország tehető felelőssé – a 2014-es ukrán választásokig nyúlnak vissza, s elsősorban a választási bizottságot célozták annak érdekében, hogy az eredményeket befolyásolni lehessen. Az akkori hírek szerint a támadás olyan sikeres volt, hogy még a biztonsági mentéseket is sikerült tönkre tenni. A szavazást segítő rendszerek végül működtek, de a választási bizottság honlapján a támadóknak sikerült meghamisított eredményt elhelyezniük, amelyet azután a média is átvett. Mindez persze a választás eredményét végül nem befolyásolta, azonban a kormányzat és a közigazgatási szervek integritását, valamint a beléjük vetett bizalmat jelentősen rombolta. A választások kapcsán történt esetet követően az ukrán bankrendszert, a vasúthálózatot és több bányaipari céget is támadás ért. Az ukrán vezetés mindvégig Oroszországot tette felelőssé a kibertámadásokért, mely állam pedig szokás szerint tagadta a vádakat. Felmerült az is, hogy Oroszország a katonai műveletek során olyan hatékonyan alkalmazta

kibertámadási képességeit, hogy az ukrán hadsereg tüzérségének jelentős veszteségei is ennek köszönhetők. A bizonyítás itt is elmarad, ráadásul a felvetés igazságtartamát illetően a szakértők között sincs egyetértés. Egyes elemzők szerint az Ukrajna ellen bevetett kiberfegyvereket ugyanaz az orosz állami támogatással működő és az orosz katonai titkosszolgálathoz kötődő Fancy Bear (APT28) néven ismert csoport alkalmazza, amelyhez az Amerikai Egyesült Államokban a DNC megtámadását is kötik. E teóriával kapcsolatosan számos pro és kontra érv felsorakoztatható, az azonban a támadó kilététől függetlenül is kijelenthető, hogy az ukrán konfliktusban jelentős szerephez jutott ismét a kibertér, illetve az ott folytatott műveletsorozat.

2016 nyarán a NATO elismerte a kiberteret a háború, illetve a hadviselés ötödik dimenziójaként, ami jelentős előrelépés több tekintetben is. Egyfelől a szövetség keretein belül ezentúl a kiberképességek fejlesztésére a többi dimenzióhoz (szárazföld, tenger, levegő, világűr) hasonlóan célzott fejlesztéseket lehet kialakítani, és erre fordítandó forrásokat allokálni, másfelől az fentiekhez hasonló esetek katonai akcióként történő elismerése egyértelműbb. Ha a kibertérből érkező támadás akár emberélet, akár gazdasági károk tekintetében felér egy fizikai támadással, előfordulhat, hogy arra válasz is érkezik, és adott esetben nemcsak a kibertérben, hanem fizikai csapás formájában is. Bár nem a NATO hajtotta végre, de a kibertérben zajló folyamatokra adott fizikai válasznak tekinthető például az Iszlám Állam első számú hackereinek az USA által történő felkutatása és likvidálása drónok segítségével.

A biztonságpolitikai elemzők számára kirajzolódó trendek azt mutatják, hogy a folyamatos kapacitás- és képességbővülés a kibertérben nagyon élénkké vált az utóbbi években. Sok esetben hosszú évek fejlesztései és ráfordításai kezdenek láthatóvá válni, és egyre több azoknak az államoknak a száma, amelyek a kibervédelmi képességek mellett támadóképességeket is fejlesztenek. Ilyen tekintetben jelenleg a top 5 ország között találjuk Oroszországot, Kínát, Iránt, Észak-Koreát és az USA-t, de egyre meghatározóbb képességekre tesz szert Izrael, Pakisztán, illetve India is. A folyamatok egyértelműen azt mutatják, hogy egyfajta kiberfegyverkezési verseny van folyamatban, ami természetesen nem az utóbbi néhány év eredménye. Pusztán arról van szó, hogy a felhalmozott képességek bevetése és alkalmazása nyomán a továbbiakban már nyíltan alatt zajlanak ezek a folyamatok.

A kiberbiztonság különböző szegmenseit tárgyalva észre kell vennünk a kapcsolódási pontokat az adatvédelem területéhez, ahol szintén komoly regionális folyamatok zajlanak elsősorban az Európai Uniónak köszönhetően. Az EU-ban már eddig is számos rendelkezés biztosította a személyes adatok védelmét, de 2018. május 25-től új szintre emelkedik az adatvédelem az EU területén. Az új adatvédelmi szabályozás megalkotásának egyik oka az volt, hogy az érvényben lévő szabályozás a rohamos léptekben fejlődő információs társadalomban zajló folyamatokra egyre kevésbé alkalmazható. Az új szabályozás kialakításának másik oka, hogy az EU döntéshozói meg kívánták erősíteni a magánszemélyek online szolgáltatásokba vetett bizalmát, illetve az online környezettel jobban harmonizáló, korszerű adatvédelmi jogszabályt szerettek volna létrehozni.

Az EU Általános Adatvédelmi Rendelete (General Data Protection Regulation, továbbiakban: GDPR) minden tagállamban, így hazánkban is adatvédelmi reformmal jár együtt, és minden személyes adatot kezelő szervezetre kiterjed. Többek között a GDPR-nak köszönhetően módosult hazánkban az adatvédelmi törvény, a Kiberbiztonsági Stratégia, valamint az Információbiztonsági törvény, továbbá azok a vonatkozó részletszabályok, amelyek nincsenek összhangban az EU-rendelettel. Ennek szövege szerint a hatálybalépést követően minden ügyfél élhet az adatok hordozhatóságához és a felejtéshez fűződő jogával, ami azt jelenti, hogy egyfelől kérhetik szolgáltatójukat, hogy adataikat adja át másik szolgáltatónak, másfelől jogosultak a személyes adatok indokolatlan késlekedés nélküli törlését kérni. További újdonság az úgynevezett profilalkotás tiltásának joga, továbbá 2018-tól biztosítani kell az ügyfél számára a betekintés jogát. A rendelet egyik, az elmúlt évek tömeges felhasználói adatlopásait figyelembe véve (gondoljunk csak az OPM- vagy a Yahoo-botrányra), kiberbiztonsági szempontból is jelentős passzusa, hogy a személyes adatot álnéven kell tárolni pont azért, hogy a felhasználói adatokat tartalmazó adatbázis kompromittálódása esetén a személyiségi jogok ne sérülhessenek. A rendelet megalkotói megelőző intézkedéseket is előírnak, így minden

olyan szervezet köteles adatvédelmi hatástanulmányt készíteni, amely jelentős mennyiségű személyes adatot kezel, illetve amelynél az érintettek adatai veszélyben lehetnek. Lényeges pont, hogy 2018-tól a szervezetek kötelesek az adatvédelmet, illetve a felmerülő költségeket beépíteni az üzleti folyamataikba és a rendszerek tervezésébe egyaránt. Az elmúlt évek milliós és milliárdos nagyságrendű adatvesztéseinek egyik sajátosságát kívánják a rendelet megalkotói felszámolni azzal is, hogy incidens esetén arról legkésőbb 72 órán belül értesíteni kell a nemzeti adatvédelmi hatóságokat. Az érintettekre nézve jelentős kockázat esetén azokat is kötelező tájékoztatni, akiknek az adatait az incidens érinti. Az EU súlyos szankciókat helyezett kilátásba bírság formájában, amely egységes mértékű lesz mindenütt, és a legsúlyosabb incidensek esetén elérheti a társaság árbevételének 4 százalékát, amit 20 millió euróban maximalizáltak.

Összességében a GDPR az egyik legfontosabb eleme az Európai Unió kiberbiztonság terén tett erőfeszítéseinek, hiszen olyan egységes, minden tagállamra kiterjedő, a személyes adatokat védő rendeletet alkotott, amely egyértelműen a felhasználók védelmében született, és erős kényszerítő hatást fejt ki az adatkezelők irányába az általuk tárolt személyes adatok biztonságának növelése érdekében. A korábban említett tömeges adatlopások nagy valószínűséggel ettől még nem fognak megszűnni, azonban jó esély van arra, hogy – elsősorban az EU területén – egyre kevesebb, a felhasználóra nézve komoly kockázatot jelentő incidens történik. Az EU rendeletbe foglalt adatvédelmi törekvései regionális szinten hatékony nemzetközi választ jelenthetnek az aktuális kiberbiztonsági kihívásokra, de csak sikeres implementáció esetén, valamint akkor, ha a kibertámadásoknak leginkább kitett kis- és középvállalkozások számára is elfogadható mértékű lesz a rendeletből fakadó plusz költségek mértéke.

5. Globális folyamatokat érintő kiberbiztonsági kihívások

Általánosságban elmondható, hogy globális szinten egyre több a kibertámadás, amelyek egyre szofisztikáltabbak is, ugyanakkor azoknak a támadásoknak is töretlenül emelkedik a száma, amelyekhez nem szükséges különösebb technikai tudás. A tudástranszfer következtében ma már minimális beruházással és informatikai tudással is könnyen válhat valakiből támadó. A kiberbiztonsági fenyegetések és kihívások kapcsán fontos tényezőknek tekinthetők az ezen a területen működő, jelentős ügyfélkörrel rendelkező biztonsági cégek, nagy tekintélyű kutatóközpontok és egyéb, kiberbiztonsági szakembereket tömörítő szakmai szervezetek, amelyek időszakos felmérésekkel, beszámolókkal, éves jelentésekkel és rendeszeres adatmegosztással segítik egymás és a kiberbiztonsági közösség munkáját.

A rendelkezésre álló legfrissebb adatok alapján az látszik, hogy csökkent a különböző rosszindulatú szoftverek által megfertőzött számítógépek átlagos helyreállítási költsége, ugyanakkor nőtt a kiberbűnözők által okozott kár. A Kaspersky Cybersecurity Index kimutatása alapján elmondható, hogy 2016 második felében a felmérésben részt vevők 74 százaléka vélte úgy, hogy őt nem érinthetik az online fenyegetések, 39 százalékuk egyáltalán nem használt védelmi megoldást, és 29 százalék volt azok aránya, akik valamilyen kárt szenvedtek kibertámadás következtében. A korábbi 2016-os index ugyanebben a sorrendben 79, 40, 29 százalékos arányt mutatott, ami azt jelenti, hogy az első fél évben több ember gondolta úgy, hogy nem eshet kibertámadás áldozatául, és maradt védtelen. Szakértők szerint mindez arra utal, hogy bár nem túl gyorsan, de pozitívan változik az emberek hozzáállása az internetes biztonsághoz, és még ha lassan is, de folyamatosan nő azok száma, akik aggódnak a kibertérből érkező fenyegetések miatt, és tudatosan szeretnék megvédeni magukat e téren. A Kaspersky felmérése alapján 2016 második fél évében 22 százalékról 20 százalékra esett azoknak a felhasználóknak az aránya, akik valamilyen kártékony programmal találkoztak. Nőtt azonban azoknak a száma, akik egyéb, más típusú fenyegetések áldozataivá váltak, például zsarolóprogramok, adathalászat, adatlopás és adatszivárgás károsultjai lettek.

A Symantec éves jelentése alapján 2016-ban több egyedüli támadásra is sor került. Volt példa több millió dollár eltulajdonításával járó virtuális csalásra, kiemelendő az USA választási folyamatába történő beavatkozás, és nem szabad megfeledkeznünk az eddigi egyik legnagyobb DDoS támadásról sem, amit IoT eszközökből alkotott gigantikus botnet segítségével hajtottak végre az elkövetők. Miközben a kibertámadások korábban nem látott mértékben zavarják meg a rendszerek működését, a támadók egyre gyakrabban használnak egyszerű eszközöket és taktikákat a nagyobb hatás érdekében. A 0. napi sérülékenységekkel és a szofisztikált malwarekkel a támadók egyre inkább takarékoskodnak, és gyakran támaszkodnak a célzott adathalászatra vagy egyéb, nem egyszer amúgy legitim eszköz nem rendeltetésszerű használatára. 2016-ban ötéves csúcsot döntött a rosszindulatú szoftvert (malware) tartalmazó e-mailek aránya: 131 elküldött e-mailből egy biztosan tartalmazott kártékony elemet. A zsarolóvírusok továbbra is töretlenül szedik áldozataikat: a Symantec mérései alapján 2016-ban 36 százalékkal nőtt az ilyen típusú fertőzések száma, és az átlagos 300 dollár körüli váltságdíj több mint háromszorosára, 1077 dollárra nőtt. Korábban viszonylag ritkán jelentek meg azok a kártevők, amelyek kifejezetten destruktív céllal működnek, azonban 2016 ebben a tekintetben is negatív tendenciát mutat. Két, egymástól független esetben is kimutatható volt a szabotázs szándéka kibertámadások során. Az egyik esetben az ukrán energiaellátó rendszereket támadták meg egy éven belül kétszer is a BlackEnergy névre keresztelt kártékony szoftverrel, míg Szaúd-Arábiában a Shamoon tűnt fel újra a különböző ipari és közigazgatási rendszerekben.

A globális kiberbiztonsági fenyegetések és kihívások további részletezése szükségtelen, hiszen a változás rendkívül dinamikus, így érdemes a fenti adatokat is minden esetben a legfrissebb, rendelkezésre álló adatokkal behelyettesíteni. Ugyanakkor a bemutatott információkból is kirajzolódik, hogy a legtöbb kiberbiztonsági kihívás az érintett felhasználók száma, az okozott kár nagysága, esetleg a megtámadott rendszer jellege miatt nemzeti és nemzetközi szinten is jelentőséggel bír. Egy a kibertérben jelen levő állam ma már nem engedheti meg magának, hogy ne foglalkozzon a kiberbiztonsággal és ne allokáljon forrásokat a biztonság szavatolására. Több kimutatás is azt bizonyítja, hogy a kiberbiztonságra költött összegek világszerte növekednek szektoroktól függetlenül, ugyanakkor a károk is egyre nagyobbak. Az International Data Corporation (IDC) 2020-ra szóló előrejelzése alapján több mint 100 milliárd dollárt költ a világ kiberbiztonsági szolgáltatásokra, szoftverekre és hardverekre. Az előrejelzés alapján ennek az összegnek közel a harmadát, mintegy 31 milliárd dollárt az USA fog elkölteni különböző kiberbiztonsági eszközökre és szolgáltatásokra, míg a második helyen Nyugat-Európa áll 19 milliárd dolláros becsült költésével. Összességében a 2016-os évhez képest 38 százalékos a növekedés a kiberbiztonsági kiadások terén, de az nem derül ki, hogy ez milyen arányban oszlik el 2020-ig. Ehhez képest a kiberbűnözők számlájára írható károk nagysága már 2015-ben is elérte a 3 billió dollárt világszerte. Érdekes, hogy a 2016-os Cybercrime Report előrejelzése alapján 2021-re a kiberbűnözésből fakadó károk nagysága világszinten megduplázódik, és eléri a 6 billió dollárt. Ez magában foglalja a sérült és megsemmisült adatokat, az ellopott pénzt, a termeléskiesést, a szellemi termékek eltulajdonítását, a személyes és pénzügyi adatok ellopását, a sikkasztást, csalást, a törvényszéki nyomozást és helyreállítást, valamint a reputációban keletkezett károkat. Az IDC adataihoz képest a 2016-os Cybercrime Report nagyságrendbeli különbséget mutat a kiberbiztonsági termékekre és szolgáltatásokra vonatkozó kiadások tekintetében, mivel azt több mint tízszeresére becsüli. Bárhogy is történjen, a következő néhány évben továbbra is folyamatos és dinamikus növekedés várható a kiberbiztonságra költött források, illetve a kibertámadásokból fakadó károk terén, és várhatóan az aránytalanság is fennmarad. A kiberbiztonsági kiadások a következő években továbbra is elmaradnak a kívánatostól, illetve jelentős problémát okoz a források nem megfelelő, illetve nem kellően hatékony elköltése is, ami elvezet egy másik globális szintű kiberbiztonsági kihíváshoz. Az eddig említett kihívásokhoz képest a kiberbiztonsági munkaerőpiacon az utóbbi időben egyre jelentősebbé váló anomáliákat – összetettségük okán –részletesebben tárgyaljuk, több tanulmány alapján.

2014 nyarán a RAND Corporation kiadott egy tanulmányt *H4CKER5 WANTED* címmel, amely alapvetően az Amerikai Egyesült Államok kiberbiztonsági munkaerőhelyzetével foglalkozott. Ha elfogadjuk, hogy az Egyesült Államokat érintő infokommunikációs technológiákkal összefüggő folyamatok – ha némi késleltetéssel is, de – érzékelhetők a világ más régióiban is, úgy a tanulmány megállapításai hasznosak lehetnek bármely ország számára. Ennek szerzői több korábbi jelentés és felmérés eredményét is feldolgozták, amelyeket például az amerikai Kormányzati Ellenőrzési Hivatal (U.S. Government Accountability Office – GAO), az amerikai kormányzat számára tanácsadói tevékenységet folytató Booz-Allen Hamilton (BAH) vállalat, az amerikai Védelmi Minisztérium (Department of Defense – DoD) vagy a Belbiztonsági Tanácsadó Testület (Homeland Security Advisory Council – HSAC) végzett. A GAO a történelem egyik legjelentősebb adatlopási incidensét elszenvedő kormányzati Személyzeti Irodával (Office of Personnel Management – OPM) közösen több követendő gyakorlatot is megfogalmazott a kiberbiztonsági munkaerő utánpótlásával kapcsolatban. A GAO munkatársai felhívták a figyelmet a nemzetbiztonsági átvilágításokból fakadó anomáliákra, amik miatt akár egy évig is elhúzódhatott egy felvételi procedúra, és listázták azokat a kormányzati kezdeményezéseket, amelyek a különböző állami szervezetek számára nyújtanak segítséget a megfelelő kiberbiztonsági munkaerő megtalálásában és képzésében. (Libicki 2014, 14–17)

Az OPM-hez hasonlóan ismerős lehet a Booz-Allen Hamilton vállalat neve is. Ez volt az a cég, amelyik munkaerő-kölcsönzés keretében Edward Snowdent kiközvetítette az amerikai Nemzetbiztonsági Szolgálathoz (National Security Agency – NSA), aminek következtében 2013-ban Snowdennek lehetősége nyílt leleplezni az amerikai titkosszolgálatok tömeges megfigyelési gyakorlatát. A BAH vállalat is készített korábban egy gyakran hivatkozott tanulmányt arról, hogy milyen elvek és módszerek mentén lehetne erősíteni az amerikai szövetségi hivatalok kiberbiztonsági munkaerőállományát. A tanulmány szerzői többek között azt is megállapították, hogy az amerikai kormányzati kiberbiztonsági munkaerőprogramok széttagoltak, az OPM tevékenysége nem megfelelő, az alkalmazási szabályok túl komplexek, miközben a megbízásos szerződéssel történő alkalmazás jóval egyszerűbb. A szolgálatért kapott ösztöndíjprogramok sem jártak teljes sikerrel, az állami szervezetek pedig egymás elől vették el a kiberbiztonsági szakembereket, miközben továbbra sem jutott elegendő pénz kiberbiztonsági képzésre és a humánerőforrás fejlesztésére. (Libicki 2014, 17–19)

A Stratégiai és Nemzetközi Tanulmányok Központ (Center for Strategic and International Studies – CSIS) kiberbiztonsági munkaerővel foglalkozó elemzése alapvetően nem pénzügyi problémákat állapított meg az amerikai kormányzat szakemberhiányával kapcsolatban, sokkal inkább a menedzsment alacsony hatékonyságát hibáztatta a kialakult helyzetért. A legfontosabb javaslatok között szerepelt az amerikai Belbiztonsági Minisztérium (Department of Homeland Security – DHS) részére a kibertérhez kapcsolódó kormányzati szerepkörök és szakismeretek rendszertanának kialakítása, az amerikai Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology) és más szereplők számára az engedélyezési követelményrendszer létrehozása, valamint az OPM számára a karrierstruktúra javítása. (Libicki 2014, 19–22.)

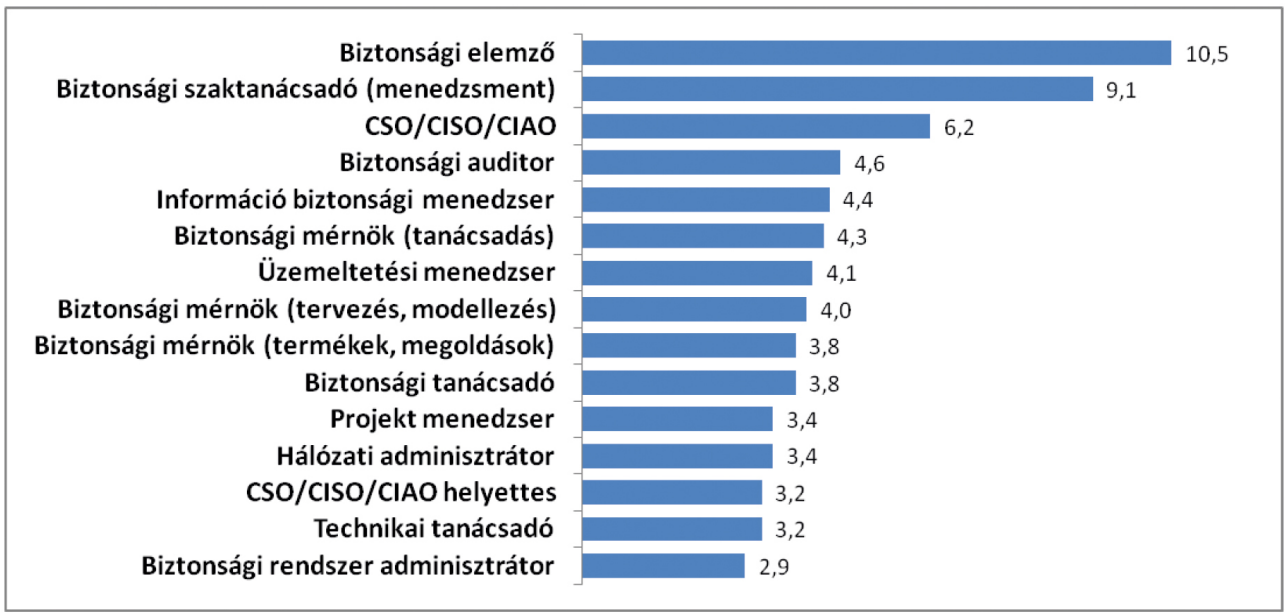
Az amerikai Védelmi Minisztériumnak (DoD) a kiberműveletek személyi állományáról szóló jelentése nagyobb létszámhiányt mutatott, illetve felhívta a figyelmet arra, hogy a különböző szolgálati ágak és haderőelemek eltérő igényekkel rendelkeznek a kiberbiztonsági szakértelem terén. Azért, hogy a DoD alá tartozó szervezetekben csökkenteni lehessen a kiberbiztonsági szakemberek hiányát, a minisztérium több programot és fejlesztést is indított, amelyek elsősorban a képzési feltételek javítását és a pénzügyi körülmények fejlesztését szolgálták. Ilyen lépés például az iCollege program létrehozása, vagy a szakmai tanúsítványokért járó bónuszrendszer kialakítása. (Libicki 2014, 22–24.)

A Belbiztonsági Tanácsadó Testület (HSAC) létrehozott egy munkacsoportot, amelynek olyan kiemelkedő személyiségek is tagjai voltak, mint például a DEF CON hackerkonferencia alapítója Jeff Moss vagy a SANS Intézetet vezetője Alan Paller. A testület arra jutott, hogy a Belbiztonsági Minisztérium (DHS) versenyképtelenné vált a munkaerőpiacon, mivel nem volt képes kellően ér-

dekes és kihívásokkal teli munkát kínálni a kiberbiztonsági szakemberek számára. Az amerikai kormányzat felé megfogalmazott legfontosabb javaslatok:

- irányadó lista elkészítése a kritikus kormányzati kiberbiztonsági feladatokról;
- gyakorlati forgatókönyvek és értékelési modell kifejlesztése;
- dedikált tanácsadó-testület felállítása a kiberbiztonsági munkaerő fejlesztésére;
- a veteránok bevonása és kiberbiztonsági tartalékos program kialakítása. (Libicki 2014, 24–25)

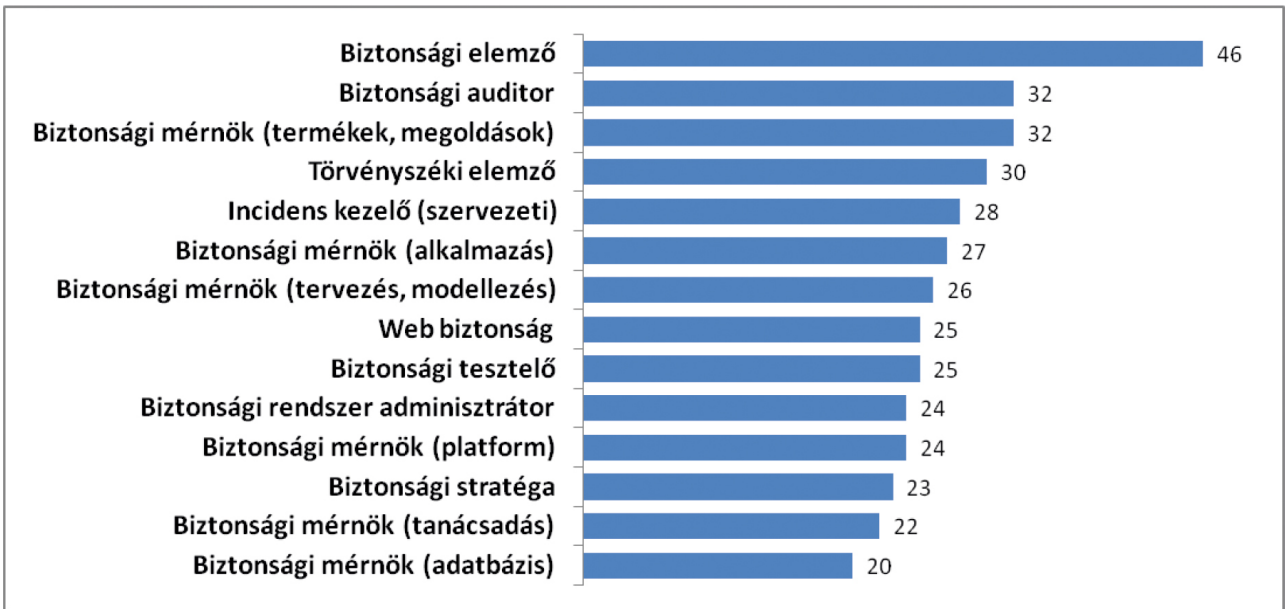
A kiberbiztonsági feladatokat és a kapcsolódó munkaköröket általában egy kategóriába sorolva emlegetik, holott rendkívül szerteágazó tevékenységet fednek le a kiberbiztonsági pozíciók, így a szükséges szaktudás is eltérő. Bizonyos munkakörök betöltéséhez elengedhetetlen az erős technikai háttértudás, adott esetben a mérnöki végzettség, míg más esetekben inkább menedzsmentismeretekre és vezetői képességekre van szükség. Az (ISC)[2] (The International Information System Security Certification Consortium) a világ legnagyobb, információ- és szoftverbiztonsági szakembereket tömörítő szervezete, amely több mint 160 országból 100 ezernél is több taggal rendelkezik. A szervezet által készített felmérés szerint 2015-ben a kiberbiztonság területén dolgozók több mint 10 százaléka biztonsági elemző volt, 9 százalék körül alakult a biztonsági tanácsadók aránya, illetve meghaladta a 6 százalékot a biztonsági és információbiztonsági vezetők aránya.



2. ábra: A Frost & Sullivan az (ISC)2 számára 14 000 válaszadóval készített felmérésének eredménye
Forrás: A szerző saját szerkesztése és fordítása az eredeti grafikon alapján.[2]

A felmérés készítői arra is kíváncsiak voltak, hogy azoknál a szervezeteknél, ahol a válaszadók dolgoznak, milyen kiberbiztonsági szakmákban van hiány, illetve melyik pozíciók feltöltése okozza a legnagyobb gondot. Az eredmények azt mutatják, hogy bár a válaszadók között is jelentős számban vannak biztonsági elemzők, még többre lenne szükség. A legnagyobb, közel 50 százalékos igény a biztonsági elemzők iránt mutatkozik, de egyformán keresettek a biztonsági auditorok és azok a mérnökök, akik a biztonsági termékek és megoldások tervezéséért felelősek.

[2] *Elérhető:* www.isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf *(utolsó letöltés: 2015. május 21.)*

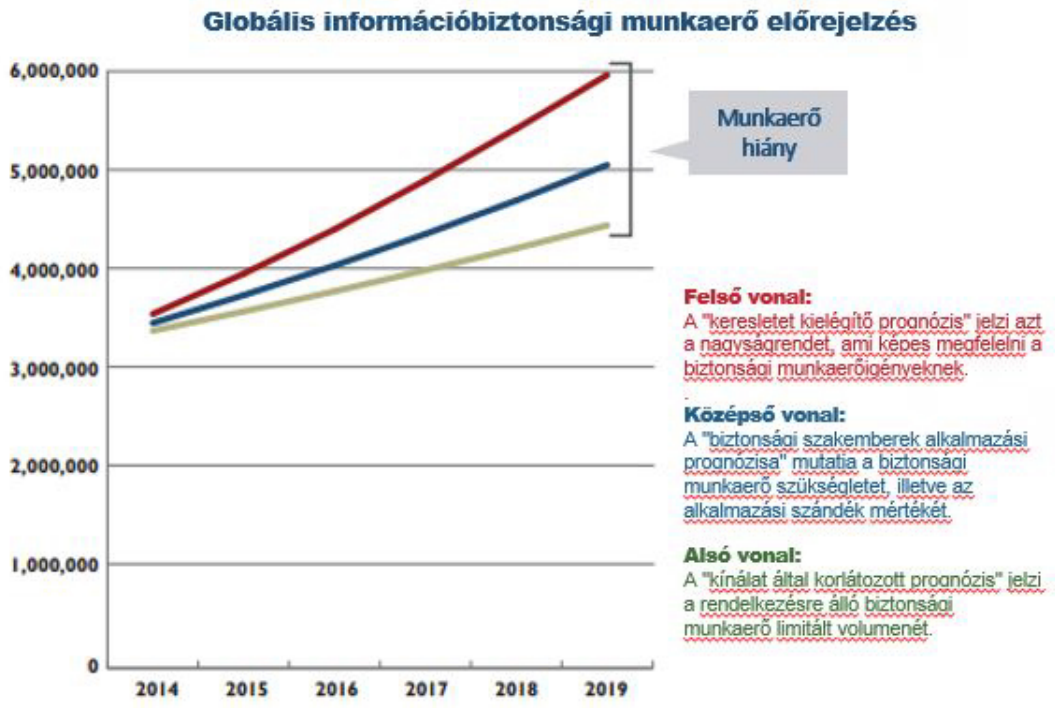


3. ábra: Az (ISC)[2] számára készült 2015-ös felmérés alapján a legkeresettebb kiberbiztonsági szakmák sorrendje
Forrás: A szerző saját szerkesztése és fordítása az eredeti grafikon alapján.[3]

A válaszokból kitűnik, hogy jelentős igény van törvényszéki, illetve nyombiztosító elemzőkre, incidensek kezelésében jártas szakemberekre, de keresettek a biztonsági tesztelők, illetve az adatbázisok, az alkalmazások és a különböző platformok biztonságához értő mérnökök is.

A 2015-ös felmérés alapján a készítők egy 2014–2019 közötti időszakra vonatkozó becslést is elvégeztek, amiből jól látszik, hogy a nagyjából 3,5 milliós szakember létszám 2019-re 4,5 millió körülire bővül. Ugyanakkor az igények ennél jóval nagyobb mértékben fognak növekedni, és a kereslet várhatóan eléri a 6 millió főt globális szinten. A mintegy 1,5 millió fős különbség olyan kihívást jelent humán oldalról a kiberbiztonságban, amire ma még nem ismerjük biztosan a válaszlépéseket. Amit viszont már most is biztosan tudunk, hogy minderre nem lesz képes egyetlen ember vagy szervezet válaszokat adni. A kiberbiztonsági közösségnek és a kibertérrel kapcsolatba kerülő összes szervezetnek, nemzetállamnak közre kell működnie abban, hogy a biztonság nagyobb figyelmet kapjon az átlag felhasználók körében éppúgy, mint a pályaválasztás előtt álló fiatalok esetében. A szükséges lépések késése vagy elmaradása csak ronthat a helyzeten.

[3] *Elérhető:* www.isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf *(utolsó letöltés: 2015. május 21.)*



4. ábra: A kiberbiztonsági munkaerő várható alakulása 2014 és 2019 között
Forrás: A szerző saját szerkesztése és fordítása az eredeti grafikon alapján.[4]

Jól látható, hogy miközben a kiberbiztonsági munkaerőhiány minden szektort érint, még az Amerikai Egyesült Államok kormánya számára is komoly nehézségeket okoz a helyzet megoldása. Az USA kormányának rendszer szintű problémákkal kell szembenéznie, és bár a munkát más országok kormányaihoz képest jóval korábban megkezdték, úgy tűnik, 2015-ben még mindig rendkívül súlyos a helyzet. Elég csak a korábban már említett OPM adatlopási botrányra gondolni, amit 2015 júniusában fedeztek fel az illetékesek, és több mint 22 millió főt, az Egyesült Államok lakosságának 7 százalékát érintette. (Zengerle–Cassella 2015) Szintén jelentős problémákra utal – még ha a forrás miatt fenntartásokkal is kell kezeljük a hírt –, hogy az amerikai biztonsági rendszerek sérülékenységének napi szintű gyarapodásával még az ország legnagyobb riválisa, Kína sem tud lépést tartani, mert nem képes elég kiberbiztonsági szakembert biztosítani a felfedezett sérülékenységek kihasználásához. (Sz.n. 2015) Szintén beszédes adatokat rejt a Raytheon amerikai védelmi ipari vállalat támogatásával az amerikai Nemzeti Kiberbiztonsági Szövetség (National Cyber Security Alliance – NCSA) által készített felmérés, ami elsősorban az Y-generáció tagjai között vizsgálta a kiberbiztonsági szakma iránti érdeklődést. A felmérés eredményéből kitűnik, hogy a Közel-Keletet leszámítva minden régióban, illetve globálisan is 60 százalék felett van azoknak a fiataloknak a száma, akik számára soha senki nem vetette fel annak lehetőségét, hogy kiberbiztonsági karriert építsenek. Ugyanakkor a válaszadók 38 százaléka szeretne többet tudni a kiberbiztonsági karrierlehetőségekről. Szintén rendszerszintű problémára mutat rá, hogy globális szinten a fiatalok 58 százaléka nem részesült kiberbiztonsággal kapcsolatos formális oktatásban. (Sz.n. 2016)

A kiberbiztonsági munkaerőhiány kapcsán még 2015-ben napvilágot látott adatok szerint az Európai Unióban az ICT szektor évente 120 ezer új munkahelyet teremt. Azonban a képzett munkaerő

[4] *Elérhető:* www.isc2.org/2013-ISC2-Global-Information-Security-Workforce-Study.pdf *(utolsó letöltés: 2015. május 21.)*

hiánya miatt 2020-ra mintegy 900 ezer ICT-állás maradhat betöltetlen az EU-ban. Tovább árnyalja a képet, hogy az EU lakosságának 20 százaléka soha nem használta az internetet, míg közel 40 százaléka nem rendelkezik megfelelő digitális képességekkel. Az EU lakóinak 14 százaléka pedig semmilyen digitális képességgel nem rendelkezik. (Ansip 2015) Az önmagában alacsonynak tűnő érték valójában több mint 70 millió embert jelent. A még csak kialakulóban lévő helyzetre nincs azonnali megoldás. Bár sokan hisznek abban, hogy néhány év múlva a legtöbb kiberbiztonsági területen az emberek szerepét átveszi a gépi tanulás és a mesterséges intelligencia, ezeknek a megoldásoknak a széles körű elterjedése 2020 előtt nem várható, és azt követően sem lehet majd minden funkciót gépekre bízni. A következő években nem várható, hogy hirtelen nagy számban jelennének meg kiberbiztonságban jártas, képzett munkavállalók a piacon, és ebben a tekintetben a bevándorlás és az agyelszívás sem jelent megoldást. Az egyetlen előremutató, hosszú távon is eredményt hozó megoldás az oktatás és a képzés, amihez nemzetközi összefogás szükséges annak érdekében, hogy a sokszor nagyon magas költségekkel képzett munkaerő ne hagyja el az adott országot vagy régiót. Jelenleg a nemzetközi kiberbiztonsági képzési és oktatási együttműködések meglehetősen fejletlenek, egy-két kivételtől eltekintve.

A nemzetközi együttműködések kapcsán gyakran jelentkező kihívás a terminológia kérdése. Bár elsőre nem tűnik komoly problémának, de ha jobban megvizsgáljuk a nemzetközi rendszer működésének alapjait és a különböző kooperatív kezdeményezéseket, hamar kiderül, hogy a kiberbiztonsági kihívások hatékony nemzetközi kezeléséhez nagy szükség lenne egy közös, egyezményes terminológia kialakítására. Ilyen azonban nem létezik, a *kiberbiztonságnak* nincs általánosan elfogadott meghatározása. Például az Európai Unió kiberbiztonsági stratégiája szerint a „kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket. A kiberbiztonság célja a hálózatok és az infrastruktúra rendelkezésre állásának és integritásának, valamint a benne lévő információk titkosságának megőrzése.” (EU 2013, 3.) Az ENSZ mellett működő Nemzetközi Távközlési Egyesület (ITU) két meghatározása is érvényben van a kiberbiztonságra vonatkozóan. A rövidebb meghatározás szerint az adatok és rendszerek védelmét jelenti azokon a hálózatokon, amelyek az internethez kapcsolódnak. A tömör definíció helyett érdemesebb inkább az ITU hosszabb meghatározását figyelembe venni, ami szerint a kiberbiztonság olyan eszközök, politikák, biztonsági koncepciók, útmutatások, kockázatkezelési törekvések, intézkedések, képzések, legjobb gyakorlatok és technológiák együttese, amelyek alkalmasak a kibertér, illetve a kibertérben működő szervezetek és személyek tulajdonának védelmére. A meghatározás kitér arra is, hogy a szervezetek és felhasználók tulajdonának értendő minden a kibertérrel kapcsolatban álló eszköz, infrastruktúra, alkalmazás, szolgáltatás, telekommunikációs rendszer és az összes küldött és tárolt információ. Az ITU meghatározása magában foglalja az információbiztonság három alapelvét is: bizalmasság, sértetlenség, rendelkezésre állás. (Mauer–Morgus 2014) *Bizalmasság* vagy *titkosság* alatt azt értjük, hogy az információhoz csak az előírt módon és csak olyan személyek férhetnek hozzá, akiket erre feljogosítottak. A *sértetlenség* vagy más néven *integritás* nem más, mint az adat és információ eredetisége és épsége, illetve az információs rendszer hiteles és pontos állapota. Egyszerűbben fogalmazva az adatokat és információkat csak azok módosíthatják, akik erre jogosultak és véletlen változás nem fordulhat elő. A *rendelkezésre állás* szintén egy állapotot határoz meg, amely egyfelől állandóságot jelent, másfelől az adatok és információk meghatározott időben történő elérhetőségét. A rendelkezésre állást értelmezhetjük úgy is, hogy a felhasználót semmi nem akadályozza abban, hogy az adatokhoz és információkhoz hozzáférjen, amikor azokra szüksége van. Ha már az euro-atlanti szövetségi rendszer szóba került, érdemes megnézni a világ legerősebb katonai szervezeteként számon tartott NATO kiberbiztonsághoz kapcsolódó kifejezéseit. Katonai szervezet lévén a NATO által alkalmazott terminológia alapvetően a védelem és a kiber kifejezéseket társítja, de több meghatározás van használatban párhuzamosan. Az egyik szélesebb információbiztonsági környezetet foglal magában, ahol a kommunikációs és információs rendszerek biztonsága a bizalmasság, az integritás és a rendelkezésre

állás megfelelő védelmének képességét jelenti. Ugyanakkor a NATO a *kibervédelem* kifejezés alatt olyan képességet ért, amivel egy műveleti kommunikációs és információs rendszer szolgáltatásai megvédhetők a kibertérből érkező rosszindulatú tevékenységekkel szemben. (Klimburg 2012) Már az említett meghatározások nyomán is jól látható, hogy az egyes kiberbiztonsági definíciók között eltérés mutatkozik attól függően, hogy melyik szervezetről vagy intézményről van szó. A helyzet csak tovább bonyolódik, ha az egyes államok szintjén vizsgáljuk a kiberbiztonság meghatározását, mivel a legtöbb ország saját megfogalmazást, egyedi definíciót alkalmaz. Ezen a szinten az eltérések sokszor jelentéktelenek, de gyakran előfordulnak komoly különbségek is. Mivel a fejezetnek nem célja a terminológiai hasonlóságok és eltérések részletes bemutatása, ezért az állami definíciók közül csak a magyar meghatározást elemezzük.

A 2013-ban megjelent Nemzeti Kiberbiztonsági Stratégia (NKBS) 5. pontja az alábbiak szerint definiálja a *kiberbiztonság* fogalmát. A stratégia szerint 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." (MK 2013, 6339.) A bemutatott meghatározások alapján jól látható, hogy a kiberbiztonság egyfelől leginkább egy állapotként írható le, amelynek három alapvető összetevője az adatok és információk bizalmassága, integritása és rendelkezésre állása, másfelől viszont mindez egy olyan eszközrendszer, illetve képesség, amely a kibertérből eredő kockázatokat elfogadható szinten tudja tartani. Fontos megjegyezni, hogy a fizikai világhoz hasonlóan a kibertérben sem érhető el abszolút biztonság.

6. Kiberbiztonság a nemzetközi béke és biztonság tükrében

Az államok az 1990-es évek óta foglalkoznak az információs és telekommunikációs technológiák nemzetközi békére és biztonságra gyakorolt hatásaival. Az azóta eltelt időszakban számos jelentős kiberbiztonsági incidens történt, melyeknek köszönhetően a kormányok új politikákat és szervezeteket kezdtek el kialakítani a kibertér katonai célú felhasználásával összefüggésben. Ennek eredményeként jelenleg is vita tárgya, hogy milyen nemzetközi normák mentén lehetne irányítani a kiberteret, és milyen módon lehetséges a bizalomépítés ebben a dimenzióban. Fontos lenne a stabilitás növelése, illetve az államok számára olyan kiberbiztonsági képességek kialakítása, amelyek segítségével hatékonyan léphetnek fel a kibertérből érkező kihívásokkal szemben saját határaikon belül és kívül egyaránt. Az elmúlt évek trendjei alapján számos ország kezdte el a kiberbiztonsági kérdéseket beépíteni a nemzeti biztonsági és védelmi stratégiájába, illetve a fejlett államok mára már önálló stratégia keretén belül foglalkoznak a kibertér biztonságának garantálásával. A politika legfelső szintjeire eljutó kiberbiztonsági kérdések nyomán nemzeti beruházások indulnak annak érdekében, hogy kibervédelmi vagy éppen támadó képességeket alakítsanak ki a kihívások és sérülékenységek kezelésére. A fokozott érdeklődésnek és beruházásoknak köszönhetően újabb kérdések merülnek fel például a hagyományos biztonsági koncepciók alkalmazhatósága, a kibertérre vonatkozó jog és a kibertér irányítási struktúrájával kapcsolatban. A kialakult párbeszédek fókuszában jellemzően a nemzetközi jog alkalmazhatósága, a kibertérre vonatkozó normák és az államok kibertérben tanúsított magatartási formái állnak. Ezen a téren az egyik meghatározó politikai irány a tömegpusztító fegyverek leszereléséhez kapcsolódó bizalom- és biztonságerősítő intézkedések nyomán próbálja meg a kiberteret biztonságosabbá tenni, és az ehhez szükséges kibervédelmi kapacitásokat kialakítani. A fizikai világra alkalmazott nemzetközi jog, illetve az annak részét képező hadijogi alapelvek kapcsán fontos kérdések merülnek fel azzal kapcsolatban, hogy a megkülönböztetés vagy az arányosság elve miként alkalmazható a kibertérben. A megkülönböztetés koncepciója szerint a hadviselő feleknek különbséget kell tenniük civil és katonai célpontok között, ami jelenleg szinte egyáltalán nem kivitelezhető a kibertérben. Hasonlóan problematikus az arányosság elve, amelynek értelmében a támadással

okozott pusztításnak arányban kell lennie a katonai előnnyel, amire a támadás következtében tesz szert valamelyik hadviselő fél. Tekintettel arra, hogy ezek az elvek nehezen vagy csak megkötésekkel alkalmazhatók a kibertérre, több olyan javaslat is napvilágot látott, amelyek értelmében a kibertérben megnövekedne az állam szerepe az információk ellenőrzése terén. Ezek az erőfeszítések azonban jelentős veszélyeket hordoznak magukban, elsősorban a szólásszabadság vonatkozásában. Ez az egyik oka annak, hogy az információ- és kiberbiztonság meghatározása és a kapcsolódó, egységes terminológia kialakítása során fontos emberi jogi kérdésekre is tekintettel kell lenni. Szintén fontos, hogy ezeknek a jelentős kérdéseknek a megvitatása korábban a nemzetállamok kiváltsága volt, a kibertérben a társadalmi szereplőknek azonban nem csak közvetett módon lehet nagy hatása a nemzetközi békére és biztonságra. A kiberbiztonság aktualitásairól számos fórumon értekeztek már e szempontokat szem előtt tartva, azonban a kibertér védelmét és biztonságát erősíteni hivatott nemzetközi együttműködések a mai napig gyerekcipőben járnak. A kooperatív kezdeményezések túlnyomó részt egyetlen régióra vagy valamilyen problémakörre próbálnak megoldást találni. Kérdés, hogy a fragmentáltság a hatékonyságot milyen mértékben befolyásolja egy olyan határok nélküli közegben, ahol minden mindennel összefügg.

7. Felhasznált irodalom

- Anglia Ruskin University Library (2008): *Harvard System of Referencing Guide.* Elérhetőség: https://library.aru.ac.uk/referencing/harvard.htm (utolsó letöltés: 2017. január 06.)
- Ansip, Andrus (2015): *Digital skills, jobs and the need to get more Europeans online*. Online: https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/digital-skills-jobs-and-need-get-more-europeans-online_en (utolsó letöltés: 2017. április 2.)
- Berzsenyi Dániel – Ványi Rajmond (2015): Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei. *Nemzet és Biztonság,* 8. évf. 3. sz. 134–143. Elérhető: http://nemzetesbiztonsag.hu/cikkek/nb_2015_3_12_berzsenyi-vanyi_-_egy_katonapolitikai_dontes_lehetseges_kiberbiztonsagi_kovetkezmenyei_iszlam_allam.pdf (utolsó letöltés: 2015. december 27.)
- Evans, Dave (2011): *The Internet of Things, How the Next Evolution of the Internet Is Changing Everything*. Cisco. Online: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (utolsó letöltés: 2022. április 4.)
- Hart, Kim (2008): Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar. *Washington Post.* Online: www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html?hpid=topnews (utolsó letöltés: 2017. április 2.)
- Klimburg, Alexander ed. (2012): *National Cyber Security Framework Manual.* Online: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf (utolsó letöltés: 2022. április 4.)
- Kovács László – Krasznay Csaba (2017): *Mert övék a hatalom.* SVKK Elemzések. Elérhető: https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/svkk-elemzesek-2017-9-az-internet-politikat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf (utolsó letöltés: 2022. április 4.)
- Libicki, Martin C. – Senty, David – Pollak, Julia (2014): *H4CKER5 WANTED, An Examination of the Cybersecurity Labor Market, RAND Corporation*. Online: www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf (utolsó letöltés: 2014. június 23.)
- Maurer, Tim – Morgus, Robert (2014): *Compilation of Existing Cybersecurity and Information Security Related Definitions.* Online: https://na-production.s3.amazonaws.com/documents/compilation-of-existing-cybersecurity-and-information-security-related-definitions.pdf (utolsó letöltés: 2022. április 4.)

- Mészáros Csaba (2016): Fenyegetések Internete. *Computerworld.* Elérhető: http://computerworld.hu/computerworld/fenyegetesek-internete.html (utolsó letöltés: 2017. január 12.)
- Rettman, Andrew (2017): *German spy chief warns Kremlin on election hack.* Euobserver 2017. Online: https://euobserver.com/foreign/137788 (utolsó letöltés: 2017. május 6.)
- *China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems* (2015). The Onion. Online: www.theonion.com/article/china-unable-recruit-hackers-fast-enough-keep-vuln-51719 (utolsó letöltés: 2015. október 26.)
- *Securing Our Future: Closing the Cybersecurity Talent Gap* (2015). Raytheon. Online: https://www.raytheon.com/sites/default/files/news/rtnwcm/groups/cyber/documents/content/rtn_278208.pdf (utolsó letöltés: 2022. április 4.)
- *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról* (2013). Magyar Közlöny. Elérhető: www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (utolsó letöltés: 2013. április 3.)
- *Overview of the Internet of Things* (2012). ITU. Online: www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (utolsó letöltés: 2014. április 21.)
- *IoT: Hottest technology to watch out for in 2015* (2015). The Economic Times. Online: http://economictimes.indiatimes.com/news/industry/jobs/iot-hottest-technology-to-watch-out-for-in-2015/articleshow/45807138.cms (utolsó letöltés: 2015. október 8.)
- *ICT Facts and Figures 2016.* ITU. Online: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf (utolsó letöltés: 2016. október 19.)
- *Word Population Prospects The 2015 Revision* (2015). Online: https://esa.un.org/unpd/wpp/publications/files/key_findings_wpp_2015.pdf (utolsó letöltés: 2016. október 19.)
- *Rendszeres internethasználók aránya (2005–2016)*. KSH. Elérhető: www.ksh.hu/docs/hun/eurostat_tablak/tabl/tin00091.html (utolsó letöltés: 2016. október 19.)
- *Measuring the Information Society* (2012). ITU. Online: www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf Letöltés ideje: 2016. október 22.
- *The Internet of Everything: 2014.* Business Insider. Online: https://www.businessinsider.com/the-internet-of-everything-2014-slide-deck-sai-2014-2 (utolsó letöltés: 2016. október 22.)
- *Symantec Internet Security Threat Report* (2017). Online: www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (utolsó letöltés: 2017. május 4.)
- Wirtz, James J. (2015): *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*. CCDCOE 2015. Online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf (utolsó letöltés: 2016. november 2.)
- Zengerle, Patricia – Cassella, Megan (2015): Millions more Americans hit by government personnel data hack. *Reuters*. Online: www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709 (utolsó letöltés: 2015. július 10.)

II. DR. BODÓ ATTILA PÁL: BIZTONSÁGI ESEMÉNY-KEZELÉSSEL KAPCSOLATOS ELVÁRÁSOK A HAZAI ÉS A NEMZETKÖZI JOGBAN

1. Bevezető gondolatok

Jelen jegyzet megírását alapvetően két irány határozta meg. Az egyik, hogy az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatályba lépése óta eltelt évek alatt eltérő jogértelmezéseket tapasztaltam, amelyek egyrészt az értelmező rendelkezések gyakorlati tapasztalatok alapján történő módosításának hiányából vagy elkésett módosításából, másrészt a szabályok törvényben és végrehajtási rendeletben való együttes előfordulásából adódtak. A másik, hogy az elektronikus információbiztonság területén nincs olyan, a biztonsági események értelmezésével és az eseménykezeléssel mint önálló témával foglalkozó, a nemzeti és nemzetközi szabályozást is bemutató szakanyag, amely a jogértelmezést és a jogalkalmazást támogató céllal foglalná össze és mutatná be a szabályozási környezetet. Szándékom szerint jelen tananyag ezeknek az elvárásoknak felel meg. Célom az volt, hogy az alapoktól a nemzetközi jó gyakorlatokig bemutassam azokat a szabályokat, amelyek meghatározzák az eseménykezelést egy szervezet életében. Egyértelműen látszik, hogy a kiber-ökoszisztéma és a technológia fejlődése miatt nem várható el a jogalkotótól, hogy a legapróbb részletekig szabályozza ezt a területet. Úgy gondolom, a meglévő nemzeti és nemzetközi szabályozás megfelelő keretet biztosít a fenntartható biztonság állapotának és a hatékony eseménykezelés működtetésének azzal, hogy a részletszabályokat szervezeti szabályozás, munka- és folyamatszervezés, illetve hatósági feladatellátás keretében szükséges biztosítani.

2. Eseménykezelés az Ibtv. és végrehajtási szabályai tükrében

2.1. Alapvetés az eseménykezeléshez

Napjaink információs hálózatait és elektronikus információs rendszereit[5] folyamatosan érik azok a fenyegetések, amelyek elhárítása és hatékony biztonsági környezetüknek megteremtése – ideértve a fizikai és a virtuális teret is – komoly kihívás mind a tulajdonosok (legyen az az állam vagy piaci szereplő), mind az üzemeltetők számára. Ebben a kontextusban a biztonságot egy olyan statikus állapotnak kell tekinteni, amely megfelel a kockázatelemzésen alapuló, várható fenyegetésekkel szemben elérni kívánt biztonságnak, amely együttesen nem más, mint a védelmi intézkedések által kifejtett hatások összessége. A biztonság eléréséhez és fenntartásához tervezett védelmi intézkedések sokaságát kell végrehajtani, azaz a védelmi rendszer megfelelő állapotát szükséges biztosítani. A védelem

[5] Elektronikus információs rendszer: elektronikus információs rendszernek tekinthető az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; valamint minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; továbbá ezen elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok. [Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény [a továbbiakban: Ibtv.) 1. § (1) bekezdés 14b. pontja.]

ebben az értelemben tehát nem más, mint a fenyegetések ellen hozott tevékenységek és intézkedések összessége.

De mit tekintünk fenyegetésnek? Ennek meghatározásához az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) értelmező rendelkezéseit szükséges előhívni, amely rögzíti, hogy 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."[6]

Ezek a fenyegetések érkezhetnek a globális[7] és/vagy a magyar kibertérből.[8] Elkerülésük érdekében kiemelt kormányzati és társadalmi érdek a közigazgatás és a társadalom működését lehetővé tevő informatikai infrastruktúrák és a nemzeti adatvagyon védelme, az úgynevezett *kiberbiztonság* és a *kibervédelem* megerősítése.

Ezen fogalmak meghatározásához szintén az Ibtv. értelmező rendelkezéseit citáljuk elő. A *kibervédelem* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését[9] míg 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.[10] A *kiberbiztonság* fogalma tehát egy olyan komplex tevékenységet takar, amely a biztonság átfogó értelmezéséből kiindulva minden lehetséges eszközt igénybe vesz.

A 2013 márciusában elfogadott Magyarország Nemzeti Kiberbiztonsági Stratégiája[11] (továbbiakban: Kiberstratégia) is tartalmazza azokat az elérendő nemzeti célokat, amelyek hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességek kiépítését szorgalmazzák, a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen. Azaz a Kiberstratégia nemzeti céljai meghatározzák a kiberbiztonság és kibervédelem állami eszközeit.

A Kiberstratégiában rögzített célok és cselekvési területek a magyar kibertérre terjednek ki, ugyanakkor a feladatok hatékony megvalósításával Magyarország hozzájárul a globális kibertér védelméhez is. Nemzeti cselekvési területként és ahhoz igazodó kormányzati intézkedésként került rögzítésre a Kiberstratégiában a szakosított intézmények létrehozása és működtetése, amely körbe tartoznak azok a speciális szakértelemmel és hatáskörrel rendelkező szervezetek, amelyek a kibervédelem területén kiemelt szerepet töltenek be (részletezve a 2.2.3. alcímben: Az eseménykezelésben részt vevő szervezetek köre).

A *fenyegetés,* a *biztonság* és a *védelem* fogalmak fontosságát jelzi, hogy már az Ibtv. preambulumában is nevesítve megjelennek: „A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága. Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre

[6] Ibtv. 1. § (1) bekezdés 19. pontja.

[7] *Globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese. [Ibtv. 1. § (1) bekezdés 22. pontja.]

[8] *Magyar kibertér:* a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatak, 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. [Ibtv. 1. § (1) bekezdés 35. pontja.]

[9] Ibtv. 1. § (1) bekezdés 27. pont.

[10] Ibtv. 1. § (1) bekezdés 26. pont.

[11] 1139/2013. (III. 21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."[12] A preambulumban foglalt alapelvekkel összhangban az Ibtv. az elektronikus információs rendszer biztonságának azt az állapotot tekinti, amelyben a védelem 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.[13] Azaz a védelem megvalósítása során az összes számításba vehető fenyegetést figyelembe kell venni, azzal, hogy a védelem az elektronikus információs rendszer valamennyi elemére kiterjed és folyamatában megvalósul, továbbá költségei arányosak a fenyegetések által okozható károkkal. Ezt tekintjük a zárt,[14] folytonos,[15] teljes körű[16] és kockázatokkal arányos védelem[17] elvének. Ezen elv érvényesítésének támogatására az Ibtv. az alábbi védelmi formákat határozza meg:

- adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések összessége és a védelemre vonatkozó oktatás;[18]
- fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni és a mechanikai, az élőerős védelem, az elektronikai jelzőrendszer, a beléptető és a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, a klimatizálás és a tűzvédelem;[19]
- logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.[20]

Ha a fenyegetések ellen felépített védelmi intézkedések a kívánt hatást nem érik el vagy sérülnek (meghibásodás vagy vis major, illetve szándékosság révén), olyan események vagy eseménysorozatok következnek be, amelyek megfelelő kezeléséhez eltérő működés szükséges mind az elektronikus információs rendszer üzemeltetése terén, valamint mind az egyén, mind a szervezet részéről. E működést – különleges szerepe miatt – szabályozási oldalról (is) kezelni kell.

2.2. Az eseménykezeléssel összefüggő szabályok

A gyakorlatban fontos, hogy az előzőekben felsorolt védelmi intézkedések által lehetőleg elkerülhető legyen a biztonsági események bekövetkezése. Az Ibtv. értelmező rendelkezései szerint azt a nem kívánt vagy nem várt egyedi eseményt vagy eseménysorozatot, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül, biztonsági eseménynek kell tekinteni.[21] E fogalom értelmezéséhez segítséget nyújt az Ibtv.-ben önállóan megjelenő *bizalmasság,*[22] *sértetlenség,*[23] és *rendelkezésre állás*[24] definíciója. Az értelmező rendelkezések rögzí-

[12] Ibtv. preambulum.
[13] Ibtv. 1. § (1) bekezdés 15. pont.
[14] *Zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem [Ibtv. 1. § (1) bekezdés 48. pont.]
[15] *Folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [Ibtv. 1. § (1) bekezdés 21. pont.]
[16] *Teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [Ibtv. 1. § (1) bekezdés 44. pont.]
[17] *Kockázatokkal arányos védelem:* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével. [Ibtv. 1. § (1) bekezdés 31. pont]
[18] Ibtv. 1. § (1) bekezdés 6. pont.
[19] Ibtv. 1. § (1) bekezdés 20. pont.
[20] Ibtv. 1. § (1) bekezdés 34. pont.
[21] Ibtv. 1. § (1) bekezdés 9. pont.
[22] Ibtv. 1. § (1) bekezdés 8. pont.
[23] Ibtv. 1. § (1) bekezdés 39. pont.
[24] Ibtv. 1. § (1) bekezdés 38. pont.

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

*Sértetlenség*nek az adat azon tulajdonságát kell érteni, amely szerint: az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles, és származása ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága is, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

Rendelkezésre állás alatt annak biztosítását kell érteni, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók legyenek.

A hatályos szabályozási környezet megkülönbözteti a *biztonsági esemény* fogalmát a *súlyos biztonsági esemény*étől. Utóbbinak[25] kell tekinteni azt az informatikai eseményt, amelynek bekövetkezése esetén:

- az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet;
- emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
- súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben;
- alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.

Kritikus adatnak[26] a személyes adat[27] vagy valamely jogszabállyal védett adat tekinthető. Utóbbi védett adatok körébe tartozik például a bűnügyi személyes adat[28] vagy a minősített adat védelméről szóló 2009. évi CLV. törvény értelmező rendelkezései által meghatározott nemzeti vagy külföldi minősített adat.[29]

---

[25] Ibtv. 1. § (1) bekezdés 41a pont.

[26] Ibtv. 1. § (1) bekezdés 32a pont.

[27] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakbak: Infotv.) 3. § 2. pontja szerint: személyes adat: az érintettre vonatkozó bármely információ

[28] nfotv. 3. § 4. pontja – bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

[29] A minősített adat védelméről szóló 2009. évi CLV. törvény 3. § 1. pontja.
Nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.
Külföldi minősített adat:
ba) megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza,
bb) a Magyar Honvédség nemzetközi műveletei és gyakorlatai keretében keletkezett, illetve felhasznált olyan adat, amelyhez történő hozzáférést a műveletben résztvevő felek - a művelet vagy gyakorlat követelményei szerinti minősítéssel - korlátozzák, attól függetlenül, hogy a részes felek által képviselt államokkal Magyarországnak van-e a ba) alpontban foglaltaknak megfelelő megállapodása a minősített adat védelmére és cseréjére, és a minősített adat kezelésére vonatkozó rendelkezéseket a Magyar Honvédség, illetve a műveletet vagy a gyakorlatot irányító más részes fél határozza meg;.

Itt szükséges megjegyezni, hogy az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban. BM rendelet) 1. mellékletének 2.6 alpontja szerint az 5. biztonsági osztályba sorolt elektronikus információs rendszer esetében kiemelkedően nagy káresemény következhet be, ha:

- kiemelten nagy mennyiségű különleges személyes adat sérülhet;
- emberi életek kerülnek közvetlen veszélybe, nagy számban következhetnek be személyi sérülések;
- a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
- a lehetséges társadalmi-politikai hatás következtében súlyos bizalomvesztés lép fel az érintett szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- az üzlet- vagy ügymenet 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 százalékát.

Fentiekből az a következtetés vonható le, hogy súlyos biztonsági esemény bekövetkezésével a legmagasabb, ötös biztonsági osztályba sorolt elektronikus információs rendszer esetében kell számolni.

Egy adott biztonsági esemény bekövetkezését követően az általa kiváltott hatásnál figyelembe kell venni, hogy az milyen időtartamban állt fenn, milyen kiterjedtségű volt – adott esetben földrajzi értelemben is –, milyen mértékű problémát, zavart okozott (adott esetben az elektronikus információs rendszer működésén túl az állam, a társadalom és a gazdaság tevékenységére), hány felhasználót és/vagy szolgáltatást érintett. A kiváltott hatás befolyásolja a választott eseménykezelést.

Az Ibtv. a biztonsági esemény kezelését fogalmi szinten határozza meg. Ide sorolja a dokumentálást, a következmények felszámolását, a bekövetkezés okainak és felelőseinek megállapítását, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet.[30]

(Megjegyezzük, hogy a fogalmi meghatározás elemei között – nyelvtani értelmezése alapján – megtalálhatók az adminisztratív, a fizikai és a logikai védelmi intézkedéseket meghatározó magatartásszabályok.)

Ha sor kerül bármely biztonsági esemény bekövetkezésére, intézkedni kell annak azonnali és hatékony kezelése iránt. Az eseménykezelés történhet a védelmi intézkedések kiegészítésével vagy megerősítésével, a szabályozás javításával, az érintettek oktatásával és egyéb módon is. A lényeg, hogy minden ilyen tevékenység hozzájáruljon ahhoz, hogy az újbóli vagy megismételt biztonsági események bekövetkezésének a valószínűsége csökkenjen, és hogy a bekövetkezhető kár minimalizálható legyen.

Ennek érvényesítése érdekében az Ibtv. alapvető követelményként rögzíti,[31] hogy az intézkedéseknek a biztonsági események kezelése mellett – a PreDeCo (Preventive-Detective-Corrective) elvet alapul véve – támogatniuk kell:

- a megelőzést, azaz a fenyegetés által okozható hatás bekövetkezésének elkerülését;[32]
- a korai figyelmeztetést, azaz olyan aktív szervezeti cselekvést, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;[33]

[30] Ibtv. 1. § (1) bekezdés 10. pont.
[31] Ibtv. 6. §.
[32] Ibtv. 1. § (1) bekezdés 36. pont.
[33] Ibtv. 1. § (1) bekezdés 32. pont.

- az észlelést, azaz a biztonsági esemény bekövetkezésének felismerését;[34]
- a reagálást, amely a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedéseket foglalja magában.[35]

Az elektronikus információs rendszerek védelmének körében – a fentebb már említett – külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedések is tartalmaznak az eseménykezelésre vonatkozó közvetlen rendelkezést.

A BM rendelet 2. melléklete[36] a 4. biztonsági szervezeti szint követelményei között előírja az azonnali és eredményes, előre meghatározott biztonsági intézkedések bevezetését 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, valamint az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrásból származó, potenciális vagy valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárás vagy biztonsági ellenőrzés elvégezését.

A BM rendelet 4. melléklete[37] az adminisztratív védelmi intézkedések között követelményeket rögzít a biztonsági események kezelésre vonatkozóan. Az intézkedések az adott elektronikus információs rendszer biztonsági osztályba sorolt értékének növekedésével arányosan szigorodnak: magasabb osztályba sorolt érték esetén egyre összetettebb cselekvést igényelnek a szervezet részéről. A BM rendelet az eseménykezelésre vonatkozóan az 1. és 2. biztonsági osztályt illetően nem rögzít önálló adminisztratív védelmi intézkedéseket. A 3. biztonsági osztálytól kezdődően az alábbi intézkedések[38] megtétele kötelező a szervezet vagy szervezeti egység számára.

A 3. biztonsági osztálytól kötelező intézkedések köre:

a) Biztonsági eseménykezelési eljárásrend készítése.

1. A szervezet kötelezettsége, hogy a biztonsági eseményekre olyan eseménykezelési eljárásrendet dolgozzon ki, amely a fentiekben említett PreDeCo elvet felhasználva magában foglalja az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást.
2. A szervezetnek a kidolgozott eseménykezelési eljárásokat egyeztetnie kell az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel. Az üzletmenet-(/ügymenet-)folytonosság tervezése során elkészített eljárásrendben[39] az informatikai erőforrás-kiesésekre vonatkozóan köteles összehangolni a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével.
    - A szervezetnek az eseménykezelési tevékenységekből levont tanulságokat be kell építenie az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba és elvárásokba, a továbbképzésekbe és a tesztelési folyamatokba.
    - Biztonsági események figyelése. A szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.
    - Biztonsági események jelentése.

[34] Ibtv. 1. § (1) bekezdés 17. pont.

[35] Ibtv. 1. § (1) bekezdés 37. pont.

[36] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: BM rendelet) 2. melléklet 4.1 alpontjának 4.1.3. és 4.1.6. alpontjai.

[37] BM rendelet 3. melléklet 2. alcíme alatt szereplő táblázat 3.1 alpontjának 3.1.5. alpontja.

[38] BM rendelet 4. melléklet 3.1.5. alcím alapján.

[39] BM rendelet 4. melléklet 3. alcím 3.1.4. alpontja.

- A szervezet minden szereplőtől, aki az elektronikus információs rendszerrel vagy annak elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet vagy veszélyhelyzetet észlelnek.
- A szervezet a jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek (lásd részletesen: 2.2.3. alcím).

b) Segítségnyújtás a biztonsági események kezeléséhez. A szervezet tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.

c) Biztonsági eseménykezelési terv készítése.

- A szervezet kötelezettsége, hogy biztonsági eseménykezelési tervet dolgozzon ki, amely:
  - iránymutatást tartalmaz a biztonsági esemény kezelési módjaira,
  - ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,
  - átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,
  - tartalmazza a szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeket,
  - meghatározza a bejelentés köteles biztonsági eseményeket,
  - meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (például súlyosság szerinti) kritériumrendszerét,
  - támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,
  - meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.
- A szervezet kihirdeti és ismerteti a biztonsági eseménykezelési tervet – ide értve annak változásait is – a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek, nyilatkoztatja őket annak tudomásulvételéről.
- A szervezet kötelezettsége, hogy a biztonsági eseménykezelési tervet:
  - meghatározott gyakorisággal felülvizsgálja,
  - frissítse, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat.
- A szervezet kötelezettsége, hogy gondoskodjon arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.
- A szervezet kötelezettsége, hogy képzést biztosítson az elektronikus információs rendszer felhasználói számára a feladatellátásban kijelölt szerepkörükkel és felelősségeikkel összhangban. A képzést:
  - a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy
  - az elektronikus információs rendszer változásainak függvényében, vagy
  - meghatározott gyakorisággal köteles megtartani.

A fentiek alapján rögzíthető, hogy a 3. biztonsági osztályba sorolt elektronikus információs rendszer esetén az eseménykezelés adminisztratív védelmi oldalról minden elemre kiterjed. Tartalmazza a szabályozási feladatokat, a fentiekben említett PreDeCo elvhez és az Ibtv. 6. §-ban előírtakhoz igazodva az észlelési és beavatkozási pontokat (figyelés, jelentés, kezelés), valamint a képzéssel összefüggő intézkedéseket.

4. biztonsági osztálytól kötelező intézkedések köre:

a) Automatizált jelentés. A szervezet automatizált mechanizmusokat (például folyamattámogató alkalmazás) alkalmaz, hogy segítse a biztonsági események jelentését.

b) Automatizált támogatás biztosítása. a szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.

c) Biztonsági események kezelésének tesztelése. A szervezet meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, és dokumentálja az eredményeket.

d) Egyeztetés. a szervezet egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért (például üzletmenet-folytonossági terv és katasztrófa elhárítási terv) felelős szervezeti egységekkel.

5. biztonsági osztálytól kötelező intézkedések köre:

a) Automatikus eseménykezelés. A szervezetnek automatizált mechanizmusokat kell alkalmaznia az eseménykezelési eljárások támogatására (például folyamattámogató alkalmazás).

b) Információ korreláció. A szervezet a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat összekapcsolja annak érdekében, hogy szervezetszintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és a reagálásokra.

c) *Automatikus nyomonkövetés, adatgyűjtés és vizsgálat.* A szervezet automatizált mechanizmusokat (például figyelő rendszerek) alkalmaz annak érdekében, hogy segítse a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését és vizsgálatát.

d) Biztonsági események szimulációja. A szervezet köteles a biztonsági esemény kezelési képzésébe szimulált eseményeket belefoglalni, annak érdekében, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.

e) Automatizált képzési környezet biztosítása. A szervezet automatizált mechanizmusokat alkalmaz, hogy biztonsági esemény kezelési képzéséhez mélyrehatóbb és valószerűbb környezetet biztosítson.

A 4. és 5. biztonsági osztályba sorolt elektronikus információs rendszerek esetében az eseménykezelés adminisztratív védelmi oldalról – a 3. biztonsági osztály esetén rögzítetteken túl – az automatizált folyamatokat és a rendszerszintű szabályozás követelményét határozza meg.

A BM rendelet 4. mellékletének 3. alcíme (Védelmi intézkedési katalógus) az *Adminisztratív védelmi intézkedések* között szervezeti szintű alapfeladatként[40] írja elő az informatikai biztonsági szabályzat (a továbbiakban: IBSZ) készítését, aminek tartalmaznia kell:

a) a biztonsági helyzet-, és eseményértékelés eljárási rendjét,

b) a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárást, ideértve a helyreállításra vonatkozó rendelkezéseket is.

Tekintettel arra, hogy az IBSZ elkészítése már 1-es biztonsági osztályba sorolt elektronikus információs rendszer esetén is kötelező, az eseménykezelés szabályozási oldalon már a legkisebb szinten, mintegy alapvetésként megjelenik azzal, hogy annak részletezettsége és minősége szigorodik a magasabb osztályba sorolási érték esetén.

A BM rendelet 4. mellékletének 3. alcíme (Védelmi intézkedési katalógus) a *Fizikai védelmi intézkedések*[41] között is rögzít a fizikai biztonsági esemény (például fizikai behatolás) észlelésére és

[40] BM rendelet 4. melléklet 3. alcím 3.1.1. alpontja.

[41] BM rendelet 4. melléklet 3. alcím 3.2.1. alpontja.

reagálására, valamint annak naplózására vonatkozó feladatokat. Ha a jogosulatlan fizikai hozzáférésre utaló információ áll rendelkezésre, a szervezet kötelezettsége, hogy összehangolja a biztonsági események kezelését, valamint a naplóátvizsgálások eredményét.

Meg kell jegyezni, hogy a *biztonsági esemény* fentebb rögzített fogalmi meghatározását alapul véve jogértelmezési kérdésként merülhet fel, hogy a fizikai biztonsági események e fogalmi körbe tartoznak vagy sem. Nehezíti a válaszadást, hogy a *súlyos biztonsági esemény* fent említett fogalma informatikai eseményt rögzít. Álláspontunk szerint a fizikai biztonsági események e körben kezelendők, hiszen a *zárt védelem* fogalmi meghatározása – amely alapján az összes számításba vehető fenyegetést figyelembe kell venni – ezt támasztja alá.

A BM rendelet 4. mellékletének 3. alcíme (Védelmi intézkedési katalógus) a *Logikai védelmi intézkedések*[42] között (Rendszer- és információsértetlenség) előírja a biztonsági riasztások és tájékoztatások kezelésének körében a szervezet részére, hogy:

a) folyamatosan figyelje a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
b) folyamatosan kísérje figyelemmel a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
c) szükség esetén belső biztonsági riasztást és figyelmeztetést adjon ki, és juttassa el az érintett személyekhez;
d) alakítsa ki és működtesse esemény bejelentési kötelezettség rendszerét;
e) megfelelő ellenintézkedéseket és válaszlépéseket tegyen biztonsági esemény bekövetkezése esetén.

Fentiek mellett a szervezet kötelezettsége, hogy olyan naplózási eljárásrendet alakítson ki, amely elősegíti az elszámoltathatóságot. A naplóbejegyzésekben elegendő információ begyűjtésére kerüljön sor annak érdekében, hogy ki lehessen mutatni milyen események történtek, azok miből származtak, és mi volt ezen események kimenetele.[43]

A BM rendeletben rögzített minden védelmi intézkedési forma tartalmaz előírást arra vonatkozóan, hogy az Ibtv-ben meghatározott zárt, teljes körű, folytonos és a kockázatokkal arányos védelem előírásai a szabályozás és a gyakorlat szintjén egyaránt megvalósuljanak.

2.3. Az eseménykezelésben részt vevő nemzeti szervezetek köre

Az Ibtv. nevesíti és meghatározza azokat a szervezeteket, amelyek részére az elektronikus információbiztonsággal összefüggésben feladat- és hatáskört telepített a jogalkotó. A továbbiakban kizárólag azokat a nemzeti szervezeteket nevesíti jelen alcím, amelyeknek az eseménykezeléssel összefüggésben feladatuk van, és csak ezeket a feladatokat vesszük sorra.

Az Ibtv. a hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét a Kormány által kijelölt hatóság (továbbiakban: Hatóság) látja el.[44] A hatósági feladatokat jelenleg a Nemzetbiztonsági Szakszolgálat látja el.[45]

A Hatóság feladata[46] az eseménykezeléssel összefüggésben és ahhoz kapcsolódóan:

a) a biztonsági eseményekkel kapcsolatos bejelentések kivizsgálására irányuló hatósági eljárást megindítása;

[42] BM rendelet 4. melléklet 3. alcím 3.3.11.1. alpontja.
[43] BM rendelet 4. melléklet 3. alcím 3.3.12. alpontja.
[44] Ibtv. 14. § (1) bekezdés.
[45] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Kormányrendelet 2. §-a.
[46] Ibtv.14. § (2) bekezdése és 15. § (1) bekezdés.

b) az eseménykezelő központokkal való kapcsolattartás;
c) a biztonsági eseményekkel kapcsolatos, az eseménykezelő központtól kapott értesítések nyilvántartása és kezelése.

A Hatóság a biztonsági esemény kivizsgálására kötelezheti a szervezetet, ha a szervezet a kötelezést nem teljesíti, bírságot szabhat ki.[47] A biztonsági esemény bekövetkezésének elhárítására fordított költségének megtérítésére kötelezi a szervezetet, ha a szervezet:

a) a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére vonatkozó hatósági felszólítást figyelmen kívül hagyja, vagy
b) a Hatóság által javasolt védelmi intézkedéseket önhibájából nem teljesíti, és ennek következtében az elektronikus információs rendszert olyan súlyos biztonsági esemény éri vagy annak közvetlen bekövetkezése fenyegeti, amely a szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár.[48]

A Hatóság jogosult véleményezési jogot gyakorolni a kormányzati eseménykezelő központnak az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban.[49]

Az Ibtv rögzíti,[50] hogy biztonsági esemény kivizsgálását a szervezet a Hatóság felhívása nélkül is kezdeményezheti – zárt célú elektronikus információs rendszerek, európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemek, valamint nemzetbiztonsági védelem alá eső szervezetek kivételével – a kormányzati eseménykezelő központnál vagy telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges szakértelemmel és infrastrukturális feltételekkel rendelkező gazdálkodó szervezetnél.

A Kormány eseménykezelő központként (a továbbiakban: Központ) a Nemzetbiztonsági Szakszolgálatot jelöli ki. A Központ ellátja az alábbi feladatokat:

a) a biztonsági események nemzeti szintű nyomon követése;
b) a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatás, korai előrejelzés, riasztás, bejelentéstétel és információterjesztés az érdekeltek számára;
c) reagálás a biztonsági eseményekre;
d) dinamikus kockázat- és eseményelemzések, valamint a biztonsági eseményekkel kapcsolatos helyzetkép készítése;
e) sérülékenységvizsgálat lefolytatása.[51]

A Központ a biztonságiesemény-kezelési feladatkörében felelős a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítéséért, a biztonsági eseményekről nyilvántartás vezetéséért, valamint a külön kormányrendelet szerinti korai figyelmeztető rendszer működtetéséért.[52]

[47] Ibtv. 18. § (1) bekezdés.
[48] Ibtv. 16. § (6) bekezdés.
[49] Ibtv. 16. § (1) bekezdése.
[50] Ibtv. 18. § (2)–(9) bekezdései.
[51] 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól, 3. § (6) bekezdés.
[52] 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól, 4. §.

3. Eseménykezelés a NIS irányelv tükrében

3.1. A NIS irányelv és ami mögötte van

Az ezredfordulót követő gazdasági, társadalmi és technológiai változások (gazdasági világválság, terrorizmus és kiberhadviselés, okoseszközök terjedése) stratégiai szintű és jövőbe mutató tervezést igényeltek az Európai Uniótól. A felmerült kihívásokra válaszul a fenntartható fejlődést megcélzó, hosszú távú, jellemzően 2020-ig szóló stratégiai tervdokumentumok születettek. Ezen tervezési időszak fókuszában a tudáson és innováción alapuló gazdaság és társadalom kialakítása szerepel.

Az Európai Unió Tanácsa a felmerült kihívásokra válaszul kiemelten foglalkozott az információbiztonság kérdésével, és 2009-ben állásfoglalást fogadott el „a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről", amely pályára állította az Európai Uniót az információbiztonság tárgykörét illetően.

A 2010-ben elfogadott Europa 2020 foglalkoztatási és növekedési stratégia (a továbbiakban: Europa 2020 stratégia) célja, hogy megteremtse az intelligens (hatékonyabb oktatási, kutatási és innovációs beruházások, valamint a digitális társadalom fejlesztése), fenntartható (erőforrás-hatékonyabb, környezetbarátabb és versenyképesebb gazdaság) és inkluzív (a gazdasági, szociális és területi kohéziót előmozdító, magas foglalkoztatási arányt biztosító gazdaság) növekedés feltételeit. Ez az alapdokumentum az európai uniós intézményeknek és a tagállamoknak a közös stratégiája, azaz valamennyi címzettnek azonosulnia kell célkitűzéseivel, továbbá úgy kell működniük, hogy az azok végrehajtását szolgáló ütemezett intézkedések megvalósuljanak.

Ezen intézkedések végrehajtása érdekében hét kiemelt kezdeményezés indult, amelyek közül jelen jegyzet tárgyát tekintve az *Intelligens növekedés* célrendszerén belül az *Európai digitális menetrendet* (a továbbiakban: digitális menetrend) kell vizsgálni, amelynek célja, hogy a digitális technológia előnyei az európai polgárok és vállalkozások számára minél szélesebb körben elérhetők legyenek.

A digitális menetrend keretében tervezett intézkedések igen széles kört foglalnak magukba, ide tartozik:

- az egységes digitális piac megteremtése;
- az uniós adatvédelmi szabályozási keret felülvizsgálata,
- a távközlési szolgáltatások egységesítése,
- a fokozott interoperabilitás és szabványok,
- a készülékek, alkalmazások, adattárolók, szolgáltatások és hálózatok átjárhatóságának növelése,
- a bizalom és az internetes biztonság megerősítése,
- a nagy sebességű és szupergyors internet-hozzáférés biztosítása,
- befektetés a kutatásba és az innovációba,
- a digitális jártasság, a digitális készségek és a digitális integráció előmozdítása,
- a technológia intelligens használatából eredő előnyök hasznosítása a társadalom számára.

A fentebb felsorolt intézkedések közül az uniós adatvédelmi szabályozási keret felülvizsgálata közvetlen, a fokozott interoperabilitás, valamint az internetes biztonság megerősítése, továbbá a készülékek, alkalmazások, adattárolók, szolgáltatások és hálózatok átjárhatóságának növelése közvetetten járult hozzá ahhoz, hogy az Európai Unió az információs rendszerek megbízhatósága és biztonsága érdekében további intézkedéseket tervezzen. Ezen elv érvényesítése érdekében a digitális menetrend hét beavatkozási területe közül a *Bizalom és biztonság intézkedési területen* célként került meghatározásra:

a) javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;

b) a számítógépes támadások elleni gyorsreagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok (a továbbiakban: CERT) hálózatának létrehozása, az Európai Hálózat- és Információbiztonsági Ügynökség (a továbbiakban: ENISA) szerepének megerősítése;
c) javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról;
d) a tudatosságnövelés, a biztonságos internethasználat iskolai oktatása;
e) a gyermekbántalmazással, a személyazonosság-lopással és a számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása;
f) a magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten és azon kívül egyaránt.

Ezen intézkedések szükségességét az ismétlődő adatlopások kiemelkedő száma – amelyek során mind személyes, mind üzleti adatok jogosulatlan megszerzésére sor kerülhet –, az adatokat tároló elektronikus információs rendszerek sebezhetősége, valamint az ezek hatására bekövetkező működési zavarok, időszakos szolgáltatás-kiesések is indokolták, mivel ezeknek hatásuk van a gazdaság és az állam működésére, a társadalom tagjainak életére.

A stratégiai tervdokumentáció részeként a digitális menetrendben kitűzött célok érvényesítése érdekében került sor a kiberbiztonság kérdéskörének átfogó rendezésére, amelynek keretében az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága 2013 februárjában közzétették közös közleményüket *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* című uniós stratégiáról (a továbbiakban: kiberstratégia). A kiberstratégia az alábbi prioritásokat határozza meg:

a) kibertámadásokkal szembeni ellenálló képesség megteremtése;
b) a számítástechnikai bűnözés és a kibertámadások visszaszorítása;
c) kibervédelmi politika kidolgozása és a kiberképességek fejlesztése;
d) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások biztosítása;
e) a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése;
f) számítógépes bűnözéssel foglalkozó nemzeti kiválósági központok hálózatának kialakítása és finanszírozása.

Fenti tervdokumentációkhoz kapcsolódóan került megalkotásra az Európai Parlament és a Tanács 2016/1148 irányelve (2016. július 19.) a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről (továbbiakban: NIS irányelv).

A NIS irányelv 2016. augusztus 8-án lépett hatályba. Uniós jogi normaként sajátossága, hogy az elérendő célt tekintve valamennyi címzett tagállamot kötelezi a végrehajtásra azáltal, hogy a nemzeti hatóságok szabadon dönthetnek arról, hogy milyen módszerek és eszközök alkalmazásával teszik az irányelv szabályait a nemzeti jog részévé. A NIS irányelv rendelkezéseit 2018. május 9-ig kellett átültetni, azaz ezen időpontig szükséges Magyarországnak a jogi szabályozását áttekinteni és az irányelvben foglaltakhoz harmonizálni.[53]

A NIS irányelv alapvetése a hálózati és információs rendszerek és szolgáltatások megbízhatósága és biztonsága, mivel ezen információs rendszereknek és szolgáltatásoknak kiemelt szerepük van az áruk, szolgáltatások és személyek határokon átnyúló mozgásának támogatásában, azok szabad áramlásában. Ezen információs hálózatoknak a működési problémái, adott esetben a szolgáltatáskiesések nemcsak az egyes tagállamokra vannak kihatással, hanem több tagállamra vagy akár az egész Eu-

[53] Stratégiai dokumentumként elfogadásra került a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat, az érintett jogszabályok pedig 2018. május 9-ig harmonizálásra kerültek.

ropai Unióra is, a cselekmény irányultságától és az adott rendszer jellegétől (kritikus infrastruktúra vagy sem) függően.

A NIS irányelv kitér arra, hogy a fenyegetettségek egyre összetettebbek, a biztonsági események nagyságrendje, gyakorisága és hatása folyamatosan növekszik, amelyek komoly kockázatot jelentenek a hálózati és az információs rendszerek működésére nézve. A működés akadályozására vagy megszakítására irányuló szándékos és célzott cselekmények, ha azokból biztonsági esemény keletkezik, hátrányos hatást gyakorolnak az Európai Unió gazdaságára, jelentős pénzügyi veszteségeket, a felhasználói bizalom elvesztését és súlyos károkat okozhatnak.

A fenyegetettségekből kialakuló biztonsági események megelőzésére és kezelésére az Európai Unió tagállamai eltérő módon vannak felkészülve, ezért a NIS irányelv célja, hogy kialakítsa a hálózati és információs rendszerek biztonságának általános szintjét az unión belül, és egyenlő versenyfeltételeket biztosítson az összes tagországra vonatkozó harmonizált szabályozás bevezetésével.

Az egységes szabályozás és a gyakorlati végrehajtás támogatása érdekében a NIS irányelv meghatározza a *biztonsági esemény* és a *kockázat* fogalmát (hasonló fogalmat rögzít az Ibtv. is – lásd a 2.2. alfejezetben). E szerint *biztonsági eseménynek* kell tekinteni minden olyan eseményt, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára.[54] A NIS irányelv szerint minden olyan észszerűen azonosítható körülményt vagy eseményt, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára *kockázatnak* kell tekinteni.[55] Minden észszerűen számításba vehető kockázatra és biztonsági eseményre kiterjedő szabályozás érdekében a NIS irányelv hatálya kiterjed az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra.

A NIS irányelv szerint *alapvető szolgáltatásokat nyújtó* szereplőnek kell tekinteni azt az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és az ivóvízelosztás, valamint a digitális infrastruktúra ágazatban működő – tagállami szinten kijelölésre kerülő – közjogi vagy magánjogi szervezetet, amely megfelel az alábbi kritériumoknak:[56]

a) a szervezet a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt;
b) az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ, és
c) az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.

Digitális szolgáltatónak minősül a NIS irányelv alapján minden digitális szolgáltatást nyújtó szereplő. Az irányelv az online piacteret, az online keresőprogramot és a felhőalapú számítástechnikai szolgáltatást tekinti digitális szolgáltatásnak.[57]

Nem terjed ki a NIS irányelv hatálya:

- a mikro- és kisvállalatokra,
- más EU-szintű IT-biztonságot érintő ágazati szabályozás hatálya alá tartozókra, például kritikus infrastruktúra (nemzeti jogban létfontosságú rendszerelem),
- a nemzeti ágazati kijelölési kritériumokat nem teljesítő alapvető szolgáltatást nyújtó szereplőkre,
- a hardvergyártókra, szoftverfejlesztőkre.

[54] NIS irányelv 4. cikk 7. pont.
[55] NIS irányelv 4. cikk 9. pont.
[56] NIS 4. cikk 4. pont, 5. cikk 2. pont.
[57] NIS 4. cikk 6. pont, III. melléklet.

Szükséges megjegyezni, hogy a NIS irányelv csak az alapvető szolgáltatásokat nyújtó szereplőként azonosított közigazgatási szervekre alkalmazandó, a hatálya nem alá nem tartozó közigazgatási szervek hálózati és információs rendszereinek biztonságáról a tagállamoknak kell gondoskodniuk.

A NIS irányelv védett jogi tárgya az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók hálózati és információs rendszere,[58] amely:

a) a 2002/21/EK irányelv[59] 2. cikkének a) pontja szerinti elektronikus hírközlő hálózat,
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, vagy
c) az általuk működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

A hálózati és információs rendszerek biztonságának a NIS irányelv az arra való képességet tekinti, hogy ezek a rendszerek adott bizonyossággal ellenálljanak az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszeren nyújtott vagy azon keresztül elérhető, kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát.[60] (Az Ibtv. a *biztonsági esemény* fogalmánál rögzíti az elektronikus információs rendszer által hordozott információ bizalmasságát, sértetlenségét, hitelességét és rendelkezésre állását. A szabályozások közötti fogalmi alapvetés összhangja tehát tetten érhető.)

Az alapvető szolgáltatásokat nyújtó szereplőknek és a digitális szolgáltatóknak, továbbá a tagállami és uniós szereplőknek egyaránt meg kell hozniuk minden olyan védelmi intézkedést, amelyek a hálózati és információs rendszerek valós biztonságát garantálják. A rosszul kiválasztott, hibás vagy eredménytelen védelmi intézkedések biztonsági esemény bekövetkezéséhez vezethetnek, amely jelentős zavart okoz a szolgáltatás nyújtásában, és amely elhárítása (megelőzése) megfelelő eljárásrend kidolgozását igényli.

3.2. A NIS eszközrendszere

A NIS irányelv szerint az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó biztonsági követelményeknek arányosaknak kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal, azaz a kockázatokkal arányos védelem alapelvét rögzíti alapvetésként. Ez a követelményrendszer az alapvető szolgáltatásokat nyújtó szereplők tekintetében jelentkező kockázatok esetében magasabb biztonsági igényeket rögzít, mint a digitális szolgáltatók vonatkozásában, mivel az alapvető szolgáltatók működőképességének fenntartása elengedhetetlen a kritikus társadalmi és gazdasági tevékenységek fenntartásához.

A követelményrendszer kialakítása tekintetében a NIS irányelv olyan többszintű rendszer kialakítását célozza, amelyben az alapvető szolgáltatásokat nyújtó szereplőkön és a digitális szolgáltatókon túl a tagállami hatóságokra és más uniós szervekre is kiterjednek az egymással összefüggő és egymásra épülő kötelezettségek, amelyhez végrehajtandó feladattűzések is társulnak.

Az alapvető szolgáltatást nyújtó szereplőkre a NIS irányelv különféle biztonsági követelményeket állapít meg:[61]

[58] NIS 4. cikk 1. pont.
[59] Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról.
[60] NIS 4. cikk 2. pont.
[61] NIS irányelv 14. cikk (1)–(3) bekezdés.

a) megfelelő és arányos műszaki és szervezési intézkedések megtétele a működés során használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében, azzal, hogy az intézkedéseknek biztosítaniuk kell a felmerülő kockázatok alapján azonosított biztonsági szintet;
b) az alapvető szolgáltatások folytonosságát biztosító intézkedések megtétele a szolgáltatásnyújtáshoz igénybe vett és alkalmazott hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére;
c) az alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak.

A digitális szolgáltatók esetében az adott hálózati és információs rendszert érintő, kockázatokkal arányos biztonsági követelményeket kell számításba venni,[62] azzal, hogy ezek a követelmények – a fentiekben ismertetett kivételi szabály alkalmazása miatt – a mikro- és kisvállalkozásokra nem alkalmazhatóak:

a) megfelelő és arányos műszaki és szervezési intézkedések meghatározása és megtétele a digitális szolgáltatás Európai Unión belül történő nyújtása során használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében, azzal, hogy az intézkedéseknek biztosítaniuk kell a felmerülő kockázatoknak megfelelő biztonsági szintet, és figyelembe kell venniük a következő tényezőket:
    1. a rendszerek és a létesítmények biztonságát,
    2. a biztonsági események kezelését,
    3. az üzletmenetfolytonosság-menedzsment követelményét,
    4. a monitoring, az ellenőrzés és a vizsgálat követelményét,
    5. a nemzetközi szabványoknak való megfelelést;
b) digitális szolgáltatások folytonosságát biztosító intézkedések megtétele annak érdekében, hogy megelőzzék és csökkentsék a hálózati és információs rendszereik biztonságát érintő biztonsági eseményeknek a digitális szolgáltatásokra gyakorolt hatásait;
c) a digitális szolgáltatásaik folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak.

Ha az érvényesített biztonsági követelmények ellenére olyan biztonsági esemény következik be, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára,[63] szükséges lefolytatni az adott biztonsági esemény észlelését, elemzését és elszigetelését, valamint az eseményre való reagálást biztosító és támogató eljárásokat[64] (lásd hozzá jelen anyag 2.2. alfejezetét, az Ibtv.-nél alkalmazott PreDeCo elvet).

A NIS irányelv mind az alapvető szolgáltatást nyújtó szereplőkre és mind a digitális szolgáltatókra elsődlegesen a jelentős zavart okozó biztonsági események bejelentési kötelezettségét írja elő, azzal, hogy a zavar jelentőségének meghatározásához a tagállamoknak ágazatközi és ágazatspecifikus tényezőket kell figyelembe venniük.

Ágazatközi tényezőknek minősülnek legalább az alábbiak:

a) az érintett szervezet által nyújtott szolgáltatásokat igénybe vevő felhasználók száma (akár közvetlenül, akár közvetetten – például digitális szolgáltatón mint közvetítőn keresztül – veszik igénybe az adott szolgáltatást);
b) az adott szolgáltatást nyújtó szereplők függelmi helyzete a jelentős zavart okozó biztonsági eseménnyel érintett szervezet által nyújtott szolgáltatásoktól;

[62] NIS irányelv 16. cikk (1)–(3) bekezdés.
[63] NIS irányelv 4. cikk 7. pont.
[64] NIS irányelv 4. cikk 8. pont.

c) a biztonsági események hatása – mértéküket és időtartamukat tekintve – a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra;
d) a jelentős zavart okozó biztonsági eseménnyel érintett szervezet piaci részesedése;
e) az adott biztonsági esemény által esetlegesen érintett terület földrajzi kiterjedése;
f) a jelentős zavart okozó biztonsági eseménnyel érintett szervezet jelentősége a szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is.[65]

Az ágazatspecifikus tényezők meghatározása igen szerteágazó, tételes ismertetése nem célja jelen jegyzetnek, amelynek kereteit meg is haladná, így példálózó jelleggel rögzíthetjük, hogy ilyen tényező lehet az egészségügyi ágazat tekintetében az, hogy a biztonsági eseménnyel érintett szolgáltató évente mennyi beteget lát el, vagy a vízszektort illetően az, hogy a szolgáltató milyen személyi és szervezeti körnek és milyen földrajzi kiterjedéssel szolgáltat.

Az előírás szerint az alapvető szolgáltatást nyújtó szereplőket és a digitális szolgáltatókat az ágazatközi és az ágazatspecifikus tényezők ismeretében egyaránt bejelentési kötelezettség terheli a jelentős zavart okozó biztonsági esemény tekintetében az illetékes hatóság felé. A tagállam által kijelölendő ezen nemzeti illetékes hatóság – amely akár több hatóság is lehet, és már létező is megbízható ezzel a feladattal – felel a hálózati és információs rendszerek biztonságáért.[66]

Kérdés, hogy Magyarországon mely már meglévő hatóság kapja ezt a feladat- és hatáskört, például a Nemzeti Adatvédelmi és Információszabadság Hatóság, a Nemzeti Elektronikus Információbiztonsági Hatóság vagy a Kormányzati Eseménykezelő Központ.

Ez a kijelölt hatóság lehet nemzeti szinten az egyedüli kapcsolattartó pont, és ilyen minőségében összekötő feladatokat lát el a tagállami hatóságok között, és a többi tagállam érintett hatóságaival, az uniós szintű együttműködési csoporttal, valamint a számítógép-biztonsági eseményekre reagáló csoportok hálózatával.[67]

Bűncselekmény elkövetésnek gyanújával összefüggésbe hozható biztonsági esemény esetén az illetékes hatóságoknak és az egyedüli kapcsolattartó pontnak együtt kell működnie az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal. Az adatvédelmi hatóságokkal további együttműködési kötelezettség áll fenn a személyes adatok biztonsági eseményekből eredő bármely megsértése esetén is.

A nemzeti intézményrendszer részét képezik a tagállamok által kijelölt, a kockázatok és a biztonsági események kezeléséért felelős szervezetek, az úgynevezett számítógép-biztonsági eseményekre reagáló csoportok (a továbbiakban: CSIRT-ek).[68]

A CSIRT-ek feladatkörébe tartozik:

a) a biztonsági események nemzeti szintű monitoringja;
b) a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára;
c) reagálás a biztonsági eseményekre;
d) kockázat- és eseményelemzés, valamint helyzetkép nyújtása;
e) a CSIRT-ek hálózatában való részvétel.

Ha a CSIRT-ek nem kapják meg közvetlenül a nemzeti intézményektől a biztonsági eseményekről szóló bejelentéseket, úgy az intézményeknek hozzáférést kell biztosítaniuk az alapvető szolgáltatásokat nyújtó szereplők, illetve a digitális szolgáltatók által bejelentett biztonsági események adataihoz.

[65] NIS irányelv 6. cikk (1) bekezdés.
[66] NIS irányelv 8. cikk (1) bekezdés.
[67] NIS irányelv 8. cikk (3)–(5) bekezdés.
[68] NIS irányelv 9. cikk.

Tagállami és uniós szinten egyaránt megvalósul az együttműködés, stratégiai szinten a tagállamok, az Európai Bizottság és az ENISA képviselőiből álló együttműködési csoport[69] keretében, operatív szinten a CSIRT-ek hálózatán[70] belül (például biztonsági eseményre vonatkozó információmegosztás).

A NIS irányelv lehetőséget biztosít a biztonsági esemény önkéntes bejelentésére is a hatálya alá nem tartozó szervezetek esetében is, ha a szervezet megítélése alapján a bejelentés közérdeket szolgál, és a biztonsági esemény jelentős zavart okozhat az általuk nyújtott szolgáltatásokban. A bejelentéseket, ha az nem jelent aránytalan vagy indokolatlan terhet az érintett tagállamok számára, az illetékes hatóságoknak vagy a CSIRT-nek kell feldolgozniuk.

A szakanyag lezárását követően a Tanács 2019. április 9-én elfogadta azt a kiberbiztonsági jogszabályként is ismert rendeletet, amely lehetővé teszi az EU számára, hogy célzott korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést jelentenek az EU vagy annak tagállamai számára.[71]

2020 decemberében az Európai Bizottság és az Európai Külügyi Szolgálat (EKSZ) új uniós kiberbiztonsági stratégiát terjesztett elő.[72] E stratégia célja, hogy:

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

2021. november 26-án az Európai Unió Tanácsa elfogadta az EU egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekkel kapcsolatos álláspontját, amely intézkedések célja, hogy tovább javuljon mind az állami, mind a magánszektornak, illetve az Unió egészének kiberrezilienciája és a kiberbiztonsági eseményekre való reagálási képessége. Elfogadását követően az új, „NIS 2” elnevezésű irányelv a hálózati és információs rendszerek biztonságáról szóló jelenlegi irányelv (NIS-irányelv) helyébe lép.[73]

4. Eseménykezelési elvárások a GDPR szabályozásában

4.1. Adat- és információvédelem, adat- és információbiztonság

Az Európai Unió Általános Adatvédelmi Rendeletének értelmezése nem végezhető el az *adatvédelem* és az *információbiztonság* fogalmi alapjainak felvázolása nélkül, mivel az állam, a gazdaság és a társadalom minden irányába folyamatosan növekszik a bekövetkezett biztonsági fenyegetések és a biztonsági események száma. Ahogy azt korábban már említettük, ezen események nemcsak az elektronikus információs rendszerek kitettségére és az elektronikus információk sebezhetőségére, hanem az adatvédelem fontosságára is rávilágítottak. De van-e különbség adat- és információvédelem, illetve adatbiztonság és információbiztonság között? E kérdések megválaszolására jelen jegyzet

[69] NIS irányelv 11. cikk.

[70] NIS irányelv 12. cikk.

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

[72] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér; http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001

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

keretein belül kizárólag a gyakorlati szempontból történő rendszertani alapvetés rögzítése révén van lehetőség, a részletes kifejtés és ismertetés célját, témáját és terjedelmét tekintve is hosszabb elemzést igényelne, azonban ez a téma szempontjából most nem szükséges.

Fenti alapvetés mellett rögzítsük azt az állítást, hogy az *adat* közlésre, megjelenítésre vagy további feldolgozásra alkalmas entitás, amely számos megjelenési formát vehet fel (például: alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása. Az *információ* valamilyen megfigyelés, tapasztalat vagy ismeret, amely által következtetések vonhatók le, és döntések alapjául szolgálhat. Az információ, ha úgy tetszik nem más, mint a jelentéssel felruházott adat, azaz adatból akkor lesz információ, ha valamiről informál.[74]

Az *adat* és az *információ* eltérő jelentéstartalommal felruházott fogalmak, amelyek tartalmukat tekintve eltérő *védelem* és *biztonság* fogalommal rendelkeznek, különösen akkor, ha elfogadjuk azt az alapvetést, hogy *védelem* az a tevékenység, amely a *biztonság* állapotának elérésére szolgál.

Ezen meghatározásból kiindulva az *adatvédelem* központi eleme az adatkezelés jogszerűségét biztosító – főként szabályozási – tevékenységek, elsősorban a védelmet biztosító szabályok és eljárások, valamint az adatkezelési eszközök és módszerek összessége. Az adatvédelemmel szemben az *adatbiztonság* meghatározása alatt alapvetően az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében.

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

Az *információbiztonság* olyan követelményrendszerként jellemezhető, amely középpontjában a korábban már említett bizalmasság, sértetlenség, és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például: alfabetikus, numerikus, grafikus, képi forma), és milyen adathordozón jelenik meg. Ezen elv mentén rögzíthető, hogy az információbiztonság a biztonsági események megelőzése, kezelése kapcsán jellemzően az IT-üzemeltetés területén jelenik meg, ahol gyakorlatban az adatok, információs rendszerek fizikai, logikai, adminisztratív védelmére helyeződik a hangsúly. Érzékelhető, hogy ebben a szabályozási környezetben nem az adatvédelem és az adatbiztonság az először vizsgált elem.

A BM rendelet 1. melléklete szerinti biztonsági osztályba sorolásánál, illetve a szervezet 2. melléklet szerinti biztonsági szintjének meghatározásánál már jelentősége van a személyes adatok vagy azok különleges típusainak kezelésének, amely utal a kapcsolódó adatvédelmi előírásokra.

A személyes adatot kezelő vagy feldolgozó személy feladata többek között, hogy az adatokat megfelelő intézkedésekkel védje a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. Annak érdekében, hogy az adatokkal végzett tevékenységek, műveletek jól körbehatárolhatók legyenek, az Infotv. mintegy gyűjtő fogalomként meghatározza mi minősül:

[74] Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehérkönyvhöz (2016): Budapest, Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, 21. oldal alapján.

- adatkezelésnek[75] [az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése], valamint
- adatfeldolgozás[76] az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.

Fentiekhez igazodóan az Infotv. rögzíti az *adatkezelő*[77] és az *adatfeldolgozó*[78] fogalmát. Előbbi az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja. Adatfeldolgozó pedig az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.

Az Infotv. meghatározza az *adatvédelmi incidens*[79] fogalmát is, mely szerint az az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Ez a definíció összhangban áll az Ibtv. által alkalmazott *biztonsági esemény* fogalmával (lásd 2.2. alfejezet); ezek együttes értelmezésével az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosítása – jogi szempontból – könnyebben elvégezhető.

Itt kell megjegyezni, hogy az Infotv. 2018-as módosítására az Európai Unió Általános Adatvédelmi Rendeletének ismeretében, az új szabályoknak történő megfelelés és összhangba kerülés érdekében került sor, amelyhez kapcsolódóan az Infotv. számos új előírást rögzít.

Az adatkezelő az általa, illetve az adatfeldolgozó által kezelt adatokkal összefüggésben felmerült adatvédelmi incidens kapcsán az alábbi adatokat rögzíti és jelenti be a Hatóságnak:

- az adatvédelmi incidens jellege, érintettek köre és hozzávetőleges száma, az incidenssel érintett adatok köre és hozzávetőleges mennyisége;
- az adatvédelmi tisztviselő vagy a további tájékoztatás nyújtására kijelölt más kapcsolattartó nevéről és elérhetőségi adatai;
- az adatvédelmi incidensből eredő, valószínűsíthető következmények;
- az adatvédelmi incidens kezelésére tett vagy tervezett, a következmények mérséklését célzó és egyéb intézkedések.[80]

Továbbá az adatvédelmi incidenst haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő hetvenkét órán belül bejelenti a Hatóságnak.

[75] Infotv. 3.§ 10. pontja
[76] Infotv. 3.§ 17. pontja.
[77] Infotv. 3.§ 9. pontja.
[78] Infotv. 3.§ 18. pontja.
[79] Infotv. 3.§ 26. pontja.
[80] Infotv. 25/J. § (1) – (5) bekezdések.

Az Infotv. rögzíti, hogy ha az adatvédelmi incidens valószínűsíthetően az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következményekkel járhat (a továbbiakban: magas kockázatú adatvédelmi incidens), a nemzetbiztonsági célú adatkezelés kivételével az adatkezelő az érintettet az adatvédelmi incidensről haladéktalanul tájékoztatja.[81]

A fentieket összefoglalva rögzíthető, hogy *adatbiztonság* alatt az Infotv. a személyes adatok információbiztonságát érti.[82]

Személyes adatok feldolgozása során az Infotv. tovább pontosítja az adatbiztonsági elvárásokat,[83] ez esetben a védelmi intézkedéseknek biztosítania kell továbbá:

a. az adatkezeléshez használt eszközök jogosulatlan személyek általi hozzáférésének megtagadását;
b. az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását;
c. az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását;
d. az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását;
e. azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá;
f. azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére;
g. azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban, ki vitt be az adatkezelő rendszerbe;
h. a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását;
i. azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen, valamint
j. azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.

Emellett az Infotv. általános jelleggel kötelezi az adatkezelőt vagy adatfeldolgozót, hogy az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel legyen a technika mindenkori fejlettségére, és „az adatkezelő és az adatfeldolgozó a kezelt személyes adatok megfelelő szintű biztonságának biztosítása érdekében az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető – így különösen az érintettek különleges adatainak kezelésével járó – kockázatok mértékéhez igazodó műszaki és szervezési intézkedéseket tesz.”[84]

[81] Infotv. 25/K. § (1) bekezdés.

[82] A NAIH adatvédelmi szótárának megfogalmazása szerint: az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere. (Adatvédelmi szótár Elérhetőség: http://naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2017. április 20.)

[83] Infotv. 25/I.§ (3).

[84] Infotv. 25/I.§ (1).

4.2. GDPR alapok

2018. május 25-től valamennyi Európai Uniós tagállamban egységesen és közvetlenül alkalmazandó az Európai Unió Általános Adatvédelmi Rendelete[85] (angolul: General Data Protection Regulation, a továbbiakban: GDPR), amely közvetlen alkalmazhatósága miatt az irányelv rendelkezéseit átültető tagállami adatvédelmi jogszabályok, közöttük az Infotv. GDPR-ban már szabályozott tárgyköreinek a helyébe lép. Ennek következtében az Infotv. közérdekű és közérdekből nyilvános adatokra vonatkozó rendelkezései, valamint egyes, a GDPR által nem rendezett adatvédelmi előírások továbbra is hatályban maradnak [például a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH) kapcsolatos előírások nem változnak].

A GDPR a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelvet (a továbbiakban: Adatvédelmi irányelv) váltja fel. Bár az Adatvédelmi irányelv 17. cikke a személyes adatok kezelésének legfontosabb elveit, köztük az adatkezelés biztonságára vonatkozó szabályokat tartalmazza, az adatbiztonság megsértésének kezelésére nem ír elő kötelezettséget az adatkezelőnek. Az adatvédelmi reform kiemelt célja az volt, hogy a személyes adatok védelme és az információbiztonsági követelmények egységesen magas szintje és koherenciája biztosított legyen, ezáltal növekedjen a felhasználók új technológiákba és az online térbe vetett bizalma, felgyorsuljon az egységes európai digitális tér létrejötte.[86]

A GDPR a személyes adatokat kezelő szervezetek számára átfogó adatbiztonsági előírásokat tartalmaz, a megfelelősség bizonyítását széleskörű és részletes dokumentációhoz köti, továbbá már az adatok kezelésének megkezdése előtt kockázatalapú[87] tervezést és az adatvédelmi garanciák számba vételét várja el az adatkezelőtől. Az új szabályozás kiemelt figyelmet fordít az adatkezelési műveletekhez kapcsolódó technológiára (például titkosítás), és rögzíti, hogy minden adatkezelő köteles dokumentálni, bizonyos esetekben bejelenteni, valamint az érintetteket is tájékoztatni a személyes adatokat érintő incidensekről.

4.3. Adatbiztonság és adatvédelmi incidens a GDPR-ban és a kapcsolódó szabályok

A GDPR a fentiekben említett célok elérése és a kihívásoknak való megfelelés érdekében számos változást tartalmaz mind az adatvédelem, mind az adatbiztonság területén az Adatvédelmi irányelv és az Infotv. korábbi változatának előírásaihoz képest, ezért a szabályoknak történő megfelelésre két év felkészülési időt adott a jogalkotó. 2018. július 26-án hatályba lépett az Infotv. átfogó módosítása, így ennek eredményeként a törvény összhangba került az általános adatvédelmi rendelettel.

Az *adatbiztonság* 2018 májusáig hatályos általános megfogalmazását[88] kiegészíti a kockázatok értékelésével és a védekezés költségeinek mérlegelésével: „a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.”

---

[85] Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) – (a továbbiakban: GDPR).

[86] Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére. Brüsszel, 2010. május 19. Elérhetőség: https://ec.europa.eu/commission/presscorner/detail/hu/IP_10_581 (utolsó letöltés: 2022. április 6.)

[87] A GDPR 32. cikkének megfogalmazása szerint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével kell kialakítani az adatbiztonsági intézkedéseket.

[88] Adatvédelmi irányelv 17. cikk.

A GDPR az adatbiztonság területén elvárt védelmi intézkedéseket is felsorolja, és rögzíti, hogy ahol szükséges és lehetséges, ott:

- alkalmazni kell a személyes adatok álnevesített kezelését;[89]
- alkalmazni kell a technológiai titkosítását;
- biztosítani kell az adatkezelőnek vagy adatfeldolgozónak, hogy a személyes adatok kezelésére használt rendszerekben és szolgáltatásokban folyamatos védelmi intézkedések működjenek;
- biztosítani kell, hogy fizikai vagy műszaki incidens esetén rendelkezésre álljon a biztonsági mentés vagy tartalékrendszer;[90]
- a védelmi intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást kell az adatkezelőnek kialakítania.[91]

A GDPR rögzíti az *adatvédelmi incidens* fogalmát, mely szerint „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”[92] adatvédelmi incidensnek tekintendő. Érzékelhető, hogy azok a vétlen vagy jogellenes magatartások jelennek meg a definícióban, melyek a jelenlegi hazai szabályozást is jellemzik.

A fogalmi meghatározás elemzése alapján rögzíthető, hogy *adatvédelmi incidensnek* az információbiztonsági események csak azon típusai tekinthetők, amelyek a személyes adatok biztonságát sértik. További megállapítás, hogy minden olyan biztonsági esemény, amely akár csak egyetlen természetes személy adatát is hátrányosan érinti, már adatvédelmi incidensnek minősül, még akkor is, ha annak minimális az érintett magánszférájára gyakorolt hatása. Ez a tág fogalmi rendelkezés a nagyobb és a közvélemény számára is ismert, kiemelt hír- és kárértékkel rendelkező adatvesztések mellett, az üzemszerű adatkezelési tevékenységek során felmerülő emberi vagy technikai hibákra, téves adatkezelési műveletekre (például tévesen címzett személyes adatokat tartalmazó e-mail) visszavezethető „soft” eseményeket is bevonja a hatókörbe.

A GDPR Preambuluma rögzíti, hogy megfelelő és jól időzített védelmi intézkedések hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az adatvédelmi incidens az adatalanyoknak. A Preambulum ide sorolja „a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.”[93]

Azon adatvédelmi incidensekről, amelyek valószínűsíthetően magas kockázatot jelentenek a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek az érintettet indokolatlan késedelem nélkül tájékoztatnia kell, amelyben rögzíteni kell annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint az érintettnek a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatait. Az indokolatlan késedelem nélküli tájékoztatás célja, hogy az értesítés hatására olyan védelmi intézkedéseket tehessen az érintett adatainak védelme érdekében

[89] A GDPR 4. cikk 5. pontja meghatározása szerint álnevesítés: „a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.”

[90] A GDPR 32. cikk (1) c) pontja megfogalmazásában: „az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani.”

[91] GDPR 32. cikk (1) a)–d) pontjai.

[92] GDPR 4. cikk 12. pont.

[93] GDPR Preambulum (85).

– például jelszavának megváltoztatása annak kompromittálódása esetén, vagy elektronikus fizetőeszközének letiltatása – amelyekkel csökkentheti az incidens által okozott károkat.[94]

Az adatvédelmi incidensek bejelentési kötelezettségét előíró szabályozás célja és lényege, hogy a megtett bejelentés alapján:

a) a nemzeti hatóság a szükséges intézkedéseket megtegye és a bejelentések tartalmából akár egyes adatkezelői csoportokra, szolgáltatási területekre nézve is adatot szerezhessen az adatbiztonság tényleges helyzetére vonatkozóan;

b) az adatkezelő a személyes adatokat ért incidenseket felismerje, körülményeit felmérje, azokat megfelelően dokumentálja, amely alapján tervezhetővé válnak a szükséges védelmi intézkedések;

c) az adatkezelő – a jó hírnevét is veszélyeztető incidensek és a hozzájuk kapcsolódó értesítési kötelezettségek előfordulásának minimalizálása érdekében – jelentős erőforrásokat fordítson az adatbiztonság szintjének növelésére, az incidenssel érintettek számának, vagy a potenciális károknak a csökkentésére.[95]

Az adatvédelmi incidensek hatékony kezelése érdekében a GDPR 33. cikke előírja, hogy az adatvédelmi incidens bekövetkezését az adatkezelő indokolatlan késedelem nélkül – ha lehetséges, legkésőbb 72 órával az után, hogy az a tudomására jutott – köteles bejelenteni az illetékes felügyelő hatóságnak.[96] A GDPR a bejelentés főbb tartalmi elemeit is meghatározza az egységes kezelés érdekében, így többek között előírja, hogy a bejelentésben rögzíteni kell:

a) az adatvédelmi incidens jellegét (körülményei), és ha az lehetséges, az arra vonatkozó adatokat (érintettek köre és száma, az incidenssel érintett adatok köre);

b) az adatvédelmi tisztviselő vagy kapcsolattartó személyének nevét és elérhetőségeit;

c) az incidens várható hatását, következményeit;

d) az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket.[97]

Ha az adatkezelő a bejelentésre előírt 72 órás maximális határidőt elmulasztja, akkor a bejelentéséhez mellékelni köteles a késedelem igazolására szolgáló indokokat is.

Nem kell bejelentenie az adatkezelőnek a hatóság részére azokat az adatvédelmi incidenseket, amelyek „valószínűsíthetően nem jár[nak] kockázattal a természetes személyek jogaira és szabadságaira nézve.”[98]

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül köteles tájékoztatni az érintetteket is,[99] kivéve, ha korábban mások számára értelmezhetetlenné tette az incidenssel érintett adatokat, vagy az incidenst követően olyan további intézkedéseket tett, amelyekkel a kockázatokat érdemben csökkentette.[100]

A GDPR az adatfeldolgozó kötelezettségeként írja elő az adatvédelmi incidensek felismerését és jelzését, azzal, hogy a maximális 72 órás időtartam sem áll rendelkezésére az adatkezelő irányába történő bejelentés megtételére, mivel az adatfeldolgozó köteles indokolatlan késedelem nélkül tájékoztatást adni a biztonsági eseményről annak érdekében, hogy az adatkezelő a szükséges intézkedéseket megtegye.[101]

---

94 GDPR Preambulum (86).

95 Szőke Gergely László (2017): Értesítési kötelezettség az adatvédelmi incidensek esetén – elméleti és gyakorlati kérdések. *JURA,* 23. évf. 1. sz. 140–154.

96 GDPR 33. cikk (1) bekezdés.

97 GDPR 33. cikk (3) bekezdés.

98 GDPR 33. cikk (1) bekezdés.

99 GDPR 34. cikk (1) bekezdés.

100 GDPR 34. cikk (3) bekezdés.

101 GDPR 33. cikk (2) bekezdés.

Az adatvédelmi incidensekről az adatkezelő részére nyilvántartási kötelezettséget is előír a GDPR, amely nyilvántartásban rögzítenie kell:

a) az adatvédelmi incidenshez kapcsolódó tényeket és annak hatásait,

b) az adatvédelmi incidens orvoslására tett intézkedéseket,

azzal, hogy a nyilvántartásnak lehetővé kell tennie, hogy a felügyeleti hatóság ellenőrizhesse a bejelentési követelményeknek való megfelelést.[102] Ez a nyilvántartási kötelezettség minden adatvédelmi incidensre kiterjed, és az elszámoltathatóság elve[103] alapján az adatkezelő köteles igazolni az incidensek bejelentéséről vagy az érintett tájékoztatásának szükségességéről hozott döntését.

A felügyeleti hatóság a nyilvántartást áttekintve ellenőrizheti, hogy az adatkezelő helyesen mérlegelte-e az adatvédelmi incidens kockázatát.[104]

A bejelentési és nyilvántartási kötelezettség megsértése esetén az eljáró adatvédelmi hatóság az adatkezelőt vagy -feldolgozót 10 millió euróig terjedő közigazgatási bírsággal, vagy vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 százalékát kitevő összeggel sújthatja, azzal, hogy a két összeg közül mindig a magasabbat kell kiszabnia a hatóságnak.[105]

A fentiek ismertetésével összefüggésben meg kell jegyezni, hogy az általános, minden adatkezelőre kiterjedő nyilvántartási és bejelentési, illetve értesítési kötelezettség a GDPR egyik legjelentősebb változása. Emellett azt is ki kell emelni, hogy az adatvédelmi incidensekre vonatkozó előírások nem a GDPR-ban jelentek meg először az Európai Unió adatvédelmi jogában, ahogy az átültetéssel járó kodifikációs eredmények is helyet kaptak már a nemzeti jogban.

Az elektronikus hírközlési ágazatban 2009 óta vonatkoznak előírások a személyes adatok biztonsága sérülésének esetkörére.[106] Az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) ültette át az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK (2002. július 12.) az Európai Parlament és a Tanács irányelvének (a továbbiakban: EU e-hírközlési adatvédelmi irányelv) incidensekre vonatkozó előírásait. Az EU e-hírközlési adatvédelmi irányelve 2. cikk *i)* pontja szerint személyes adatok megsértése „a biztonság olyan megsértése, amely a Közösségben nyilvánosan elérhető hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elveszítését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.” Ezen szabályozásban is megjelenik a jogellenes magatartási formák felsorolása, azzal, hogy itt egy szűkebb adatkezelői kör, a hírközlési szolgáltatók a jogalanyok, és egyes magatartási formák hiányoznak (például véletlen vagy jogellenes adatkezelés vagy feldolgozás).

Az Eht. előírásai szerint az „előfizetői személyes adatok megsértését jelenti a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt, vagy más egyéb módon kezelt vagy feldolgozott személyes adatok véletlen, vagy jogellenes kezelése vagy feldolgozása, így különösen megsemmisítése, elvesztése, módosítása, jogosulatlan felfedése, nyilvánosságra hozatala, vagy az azokhoz való jogosulatlan hozzáférés.”[107]

Az Eht. hatálya alá tartozó hírközlési szolgáltatók kötelezettsége a személyes adatok megsértése esetén haladéktalanul, de legkésőbb 24 órán belül bejelentést tenni Nemzeti Média- és Hírközlési Hatóságnak (a továbbiakban: NMHH)[108]

---

[102] GDPR 33. cikk (5) bekezdés.

[103] GDPR Preambulum (85), valamint 5. cikk (2) bekezdésében foglaltak szerint.

[104] GDPR 33. cikk (5) bekezdés és 34. cikk (1) bekezdés.

[105] GDPR 83. cikk (4) bekezdés a) pontja alapján.

[106] Az Európai Parlament és a Tanács az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK (2002. július 12.) irányelv (a továbbiakban: EU elektronikus hírközlési adatvédelmi irányelv) rendelkezései közé a 2009/136/EK irányelv ültette át a kötelezettséget.

[107] Az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) 156. § (2) bekezdése.

[108] Eht. 156. § rendelkezései alapján.

A hírközlési szolgáltatókra vonatkozó rendelkezések szerint, ha egy incidens várhatóan hátrányosan érinti az előfizető vagy más magánszemély személyes adatait vagy magánéletét, erről az előfizetőt vagy magánszemélyt indokolatlan késedelem nélkül értesítenie kell a szolgáltatónak, amely kötelezettség alól csak akkor mentesülhet, ha igazolni tudja, hogy végrehajtotta a megfelelő technikai védelmi intézkedéseket (például technológiai titkosítás), illetve, hogy ezen intézkedéseket alkalmazták is az incidenssel érintett adatok tekintetében, és ezzel értelmezhetetlenné teszik azokat az adatokhoz jogosulatlanul hozzáférő számára.[109] Ez a rendelkezés a GDPR fentebb ismertetett azon előírásával állítható párhuzamba, amely szerint az érintettet nem kell indokolatlan késedelem nélkül tájékoztatni, ha „az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat."[110] A hírközlési szolgáltató az Infotv. nyilvántartási előírásához képest az Eht rendelkezése szerint speciális, azt helyettesítő incidensnyilvántartást köteles vezetni annak érdekében, hogy az NMHH ellenőrizni tudja, hogy a szolgáltató megfelelően értesítette-e az érintetteket, vagy az értesítés mellőzése esetén helyesen mérlegelte-e az incidens következményeit, illetve alkalmazta a technikai és védelmi intézkedéseket.[111]

Összegezve megállapítható, hogy az *adatvédelmi incidens* fogalmi meghatározása alapján (ideértve az Infotv. és az Eht. rendelkezéseit is) személyes adatokat jogellenes – célhoz kötöttség elvét figyelmen kívül hagyó, vagy tévesen meghatározott jogalappal történő – adatkezeléssel vagy a tájékoztatási kötelezettség elmulasztásával lehet megsérteni, és ez (az Ibtv. szerinti biztonsági vagy súlyos biztonsági esemény meghatározására figyelemmel) nem azonosítható egyértelműen a bizalmasság, sértetlenség, rendelkezésre állás követelményeinek együttes vagy egyenkénti megsértésével. A fogalmi összhang és a gyakorlati egységesítés a GDPR 2018-as kötelező alkalmazásától várható.

A GDPR tehát általános, a magas kockázatot nem jelentő biztonsági eseményekre is kiterjedő nyilvántartási kötelezettséget ír elő valamennyi adatvédelmi incidensre vonatkozóan, és tevékenységtől vagy szektortól függetlenül valamennyi adatkezelő részére; valamint maximalizálja az adatkezelő részére az incidens bejelentésére nyitva álló határidőt a tudomásszerzéstől számított legfeljebb 72 órában, amely az eddigieknél gyorsabb reagálási képességet követel meg.

Következtetésként vonható le továbbá, hogy mind az adatkezelőnek, mind az adatfeldolgozónak úgy kell megterveznie, kialakítania és szerveznie adatkezelési rendszereit, ügyviteli folyamatait, és úgy kell biztosítania az üzletmenet folytonosságát, hogy az adatvédelmi incidens(eke)t képes legyen felismerni, annak érdekében, hogy azokat nyilvántartásba vehesse, majd mérlegelhesse az érintettre vonatkozó várható kockázat mértékét, és még határidőben eleget tehessen az esetleges bejelentési és értesítési kötelezettségének. Mindezt úgy, hogy természetesen az incidens elhárításának és az ebből eredő károk kezelésének is eleget tegyen, Ehhez szükséges, hogy a szervezet belső szabályaiban az incidensek észlelésére és nyilvántartására vonatkozó felelősségi szabályokat, valamint a munkatársak feladatait rögzítse. Szükséges továbbá, hogy a prevenció jegyében továbbképzések, figyelemfelhívó üzenetek útján tájékoztassa a munkatársakat az adatvédelmi elvekről és alapfogalmakról, hogy ők is képesek legyenek az esetleges adatvédelmi incidensek azonosítására. Az érintettek értesítésére vonatkozó kötelezettségek miatt indokolt a technikai titkosítás és az álnevesítés alkalmazása a személyes adatokat tartalmazó adatbázisaikon. Ezek jelentős könnyebbséget jelenthetnek a szervezet számára a GDPR értesítési kötelezettsége alóli mentesülés miatt.

[109] Eht. 156. § (5) bekezdése.
[110] GDPR 34. cikk (3) bekezdés *a)* pontja.
[111] Eht. 156. § (4) bekezdés.

5. Intézkedési terv a biztonsági események kezelésére

Az Ibtv. a szervezet vezetőjének felelősségi körébe tartozóan rögzíti,[112] hogy a szervezet elektronikus információs rendszereinek védelme körében:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
d) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
e) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
f) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
h) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
i) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
j) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
k) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
l) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.[113]

Az Ibtv. szerint, ha a biztonsági osztályba és a biztonsági szintbe sorolás alkalmával az adott elektronikus információs rendszerre vonatkozóan hiányosságot állapítanak meg, vagy a szervezet biztonsági szintje alacsonyabb, mint az előírt alap biztonsági szint, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készíteni a hiányosság megszüntetésére és az előírt biztonsági szint elérésére.[114] A cselekvési terv készítése az elektronikus információs rendszer biztonságát érintő változás vagy új elektronikus információs rendszer bevezetésekor elvégzett soron kívüli felülvizsgálat esetén is kötelező, amennyiben a felülvizsgálat eredménye alapján meghatározott biztonsági szint alacsonyabb, mint a szervezetre vagy szervezeti egységre előírt alap biztonsági szint.[115]

A NIS irányelv és a GDPR nem tartalmazza nevesítve az eseménykezeléssel kapcsolatban (legyen az adatvédelmi incidens vagy biztonsági esemény) a cselekvési vagy az intézkedési terv készítését. Erre vonatkozó tételes norma az Ibtv. szabályai között lelhető fel.

[112] Ibtv. 11. § (1) bekezdés.
[113] Ibtv. 11. § (1) bekezdés.
[114] Ibtv. 8. § (5) bekezdés és 10. § (2) bekezdés.
[115] Ibtv. 8. § (2) és 10. § (6).

Mind a cselekvési, mind az intézkedési terv önálló dokumentum, amely a feladatszabás mellett a határidőket és az ütemezést, valamint a felelősök és a résztvevők körét is meghatározza, szükség esetén rögzíti a végrehajtást igénylő források körét is. Rögzíti továbbá a biztonsági események kezelésére szolgáló preventív és kárelhárító intézkedéseket is, amely intézkedések az elektronikus információs rendszerek biztonsági osztályba sorolása alkalmával elvégzett kockázatelemzéshez kapcsolhatók. Ezekbe a tervekbe a konkrét intézkedések meghatározása mellett az úgynevezett PDCA elv[116] beépítése is szükséges, mivel az eseménykezelésnél az ellenőrzés és annak tapasztalatainak visszacsatolása elengedhetetlen feltétel, hiszen ezáltal biztosítható az Ibtv. 6. §-ban rögzített – és a 2.2 alcímben említett PreDeCo elven alapuló – intézkedések köre.

6. Felhasznált irodalom

- *Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér könyvhöz* (2016). Budapest, Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete. Elérhető: https://fr.scribd.com/doc/314353569/Megalapozo-tanulmany-a-nemzeti-adatpolitikarol-szolo-FEHER-KONYVHOZ (utolsó letöltés: 2017. 04. 20.)
- Nemzeti Adatvédelmi és Információszabadság Hatóság adatvédelmi szótára. Elérhető: www.naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2017. 04. 20.)
- *Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére* (2010). Brüsszel. Elérhető: http://infoter.eu/attachment/0003/2807_com2010_0245hu01.pdf (utolsó letöltés: 2017. 04. 20.)
- Szőke Gergely László (2017): Értesítési kötelezettség az adatvédelmi incidensek esetén – elméleti és gyakorlati kérdések. *JURA,* 23. évf. 1. sz. 140–154.

[116] PDCA elv – (Plan-Do-Check-Act = Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás).

III. SÁGI GÁBOR – SEBŐK VIKTÓRIA: AZ ESEMÉNYKEZELÉS MŰSZAKI ESZKÖZTÁRA – ÜZEMELTETŐI, FEJLESZTŐI FELADATOK

1. Az incidensmenedzsment műszaki eszköztára – általános áttekintés

Az incidensmenedzsment tevékenységét támogató műszaki eszközök mennyiségét, fajtáját elsősorban a szervezet által üzemeltetett rendszerek, a szervezettel szemben támasztott jogi elvárások, illetve a rendelkezésre álló erőforrások határozzák meg. Kisebb, információbiztonsági szempontból kevésbé kockázatos rendszereket üzemeltető szervezetek általában nem alakítanak ki önálló szervezeti és műszaki infrastruktúrát az incidensek észlelésére, az incidensmenedzsment támogatására. Ugyanakkor nagyobb, információbiztonsági szempontból kockázatos rendszereket üzemeltető szervezetek a jogszabályi megfelelés, illetve a rendelkezésre álló erőforrások figyelembevételével, akár önálló egységként működő incidensmenedzsmentet végző szervezetet alakíthatnak ki, akár a többi – jellemzően IT – szervezeti egységtől független informatikai támogatással.

Az incidensmenedzsmentet[117] teljes folyamatában – informatikai biztonsági esemény észlelésére történő felkészüléstől, az esemény észlelésén, vizsgálatán át, az incidens lezárásáig –, ahogy az incidenskezelést folytató szakemberek munkáját is, számos, egymással általában összeköttetésben lévő, önálló vagy a felhőben működő informatikai eszköz, szolgáltatás támogatja.

Az incidensmenedzsment során a szervezet információs infrastruktúrájában működő rendszerek folyamatosan információt szolgálhatnak az incidenskezelők számára az incidens észlelését, elemzését, kezelését támogató rendszereken keresztül, valamint a szervezet ezzel párhuzamosan általában működtet az incidens vizsgálatát, illetve az incidenskezelési folyamatot támogató rendszert is. Az incidenskezelési folyamatok hatékonyságának érdekében ezen rendszerek – különböző mértékben – integrálva vannak egymással, így a rendszerekben keletkező információk könnyen megoszthatók más rendszerelemek részére.

A támadások megelőzésének, gyors észlelésének és hatékony kezelésének érdekében a szervezet igénybe vehet rajta kívül üzemeltetett rendszereket, szolgáltatásokat [például publikus felhőben működő malware detektáló szolgáltatást, fenyegetettségi információszolgáltatást (TI), reputációs információkat biztosító szolgáltatást], illetve igénybe veheti a Kormányzati Eseménykezelési Központ vagy egyéb információbiztonsági tevékenységet folytató vállalatok információmegosztó szolgáltatásait. Amennyiben a szervezet rendelkezik a káros tevékenység részletes elemzési képességével (például malware-elemzés), lehetőség van az elemzett esemény információinak mások részére történő megosztására (például fájl hash-ek,[118] káros IP-címek).

Az incidenskezelés műszaki támogatása megvalósítható nyílt forráskódú – általában ingyenesen elérhető (opensource) – vagy dobozos termékekkel is. Nagyvállalti környezetben a „dobozos" termékek használata elterjedtebb, kiegészítve ingyenesen elérhető célszoftverekkel. Kis- és közepes

[117] Jelen könyvfejezet vonatkozásában incidensnek tekintjük azon információbiztonsági eseményeket (ezek eseménysorozatot is alkothatnak), amelyek károsítják vagy veszélyeztetik az elektronikus információs rendszer sértetlenségét, rendelkezésre állását, illetve a rendszerben kezelt adatok bizalmasságát, sértetlenségét, illetve rendelkezésre állását.

[118] Hash: adott fájl tartalmáról készült egyedi lenyomat, amelyből általában nem állítható vissza a fájl eredeti tartalma.

vállaltoknál sok esetben ingyenes megoldásokból felépített incidenskezelési képességet alakítanak ki. Általánosságban elmondható, hogy nyílt forráskódú eszközökkel közel hasonló védelmi képesség alakítható ki, mint amilyenek az opensource megoldások, ugyanakkor a rendszerek közötti integráció, illetve a rendszer hibaelhárítása, fejlesztése, frissítése kockázatokat hordozhat magában.

2. Az incidenskezelést végző szervezet elhelyezkedésének műszaki támogatása

Az információbiztonsági incidensmenedzsment folyamata, az abban használt műszaki eszközök, igénybe vett szolgáltatások, az incidensekkel kapcsolatos információk az adott szervezet féltett titkai közé tartoznak. Illetéktelenek kezébe kerülve az incidensmenedzsmenttel kapcsolatos információk jelentős kockázatot hordoznak a szervezet hatékony védelmi képességének fenntartásában. Az információk megőrzésének érdekében különösen fontos, hogy az incidenskezelés során használt helyiségeket, illetve informatikai rendszereket megfelelő fizikai (például beléptetőkártyával védett helyiség) és logikai védelemmel (például szeparált, incidenskezelők által menedzselt informatikai infrastruktúra) kell ellátni.

Az incidenskezelés folytonosságának biztosítása érdekében a szervezet informatikai rendszereinek vagy külső szolgáltatótól igénybe vett szolgáltatásoknak a leállása esetén is biztosítani kell az incidenskezelők részére a tartalék infrastruktúrát (például tartalék helyiség, kommunikációs vonalak, informatikai rendszerek).

Az incidenskezelés helyiségében valamennyi érintett számára biztosítani kell, hogy az incidens jelzésére hivatott eszközök (telefon, monitor, falra szerelt képernyő) elérhetők, láthatók legyenek. Amennyiben a szervezet káros kódelemzési tevékenységet is végez, úgy a vállalati IP-címtartomány kompromitálódásának elkerülése érdekében olyan internetelérést (dirty line) kell biztosítani, amely független a vállalati internet kijáratától.

Jelentősebb incidensek esetén – a szervezet belső szabályainak megfelelően – összehívhatják az operatív törzset, amely számára ugyancsak biztosítani kell a megfelelő elhelyezést (warroom), illetve a hatékony döntéshez szükséges információkat.

3. Az incidens észlelésének, elemzésének, kezelésének eszköztára

Az incidenskezelési folyamat egy esemény értékelése után indul. Amennyiben az értékelés során az eseményről megállapításra kerül, hogy információbiztonsági incidens, elindul az incidenskezelési folyamat. Megkezdődik az incidens körülményeinek, hatásának vizsgálata, a válaszadás, majd az incidens lezárása. Az incidenskezelés során a szervezet az incidens fajtájától, a szervezetben elérhető képességektől, rendelkezésre álló technikai eszközöktől, erőforrásoktól, illetve az incidens által okozott kártól vagy kockázatától függően vesz igénybe informatikai támogató eszközöket, szolgáltatásokat.

3.1. Az incidensek észlelését támogató műszaki rendszerek

Az incidens kezelésére hivatott szervezet ügyfelektől, partnerektől, gyártóktól, a szervezet által üzemeltetett rendszerekből vagy egyéb külső forrásból – például publikus internet – kaphat információt az incidensről vagy annak gyanújáról.

A biztonsági eseményekről vagy azok gyanújáról szóló jelzés érkezhet az informatikai rendszerek védelmére hivatott eszközökből közvetlenül vagy olyan – jellemzően központi – naplóelemző rendszerből, amely képes a különböző (nem csak védelmi) rendszerekben keletkező események együttes vizsgálatára. A védelmi és naplóelemző rendszerek általában rendelkeznek grafikus megjelenítő felülettel, amelyen az incidenskezelők számára látványos módon megjelenhet az incidens gyanús esemény.

3.2. Naplógenerálás

Ahhoz, hogy utólag megállapítható legyen, pontosan mi is történt az elektronikus információs rendszerben, mindenképpen szükséges a rendszerben zajló eseményekre vonatkozó információk rögzítése. A rendszerben zajló tevékenységekről – a rendszer képeségétől, illetve a konfigurációs beállításoktól függően – készült naplóbejegyzések feldolgozása támogatást nyújthat többek között a rendszer optimalizálásához, a rendszerben meglévő hibák javításához, illetve biztonsági események felderítéséhez, rekonstruálásához és ezeken keresztül a rendszer hiányosságainak javításához.

A régóta működő egyedi fejlesztések kivételével napjainkban már csak elvétve találkozhatunk olyan elektronikus információs rendszerrel, amely ne rendelkezne valamilyen szintű naplógenerálási képességgel, legyen szó alkalmazásról, operációs rendszerről, adatbázis-kezelőről, információbiztonságot biztosító rendszerről vagy hardver eszközről. A rendszerek jelentős részénél lehetőség van többszintű és esetenként eseménycsoporthoz rendelt naplózás beállítására. A naplózandó események rendszertípusonként nagyon eltérők lehetnek (például operációs rendszer esetén: be- és kilépések, folyamatokkal kapcsolatos és felhasználói tevékenységek; hálózati eszközök esetén: kapcsolat adatai; védelmi rendszerek esetén: észlelt eseményekről riasztás).

A biztonsági naplózás célja, az elektronikus információs rendszerekben zajló biztonsági események felderítésének támogatása, a biztonsági eseményre irányuló elemzés alapjainak megteremtése, a rendszerben zajló események utólagos visszakövethetőségének biztosítása. Ennek érdekében a naplózási tevékenység során rögzítésre és feldolgozásra kerülnek az elektronikus információs rendszerekben zajló információbiztonság szempontjából releváns cselekmények. A biztonsági naplóbejegyzések az üzemeltetői naplóbejegyzések egy jól körül határolható része, amelyet általában az üzemeltetői naplóbejegyzésektől külön is tárolnak.

Az idők folyamán számos – az adott rendszer funkciójától függő – naplózási protokoll alakult ki, amelyből a három leggyakrabban használt a *syslog,* amely elsősorban hálózati eszközök, Linux rendszerek által alkalmazott naplózási protokoll; a *Microsoft Event log,*[119] amelyet a Windows alapú rendszerek használnak; és a *SNMP* (Simple Network Management Protocol).

A fejlett adatbáziskezelő rendszerek rendelkeznek audit naplózási képességgel, amely (beállítástól függően) rögzíti az adatbázisban zajló tevékenységeket.

Egyedi alkalmazások esetén a fejlesztő által leprogramozott módon történik az eseményről készült naplóbejegyzések generálása, tárolása.

Az egyes protokollok meghatározhatják a naplóbejegyzés összetevőit, annak sorrendjét, jellemzőit, de iránymutatást adhatnak a naplóállományok gyűjtésével kapcsolatban is.

A naplógenerálás akár jelentős mértékben is csökkentheti a rendszer teljesítményét, így különösen fontos, hogy a naplózási szint beállításakor figyelembe vegyék a rendszer kockázati szintjét.

3.3. A központi naplógyűjtési infrastruktúra

Az elektronikus információs rendszer funkciójától, kockázatától, a szervezet rendelkezésre álló erőforrásaitól, a szervezet biztonságtudatosságától, illetve a szervezetre vonatkozó jogszabályoktól függően a naplóbejegyzések tárolása történhet helyben az információs rendszerben és/vagy központi naplógyűjtő rendszeren és/vagy központi biztonsági naplógyűjtő és elemző rendszeren.

A helyben történő tárolás nem igényli központi infrastruktúra fenntartását, ezáltal üzemeltetése kevés anyagi és emberi erőforrást igényel, ugyanakkor mellette jelentősen nehezebb a biztonsági incidensek észlelése és elemzése (beleértve az okok meghatározását, a kiterjedést is). A helyben történő tárolás a rendelkezésre álló tárolókapacitás miatt általában erősen korlátozott. Az informatikai

[119] Chuvakin, Anton – Schmidt, Kevin – Phillips, Chris (2012): Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress, 52.

rendszert érő támadás esetén – a helyben tárolt naplók törlésével[120] – ellehetetlenülhet az incidens felderítése.

Központi naplógyűjtő infrastruktúra üzemeltetése esetén az informatikai környezetben üzemelő rendszerek által generált naplóbejegyzések egy központi helyen kerülnek összegyűjtésre és hosszabb távú eltárolásra. A központi naplógyűjtés már jelentős segítséget nyújthat az incidenselemzők számára, mivel lehetőség van több rendszerből érkező naplóbejegyzések összefüggő vizsgálatára. Ugyanakkor elemzői képesség hiányában a naplóbejegyzések vizsgálata általában manuálisan vagy szkriptek segítségével történhet.

Nagyobb szervezetek megvalósíthatnak központi biztonsági naplógyűjtést és elemzés is, amely általában az információbiztonsági szervezet által üzemeltetett rendszerben gyűjti és tárolja a biztonsági naplóbejegyzéseket.

A központi helyen történő tárolás esetén lehetőség van az egymástól eltérő naplóforrásokban lezajló események közötti összefüggések vizsgálatára. A központi tárolással biztosítható továbbá, hogy egy rendszer kompromittálódása esetén is felderíthető legyen az esemény lefolyása.

A forrásrendszer fájljaiban vagy adatbázisában tárolt naplóbejegyzéseit elküldheti a központi naplógyűjtő rendszerbe egy program vagy folyamat (agent) segítségével, vagy a központi naplógyűjtő rendszer hozhatja el a bejegyzéseket (agentless) a forrásrendszerből. Az agenttel történő naplóküldés – számos előnye ellenére – az üzemeltetési terület által kevésbé kedvelt megoldás.

A forrásrendszerekből többféle protokoll használatával juthat el a naplóbejegyzés a központi loggyűjtő rendszerbe. Az átviteli protokollt a küldő és a fogadó rendszer képességei határozzák meg.

Amennyiben nincs szükség vagy előírás a naplóbejegyzések hosszabb idejű tárolására, úgy a régebbi vagy a kevésbé fontos bejegyzéseket célszerű meghatározott időközönként törölni.

A naplóbejegyzések helyi tárolás esetén viszonylag rövid ideig (1-2 naptól néhány hónapig terjedhet), központi naplógyűjtő esetén általában fél és egy év közötti időszakig érhetők el a rendszerben közvetlenül. Hosszabb távú naplómegőrzésre általában lassabban elérhető vagy külső adathordozóra történik.

Jogszabályi megfelelés vagy üzleti okok miatt sok esetben szükséges a rendszerben végrehajtott naplóbejegyzések hosszú távú megőrzése, oly módon, hogy egy esetleges későbbi vizsgálat során bizonyítékként felhasználható legyen az adatállomány. Ahhoz, hogy egy naplóbejegyzés bizonyítékként felhasználható legyen, a keletkezéstől a felhasználásig biztosítani kell a naplóbejegyzés sértetlenségét, azaz garantálni kell, hogy a naplóbejegyzés nem változott a keletkezés pillanatától. A sértetlenség bizonyítása történhet elektronikus aláírással, vagy olyan meghajtó használatával, amely nem engedi az utólagos módosítást.

A naplóállományok tárolása (és feldolgozása) során különös figyelmet kell fordítani a tartalom bizalmasságának megőrzésére is. A szervezetnek meg kell határoznia, hogy milyen naplóbejegyzésekhez ki és milyen módon férhet hozzá.

Amennyiben jogszabály alapján kerül meghatározásra a személyes adat megőrzésének ideje, úgy az előírás szerinti ideig a naplóbejegyzés megőrzendő. Ugyanakkor önkéntes hozzájáruláson alapuló adatkezelés esetén a hozzájárulás megszűnésekor – néhány esetet kivéve – megszűnik az adatkezelés jogszerűsége, vagyis az érintett személyes adatait is törölni kell, beleértve a naplóbejegyzésekben megtalálható adatokat is. Egy naplóállományból néhány adat törlésének jelenleg nincs kialakult technikai gyakorlata, jellemzően az adatkezelők vállalják fel a jogi kockázatot.

Amennyiben a naplóbejegyzések nem kerülnek elemzésre, úgy azok központi tárolása az eredeti formában (nyers naplóbejegyzés), az adattaralom módosítása nélkül valósul meg.

A naplóbejegyzések elemzési célú gyűjtése esetén a központi naplógyűjtő rendszerbe érkezett naplóbejegyzések előfeldolgozásra kerülnek, amelynek lényege, hogy a naplóbejegyzésből kiválogatásra,

[120] A támadás során az egyik legfontosabb tevékenység a láthatatlanság és felderíthetetlenség, aminek egyik kulcsa a tevékenységnyomok eltüntetése, amely a naplózás kikapcsolásával vagy a naplóbejegyzések törlésével érhető el leghatékonyabban.

címkézésre és tárolásra kerülnek az elemzés szempontjából fontos részek. A folyamat történhet a naplógyűjtő rendszer szállítója által biztosított vagy egy egyedileg készített parser segítségével, illetve automatikusan is. Ez utóbbi esetben a naplóbejegyzés jellemzője alapján kerül meghatározásra annak címkéje. Ilyen címkék lehetnek például forráscím, célcím, felhasználói név, minden olyan, amely a naplóbejegyzésben található érték.

3.4. Naplóforrások

A naplóforrások kiválasztása elengedhetetlen feltétele a hatékony incidenskezelési folyamatnak. Az üzleti folyamatot kiszolgáló rendszerek, a hálózati és védelmi eszközök bevonása nélkül könnyen előfordulhat, hogy egy incidens rejtve marad, illetve egy utólagos vizsgálat során nem deríthető fel, hogy egy támadást milyen módon hajtottak végre, és mely rendszerekből, milyen adatok kompromittálódtak. A nem megfelelő vizsgálati eredmény következtében könnyen elképzelhető egy korábban sikeresen végrehajtott támadáshoz hasonló újabb sikeres támadás a szervezet informatikai rendszerei ellen. A naplóforrások meghatározása a jogszabályi elvárásokon túl kockázatelemzési folyamat eredményeként állhat elő.

A naplóforrások meghatározásánál fontos szempont, hogy egy lehetséges támadási folyamat valamennyi fázisáról legyen naplóinformáció, ami segítheti a támadás felismerését annak korai szakaszában, illetve a bekövetkezett támadás utólagos vizsgálatában.

3.5. Infrastruktúraelemek naplózása

Az infrastruktúraelemek naplózása többféle módon is lehetséges: operációs rendszerek és virtuális szerverek révén, adatbázis-kezelő rendszerek segítségével, rendszeralkalmazásokkal, az infrastruktúra működését támogató rendszerek, valamint védelmi eszközök révén.

Az *operációs rendszerek* képességeiktől és beállításaiktól függően képesek akár valamennyi, a rendszerben lezajlott eseményről bejegyzést készíteni. Mind Windows, mind *nix[121] operációs rendszerek különböző típusú naplókat ismernek (például rendszer, rendszerkomponensek, alkalmazások, felhasználói tevékenységek, biztonság események naplói), amelyeket külön-külön naplóállományba ment az operációs rendszer.

Incidenskezelés szempontjából az operációs rendszer eseményei közül kiemelt figyelmet érdemelnek a bejelentkezéshez kapcsolódó események, a jogosultság változásai, illetve a rendszerfolyamatokkal kapcsolatos események.

A modern informatikai rendszerek *adatbázisokban* tárolják a feldolgozandó adatokat. Ez az adatbázis-kezelő képességeitől, illetve a jogszabályi elvárásoktól függően különböző szinten valósulhat meg: naplózás teljes mellőzésétől egészen a rendszerben történő valamennyi esemény (adatmódosítás, lekérdezés, létrehozás, törlés, konfigurációváltozás) naplózásáig. A teljes körű naplózás ugyanakkor jelentős erőforrást igényel, így a helyes egyensúly megtalálása fontos feladat. Az adatbázis-kezelő rendszerek naplózása adatszivárgás, illetve illetéktelen adatmódosítás felderítésében játszhat fontos szerepet.

Az üzleti alkalmazások futtatásához számos *kiegészítő szoftver* lehet szükséges (például webszerverek, alkalmazásszerverek). Ezek gyakori célpontjai a támadóknak, így az ezen rendszerekben zajló eseményekről készült naplóbejegyzések is segíthetnek biztonsági incidensek felderítésében. A rendszerelemekből származó naplóbejegyzések vizsgálata általában az üzleti alkalmazásokkal és a határvédelmi eszközökből származó naplóbejegyzésekkel korreláltan hozhat eredményt.

[121] Unix, Linux disztribúciók.

Az informatikai infrastruktúra hatékony működését számos *egyéb eszköz támogatja* (például: címtárak, SSO),[122] amelyek egyfelől hasznos információt szolgáltathatnak illetéktelen tevékenység feltárásához, másfelől kiegészítő információkat is (például munkaállomás elhelyezkedése vagy a felhasználó adatai) az incidenskezelő számára.

3.6. Védelmi és hálózati eszközök

A *védelmi eszközök* alapvetően kétféle működési mechanizmussal érzékelik a támadást.[123] A „hagyományos" eszközök úgynevezett szignatúra alapú vizsgálatot alkalmaznak, amelynek lényege, hogy egy – a termék szállítója által – már korábban elemzett és a védelmi rendszer számára ismert minta esetén képes a támadást detektálni. A szignatúra alapú vizsgálat során nagy biztonsággal és gyorsan megállapítható, hogy egy viselkedésminta vagy kódrészlet káros-e, így a fals pozitív[124] riasztások száma alacsony. Legnagyobb hátránya ugyanakkor, hogy nem ismert minta esetén ezen rendszer nem képes a támadást felismerni.

A viselkedésanomália alapú védelmi rendszerek egy korábban betanított viselkedési profiltól történő eltérést vizsgálnak és egy kockázati értéket párosítanak az eltéréshez. Az anomália vizsgálatán alapuló rendszerek a megfigyelt tevékenységek számától és fajtájától, illetve a rendelkezésre álló tudás függvényében képesek egy eseményről megmondani, hogy az biztonsági incidens-e. Incidens észlelés szempontjából fontos szerepet játszhat, hogy a rendszer milyen tulajdonságok alapján jelzett lehetséges incidenst, például egy korábbi nem tapasztalt éjszakai munkavégzés utalhat akár biztonsági incidensre, ugyanakkor, ha új beosztásba kerül a dolgozó vagy messzire utazik, akkor ez az esemény normálisnak tekinthető. Ugyanakkor, ha például biometrikus (például billentyűzet leütés vagy egérmozgás) viselkedésben van eltérés, akkor az önmagában is gyanúra adhat okot. Viselkedési anomália alapú eszközök a kezdeti betanulási folyamat után felügyelt vagy felügyelet nélküli módon képesek a viselkedési profil módosítására.

Napjainkban a felhasználói (kiemelt felhasználói) tevékenységnek, az állományok viselkedésének, illetve a hálózati forgalomnak a karakterisztikáját vizsgáló, anomália alapú rendszerek használhatók a védelem erősítésére.

A szignatúra alapú rendszer által történő riasztásokról nagyobb biztonsággal és általában kevesebb elemzési tevékenységgel állapítható meg, hogy valóban incidensről beszélhetünk-e, ugyanakkor a viselkedésanomália alapú rendszerek jelenthetnek megoldást az úgynevezett ATP[125] jellegű támadásokkal szemben.

A *behatolás detektáló (IDS), valamint azt megelőző (IPS) eszközök* célja, hogy a hálózati forgalom elemzésével jelezzék és/vagy megakadályozzák az esetleges támadást. Az IPS/IDS rendszerek általában rendelkeznek saját felülettel, amely beállítástól függően jelezheti a folyamatban lévő támadást, illetve a jelzéssel párhuzamosan naplóbejegyzést küldhet a naplóelemző rendszer számára. Ahhoz azonban, hogy ténylegesen csak a releváns támadásokról keletkezzen jelzés a rendszerben, számos konfiguráció beállítása lenne szükséges: minden egyes rendszer/rendszerelem vonatkozásában be kellene állítani azokat a támadási mintákat, amelyeknél jelzés szükséges, ráadásul ezt naponta akár több alkalommal is meg kellene tenni. Például egy Linux rendszer irányába indított, de Windows sérülékenységet kihasználó támadás esetén nem szükséges jelzés, de nem szükséges arról sem, ha egy rendszer frissítve lett és az adott támadási módszer már nem érheti el a célját.

---

[122] SSO: Single sing-on: egyszeri beléptető rendszer. Segítségével nem kell minden alkalmazásba külön bejelentkezni, hanem a rendszer elvégzi az authentikációt.

[123] Lásd: https://pdfs.semanticscholar.org/cbfc/880bf348fb1471c507fb296128a7105b6a2d.pdf (utolsó letöltés: 2017. április 20.)

[124] Fals pozitív: téves riasztás.

[125] ATP: Advanced PersistentThreat: fejlett támadás, amelyet a mai védelmi eszközök nem detektálnak, így a felfedezés hosszabb időt (akár hónapokat, éveket) vesz igénybe.

Incidenskezelés szempontjából az IPS rendszer egy utólagos jelzést fog küldeni a naplógyűjtő rendszer részére egy megakadályozott támadásról, ami ugyan fontos lehet más rendszerek szempontjából, vagy információmegosztás okán, de nem igényel azonnali beavatkozást. Ugyanakkor az automatikus válasz generálhat üzletmenet-folytonossági problémákat, amelyeket kezelni kell (például olyan IP-cím letiltása, amely egy üzleti folyamat része). IDS rendszer esetén a releváns jelzést az incidenskezelőknek kezelni kell.

Az incidenskezelési folyamat része lehet az *adatszivárgás* jellegű incidensek kezelése. A *DLP-eszközök* a hálózati forgalom, illetve az elektronikus levelezés figyelésével akadályozzák meg az illetéktelen adattovábbítást. A beállításától függően a rendszer működhet monitorozó üzemmódban, illetve észlelt szabálysértés esetén akár közbe is avatkozhat. Az üzemmódtól függetlenül a DLP rendszer naplóbejegyzéseket küldhet a kimenő adatokról, illetve az észlelt eseményekről. Az incidenskezelő a kapott jelzés alapján a rendelkezésre álló egyéb eszközök (például hálózati csomagrögzítő, elemző) segítségével további elemzést végezhet.

Amennyiben a szervezet rendelkezik *DoS, DDoS*[126] *védelmi rendszerrel,* akkor a rendszer feladata a támadás fajtájától függetlenül megakadályozni, hogy a támadás során a sávszélesség vagy valamely eszköz egyéb erőforrása (például alkalmazás session, processzor) elfogyjon. A terheléses támadások kezelése elsősorban üzemeltetési feladat, ugyanakkor a támadás forrásának, módjának feltárásában, a válaszlépés megadásában, hasonló támadás megelőzésében, illetve információmegosztásban az incidenskezelőnek is fontos szerepe van.

A *végpontvédelmi eszközök* feladata a hálózati végpontokon működő rendszerek (munkaállomások, szerverek) védelme káros tevékenységgel szemben, legyen szó vírusok, malware-ek által okozott tevékenységről. Ezen rendszerek a védelmi tevékenységük mellett jellemzően információt szolgáltatnak a védett rendszerelemről a központi felügyeleti rendszer, illetve a naplógyűjtő rendszer számára.

A felügyelt rendszerek rendelkezésre állását az üzemeltetők folyamatosan figyelik *monitoring rendszereken* keresztül. Incidenskezelési szempontból a rendszerek által generált riasztások önmagukban kevés információt hordoznak, ugyanakkor egyéb rendszerek által jelzett riasztásokkal együtt hasznos segítséget nyújthatnak az incidens kezelésében [például a processzor használata megnő, és egy károsként nem ismert állomány felmásolása, futtatás a szerveren külön-külön nem biztos, hogy elindítana egy incidenst, de együtt utalhat egy zsarolóvírus (ransomware) tevékenységére].

A *hálózati eszközök* (például DNS szerverek, tűzfalak, routerek, hálózatirányítási, hálózatvédelmi eszközök) működésük mellett képesek a tevékenységükről naplóbejegyzést készíteni, és azt eljuttatni a központi naplógyűjtő rendszerbe. A naplóbejegyzések eszköztől függően tartalmazhatják a tevékenység adatait: többek között, de nem kizárólagosan a tevékenység időpontját, a kapcsolatban részt vevők IP-címét, a kommunikációs portokat, a kommunikációs protokollt, a kapcsolat felépítésének eredményét, felhasználói neveket, domaincímeket.

Az elmúlt időszak tapasztalatai azt mutatják, hogy a kapcsolati adatok, illetve egyéb rendszerek által szolgáltatott információk mellett egyre nagyobb szerep jut a hálózati csomagok elemzésének. A hálózati csomagelemzés során a fejlécben található információk mellett hatékony eszköz lehet a csomag tartalmának elemzése is, akár a titkosított csomag visszafejtésével és újbóli titkosításával.

A szervezet által vásárolt dobozos vagy fejlesztett alkalmazások a rendszer képességeitől, funkciójától függően eltérő szinten képesek az alkalmazásban végrehajtott tevékenységekről naplóbejegyzést készíteni. Ezen naplóbejegyzések segíthetnek a rendszerben történő jogosulatlan belépések, tevékenységek észlelésére, utólagos vizsgálatára. Az alkalmazások naplózása nélkül rejtve maradhatnak az olyan tevékenységek, amelyek nem járnak adatbázis vagy más rendszerben naplózott művelettel. Az alkalmazások naplóbejegyzései általában egyedi formátumúak. Az *üzleti alkalmazások*

[126] DoS (Denial of Service) szolgáltatásmegtagadással járó támadás, DDoS (DistributedDenial of Service) elosztott szolgáltatásmegtagadással járó támadás. Mindkét támadás célja a támadott rendszer elérhetetlenné tétele, működésének leállítása.

naplózása elsősorban a jogosultságokkal történő visszaélés, illetve a jogosulatlan hozzáférés felderítésében játszhat fontos szerepet.

A *fizikai védelmi rendszerek* működtetése és a fizikai biztonsági incidensek kezelése jellemzően nem az információbiztonsági terület feladata, aminek következtében a két terület informatikai rendszerei ritkán vannak összekötve, így a fizikai védelmi rendszerekben lévő információk csak közvetve érhetők el az incidenskezelő számára, az incidens felderítésben pedig szinte semmilyen mértékben nem segítenek.

A fizikai védelmi rendszerek információt adhatnak arról, hogy éppen ki melyik telephelyen, irodában, helyiségben tartózkodik. A beléptető rendszerek fő funkciója kontrollálni a mozgást, amely a rendszer képességeitől függően akár meg is tudja akadályozni az illetéktelen belépést. A fizikai belépési és az információs rendszerbe történő belépési információk korrelált vizsgálata fontos információval szolgálhat az incidens észlelési és vizsgálati folyamatban.

A kamerafelvétel felhasználható bizonyítékként, illetve az incidensvizsgálat támogatására.

3.7. Naplóelemzés, eseménykezelés

Az incidenskezelés legfontosabb eleme a biztonsági esemény- és incidenskezelő rendszer (SIEM). A SIEM rendszer feladata egyebek mellett a forrásrendszerekben történő események vizualizációja, az események (korrelált) vizsgálata során automatikusan feltárt incidensek (riasztások) jelzése, az incidenskezelés folyamatának támogatása, riportolás, illetve a naplógyűjtő rendszer paramétereinek (például naplóforrások, küszöbértékek) beállítása.

Az incidenskezelő (operátori) személyzet a SIEM felületén keresztül értesül a bekövetkezett incidensekről, illetve az incidensvizsgálat is ezen eszköz használatával indulhat el. A jól kiépített SIEM rendszer a naplóforrásokból nyert információkon kívül – az incidenskezelést jelentősen megkönnyítve – számos kiegészítő (enrichment) információt tartalmazhat, például egy adott IP-címhez tartozó geolokációs információk, a felhasználói névhez kapcsolt elérési információk, domainnévhez kötött reputációs információk.

A SIEM rendszerek számos lehetőséget biztosítanak a naplógyűjtőbe érkezett és feldolgozott események elemzésére, az elemzés eredményétől függően riasztás generálására, illetve incidenskezelési tevékenység támogatására vonatkozóan.

Az eseménybejegyzések elemzése történhet automatikusan, előre beállított feltételek megadásával, vagy incidens vizsgálat során az incidenselemző által. Manuális elemzés esetén az elemző dönti el, mely naplóbejegyzéseket, tevékenységsorozatot vizsgálja meg alaposabban. Az irányt az elemző számára rendelkezésre álló információk vagy sejtés határozzák meg, de nagymértékben függ az elemzést végző tudásától, tapasztalatától. Sok esetben a manuális elemzés az egyetlen út egy biztonsági incidens felderítéséhez, az események feltárásához.

Amennyiben az elemzés során a vizsgált események küszöbértéke meghalad egy bizonyos szintet (elér egy kockázati szintet), a rendszer különböző szintű riasztásokat generál, amelyek megjelennek az incidenskezelő képernyőjén, és elindulhat az incidenskezelés. A riasztás jelentkezhet egy magasabb kockázatú tevékenység bekövetkezésekor, de előfordulhat, hogy ehhez több esemény szükséges.

A naplóelemző rendszerek a gyorsabb elemzés érdekében *drill down* képességgel rendelkeznek, amelyek – egy eseményre kattintva – lehetőséget biztosítanak néhány lépésen belül, egyszerűen eljutni az eredeti naplóbejegyzésig.

Egy szervezet általában nem rendelkezik annyi erőforrással, hogy valamennyi incidenst, incidensgyanút kivizsgáljon és kezeljen. Emiatt a bejövő incidenseket priorizálni kell. Ennek során egyrészről figyelembe kell venni az érintett rendszer „értékét” (amelyet elsősorban az üzletmenet szempontjából betöltött szerepe, illetve a benne tárolt adatok határoznak meg), másrészről az incidens lehetséges hatását. Amennyiben a szervezet rendelkezik az egyes rendszerei vonatkozásban információbiztonsági kockázati adatokkal, az nagyban megkönnyítheti – automatikussá teheti – az incidens besorolását.

Az incidensvizsgálatot jelentős mértékben segíti, ha a bejövő naplóinformációk ki vannak egészítve praktikus, látható információkkal. Leggyakoribb ilyen az IP-címhez tartozó ország neve, a felhasználói név alapján a felhasználó teljes neve, beosztása, elérhetőségi információi, vagy egy munkaállomás fizikai adatai.

Számos incidenskezelő rendszer lehetőséget biztosít arra, hogy egy előre definiált incidens esetén bizonyos műveleteket automatikusan végrehajtson, ezzel jelentősen felgyorsítva az incidenskezelés folyamatát, ilyen művelet lehet például a riasztás automatikus eszkalációja, egy fertőzöttnek vélt állomány vizsgálata vagy egy weboldal alapos vizsgálata.

Az incidens észlelése és kezelése során számos, egymástól független biztonsági, üzleti informatikai rendszertől érkezhetnek információk az incidenskezelők számára. Ezen információk egységes felületen történő megjelenítésére, elemzésére és riportolására szolgálnak a *biztonsági műveleti, elemző és riport (SOAR) rendszerek.* A rendszer képes a több forrásból beérkező információk korrelált kezelésére, támogatást nyújt az incidenskezelés során. A támogatás kiterjedhet az incidenskezelési munkafolyamat támogatására, automatikus folyamatlépésekre (például fertőzött gyanús állomány elemzésének indítása), válaszadásokra (például támadó IP-címének tiltása) és riportok elkészítésére is.

4. Az incidensvizsgálat eszközei

A központi biztonsági naplóelemző mellett számos egyéb rendszer áll az incidenskezelők rendelkezésére az események vizsgálatára, a gyökérokok, a kiterjedés meghatározására. Ezen eszközök általában részben vagy egészben hozzá vannak rendelve a SIEM rendszerekhez, de használatuk önállóan is történhet.

A hálózati forgalomban, a számítógéphez csatolt adathordozókat vagy az elektronikus levelek forgalmát felügyelő eszközök nem mindig képesek a rajtuk áthaladó állományokban lévő káros kódot megtalálni, így ezen kódok észrevétlenül juthatnak el a célszámítógépre, s hajtódhatnak végre.

A káros állományok utólagos elemzése kiemelten fontos lehet az elemző számára, vagyis az, hogy meglegyen a képesség a külső forrásból érkező állományok manuális vizsgálatára. A vizsgálat során az elemző jellemzően sandboxba[127] küldi a gyanús állományt, ahol automatikus módszerekkel megtörténik az állomány tevékenységének vizsgálata. A sandbox keretein belül számos informatikai környezetben megtörténik a gyanús állomány futtatása és a viselkedés alapján az állomány kockázatának meghatározása, amely akár automatikusan is megjelenhet az incidenskezelő rendszerben.

Az automatikus elemzésen kívül számos esetben szükség lehet a káros tevékenység pontos megismerésére. Az elemző a számítógép tevékenységének (például telepített állományok, registry módosítások, hálózati forgalomelemzés) vizsgálatától eljuthat akár a kód visszafejtéséig és a kód elemzéséig is.

A hálózati forgalom rögzítése és utólagos elemzése hatékony támogatást nyújthat az incidens pontos lefolyásával kapcsolatban. A rögzített hálózati csomagok elemzése lehetőséget biztosít a hálózati védelmi eszközök által fel nem ismert támadások elemzésére. A rendelkezésre álló erőforrások függvényében megtörténhet a teljes hálózati forgalom rögzítése (és általában néhány napos) tárolása vagy csak a csomag fejrészének (header) rögzítése. A teljes csomag tárolása esetén van lehetőség például a letöltött állományok utólagos elemzésére, a támadó pontos tevékenységének feltérképezésére, illetve a kiszivárgott adatok körének meghatározására is. A teljes hálózati csomagrögzítés – annak nagyon jelentős erőforrásigénye miatt – csak indokolt esetben (például kiemelt rendszerek esetében) szokott megvalósulni. A hálózati csomag fejrészének rögzítése jelentősen javíthatja az incidenskezelés

[127] Sandbox: olyan ellenőrzött – valós világhoz közeli – informatikai környezet, ahol megfigyelhető egy állomány futtatása során annak tevékenysége, úgy, hogy az ne jelentsen veszélyt a teljes informatikai rendszerre. A sandbox futhat helyben (on-premise) vagy felhőben.

hatékonyságát, így, mivel nem igényel túl jelentős erőforrást, alkalmazása a kockázatok figyelembe vétele mellett megfontolandó.

A 3.6. alfejezetben említett végpontvédelmi eszközök közül az Endpoint Detection and Response (EDR)[128] rendszerek képesek – a végponton történő védelem biztosításán kívül – hatékonyan támogatni az incidens vizsgálatot. A támogatás során figyelik a rendszer folyamatait, másolat készülhet a memóriatartalomról, de káros tevékenységre utaló IoC-k megkeresése is lehetővé válik a teljes infrastruktúrában.

Az incidenskezelés során nagyon fontos az incidens pontos okának felderítésén túl a rendelkezésre álló bizonyítékok hiteles összegyűjtése, tárolása. A bizonyítékok gyűjtése irányulhat a felhasználó tevékenységét leíró naplóbejegyzésekre, az eszköz bizonyos részeinek (például memória, merevlemez), a hálózati forgalomnak a megőrzésére.

5. Válaszadás eszközrendszere

Az incidens bekövetkezése és az észlelés között akár hónapok is eltelhetnek, ugyanakkor az észlelés és a beavatkozás között általában már rövidebb idő telik el. Az első beavatkozás ideje nagymértékben függ az incidens elemzésének idejétől, az elemző vagy incidenskezelő tapasztalatától, illetve a válaszadást támogató folyamatoktól, az informatikai rendszer képességeitől. Általában minél több az emberi munka, annál hosszadalmasabb a válaszadás. Persze adott egy időintervallum, ami alá már nem fog csökkeni. Mindezzel szemben az automatikusan működő rendszerek akár néhány másodperc alatt hatékony választ adnak.

Napjaink korszerű tűzfalai, IPS, EDR rendszerei képesek külső fenyegetettségi információszolgáltatók (TI) által biztosított információk (IoC – Indicator of Compromise) vagy külső rendszerből érkező kérések (például SIEM) alapján automatikusan módosítani konfigurációjukat, így megvédve az informatikai rendszert.

Az automatikus beavatkozás nagy körültekintést igényel, mivel egy nem megfelelő konfiguráció beállítása akár meg is állíthatja az üzletmenetet. A fejlettebb incidenskezelő rendszerek képesek a kapott IoC-at korrelálni egyéb információkkal, így nagyobb valószínűséggel kerülhetik el az egy automatikus tevékenység következtében fellépő nem kívánatos mellékhatásokat. Amennyiben az automatizmus nem fogadható el, általában különböző szintű integrációk segítségével támogatható a hatékony válaszadás.

Az integráció történhet az incidenskezelő rendszer és a vállalati hibakezelő rendszer összekapcsolása révén, de akár a védelmi rendszerrel történő integráció által is.

6. Külső fenyegetettségi információforrások (TI)[129]

Napjainkban – a napi szinten sokmillió számra megjelenő új fenyegetés miatt – külső fenyegetettségi információk nélkül elképzelhetetlen a hatékony incidensészlelés. Az információk érkezhetnek a szervezet által üzemeltetett rendszerekből vagy külső forrásból (például TI-szolgáltatók, Kormányzati Eseménykezelő Központ, CERT-ek).[130] Az információk megjelenhetnek stratégiai, operatív és taktikai-technikai szinten.[131]

---

[128] EDR (Endpoint and Response): olyan végponti védelmi eszközök, amelyek az incidens felismerésén kívül képesek automatikus választ adni, és hatékonyan támogathatják az incidens vizsgálatot.

[129] TI – Threat Intelligence: Threat Intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. Online: www.gartner.com/doc/2487216/definition-threat-intelligence (utolsó letöltés: 2017. április 20.)

[130] Computer Emergeny Response Team: számítógépes hálózati incidenskezelő központ.

[131] Lásd: www.sans.org/reading-room/whitepapers/threats/threat-intelligence-planning-direction-36857 (utolsó letöltés: 2017. április 20.)

A *stratégiai* szint szervezeti vezetők, informatikai, információbiztonsági döntéshozók számára hordoz információt elemzések, tanulmányok formájában. Az általában online formában elérhető dokumentumok vállalatok, szervezetek információbiztonsági környezetével kapcsolatos információkat tartalmaznak, többek között fenyegetettségi trendekről, technológiai változásokról, kockázatelemzéshez, compliance tevékenységhez kapcsolódó információkról.

Az *operatív* információk a biztonsági csapat számára nyújtanak segítséget, hogy megismerjék többek között az aktuális fenyegetettségeket, támadási technikákat, incidenskezelési trendeket, új biztonsági megoldásokat, termékeket.

Amíg a stratégiai és az operatív információk embereknek szólnak, a *taktika vagy technikai információk* általában olyan IoC-k,[132] amelyeket gépi feldolgozásra szánnak. Ezen információk beépülhetnek az elemzési térbe, vagy alapjául szolgálhatnak automatikus konfigurációmódosításnak a védelmi eszközökben.

7. Az incidensmenedzsment támogatásának eszközrendszere

Az incidensmenedzsment hatékonyságának biztosítása érdekében számos kiegészítő folyamatot, tevékenységet célszerű működtetni, melyek közvetve vagy közvetlenül hozzájárulnak a megelőző tevékenységhez, az incidensek hatékonyabb felismeréséhez, illetve gyorsabb kezeléséhez.

Első látásra a *sérülékenységmenedzsment* nem szerves része az incidenskezelő feladatoknak, ugyanakkor az incidenskezelők számára egy adott rendszer sérülékenysége az egyik legfontosabb információ.

A sérülékenységet vizsgáló eszköz automatikusan vagy manuálisan indítva megkeresi a vizsgált rendszer elemeiben található ismert sérülékenységeket, és javaslatot tesz a sérülékenység megszüntetésére. Az incidenskezelő szervezeti egység feladata a sérülékenység megszüntetéséig beállítani azokat az indikátorokat, amelyek segítségével detektálható a sérülékenység kihasználására irányuló támadási kísérlet, illetve beállítani az ilyen típusú kísérlethez megfelelő prioritású riasztást.

A sérülékenységmenedzsment eszközei általában rendelkeznek folyamattámogatással, mely segítségével a sérülékenység javítása kioszthatóó az illetékes szakterület számára, illetve nyomon követhető a javítás állapota.

Az informatikai rendszerek frissítése elengedhetetlenül fontos a biztonságos üzemeltetés szempontjából, ugyanakkor ez sok esetben vagy késve (például az új verzió tesztelése, erőforráshiány miatt), vagy egyáltalán nem történik meg (például, ha az új verzió alatt nem fut az üzleti szoftver). A frissítések hiánya biztonsági kockázatot hordoz, amire fel kell készülnie az incidenskezelőknek is. A *patchmenedzsment* rendszerek információt nyújthatnak a sérülékeny szoftververziókról, ami segítséget nyújt például a biztonsági esemény relevanciájának megállapításához, illetve az incidens prioritásának meghatározásához.

A *vállalati irányítási, kockázat- és megfelelőségmenedzsment* rendszere az úgynevezett GRC. A GRC rendszert jellemzően nem az incidenskezelő terület működteti, a rendszerben lévő adatokat a vállalat egyéb szervezetei (jellemzően üzleti, informatikai fejlesztési, üzemeltetési, biztonsági területek) aktualizálják, ugyanakkor a rendszerben tárolt adat fontos forrás lehet az incidenskezelők számára.

A vállalat incidenskezelése során ritkán adatik meg, hogy valamennyi észlelt incidenssel érdemben foglalkozzanak, vagyis a kezelendő incidenseket valamilyen módszer szerint ki kell választani. A kiválasztás történhet előre beállított paraméterek alapján (például egy támadástípus egy adott eszköz ellen), amely kiegészülhet a GRC rendszerből kapott egyéb információkkal (például a támadott rendszerelem kockázati információi, a rendszer napi üzletmenet során betöltött szerepe).

[132] IoC (Indicator of Compromise): olyan indikátor, amely fenyegetettségre utal, például: fertőző domainnevek, fertőzött fájlokról készül lenyomat.

Az incidenskezelés folyamán szerzett tudás tematikus tárolása alapja a hosszú távú hatékony incidenskezelésnek, amely lehetőséget biztosít az újonnan érkező munkatársak számára a gyors ismeretszerzéshez, a helyi sajátosságok, folyamatok, eljárások megismeréséhez.

A *tudásmenedzsment* rendszere amellett, hogy hasznos segítség lehet a mindennapi munkában, közös platformot biztosíthat a fontosabb dokumentumok tárolására, illetve kommunikációs terepként is működhet az eltérő időben dolgozó munkavállalók között.

Mind a meglévő incidenskezelők, mind az újonnan érkező munkatársak számára kiemelten fontos, hogy rendelkezzenek azon tudással, amely biztosítja az incidenskezelés során alkalmazott eszközök magas színvonalú használatát. Mindenki számára fontos, hogy naprakészen tartsa tudását az informatikai rendszerek fenyegetettségeinek változásairól.

Az újonnan érkező kollégák számára fontos megismerni a szervezetet, illetve a szervezeten belüli szokásokat, szabályokat. Amennyiben a szervezet használ saját *oktatási anyagot,* akkor célszerű az érintett kollégákat ennek segítségével oktatni. Az incidensmenedzsment során alkalmazott eszközök használatának sikeres elsajátításához a gyártói oktatói anyagok a leghatékonyabbak. A helyi ismeretek, illetve eszközök megismerése során fontos szerepe van a „régi" kollégák által szerzett tapasztalat átadásának.

Speciális – nem gyártóspecifikus – *képzések* széles körben elérhetők, akár online, osztálytermi vagy virtuális osztálytermi formában.

A képzéseken való részvétel – annak formájától függően – akár jelentős költséggel is járhat, ugyanakkor a megszerzett ismeretek bármely incidens kezelése során megtérülhetnek.

Hazánkban is számos ingyenes információbiztonsági rendezvényt szerveznek, ahol hasznos információkat lehet szerezni új termékekről, technológiákról, illetve hasznos kapcsolatot lehet kiépíteni szakmabeli kollégákkal.

8. Referenciaarchitektúrák kis, közepes és nagy szervezetek számára

A technológiák konvergenciájának eredményeképpen, valamint az eddig elvárt szolgáltatási szint fenntartása, illetve más technológiákra történő kiterjesztése miatt a hálózatüzemeltetőkre a megszokottnál nagyobb teher hárul. A biztonságos üzemeltetés és a szolgáltatási szintek fenntartása érdekében a megfelelő menedzsmenteszközök alkalmazása hatékonyabbá teheti a működést.

Az infokommunikációs hálózati megoldások terén tapasztalható paradigmaváltásnak köszönhetően lehetővé vált, hogy az üzemeltetők több megoldás és technológia közül válasszanak. Az ITIL módszertan filozófiája azért vált be, mert folyamatorientált megközelítést alkalmaz; ennek köszönhetően alkalmazzák ezt megoldásaik során például a Magyarországon is tevékenykedő nemzetközi informatikai cégek – többek között a HP, a Microsoft vagy az IBM.

A legfontosabb elvárások egy informatikai infrastruktúrával és architektúrával szemben a következők:

- minden olyan alkalmazás, amely az üzletmenet szempontjából fontos, a jogosult felhasználók számára bármikor, bárhol elérhető legyen, és ezeket optimálisan szolgálja ki az IT-infrastruktúra;
- legyenek biztonságban az üzletileg fontos információk mind külső, mind belső hozzáférés szempontjából;
- menjen át az infrastruktúra az auditokon;
- mindezt a lehető legalacsonyabb költséggel valósítsák meg.

Ezeknek az elvárásoknak nem egyszerű megfelelni, így az üzemeltetőkre nagyobb terhelés, növekvő felelősség nehezedik, mert az infrastruktúra – és ezen belül a hálózatok – régebben csupán PC-k és telephelyek adatcélú összekapcsolására szolgáltak, ma viszont már hang- és videoszolgáltatások, beléptető- és kamerarendszerek, felhő alapú számítási és tároló rendszerek kezelését is végzik. A mobil

munkavégzés eredményeképpen egyre több hálózati végpontra van szükség, ezáltal növekszik a hálózat komplexitása, miközben a megbízhatóság kérdése is fontosabb, mint valaha. A hálózati infrastruktúra fejlesztése rendszerint megáll a végpontok számának növelésénél, arra azonban kevesen gondolnak, hogy az új feladatok optimális megvalósításához új funkciókat építsenek be a rendszerekbe.[133]

Összegezve tehát igazi kihívás ma olyan komplex infrastruktúrát összerakni, amely teljes mértékben kiszolgálja egy vállalat állandóan változó igényét, amellett, hogy a szigorú biztonsági követelményeknek is megfelel. Ezért ebben a fejezetben olyan gyártói megoldások és kapcsolódó esettanulmányok kerülnek bemutatásra, amelyek hozzájárulhatnak a biztonságos és összetett üzemeltetés és fejlesztés gyakorlati ismereteihez.

8.1. Microsoft: Azure, az Azure Site Recovery megoldásarchitektúra vészhelyreállításhoz

Az alábbi táblázat azt részletezi, mire van szükség ahhoz, hogy a VMware virtuális gépeket Azure-ba lehessen replikálni:

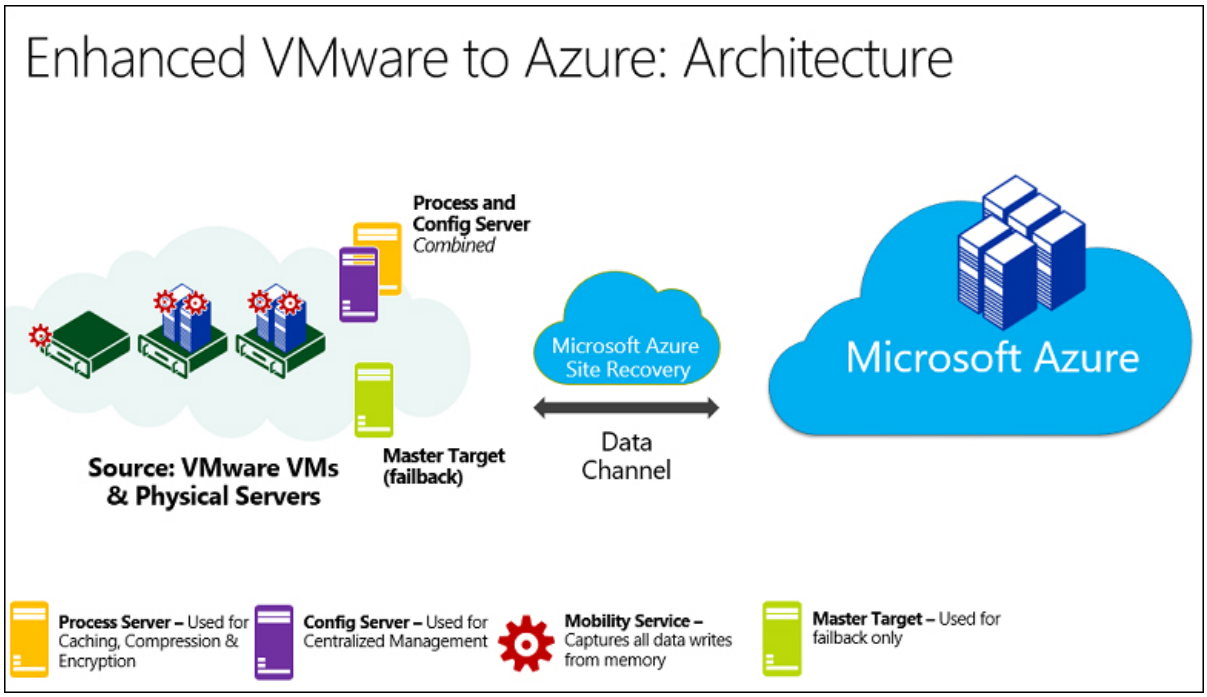
1. táblázat: Azure–Vmware-kapcsolat

Terület	Összetevő	Részletek
Azure	Az Azure-ban szükség van egy Azure-fiókra, egy Azure Storage-fiókra és egy Azure-hálózatra.	A Storage és a hálózat lehet Resource Manager vagy klasszikus fiók. A replikált adatokat a tárfiók tárolja, ha pedig feladatátvétel következik be a helyszíni helyről, a rendszer Azure virtuális gépeket hoz létre a replikált adatokkal. Az Azure virtuális gépek a létrehozásukkor csatlakoznak az Azure virtuális hálózathoz.
Konfigurációs kiszolgáló	Egyetlen felügyeleti kiszolgáló (VMware virtuális gép) futtatja az összes helyszíni összetevőt – a konfigurációs kiszolgálót, a folyamatkiszolgálót és a fő célkiszolgálót.	A konfigurációs kiszolgáló koordinálja a helyszíni rendszer és az Azure közötti kommunikációt, és felügyeli az adatreplikációt.
Folyamatkiszolgáló	Alapértelmezés szerint telepítve van a konfigurációs kiszolgálón.	Replikációs átjáróként üzemel. Fogadja a replikációs adatokat, gyorsító tárazással, tömörítéssel és titkosítással optimalizálja őket, majd továbbítja az Azure Storage-nak. A folyamatkiszolgáló ezenfelül kezeli a mobilitási szolgáltatás leküldéses telepítését a védett gépekre, és elvégzi a WMware virtuális gépek automatikus felderítését. Az üzemelő példány bővülésével további, önálló és dedikált folyamat-kiszolgálókat helyezhet üzembe, amelyek segítségével képes lesz a megnövekedett replikációs forgalom kezelésére is.

[133] Network Management System Database (NMSDB) – Üzemeltetés és dokumentáció kis költséggel, kis munkával. T-Systems. Elérhetőség: www.t-systems.hu/static/sw/file/Network_management_system_database.pdf (utolsó letöltés: 2017. április 20.)

Terület	Összetevő	Részletek
Fő célkiszolgáló	Alapértelmezés szerint telepítve van a helyszíni konfigurációs kiszolgálón.	Az Azure-ból történő feladat-visszavétel során kezeli a replikációs adatokat. Ha a feladat-visszavételi adatforgalom kötetei nagyok, a feladat-visszavételhez üzembe helyezhető egy másik fő célkiszolgáló.
VMware-kiszolgálók	A VMware virtuális gépek vSphereESXi-kiszolgálókon futnak, és a gazdagépek felügyeletéhez egy vCenter-kiszolgáló üzembe helyezését javasolják.	Szükséges a VMware-kiszolgáló felvétele a RecoveryServices-tárolóba.
Replikált gépek	A mobilitási szolgáltatás az összes replikálni kívánt VMware virtuális gépen telepítve lesz. A szolgáltatás manuálisan is telepíthető az egyes gépekre, de leküldéses telepítés is végrehajtható a folyamat-kiszolgálóról.	

Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2019. április 20.)



5. ábra: Összetevők VMware-ről Azure-ra
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 20.)

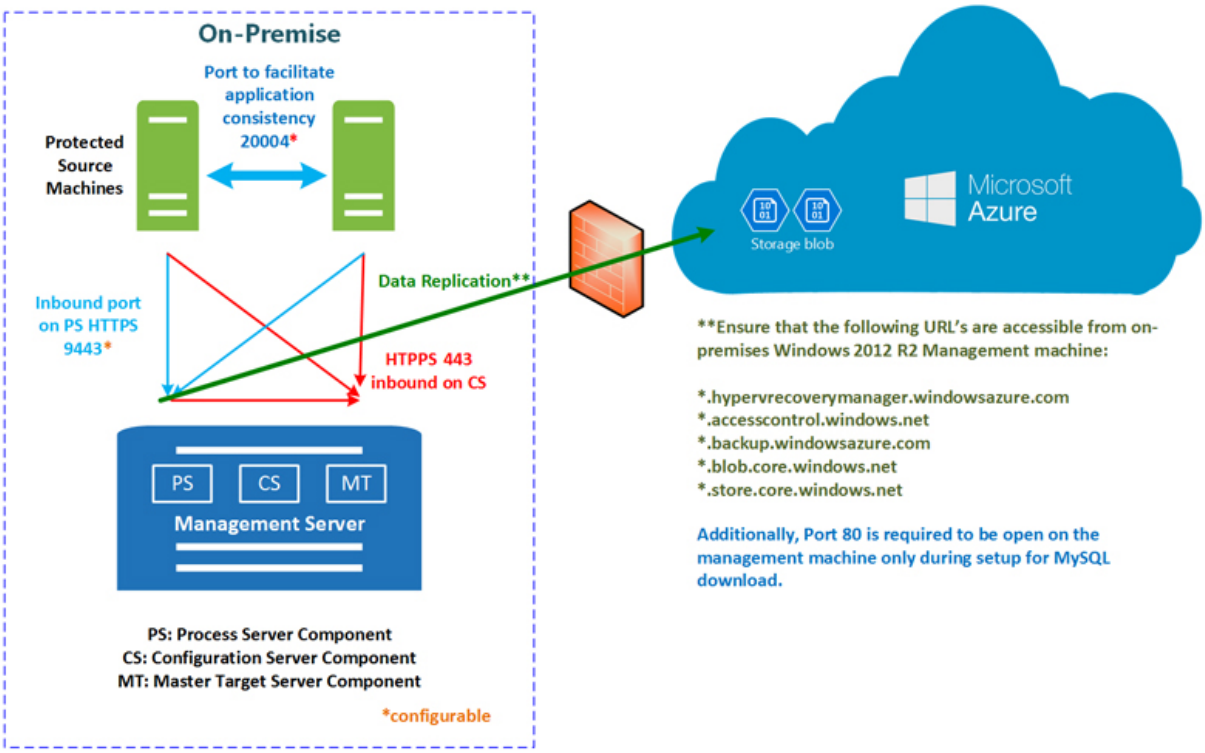
Az üzemelő példány beállításának részeként az Azure-összetevőket és egy RecoveryServices-tárolót is be kell állítani. Ezért a tárolóban:

- meg kell adni a replikáció forrás- és célhelyét;
- be kell állítani a konfigurációs kiszolgálót;

- fel kell venni VMware-kiszolgálókat;
- replikációs szabályzatot kell létrehozni;
- üzembe kell helyezni a mobilitási szolgáltatást;
- engedélyezni kell a replikálást;
- futtatni kell egy feladatátvételi tesztet.

A gépek a replikációs szabályzat szerint kezdik meg a replikálást, és az adatok kezdeti másolata az Azure-tárolóba lesz replikálva.

Az Azure változáskülönbözeteinek replikációja a kezdeti replikálás befejezése után kezdődik el. A gépek nyomon követett módosításait a rendszer egy .hrl fájlban tárolja. A replikációs folyamat kezelése érdekében a replikálást végző gépek a 443-as bejövő HTTPS-porton kommunikálnak a konfigurációs kiszolgálóval. A replikálást végző gépek a 9443-as bejövő HTTPS-porton küldik el a replikációs adatokat a folyamatkiszolgálónak (ez a beállítás konfigurálható). Az Azure-replikációs folyamat kezelését a konfigurációs kiszolgáló a 443-as kimenő HTTPS-porton keresztül végzi el. A folyamatkiszolgáló adatokat fogad a forrásgépekről, amelyeket optimalizál és titkosít, majd a 443-as kimenő porton küldi az Azure-tárolóba. Ha engedélyezve van a több virtuális gépre kiterjedő konzisztencia, a replikációs csoportban található gépek a 20004-es porton kommunikálnak egymással. Több virtuális gépes környezetről akkor beszélünk, ha a gépek feladatátvételkor azonos összeomlásbiztos és alkalmazáskonzisztens helyreállítási pontokat használó replikációs csoportokba vannak rendezve. Ez akkor lehet hasznos, ha a gépek ugyanazt a számítási feladatot futtatják, így konzisztensnek kell maradniuk. Az adatforgalmat a rendszer az interneten keresztül az Azure Storage nyilvános végpontjaira replikálja. Erre a célra az Azure Express Route nyilvános társviszony-létesítési szolgáltatását is használhatja. Az adatforgalmat helyszíni helyek és az Azure között VPN-en keresztül nem lehet replikálni.



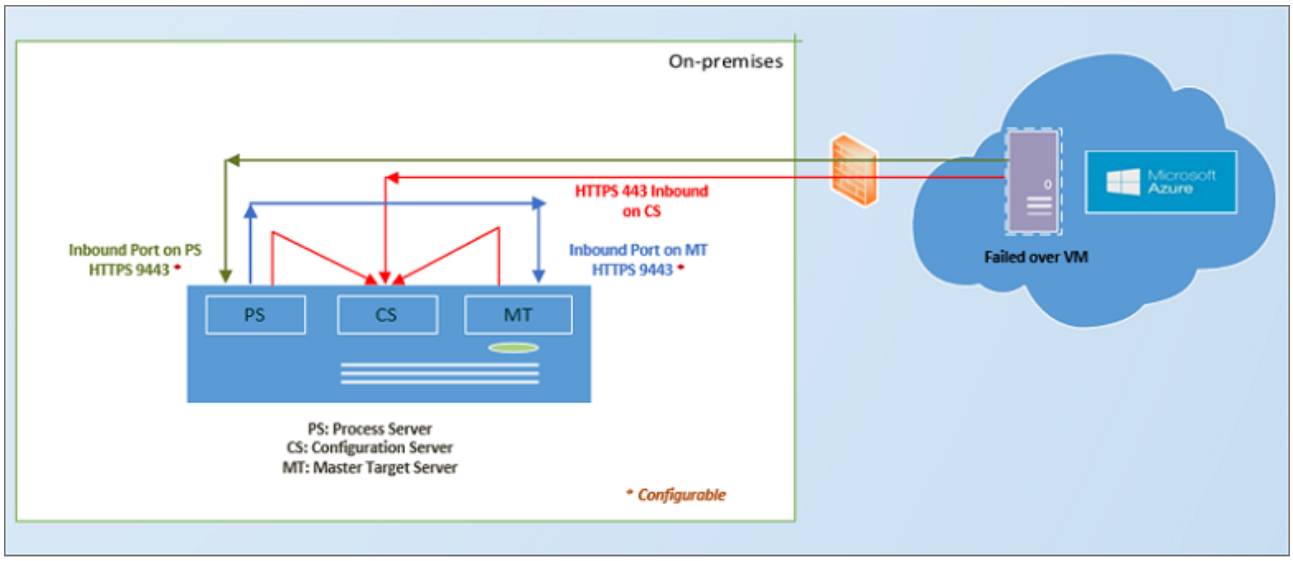
6. ábra: Replikáció VMware-ről Azure-ra
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 20.)

Feladatátvétel és feladat-visszavétel

Ellenőrizni kell, hogy a feladatátvételi teszt a várt módon működik-e. Igény szerint lehetőség van nem tervezett feladatátvételeket futtatni az Azure-hoz. A tervezett feladatátvétel nem támogatott. Elvégezhető egyetlen gép feladatátvétele, vagy létrehozható több virtuális gép feladatátvételét tartalmazó helyreállítási terv is. Feladatátvétel futtatásakor az Azure-ban replikaként létrehozott virtuális gépek jönnek létre. Akkor kell feladatátvételt végezni, ha hozzá akarunk férni a replikaként létrehozott Azure virtuális gép számítási feladataihoz. Amint az elsődleges helyszíni hely megint elérhetővé válik, visszaadható a feladat. Ehhez be kell állítani a feladat-visszavételi infrastruktúrát, el kell kezdeni a gép replikálását a másodlagos helyről az elsődlegesre, valamint nem tervezett feladatátvételt kell futtatni a másodlagos helyről. Ezen feladatátvétel végrehajtását követően az adatok visszakerülnek a helyszíni helyre, és az Azure-ba történő replikációt újra engedélyezni kell.

A feladat-visszavételre vonatkozó követelmények a következők:

- Ideiglenes folyamatkiszolgáló az Azure-ban: ha feladatátvételt követően szeretnénk visszaadni a feladatokat az Azure-ból, be kell állítani egy folyamatkiszolgálóként üzemelő Azure virtuális gépet, amely kezeli az Azure-ból való replikációt. Ez a virtuális gép a feladatok visszaadását követően törölhető.
- VPN-kapcsolat: a feladat-visszavételhez szükséges egy VPN-kapcsolat (vagy Azure Express Route), amelyet a helyszíni hely Azure-hálózatában kell beállítani.
- Önálló helyszíni fő célkiszolgáló: a helyszíni fő célkiszolgáló kezeli a feladat-visszavételt. A fő célkiszolgálót alapértelmezés szerint a felügyeleti kiszolgálóra kell telepíteni, de nagyobb mértékű forgalom feladat-visszavétele esetén érdemes ebből a célból egy önálló helyszíni fő célkiszolgálót is létrehozni.
- Feladat-visszavételi szabályzat: a helyszíni helyre történő újbóli replikáláshoz feladat-visszavételi szabályzatra van szükség. A replikációs szabályzat létrehozásakor a rendszer ezt automatikusan létrehozza.



7. ábra: VMware-/fizikai gépek közötti feladat-visszavétel
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 20.)

Amikor fizikai helyszíni kiszolgálókat replikál az Azure-ba,[134] a replikációs forgatókönyv ugyanazokat az összetevőket és folyamatokat használja, mint a VMware–Azure-replikálás, a következő eltérésekkel:

- VMware virtuális gép helyett fizikai kiszolgálót használhat konfigurációs kiszolgálóként;
- A feladat-visszavételhez helyszíni VMware-infrastruktúrára van szükség. Fizikai gép nem használható a feladat-visszavételhez.

2. táblázat: A Hyper-V – Azure-kapcsolat

Terület	Összetevő	Részletek
Azure	Az Azure-ban szükség van egy Microsoft Azure-fiókra, egy Azure Storage-fiókra és egy Azure-hálózatra.	A Storage és a hálózat lehet Resource Manager-alapú vagy klasszikus fiók. A replikált adatokat a tárfiók tárolja, ha pedig feladatátvétel következik be a helyszíni helyről, a rendszer Azure virtuális gépeket hoz létre a replikált adatokkal. Az Azure virtuális gépek a létrehozásukkor csatlakoznak az Azure virtuális hálózathoz.
VMM-kiszolgáló (VirtualMachine Manager)	VMM-felhőkben lévő Hyper-V-gazdagépek	Ha a Hyper-V-gazdagépeket VMM felhőben felügyeli, a Recovery Services-tárolóban regisztrálja a VMM-kiszolgálót. A VMM-kiszolgálón telepíteni kell a Site Recovery Providert az Azure-ral való replikáció vezényléséhez. A hálózatleképezés konfigurálásához logikai és virtuálisgép-hálózatokat is be kell állítani. Egy virtuális géphálózatot össze kell kötni egy felhőhöz társított logikai hálózattal.
Hyper-V gazdagép	A Hyper-V-kiszolgálók VMM-kiszolgálóval vagy anélkül is üzembe helyezhetők.	Ha nincs VMM-kiszolgáló, a Site Recovery Providert a gazdagépen kell telepíteni, hogy vezényelni tudja az internetes replikációt a Site Recovery-val. Ha van VMM-kiszolgáló, a Provider azon van telepítve, és nem a gazdagépen. A Recovery Services-ügynököt a gazdagépen kell telepíteni az adatreplikáció kezelése érdekében. A Provider és az Agent kommunikációja biztonságos, titkosított csatornákon történik. Ezenfelül az Azure-tárfiókba replikált adatok is titkosítást kapnak.
Hyper-V virtuális gépek	A Hyper-V gazdakiszolgálón legalább egy virtuális gépnek kell lennie.	A virtuális gépekre semmit nem kell explicit módon telepíteni.

Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2019. április 20.)

[134] Lásd: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components (utolsó letöltés: 2017. április 20.)

Replikációs folyamat

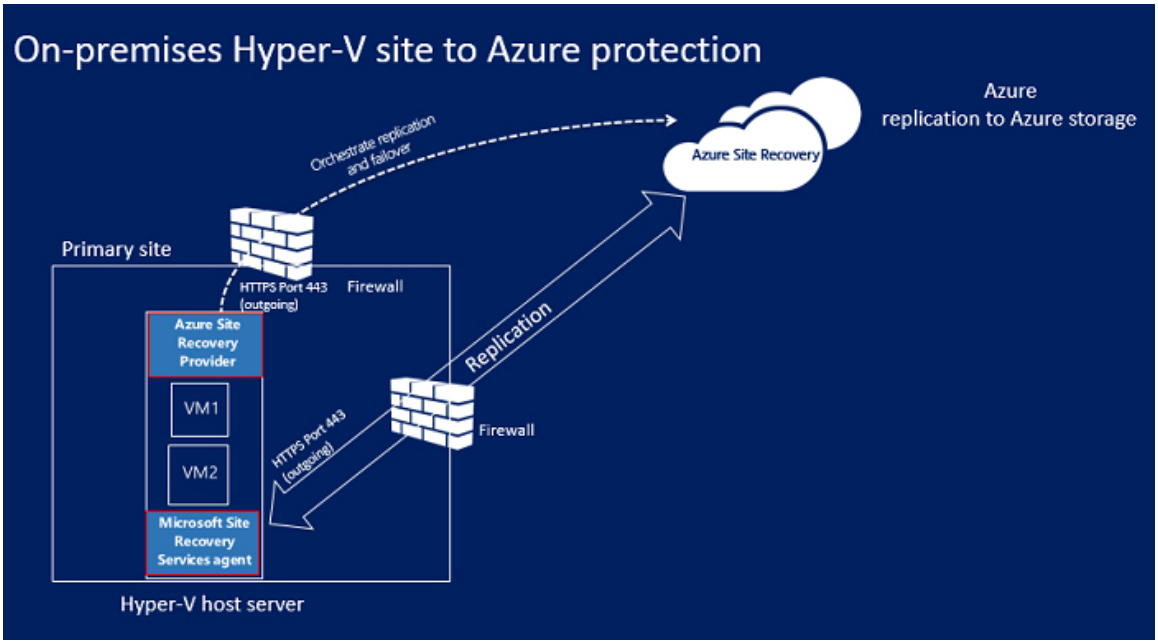
Az Azure-összetevők beállítása: a Site Recovery üzembe helyezésének megkezdése előtt érdemes létrehozni Storage- és hálózati fiókokat.

A replikációs folyamat létrehoz egy replikációs szolgáltatástárolót a Site Recoveryhez, és konfigurálja a tároló beállításait. Ha a Hyper-V-gazdagépeket nem VMM-felhőben felügyelik, létre kell hozni egy Hyper-V helytárolót a cél számára, és hozzáadni Hyper-V-gazdagépeket. Ha a Hyper-V-gazdagépeket VMM-ben felügyelik, a forrás a VMM-felhő, és cél az Azure.

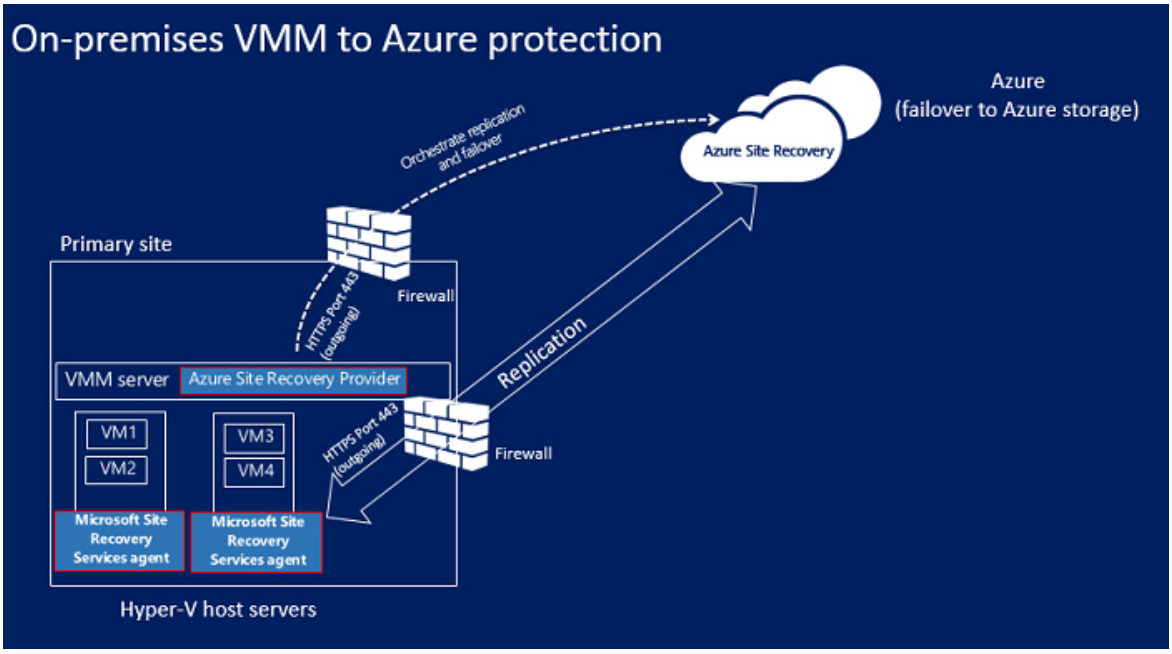
Ha rendelkezésre áll VMM, a Provider arra lesz telepítve, az ügynök pedig az egyes Hyper-V gazdagépekre. Ha nem rendelkezik a szervezet VMM-mel, a Provider és az ügynök is az egyes gazdagépekre lesz telepítve.

Létre kell hozni egy replikációs házirendet a Hyper-V helyhez vagy a VMM-felhőhöz. Azt ezután a rendszer minden, a helyen vagy a felhőben lévő gazdagépen található virtuális gépre alkalmazza. Engedélyezni kell a replikációt a Hyper-V virtuális gépek számára. A kezdeti replikálás a replikációs házirend beállításainak megfelelően történik. Az adatváltozásokat a rendszer nyomon követi, és az Azure változáskülönbözeteinek replikálása a kezdeti replikálás befejezése után kezdődik meg. Az elemek nyomon követett módosításait a rendszer .hrl fájlokban tárolja. Egy teszt feladatátvétel futtatásával ellenőrzi, hogy minden jól működik-e.

Futtatható tervezett vagy nem tervezett feladatátvétel a helyszíni Hyper-V virtuális gépekről az Azure-ra. Ha tervezett feladatátvételt kell elvégezni, a virtuális forrásgépek leállnak, így nincs adatvesztés. Elvégezhető egy gép feladatátadása, de létrehozható akár több gép összehangolt feladatátadását tartalmazó helyreállítási terv is. A feladatátvétel futtatása után a létrehozott replika virtuális gépeknek meg kell jelenniük az Azure-ban. Hozzárendelhető egy nyilvános IP-cím a virtuális géphez, amennyiben szükséges. Ezután véglegesíthető a feladatátvétel, hogy hozzáférhetővé váljanak a replika Azure virtuális gép számítási feladatai. Amint az elsődleges helyszíni hely megint elérhetővé válik, visszaadhatók a feladatok. A folyamat elindít egy tervezett feladatátvételt az Azure-ból az elsődleges helyre. Tervezett feladatátvétel esetében beállítható, hogy a feladat-visszavétel ugyanarra a virtuális gépre vagy egy másik helyre történjen, és szinkronizálhatóvá válnak a módosítások az Azure és a helyszíni hely között. Ennek köszönhetően elkerülhető az adatvesztés. Ha a helyszínen létrejöttek a virtuális gépek, véglegesíthető a feladatátvétel.



8. ábra: Replikálás Hyper-V-helyről az Azure-ba
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 20.)



9. ábra: Replikálás a VMM-felhőkben futó Hyper-V-ről az Azure-ba
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 20.)

Replikálás másodlagos helyre:

- VMware: támogatott gazdagépen futó helyszíni VMware virtuális gépek. A támogatott operációs rendszereket futtató VMware virtuális gépek replikálhatók.
- Fizikai gépek: támogatott operációs rendszereken Windowst vagy Linuxot futtató helyszíni fizikai kiszolgálók.
- Hyper-V: VMM-felhőkben felügyelt, támogatott Hyper-V-gazdagépeken futó helyszíni Hyper-V virtuális gépek, támogatott gazdagépek. A Hyper-V és az Azure által támogatott bármilyen vendég operációs rendszert futtató Hyper-V-alapú virtuális gépet replikálhat.

A VMware-alapú virtuális gépek és a fizikai kiszolgálók az InMageScout használatával replikálhatók egy másodlagos helyre.

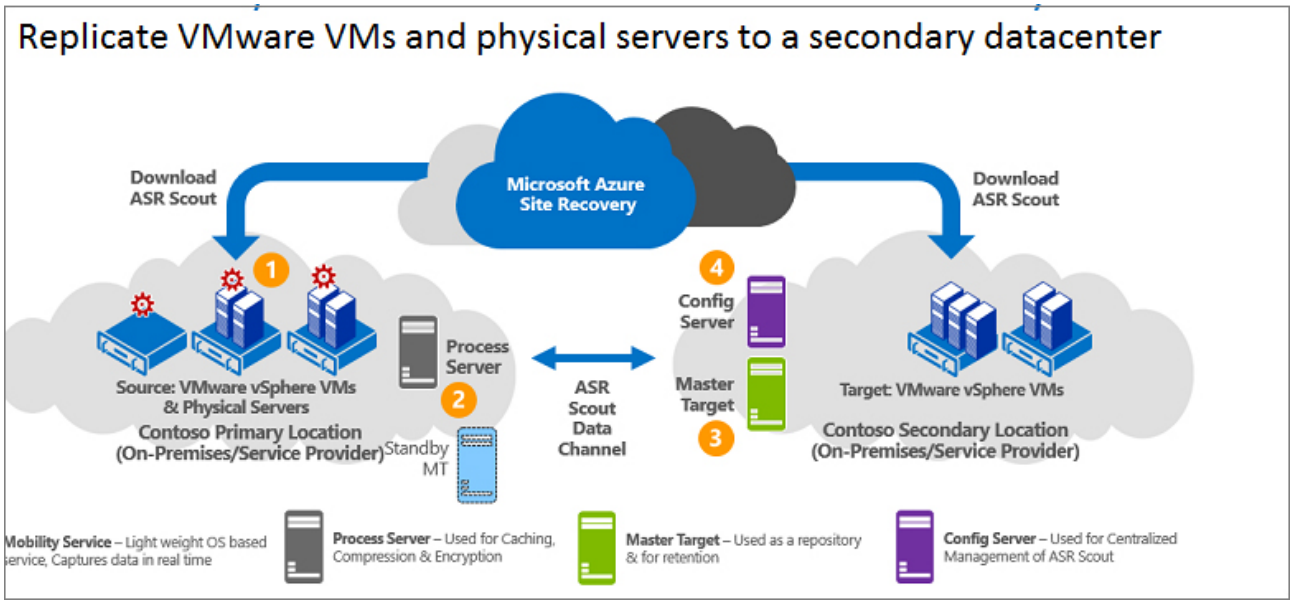
3. táblázat: A VMware alapú gépek és a fizikai kiszolgálók kapcsolata

Terület	Összetevő	Részletek
Azure	InMageScout.	Az InMageScout beszerzéséhez Azure-előfizetésre van szükség. A Site Recovery-tároló létrehozása után, le kell tölteni az InMageScoutot, és telepíteni szükséges a legújabb frissítéseket az üzembe helyezés előkészítéséhez.
Folyamat kiszolgáló	Az elsődleges helyen található.	A folyamatkiszolgáló üzembe helyezésével van lehetőség az adatok gyorsító tárazására, tömörítésére és optimalizálására. Ezenfelül ez az összetevő kezeli a UnifiedAgent ügynöknek a védeni kívánt gépekre történő leküldéses telepítését.

Terület	Összetevő	Részletek
Konfigurációs kiszolgáló	A másodlagos helyen található.	A konfigurációs kiszolgáló végzi az üzemelő példány felügyeleti webhelyen vagy a vContinuum-konzolban végzett felügyeletét, konfigurálását és megfigyelését.
vContinuum-kiszolgáló	Választható. Ugyanoda kell telepíteni, mint a konfigurációs kiszolgálót.	Ez az összetevő elérhetővé tesz egy konzolt, amelyről felügyelhető és figyelhető a védett környezet.
Fő célkiszolgáló	A másodlagos helyen található.	A fő célkiszolgáló tárolja a replikált adatokat. Ez fogadja a folyamatkiszolgáló által küldött adatokat, létrehozza a replikagépet a másodlagos helyen, és tárolja az adatmegőrzési pontokat. Az, hogy hány fő célkiszolgálóra van szükség, attól függ, hogy mennyi gépnek kívánunk védelmet biztosítani. A UnifiedAgent ügynök nincs telepítve ezen a kiszolgálón.
VMware ESX/ ESXi- és vCenter-kiszolgáló	A virtuális gépek ESX-/ ESXi-gazdagépeken futnak. A gazdagépeket egy vCenter-kiszolgáló felügyeli.	A VMware virtuális gépek replikálásához VMware-infrastruktúrára van szükség.
Virtuális gépek/ fizikai kiszolgálók	A replikálni kívánt VMware virtuális gépeken és fizikai kiszolgálókon telepített Unified Agent.	Ez az ügynök valósítja meg az összetevők közötti kommunikációt.

Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2019. április 20.)

A replikációs folyamat során mindkét oldalon be kell állítani az összetevő kiszolgálókat (konfigurációs, folyamat- és fő célkiszolgáló), majd telepíteni kell a replikálni kívánt gépekre a Unified Agent ügynökprogramot. A kezdeti replikációt követően a gépek ügynökprogramjai továbbítják a változás replikálásmódosításait a folyamatkiszolgálónak. A folyamatkiszolgáló optimalizálja az adatokat, majd átviszi őket a másodlagos hely fő célkiszolgálójára. A replikációs folyamatot a konfigurációs kiszolgáló kezeli.



10. ábra: VMware és VMware közötti replikáció
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 20.)

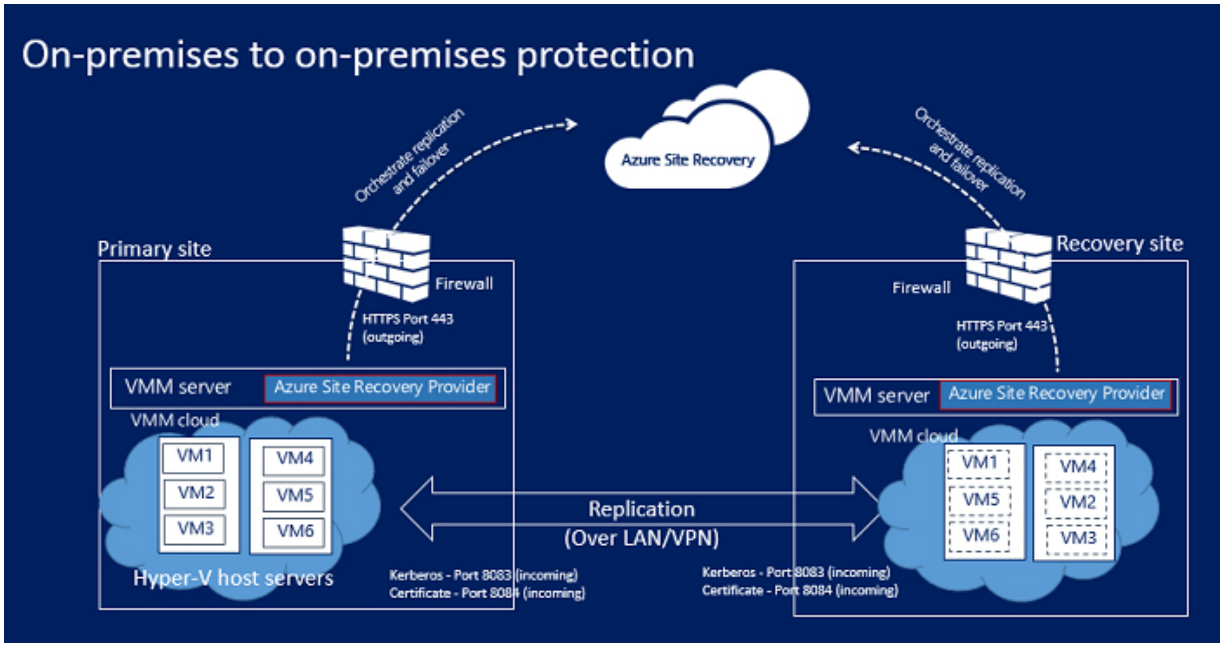
4. táblázat: A Hyper-V-alapú virtuális gépek egy másodlagos helyre való replikálásának feltételei

Terület	Összetevő	Részletek
Azure	Szükség van egy Microsoft Azure-fiókra.	
VMM-kiszolgáló	Javasolt, hogy legyen egy VMM-kiszolgáló az elsődleges helyen, és egy a másodlagos helyen	Mindegyik VMM-kiszolgálónak csatlakoznia kell az internethez. Minden kiszolgálón legyen legalább egy VMM-magánfelhő beállított Hyper-V-kapacitásprofillal. Telepíteni kell az Azure Site Recovery Providert a VMM-kiszolgálóra. A Provider az interneten keresztül koordinálja és valósítja meg a Site Recovery szolgáltatással történő replikációt. A Provider és az Azure közötti kommunikáció biztonságos, titkosított csatornákon történik.
Hyper-V kiszolgáló	Legalább egy Hyper-V gazdakiszolgáló az elsődleges és a másodlagos VMM-felhőkben. A kiszolgálóknak csatlakozniuk kell az internethez. A rendszer LAN vagy VPN hálózaton keresztül replikálja az adatokat az elsődleges és másodlagos Hyper-V gazdakiszolgálók között Kerberos vagy tanúsítványalapú hitelesítés használatával.	

Terület	Összetevő	Részletek
Hyper-V virtuális gépek	A forrás Hyper-V gazdakiszolgálón található.	A forrás gazdakiszolgálókon legalább egy replikálni kívánt virtuális gépnek kell futnia.

Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 10.)

A replikációs folyamat végzője először is beállítja az Azure-fiókot, majd létrehoz egy replikációs szolgáltatástárolót a Site Recoveryhez, és konfigurálja a tároló beállításait, például a replikációs forrást és célt (elsődleges és másodlagos helyek). Ezután az Azure Site Recovery Provider és a Microsoft Azure Recovery Services ügynök telepítése következik. A Provider VMM-kiszolgálókon, az ügynök pedig az egyes Hyper-V gazdagépeken van telepítve. Létre kell hozni egy replikációs házirendet a forrás VMM-felhőhöz. A házirendet ezután a rendszer minden, a felhőben lévő gazdagépen található virtuális gépre alkalmazza. A replikációs folyamat engedélyezi a replikációt a Hyper-V virtuális gépek számára. A kezdeti replikálás a replikációs házirend beállításainak megfelelően történik. Az adatváltozásokat a rendszer nyomon követi, és a változáskülönbözetek replikálása a kezdeti replikálás befejezése után kezdődik meg. Az elemek nyomon követett módosításait a rendszer *.hrl* fájlokban tárolja. Egy feladatátvételi teszt futtatásával ellenőrizni kell, hogy minden jól működik-e.



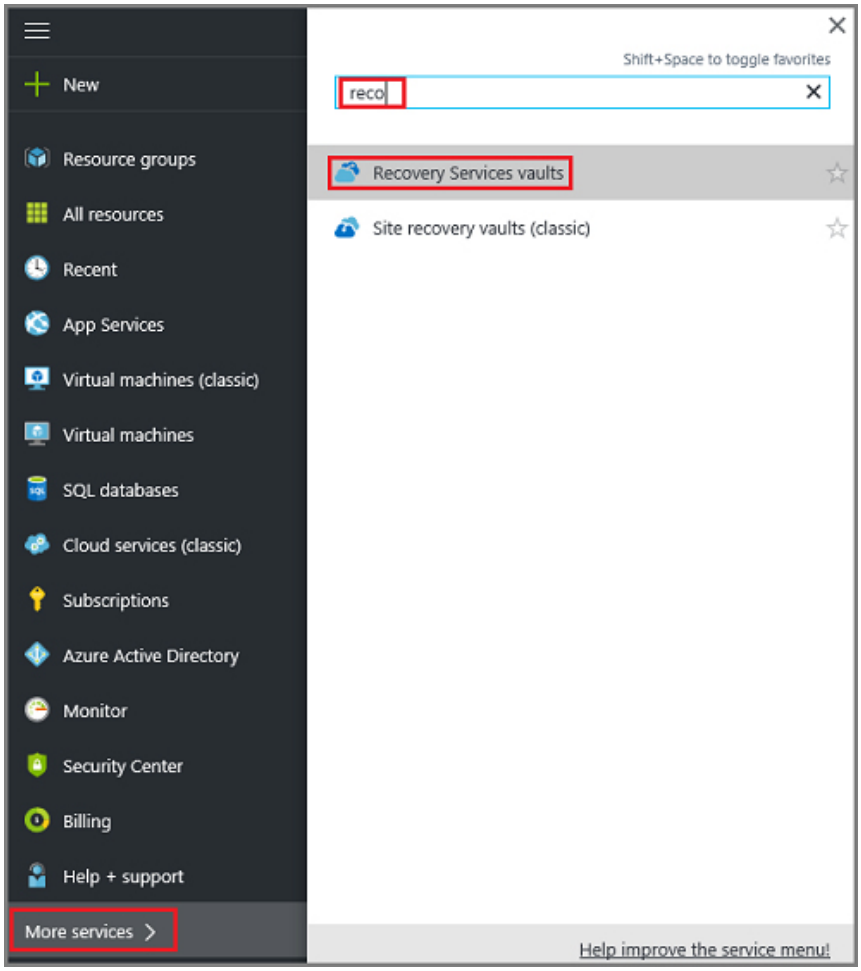
11. ábra: VMM és VVM közötti replikáció
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 10.)

Feladatátvétel és feladat-visszavétel

Futtatható tervezett vagy nem tervezett feladatátvétel a helyszíni helyek között. Ha tervezett feladatátvétel történik, a forrás virtuális gépek leállnak, így nincs adatvesztés. Elvégezhető egy gép feladatátadása, de létrehozható több gép összehangolt feladatátadását tartalmazó helyreállítási terv is.

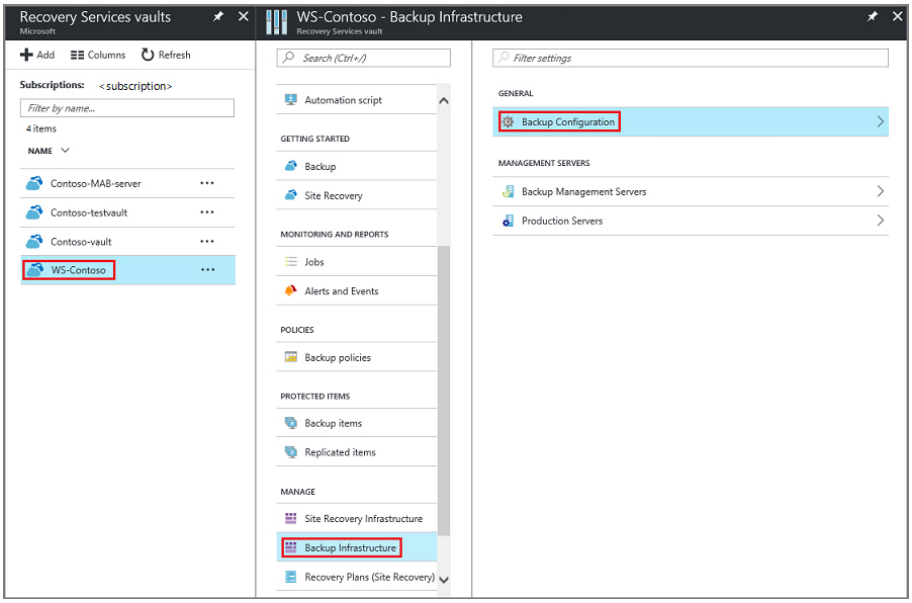
Ha egy nem tervezett feladatátvétel történik egy másodlagos helyre, a feladatátvétel után a másodlagos hely gépei nem engedélyezettek védelemhez vagy replikáláshoz. Ha tervezett feladatátvétel futott, a feladatátvétel után a másodlagos hely gépei védettek lesznek. Ekkor véglegesíthetővé válik a feladatátvétel, így hozzáférhető válnak a replika virtuális gép számítási feladatai is. Amikor az elsődleges hely újra elérhetővé válik, fordított replikálást hajt végre a másodlagos helyről az elsődleges helyre való replikáláshoz. A fordított replikáció során a virtuális gépek védett állapotba kerülnek, de a másodlagos adatközpont marad továbbra is az aktív hely. Ha újra az elsődleges helyet szeretnénk aktív helyként, akkor egy tervezett feladatátvételt kell kezdeményezni a másodlagos helyről az elsődleges helyre, majd ismét fordított replikálást kell végrehajtani.

Recovery Services-tároló létrehozása[135] során a fájlok és mappák biztonsági mentéséhez nyitni kell egy Recovery Services-tárolót abban a régióban, ahol az adatokat tárolni szeretnénk. Emellett a tároló replikálásának módját is meg kell határozni. Ezt követően be kell jelentkezni az Azure Portalra az Azure-előfizetéssel. A központi menüben a *További szolgáltatások* elemre kell kattintani, majd az erőforrások listájába be kell írni a Recovery Services szöveget. Ez után ismét kattintani kell, ezúttal a Recovery Services-tárolók elemeire. Ha az előfizetés Recovery Services-tárolókat tartalmaz, a tárolók fel vannak sorolva. A *Recovery Services-tárolók* menüben a *Hozzáadás* elemre kell kattintani.



12. ábra: Microsoft Azure Portál felülete: RecoveryServices-tárolók
Forrás: https://docs.microsoft.com/hu-hu/azure/backup/backup-try-azure-backup-in-10-mins
(Letöltés ideje: 2017. április 10.)

[135] Forrás: https://docs.microsoft.com/hu-hu/azure/backup/backup-try-azure-backup-in-10-mins (utolsó letöltés: 2017. április 20.)

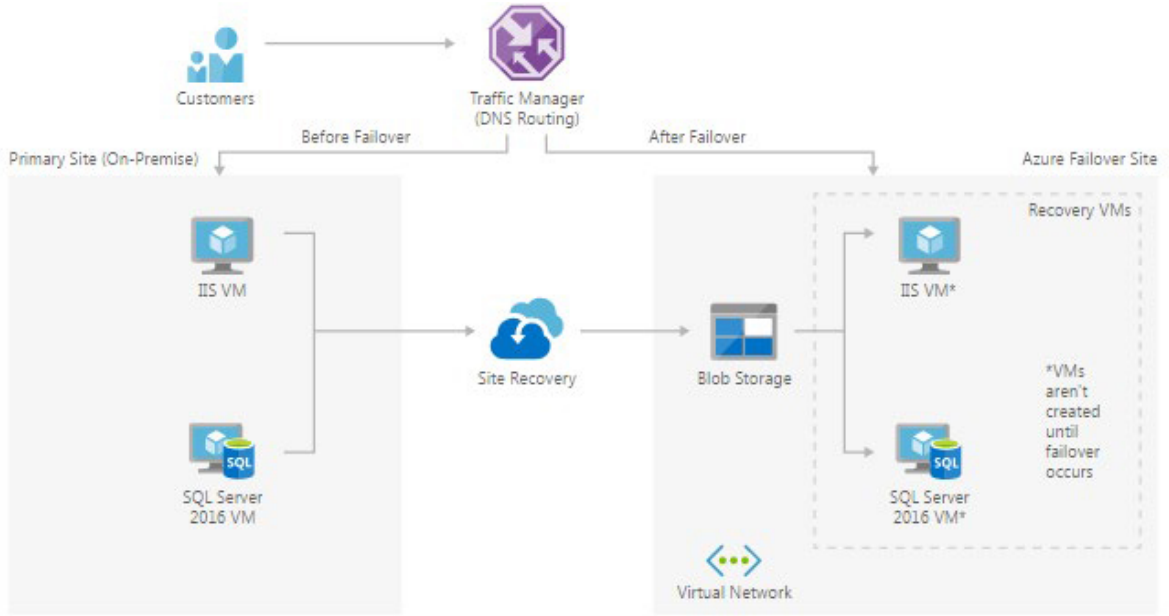


13. ábra: Tároló replikációs beállítás (backup konfiguráció)
Forrás: https://docs.microsoft.com/hu-hu/azure/backup/backup-try-azure-backup-in-10-mins
(utolsó letöltés: 2017. április 10.)

A kis- és középvállalatok az Azure Site Recovery[136] segítségével alacsony költségből valósíthatnak meg vészhelyreállítást a felhőbe. Ez a megoldás az alábbi, Azure által felügyelt szolgáltatásokra épül:

- Traffic Manager,
- Site Recovery és
- Virtual Network.

Ezek a szolgáltatások magas rendelkezésre állású környezetben futnak.



14. ábra: Kis- és középvállalati vészhelyreállítási megoldásarchitektúra az Azure Site Recovery segítségével
Forrás: https://azure.microsoft.com/hu-hu/solutions/architecture/disaster-recovery-smb-azure-site-recovery/
(utolsó letöltés: 2017. április 20.)

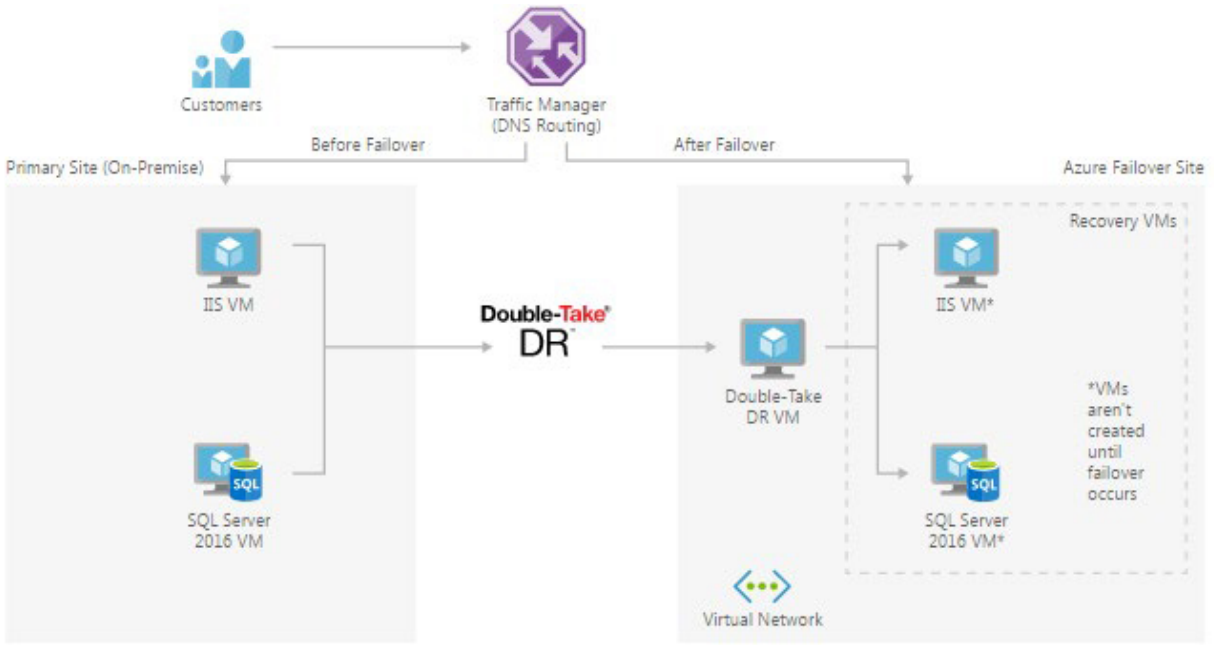
[136] Forrás: https://azure.microsoft.com/hu-hu/solutions/architecture/disaster-recovery-smb-azure-site-recovery/ (utolsó letöltés: 2017. április 20.)

A kis- és középvállalatok alacsony költséggel valósíthatnak meg vészhelyreállítást a felhőbe például a *Double-Take DR* segítségével.

Ez a megoldás az alábbi, Azure által felügyelt szolgáltatásokra épül:

- Traffic Manager,
- VPN Gateway és
- Virtual Network.

Ezek a szolgáltatások magas rendelkezésre állású környezetben futnak.



15. ábra: Kis- és középvállalati megoldás architektúra: SMB vészhelyreállítás a DoubleTake DR megoldással
Forrás: https://azure.microsoft.com/hu-hu/solutions/architecture/disaster-recovery-smb-azure-site-recovery/
(utolsó letöltés: 2017. április 20.)

További, az Azure-megoldások létrehozására szolgáló architektúrákért lásd a következő honlapot: https://azure.microsoft.com/hu-hu/solutions/architecture/ (utolsó letöltés: 2017. április 10.)

8.2. Microsoft Dynamics NAV[137]

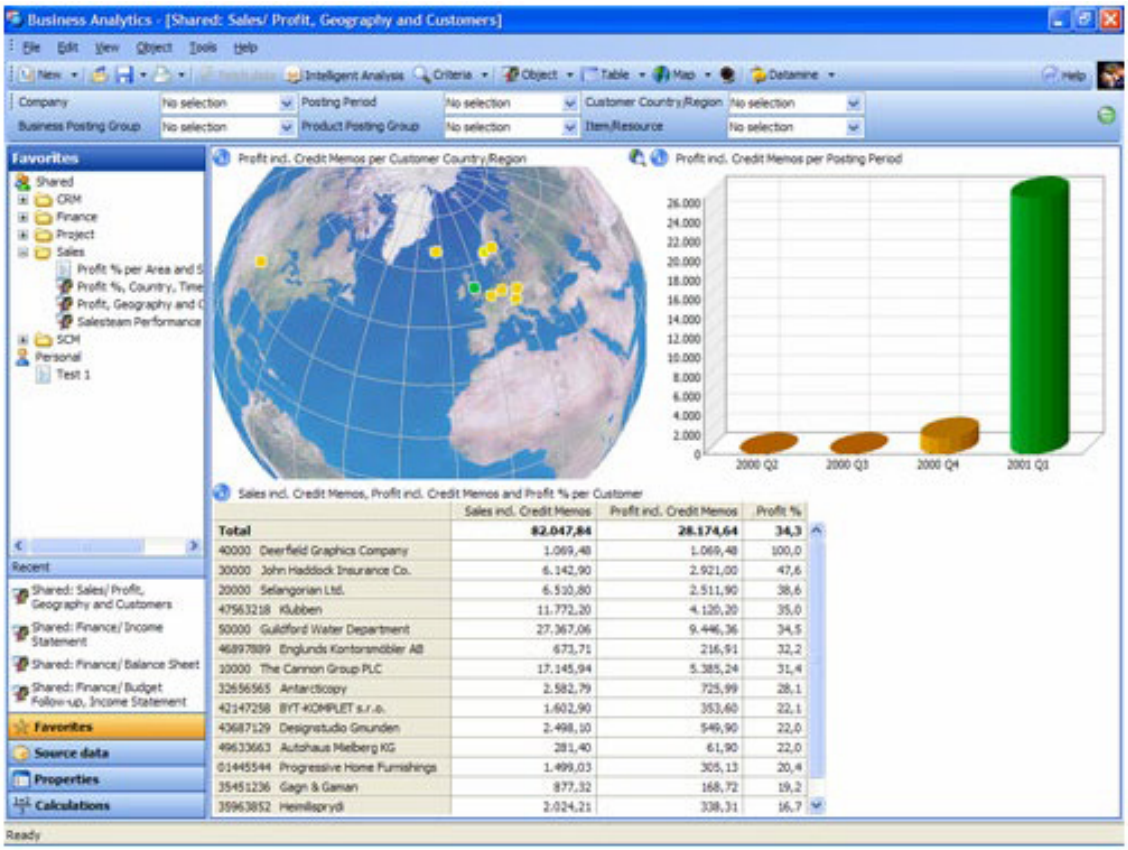
Kritikus informatikai rendszernek számít, tekintve, hogy pénzügyi adatokat kezel, a Microsoft Dynamics NAV (korábbi nevén Navision), amely kis- és középvállalatok számára készült integrált vállalatirányítási rendszer. A Navision nem csupán a már meglévő rendszerek teljes kiváltására alkalmas, hanem részterületekre is bevezethető. A Microsoft vállalatirányítási rendszere együttműködik a meglévő vállalati rendszerekkel, integrált részét képezi a teljes informatikai infrastruktúrának, amellett, hogy a szükséges adatvédelmi paramétereket is tartalmazza.

[137] Forrás: https://navision.hu/microsoft-dynamics-365-business-central/ (utolsó letöltés: 2022. április 6.)

A Microsoft Dynamics NAV vállalatirányítási rendszer az alábbi területeken támogatja a vállalkozások tevékenységét:

- pénzügy;
- eladás és marketing;
- beszerzés;
- raktárkezelés;
- termelésirányítás;
- projektek;
- erőforrás-tervezés;
- szerviz;
- emberi erőforrások.

A Microsoft Dynamics NAV vállalatirányítási rendszer nyitott architektúrája lehetővé teszi, hogy a vállalat üzletmenetéhez igazítsák. A Microsoft Dynamics NAV és a Microsoft technológiák együttes és összehangolt alkalmazása, köztük az Office 365 valamint a Windows Azure biztosítja a vállalati rendszerek integrációját. Az együttműködés eredményeként növekszik a működési biztonság és csökkennek az üzemeltetési költségek.



16. ábra: A Microsoft Dynamics NAV (Navision) felülete (üzleti analitika funkcióival)[138]
Forrás: www.karadi.hu/navision-modulok-reszletes-leirasa *(utolsó letöltés: 2017. április 20.)*

[138] Lásd: http://www.karadi.hu/navision-modulok-reszletes-leirasa (utolsó letöltés: 2017. április 20.)

1. esettanulmány – Fujifilm Magyarország Kft.[139]
Iparág: kereskedelem
Megoldás: Microsoft Dynamics NAV

2010-ben a Fujifilm Magyarország Kft.-nél a több mint tíz éve működő vállalatirányítási rendszert két okból is korszerűbbre kellett cserélni: a tulajdonosváltás következtében új struktúrájú riportokat, és azokat is rövidebb határidővel kellett küldeni, amit azonban a régi ERP megoldással már nem lehetett megvalósítani. Ráadásul a rendszer üzemeltetőitől már semmilyen új fejlesztés nem volt megrendelhető, az alap supportszolgáltatás is legfeljebb a szoftver minimális karbantartására szorítkozott.

2. esettanulmány – Adecco Kft.[140]
Iparág: munkaerő-kölcsönzés
Megoldás: Microsoft Dynamics NAV

Az Adecco Kft.-nél implementált Microsoft Dynamics NAV vállalatirányítási rendszer bevezetésének egyik érdekessége, hogy nem informatikai specialistát bíztak meg a projekt levezénylésével, hanem a gazdasági igazgatót.

3. esettanulmány – Herlitz Hungária Kft.[141]
Iparág: nagy- és kiskereskedelem
Megoldás: Microsoft Dynamics NAV, MobileNAV

A 2011-es zárókészlethez képest a 2012-es évet 30%-kal alacsonyabb készletszinttel zárták, ami nagyjából 20 millió forintos megtakarítást jelentett. Már az első hónapban megtérült a beruházás.

8.3. Az IBM InfoSphere eDiscovery Manager architektúrája (Változat 2.1.1)[142]

Az IBM® InfoSphere eDiscovery Manager strukturálatlan tartalom keresésére, és az IBM FileNet P8 vagy a DB2 Content Manager kiszolgálón tárolt dokumentumok lekérésére szolgál. Az eDiscovery Manager egy olyan alkalmazás, amely Web Sphere Application Server kiszolgálón fut, és dokumentumokat kérdez le a tartalomkezelő rendszerekről. A felhasználók bármilyen támogatott webböngésző segítségével elérhetik az eDiscovery Manager terméket.

Az eDiscovery Manager terméket teljesítménybeli szempontok alapján érdemes az archívumkiszolgálótól eltérő kiszolgálóra vagy logikai partícióba telepíteni.

Az eDiscovery Manager rendszer a következő összetevőket tartalmazza:

- webböngésző;
- e-mailes ügyfél (csak e-mailes dokumentumok esetén szükséges);
- Web Sphere Application Server;
- tartalomkezelő kiszolgáló;
- e-mailes archívumkiszolgáló (csak e-mailes dokumentumok esetén szükséges);
- Rekordkezelő szoftver (nem kötelező).

[139] Lásd: https://navision.hu/microsoft-dynamics-nav-referenciak/ (utolsó letöltés: 2017. április 20.)
[140] Lásd: https://navision.hu/microsoft-dynamics-nav-referenciak/ (utolsó letöltés: 2017. április 20.)
[141] Lásd: https://navision.hu/microsoft-dynamics-nav-referenciak/ (utolsó letöltés: 2017. április 20.)
[142] Lásd: www.ibm.com/support/knowledgecenter/hu/SS8JHU_2.1.1/com.ibm.edc.doc/edcao001.htm (utolsó letöltés: 2017. április 20.)

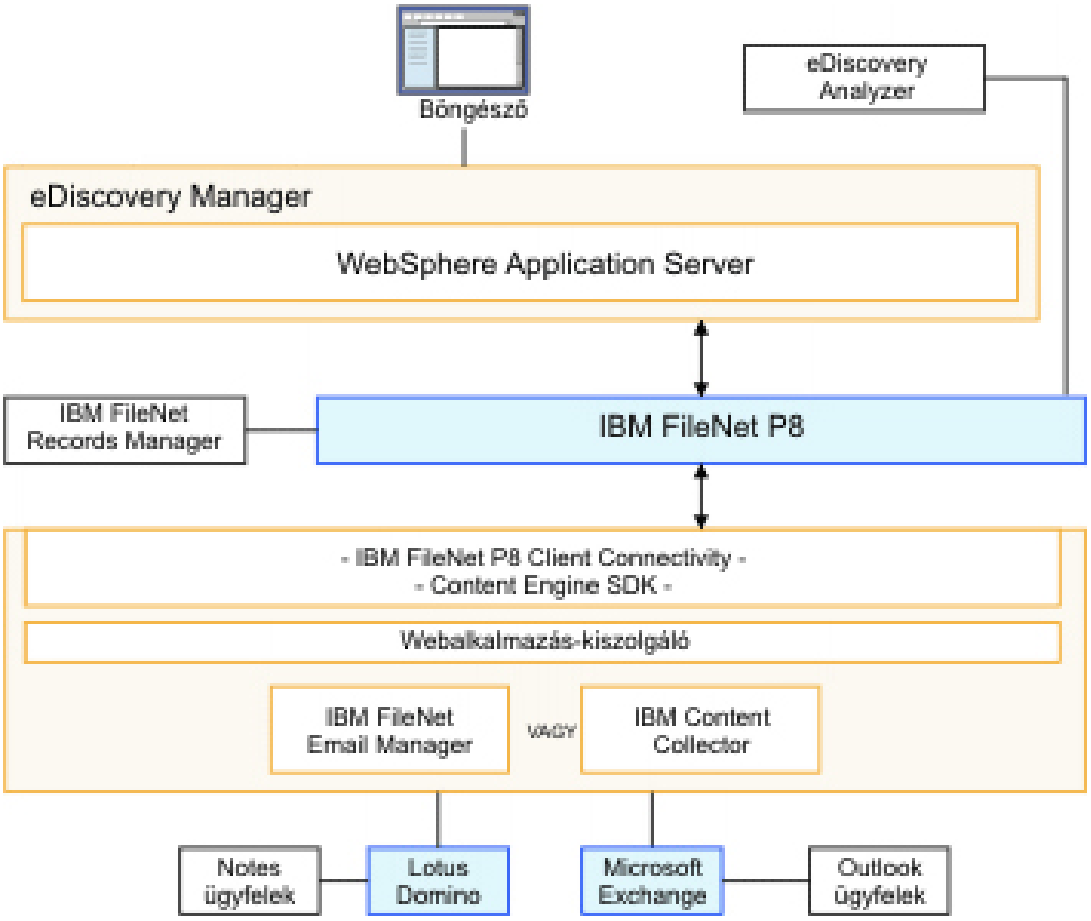
A rendszert eltérő módon kell konfigurálni, attól függően, hogy DB2 Content Manager vagy IBM FileNet P8 terméket használnak.

A Web Sphere Application Server és az archívumkiszolgáló kapcsolatának léteznie kell az eDiscovery Manager számítógépén.

Az eDiscovery Manager Lotus Domino és Microsoft® Exchange e-mail dokumentumokat támogat.

Az eDiscovery Manager integrálható IBM Records Manager termékkel vagy IBM FileNet Records Manager termékkel a megtartási ütemtervek betartatásához. Ha a rekordkezelés integrálva van, az eDiscovery Manager webes ügyfélből rekordként deklarálható egy mappa tartalma. Azonban a rekordkezelés integrációjával, vagy anélkül is az eDiscovery Manager automatikusan is elhelyez felfüggesztéseket azokon a dokumentumokon, amelyeket hozzáad egy esethez, hogy megelőzze azok törlését az archívum kiszolgálón, és megtartsa a tartalmat, amelyre a bírósági eljárás során szükség lehet.

A következő ábra mutatja be az eDiscovery Manager termék és az IBM FileNet P8 archívum kiszolgáló együttes működésének jellemző architektúráját.



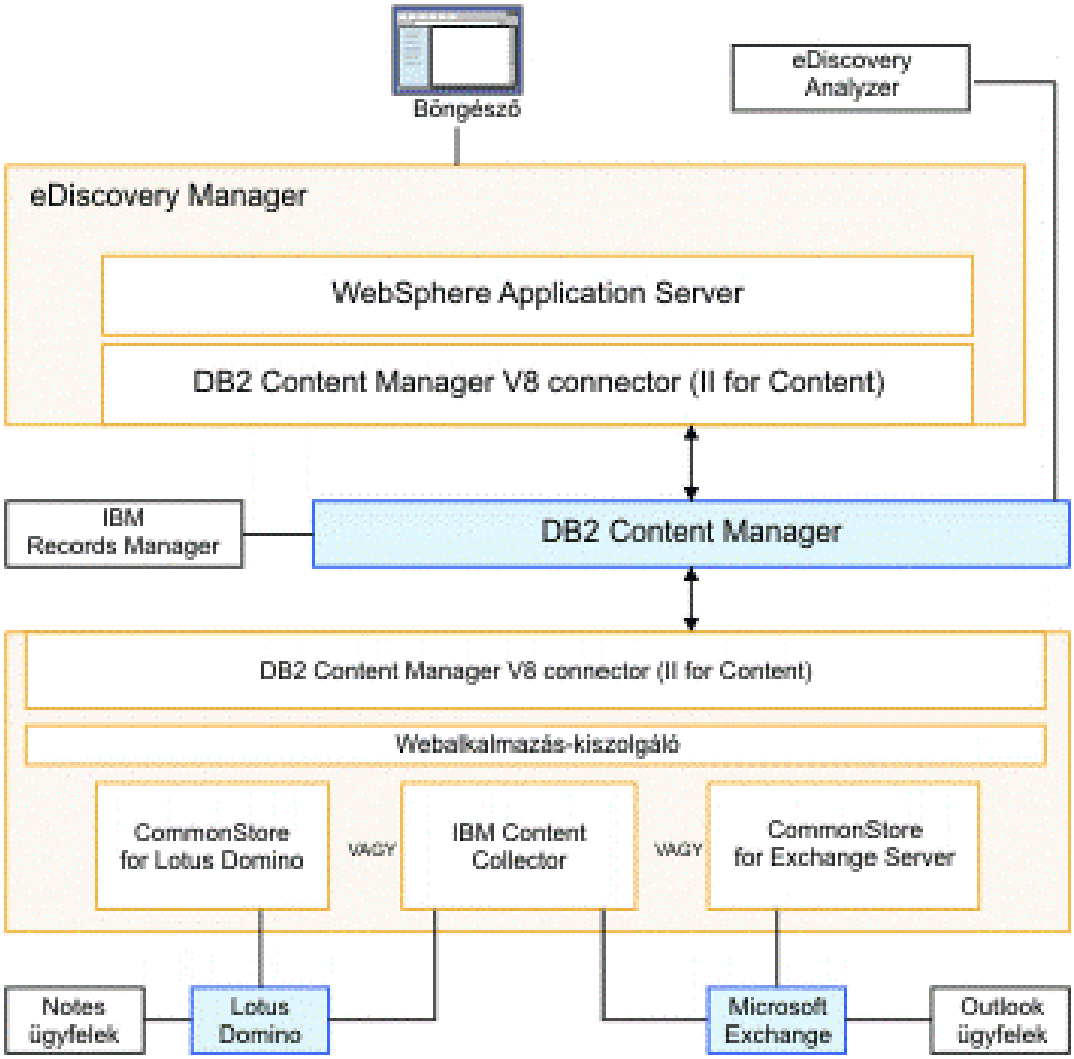
17. ábra: Az eDiscovery Manager és az IBM FileNet P8 archívum kiszolgáló együttes működését jellemző architektúra
Forrás: www.ibm.com/support/knowledgecenter/hu/SS8JHU_2.1.1/com.ibm.edc.doc/edcao001.htm *(utolsó letöltés: 2017. április 12.)*

Ha az IBM FileNet Email Manager terméket IBM FileNet P8 termékkel használják archívumkiszolgálóként, akkor nem végezhető keresés az e-mail törzsében és mellékleteiben.

Az IBM FileNet P8 számára a kapcsolat összetevőt az eDiscovery Manager telepíti.

8.4. DB2 Content Manager

A következő ábra az eDiscovery Manager termék és a DB2 Content Manager archívumkiszolgáló együttes működésének jellemző architektúráját mutatja be.



18. ábra: Az eDiscovery Manager termék és a DB2 Content Manager archívum kiszolgáló együttes működésének jellemző architektúrája
Forrás: www.ibm.com/support/knowledgecenter/hu/SS8JHU_2.1.1/com.ibm.edc.doc/edcao001.htm *(utolsó letöltés: 2017. április 12.)*

A DB2 Content Manager számára telepíteni kell a DB2 Information Integrator for Content DB2 Content Manager v8 kapcsolatot.

8.5. IBM Tivoli Security Policy Manager[143]

Az IBM Tivoli Security Policy Manager leválasztja a biztonsági irányelveket az alkalmazásokról, lehetővé téve az alkalmazásjogosítványok központosítását és egyszerűsítését, valamint az adathozzáférés részletes szabályozását. Az eredmény az alkalmazások és a szolgáltatások megerősített hozzáférés-felügyelete, amely a vállalat egészében javítja a jogszabályi megfelelést és a kormányzást.

[143] Lásd: www-03.ibm.com/software/products/hu/security-policy-manager (utolsó letöltés: 2017. április 20.)

Tivoli Security Policy Manager jellemzői:

- Egyesített, következetes irányelvkezelést és futtatókörnyezet-kikényszerítést nyújt, az alkalmazásokat, adatbázisokat és közvetítőket lefedve.
- A vállalati biztonsági irányelveket IT üzemeltetési utasításokká alakítja át, egyszerűbbé téve az IT-szervezetek számára az igazodást az üzletági döntésekhez.
- Segítséget nyújt a biztonsági irányelvek kezeléséhez szolgáltatásorientált felépítés (SOA) környezetekben, valamint részletes jogosítványok kikényszerítéséhez azzal, hogy központosított adminisztrációs pontként szolgál.
- Lehetővé teszi a jogosítványok kikényszerítésének méretezését és kiváló teljesítményét azzal, hogy láthatóvá teszi a jogosítványokkal kapcsolatos döntéseket távoli vagy helyi módon.
- Nyílt szabványok alkalmazásával nyújt együttműködési képességet és integrációt az adatbiztonsági képességek kiterjesztésére és az IT-befektetések optimalizálására.
- Egyesített, következetes irányelvkezelést és futtatókörnyezet-kikényszerítést nyújt.
- Egyetlen nézetben teszi elérhetővé az alkalmazásszerepeket, az adatjogosítványokat és a részletes irányelv-kényszerítést.
- Központi irányelvdöntési forrást biztosít az üzenetvédelem és az összetett jogosultsági irányelvek kezelésére.
- A megfelelés bemutatásának elősegítésére lehetővé teszi a vállalati biztonsági irányelvek összeállítását, átalakítását, elosztását, kikényszerítését és megfigyelését.
- Robusztus biztonsági futtatókörnyezetet kínál szolgáltatásként, leválasztva a natív hitelesítési és jogosultsági képességeket az alkalmazásokról.
- A vállalati biztonsági irányelveket IT üzemeltetési utasításokká alakítja át.
- A vállalat által megadott paraméterek használatával teszi lehetővé a biztonsági irányelvek és üzleti jogosítványok meghatározását és rögzítését.
- Varázsló alapú felhasználói felületet kínál, amellyel az alkalmazástulajdonosok meghatározhatják az alkalmazás- és adatjogosítványokat.
- Leképezi a paramétereket az IT számára, konfigurálva és elosztva az utasításokat a célirányelv-kikényszerítési pontok számára.
- Lehetővé teszi az adminisztrátorok számára a biztonsági szabályok szervezését, kezelését és kikényszerítését.
- Lehetővé teszi az egyesített irányelvkezelést a több tartományon és üzletágon átnyúló együttműködés érdekében.
- Segítséget nyújt a biztonsági irányelvek kezeléséhez szolgáltatásorientált felépítés (SOA) környezetekben, valamint részletes jogosítványok kikényszerítéséhez.
- Közzéteszi a webszolgáltatás-irányelveket a szolgáltatás-nyilvántartás számára, vagy terjeszti több kikényszerítési pont számára.
- Szerepek, tranzakciók és szolgáltatás/erőforrásszint-kontextusok használatával teszi lehetővé az adminisztrátorok számára az alkalmazás- és adatjogosítványok létrehozását és kezelését.
- Lehetővé teszi a jogosítványok kikényszerítésének méretezését és kiváló teljesítményét.
- Horizontálisan és vertikálisan is méretezhető a változó üzleti igényekhez történő alkalmazkodás érdekében.
- Támogatja az azonosságközvetítési és jogosultságellenőrzési szolgáltatásokat, a részleges irányelv-replikálást és a döntés-gyorsítót árazást.
- Támogatja azokat a beépülő modulokat, amelyek natív módon kényszerítik ki a szabványalapú irányelv-lekérdezéseket, és képes az olyan egyedi alkalmazások támogatására, mint a Java, a .net és a nagyszámítógépes alkalmazások.
- A döntések értékeléséhez és megjelenítéséhez több ponttól származó információkat használ.
- Nyílt szabványok alkalmazásával nyújt együttműködési képességet és integrációt.
- Integrációt nyújt az adat- és alkalmazásjogosítványok kezeléséhez többek között a következőkhöz: Java, portálok, webszolgáltatások, vállalati tartalomkezelők.

- Képes az alkalmazásszerepek importálására és integrálható a meglevő identitásrendszerekkel és szabványokkal, például XACML, WS-Trust és WS-Policy.
- Nyílt szabványokra épülő integrációt nyújt szolgáltatás-nyilvántartásokkal, Microsoft, Oracle, SAP és egyéb külső alkalmazásokkal.
- Szolgáltatásfelületek és irányelvkifejezések széles skáláját támogatja.

8.6. A HP iparági szabványai

A HP felügyeleti megoldásai más rendszerfelügyeleti alkalmazásokba integráltak, és az alábbi szabványokra épülnek:

- Web-Based Enterprise Management (WBEM);
- Windows Management Interface (WMI);
- hálózatról történő rendszerindítás technológiája;
- ACPI;
- SMBIOS;
- rendszerindítást megelőző végrehajtás (PXE) támogatása.

8.7. A Symantec HP Client Manager szoftvere[144]

A Symantec és az Altiris közös fejlesztésű HP Client Management szoftvere minden támogatott üzleti célú és hordozható számítógéphez, illetve munkaállomáshoz ingyenesen beszerezhető. Az SSM a HP Client Manager beépített része, használatával lehetőség nyílik a HP ügyfélrendszerek hardvereszközeinek központi felügyeletére, nyomon követésére és ellenőrzésére.

A Symantec HP Client Manager szoftverének alkalmazási területei:

- Tájékozódás a hardverre vonatkozó fontos információkról (például a processzor-, memória-, video- és biztonsági beállításokról).
- A rendszerállapot figyelése a problémák előfordulásuk előtt történő kijavítása érdekében.
- Az illesztőprogramok és BIOS-frissítések automatikus másolása és telepítése, az egyes számítógépek felkeresése nélkül.
- A BIOS- és a biztonsági beállítások távoli konfigurálása.
- Folyamatok automatizálása a hardverproblémák gyors megoldása érdekében.
- Szoros integráció a HP Instant Support eszközökkel, amely csökkenti a hardverhibák elhárításához szükséges időt.
- Diagnosztika – jelentések távoli futtatása és megtekintése a HP asztali számítógépeken, hordozható számítógépeken vagy a munkaállomásokon.
- Rendszerállapot felmérése – a HP ügyfélrendszereket érintő ismert hardverproblémák ellenőrzése.
- Csevegés – kapcsolatfelvétel és problémamegoldás a HP ügyféltámogatással.
- HP Tudásbázis – hozzáférés a szakemberek információihoz.
- Automatikus SoftPaq összegyűjtési és kézbesítési folyamat a hardverproblémák gyors megoldásához.
- Rendszerek azonosítása, leltározása és indítása a HP ProtectTools beágyazott biztonsági lapkával.

[144] Útmutató a számítógépek felügyeletéhez Üzleti célú asztali számítógépek (2008). Harmadik kiadás. Hewlett-Packard Development Company, 9. Elérhetőség: http://h10032.www1.hp.com/ctg/Manual/c01536262 (utolsó letöltés: 2017. április 20.)

- Rendszerállapot-riasztások megjelenítésének lehetősége az ügyfélszámítógépen.
- Alapvető leltárinformációk jelentése nem HP-ügyfelek számára.
- A TPM biztonsági áramkör telepítése és konfigurálása.
- Az ügyfelek biztonsági mentésének és helyreállításának központi ütemezése.
- Az Intel AMT technológiájának bővítményeken keresztüli támogatása.

8.8. HP ProtectTools Security Manager[145]

A HP ProtectTools Security Manager szoftver olyan biztonsági szolgáltatásokat biztosít, amelyek védelmet nyújtanak a számítógéphez, a hálózatokhoz és a kritikus adatokhoz való illetéktelen hozzáféréssel szemben. A fokozott biztonsági funkcionalitást a következő szoftvermodulok biztosítják:

- Credential Manager for HP ProtectTools;
- Embedded Security for HP ProtectTools;
- Java Card Security for HP ProtectTools;
- BIOS Configuration for HP ProtectTools;
- Drive Encryption for HP ProtectTools;
- Device Access Manager for HP ProtectTools;
- File Sanitizer szoftvermodul a HP ProtectTools programhoz;
- Privacymanager szoftvermodul a HP ProtectTools programhoz.

A számítógéphez választható szoftvermodulok a modelltől függően változhatnak. Az Embedded Security for HP ProtectTools modul például csak olyan gépeken érhető el, amelyek fel vannak szerelve Trusted Platform Module (TPM) beágyazott biztonsági lapkával.

8.9. HP Backup and Recovery Manager[146]

A HP Backup and Recovery Manager egy egyszerűen használható és sokoldalú alkalmazás, amelynek segítségével biztonsági mentés készíthető a számítógép elsődleges merevlemezéről, és szükség esetén helyreállíthatók az adatok. Ez az alkalmazás a Windows rendszeren belül működik, és arról, valamint minden alkalmazásról és minden adatfájlról készít biztonsági másolatot. A biztonsági mentések ütemezhetők úgy, hogy meghatározott időközönként automatikusan megtörténjenek, de manuálisan is elindíthatók. A fontos fájlok a rendszeres mentésektől külön is archiválhatók

A HP Backup and Recovery Manager program előre van telepítve a C: meghajtón, és egy helyreállítási partíciót hoz létre.

A HP kifejezetten ajánlja, hogy még a számítógép használatba vétele előtt készüljenek helyreállító lemezek, és a helyreállítási pontok rendszeres és automatikus biztonsági mentése ütemezve legyen.

A különböző típusok vPro vagy hagyományos technológiát tartalmaznak. Mindkét megoldás lehetővé teszi a hálózatba kapcsolt számítástechnikai eszközök hatékony felismerését, javítását és védelmét. Mindkét technológia lehetővé teszi a személyi számítógépek felügyeletét a rendszer bekapcsolt, kikapcsolt és az operációs rendszer felfüggesztett állapotában is.

---

145 Útmutató a számítógépek felügyeletéhez Üzleti célú asztali számítógépek (2008). Harmadik kiadás. Hewlett-Packard Development Company, 7. Elérhetőség: http://h10032.www1.hp.com/ctg/Manual/c01536262 (utolsó letöltés: 2017. április 20.)

146 Útmutató a számítógépek felügyeletéhez Üzleti célú asztali számítógépek (2008). Harmadik kiadás. Hewlett-Packard Development Company. Elérhetőség: http://h10032.www1.hp.com/ctg/Manual/c01536262 (utolsó letöltés: 2017. április 20.)

A felügyeleti technológia funkciói:

- hardverleltár;
- riasztás;
- energiagazdálkodás (be- és kikapcsolás, újraindítás);
- távoli diagnosztika és javítás (Serial-over-LAN: távoli számítógép irányítása a konzolról a rendszerindítási fázisban; IDE-átirányítás: rendszerindítás távoli rendszerindító meghajtóról, lemezről vagy ISO képfájlról);
- hardveralapú elkülönítés és helyreállítás: a számítógép hálózati elérésének korlátozása vagy megszüntetése vírusgyanús tevékenység észlelése esetén.

A rendelkezésre álló felügyeleti technológiák az AMT (DASH 1.0-val) és az ASF.

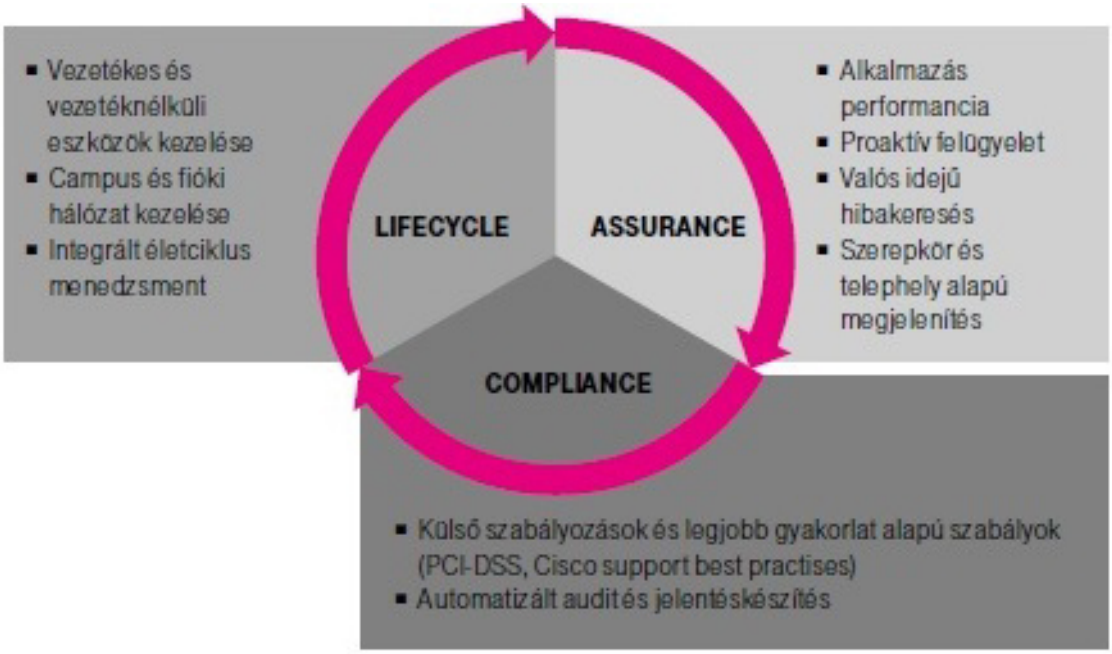
8.10. T-Systems – Cisco Prime architektúra[147]

A kommunikációt kezelő infrastruktúrák szintén a kritikus rendszerek közé sorolhatók, mint ahogy például a T-Systems Magyarországnál alkalmazott Cisco Prime Infrastructure konvergens szolgáltatás is, amely a vezetékes és vezeték nélküli eszközök teljes életcikluson átívelő menedzsmentjére (akár campus-, akár telephelyi hálózat esetén) megoldást jelent. Ugyanis nagyfokú segítséget nyújt a végfelhasználói kapcsolatokkal és az alkalmazások teljesítményével összefüggő problémák felderítéséhez. Robusztus megfelelőségi és jelentéskészítési képességek jellemzik, amellett, hogy lehetővé teszi az alkalmazások teljesítményének mélyreható vizsgálatát, és az üzemeltetők számára eszközkészletet biztosít a hatékony hibaelhárításhoz. A legfontosabb dolog, hogy az üzemeltetéshez elengedhetetlen funkciók elérésére egy közös felület áll rendelkezésre.

Az egyszerűsített Lifecycle, Compliance és Assurance licencmodell segítségével választható ki, határozható meg a kívánt funkcionalitás:

- design: felmérés, tervezés, új szolgáltatások létrehozása, szabályok definiálása;
- deploy: hálózati változások időzített terítése, audit baseline-ok definiálása;
- operate: napi üzemeltetési feladatok ellátásának biztosítása, központosított eseménykezelés és értesítés;
- administer: menedzsmentszolgáltatások kezelése, frissítése, magas rendelkezésre állás, integrációk.

[147] CisCo Prime Infrastructure – Új generációs hálózatfelügyeleti megoldás. T-System. Elérhetőség: www.t-systems.hu/static/sw/file/cisco_prime_infrastructure.pdf (utolsó letöltés: 2017. április 12.)



19. ábra: Üzemeltetési feladatok támogatása a teljes életcikluson keresztül
Forrás: CisCo Prime Infrastructure – Új generációs hálózatfelügyeleti megoldás. T-System.
Elérhető: www.t-systems.hu/static/sw/file/cisco_prime_infrastructure.pdf
(utolsó letöltés: 2017. április 12.)

A megoldás alkalmazása során realizálható előnyök közé tartozik például, hogy egyetlen központosított felületen láthatók az üzemeltetés számára kritikus adatok, valamint, hogy lehetséges az eszközök központi konfigurálása template-ek segítségével – legyen az vezetékes vagy vezeték nélküli. Az eszközök szoftverfrissítése központosítottan végrehajtható és adott a biztonsági megfelelőség automatizált ellenőrzése és biztosítása.

8.11. T-Systems: NMSDB-megoldás az optimalizált üzemeltetésért[148]

Egy másik T-Systems megoldás az eddig felmerült ügyféligényekre épülő, saját fejlesztésű szoftverrel támogatott hálózatfelmérési, -dokumentálási és -üzemeltetési szolgáltatás, amelynek neve NMSDB (Network Management System Database).

Ez segíti az információk konzisztens tárolását, kezelését, valamint a nyilvántartási hibák kiszűrését, megakadályozza ilyen hibák létrehozását, ugyanakkor jelentősen redukálja a kezelés munkaigényét. Önmagában, illetve más szoftvereszközökkel együttműködve komplett monitoring szolgáltatást ad, és minimális adatbevitel mellett komplett dokumentációt állít elő.

Kliensmentes webfelület, manuálisan és automatikusan is használható adat import-export funkciók jellemzik. A rendelkezésre állást méri, és riportolja a menedzseltnek beállított eszközökre, illetve interfészekre. Főbb funkciói közé tartozik a hardware inventory (standard Entity MIB) és az eszközkonfiguráció begyűjtése (alapvetően Cisco IOS-alapú hálózati eszközökre), valamint az eszközök automatikus felvétele, karbantartása MS DHCP log alapján. Szinkronizálja az eszközökből az interfészeket, azok leírásait és IP-címeit az adatbázisba, rögzíti a tervezett eszközt, interfészt, IP-címet. A foglalt IP-címeket tetszőleges IP-tartományra riportolja. MAC- és ARP-tábla kiolvasásával követi

[148] Lásd: www.t-systems.hu/static/sw/file/Network_management_system_database.pdf
(utolsó letöltés: 2017. április 12.)

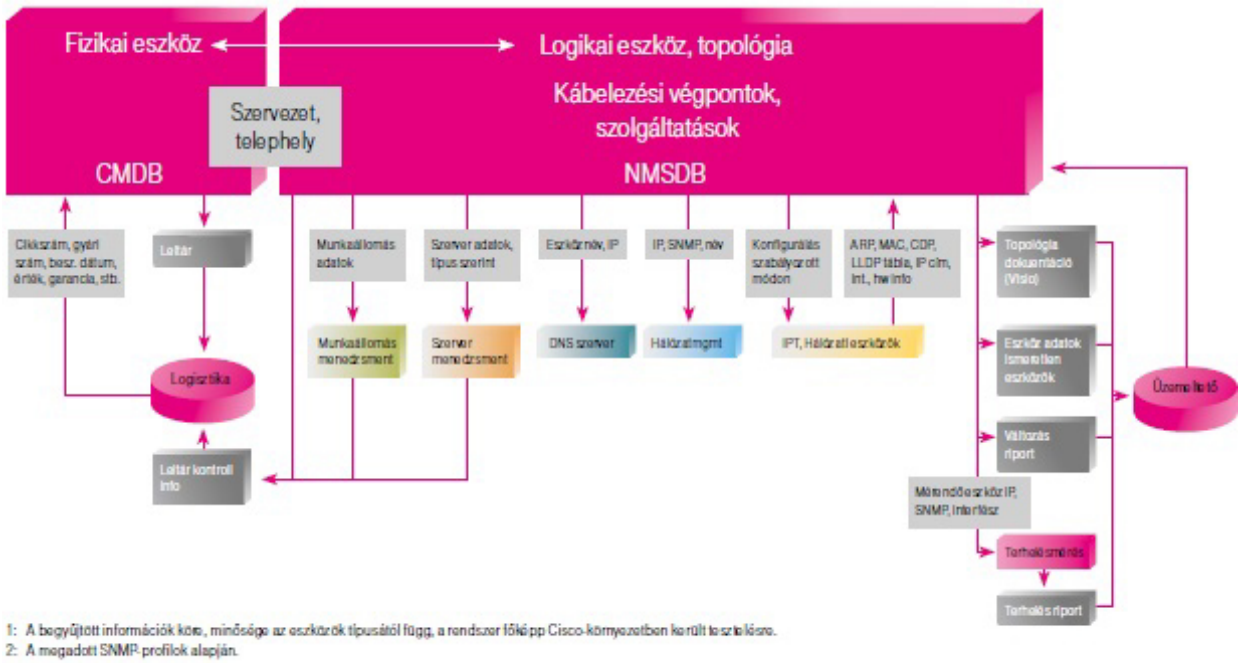
az eszközöket (melyik switchporton, milyen felhasználói MAC forgalmazott). Az NMSDB felderíti az eszközök közti Layer2-kapcsolatokat (CDP, eszközkövetés, a kapcsolatok eltárolása), automatikus kereső funkció jellemzi. Ez a T-System megoldás gyűjti be a Layer3-topológiát az eszközökből, s a felderített Layer2-, Layer3-topológiát telephelyi bontásban tartalmazó dokumentációt automatikusan elkészíti MS Visióban. E szolgáltatás révén biztosított a lehetőség a LAN-on forgalmazó eszközök automatikus felvételére (passzív módú, azaz pollozás nélküli automatikus végpontkeresés, ami IP-címmel nem rendelkező eszközöket is felfedez), IP-címes eszközöknél a DNS figyelembevételével. Elvégzi a konfigurációmentést a hálózati eszközökből, és megjeleníti azokat a webfelületen. Tárolja és kapcsolókhoz köti a LAN-kábelezési végpontokat.

Az NMSDB szolgáltatás további főbb funkciói:

- Cisco IP-telefonok automatikus importja CallMangerből, típus, gyári szám, MAC, telefonszám, csengetési név szerinti keresés;
- Cisco switch portok konfigurálása webfelületről (sebesség, duplexitás, VLAN, port védelem) oly módon, hogy a kezelhető portok köre, az ott beállítható VLAN-ok eszközönként és felhasználónként korlátozhatók;
- nem regisztrált eszközök felderítése (eszközkövetés alapján) ;
- interfészeken forgalom és hiba mérése és grafikonos megjelenítése, előbbi CBWFQ-osztályok szerint is;
- ICMP- és SNMP-alapú státuszfigyelés, topológiaalapú korreláció;
- a monitorozott eszközök, interfészek köre testre szabáskor szabály alapúra beállítható, így egy új eszköz a megjelenése után azonnal a kívánt szabályok alapján monitorozottá válhat;
- a kiesések tárolása adatbázisban;
- fejlett topológia alapú korreláció tetszőleges topológiára, beleértve a multipont L2- és L3-hálózatokat, csatornás kialakítást. Például egy fiók vonalhibája esetén a kapcsolódó csatorna interfészek hibája fiók- és központoldalon is elnyomásra kerül, a vonalat fogadó interfész hibájából pedig egyből vonali hiba generálódik;
- időbeni korreláció (rövid hibák elnyomása, billegés észlelése);
- az adatbázisból tetszőleges riport készíthető webfelületen, jogosultsággal elérhető módon, ez XLS, PDF, CSV formátumba exportálható módon;
- szolgáltatások nyilvántartása (analóg telefonvonal, bérelt vonal stb.) eszközinterfészekhez rendelhető módon, tetszőleges egyéb attribútum (például költséghely) hozzárendelésével.

Ezen elvárásokat összességében csak egy olyan üzemeltetéstámogató rendszerrel lehet megvalósítani, amely biztosítja a csak manuálisan bevihető információk konzisztens tárolását, monitorozást végez (jelzi a hibákat, jó esetben még a bekövetkezés előtt), amit lehet, azt a tényleges rendszerekből olvassa ki (felderítéssel), és ezzel automatizálja a dokumentációfrissítést, továbbá felszínre hozza az ismeretlen eszközöket, és támogatja a hardverleltár ellenőrzését.

Az NMSDB gyakorlatilag egy olyan virtuális berendezés, amely minden olyan eszközt észlel és nyilvántartásba vesz, amely IP-címmel rendelkezik: switcheket, routereket, IP-alapú telefonkészülékeket, szervereket és minden egyéb hálózati „entitást”.



20. ábra: NMSDB (Network Management System Database) felépítése
Forrás: www.t-systems.hu/static/sw/file/Network_management_system_database.pdf
(utolsó letöltés: 2017. április 12.)

9. Nyilvános kulcsú infrastruktúraarchitektúrák (Public key infrastructure models)[149]

Kritikus információs rendszerek közé tartozik a magyar kormányzat infrastruktúrája is, ezért a magyar honvédségnek készült PKI rendszerprojektből kiragadva kerülnek bemutatásra a PKI architektúrák.

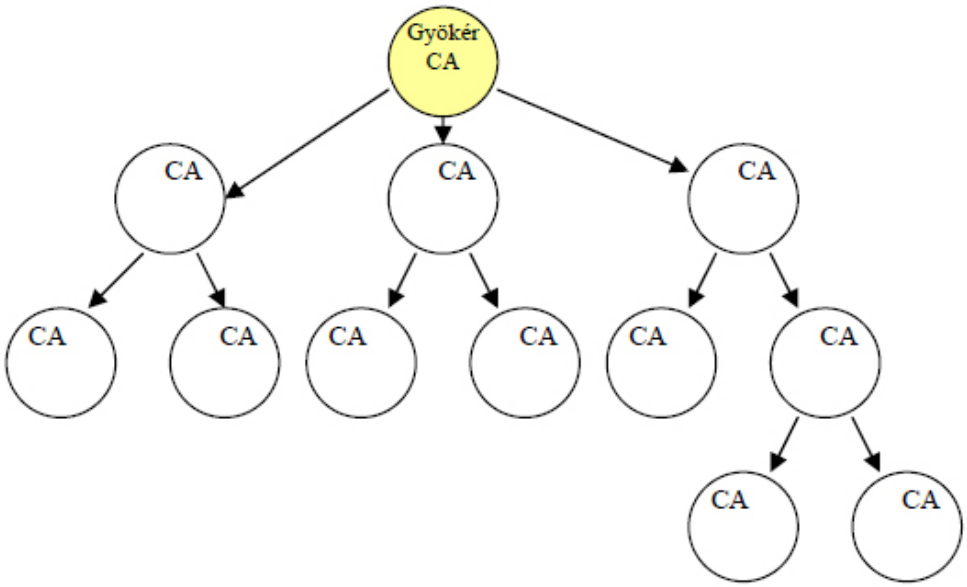
A magyar honvédség esettanulmányából kiderült, hogy kialakításra került a nyilvános kulcsú infrastruktúra (Public Key Infrastructure – PKI).

A rendszerrel szemben támasztott nyilvánvaló követelmény többek között az volt, hogy illeszkedjen azokhoz a PKI architektúrákhoz, amelyekkel küldetéséből adódóan kapcsolódnia kell (például a magyar kormányzati PKI, a NATO-PKI és az EU-val kialakítandó PKI rendszerrel is).

A PKI elemeit különböző architekturális felépítésben lehet elhelyezni:

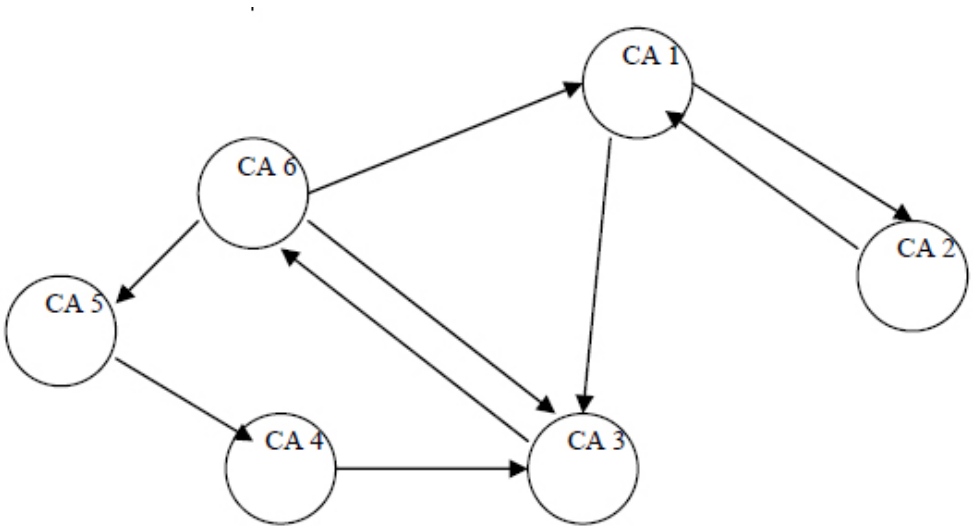
Hierarchikus architektúra: lényege, hogy létezik egy gyökér CA (Hitelesítés Szolgáltató – Certification Authority; CA), amely minden alárendelt CA, illetve felhasználó bizalmát élvezi. A gyökér CA a hierarchiában alatta elhelyezkedő CA-k részére bocsát ki tanúsítványokat, akik részükről szintén, a hierarchiában alattuk levő CA-k részére állítanak ki tanúsítványokat. Minden CA kiállíthat felhasználók számára is tanúsítványt.

[149] Spisák Andor (2006): Nyilvános kulcsú infrastruktúra architektúrák – Public Key Infrastructure Models. Hadmérnök, 1. évf. 1. sz. 31.



21. ábra: Hierachikus PKI architetktúra
Forrás: Spisák (2006): i. m., 33.

Szövevényes architektúra:[150] ebben az esetben számos CA szövevényes vagy részben szövevényes módon lehet összekötve. A CA-k ekkor egymásnak állíthatnak ki (de nem szükségszerűen) tanúsítványokat. Amennyiben két CA egymás számára állít ki tanúsítványt, úgy kereszttanúsításról beszélünk.

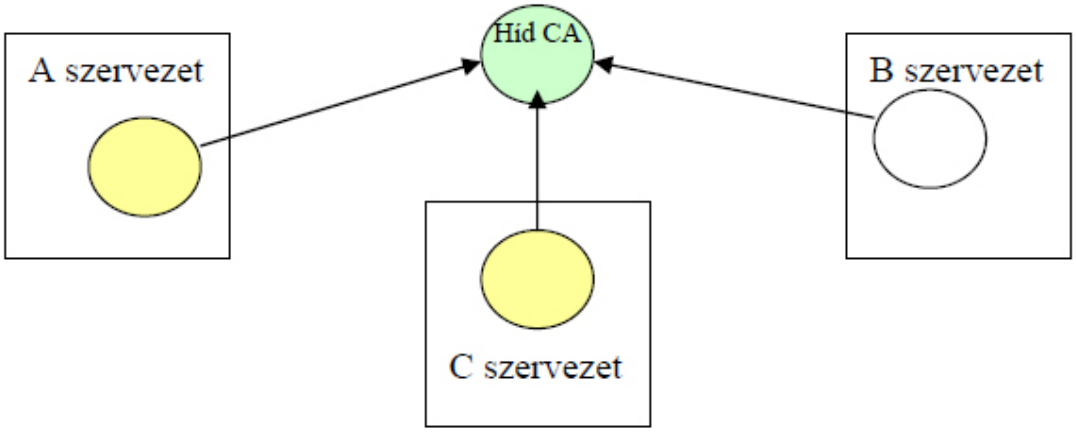


22. ábra: Példa egy részben szövevényes PKI hierarchiára
Forrás: Spisák (2006): i. m. 34.

Híd architektúra: hídarchitektúráról akkor beszélünk, ha egy kitüntetett CA (híd CA) több, önmagában zárt PKI-t köt össze azzal a céllal, hogy az egyes PKI-k által tanúsított felhasználók egymással hiteles módon kommunikálhassanak. A hídarchitektúra esetén minden CA, amelyik a híd CA szolgáltatásait igénybe veszi, tanúsítványt bocsát ki részére. Ezzel biztosítja a saját felhasználói számára a hiteles kommunikációt. Amennyiben a szervezet PKI rendszere hierarchikus felépítésű (mint az A és

[150] Spisák (2006): i. m. 34.

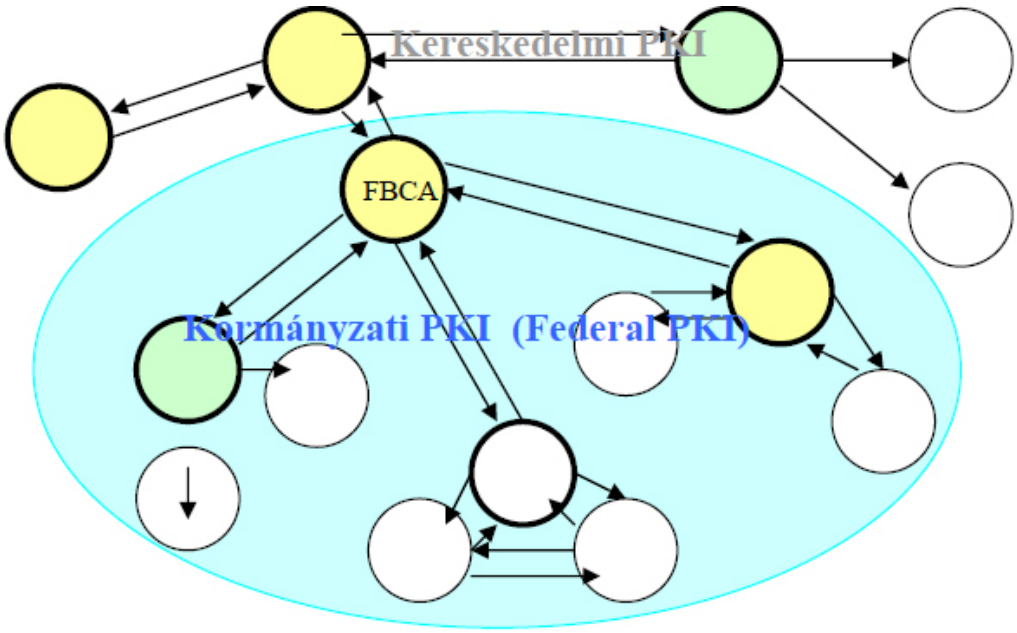
C szervezetek esetében), úgy a híd CA a gyökér CA-val áll kapcsolatban, amennyiben szövevényes, úgy egy kitüntetett CA-val.



23. ábra: Híd architektúrájú PKI
Forrás: Spisák (2006): i. m. 31.

Az *USA kormányzati PKI a rchitektúra modellje* lényegesen eltér a magyartól. A különbségnek feltehetően történelmi okai vannak. Amíg Magyarországon a kormányzati PKI létrejöttét megelőzően a közigazgatási szerveknek nagyrészt nem volt, vagy csak kezdetleges stádiumban kiépített PKI rendszere volt, addig az USA közigazgatási szervei elég korán elkezdtek önálló PKI rendszereket működtetni. Ezen kívül lényegesen nagyobb igény merült fel a kereskedelmi hitelesítés szolgáltatókkal történő kereszttanúsításokra is.

Az USA kormányzati PKI elsődleges célja, hogy olyan tanúsítványláncokat hozzon létre a közigazgatási szervek között, amelyek megteremtik a széles körű és magas fokú bizalom légkörét. Ehhez – a magyar modelltől eltérően – a hídarchitektúra bizonyult célszerűnek.[151]



24. ábra: Az Amerikai Egyesült Államok Kormányzati PKI architektúra modellje
Forrás: Spisák (2006): i. m. 31.

[151] Spisák (2006): i. m. 39.

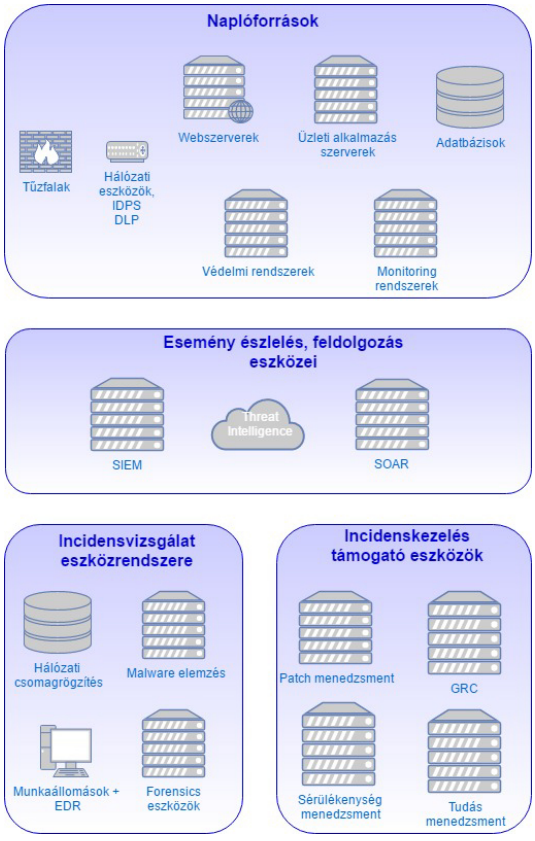
10. Referenciaarchitektúra nagyvállalatok számára

A nagyvállalatok, kormányzati szervek fokozottan ki vannak téve a kibertérből érkező támadásoknak, amik a legkülönfélébb tudású, képességű, illetve erőforrással rendelkező személyektől, szervezetektől érkezhetnek. A támadó eszközök lehetnek a legegyszerűbb programok, de a legfejlettebb megvalósítások is. Azaz fel kell készülni akár a nulladik napi sérülékenységet[152] kihasználó támadás gyors felismerésére, megakadályozására.

Nagyvállalatok, kormányzati szervek – a kezelt rendszerek, adatvagyon kockázatai miatt – széles körű eszközkészletet működtetnek vagyonelemeik védelmében. A működtetett védelmi eszközökön túl, általában van kialakított incidenskezelési folyamat, és rendelkezésre állnak a személyi feltételek is.

A következő példában egy elképzelt nagyvállalat által működtetett incidenskezelő csoport technikai eszköztára kerül bemutatásra. Az incidenskezelő csoport látja a határvédelmi eszközök, a végpontvédelmi eszközök jelzéseit, megkapja a vállalat által helyben üzemeltetett rendszerek, valamint a felhő szolgáltatásból igénybe vett szolgáltatásának naplóbejegyzéseit.

A csoport számos incidenselemzést támogató, valamint sérülékenységmenedzselő rendszert használ. A vállalat informatikai szolgáltatóként nem biztos, hogy valamennyi rendszerelemről gondoskodik, hiszen lehet, hogy csak infrastruktúrát (Iaas), platformot (PaaS) vagy szoftvert (SaaS) biztosít, ugyanakkor vannak olyan szervezetek, amelyek részére biztonsági szolgáltatást (SECaaS) is nyújt. A szervezet fejlett információbiztonsági, irányítási rendszert üzemeltet, így lehetősége van abból információkat begyűjteni.



25. ábra: Nagyvállalati incidensmenedzsment-referenciamodell
Forrás: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components
(utolsó letöltés: 2017. április 20.)

[152] 0-day (zero-day) sérülékenység: olyan program hiba, amely segítségével a támadó káros tevékenységet hajthat végre a rendszeren és a sérülékenység nincs publikálva, javítására, kezelésére nincs megoldás.

11. Üzemeltetői és fejlesztői feladatok az ITIL módszertanon keresztül

Az egyik leggyengébb láncszem egy szervezet struktúrájában, sebezhetősége miatt, az informatikai rendszer. Amennyire a 21. század kiváltsága, hogy előremutató technológiákat fejlesztett ki, úgy nyílt általuk rés a pajzson. Fő célpontnak a nagyhatalmak számítanak (például Amerikai Egyesült Államok, Oroszország vagy Kína), vagyis Magyarországot egyelőre nem tekintik a kibertámadások elsődleges terének. Ennek ellenére az elmúlt időszakban számos informatikai rendszerleállást okozott már hazai környezetben is szándékos támadás, amelyekről a sajtó is beszámolt (a legtöbb rendszerkiesést azonban adatvédelmi okokra hivatkozva nem közölték a nyilvánossággal).

Annak ellenére, hogy a támadók mindig egy lépéssel előrébb járnak, nem kétséges, hogy a biztonsági események, incidensek megfelelő kezeléséhez és a válaszlépések megtételéhez elengedhetetlenül fontos, hogy megismerjük a megfelelő műszaki védelmi háttér paramétereit, bevált gyakorlatait vagy a jelenleg elérhető gyártói megoldásokat. A rendelkezésre álló információk alapján a szakanyag két lépcsőben elemzi a kérdést: az elméleti ismereteket az Information Technology Infrastructure Library (továbbiakban: ITIL) informatikaszolgáltatás módszertan, ajánlások és törvényi szabályozások gyűjteményén keresztül mutatjuk be. Ezenkívül, nagy hangsúlyt kap az *incidens* és a kapcsolódó fogalmak magyarázata, melyek segítségével könnyebben meg lehet érteni az üzemeltetési feladatokat is. Az elméleti ismeretek mellett másodsorban a gyakorlati tapasztalatok keretében olyan gyártói megoldások és architektúrák kerülnek alaposabb elemzésre, amelyek a legkisebb szervezetek és a legnagyobb intézmények igényeit is figyelembe veszik a hatékony incidensmenedzsmenthez. A felvázolt biztonsági szolgáltatások és architektúraminták segítségül szolgálhatnak, hogy egy rendszer kiesésekor az üzemeltetési vagy fejlesztéseket végző munkatárs a helyreállításhoz szükséges információkkal rendelkezzen.

Az eszközrendszereket, fogalmakat és jogszabályokat a rendelkezésre álló szakirodalomból gyűjtöttük ki, mivel azonban az informatikában és a műszaki tudományokban nincs nyugvópont, ezek folyamatos változásban és fejlődésben vannak, így a most megírt tanulmány egy pillanatnyi állapotot ad vissza.

11.1. ITIL, az informatikaszolgáltatás módszertana

Az informatikai szolgáltatásmenedzsment kezelésére és megvalósítására több keretrendszert is kidolgoztak. Ezek általában a nemzetközi terepen már bevált gyakorlatokat gyűjtik össze és rendszerezik. A metodikák segítségével az informatikai vezetők és az IT-s szakemberek megérthetik az üzlet és az informatika kapcsolatát, valamint útmutatást kapnak az informatikai folyamatok megszervezéséhez, megvalósításához és méréséhez. A keretrendszerek között azonban eltérések adódnak, amelynek az oka, hogy más szemszögből vizsgálják a feladatokat, más-más szakmai szervezet dolgozta ki őket, illetve más az informatika területén tevékenykedő megcélzott közönségük.[153]

A három leginkább elterjedt keretrendszer a *COBIT,* a *MOF* és at ITIL. A COBIT-ról azt érdemes tudni, hogy az *Information Systems Audit and Control Association* (ISACA) és az *IT Governance Institute* (ITGI) hozta létre 1996-ban. Célja, hogy segítse az üzleti vezetők és auditorok mindennapi munkáját. Kutatja és fejleszti az általánosan elfogadott informatikai technológiák irányítási céljainak halmazát. A vezetőknek az informatikai döntések és befektetések alapjait nyújtja. Segíti a stratégiai tervek és az informatikai rendszerek felépítésének megalkotását. Tanácsot ad a folyamatos szolgáltatáshoz és a teljesítménymonitorozáshoz szükséges hardver és szoftver kiválasztásában. A COBIT által meghatározott kritériumok biztosítják az ügyfeleket az irányítás, a biztonság és a folyamatok kezelésének megfelelő szintjéről. Azonosítja az informatikai irányítás témáit a cég informatikai infrastruktúráján belül.[154]

[153] Erdélyi Krisztina – Dr. Schubert Tamás (2011): Informatikai Rendszerek Felügyelete. Budapest, Typotex Kiadó. 12.
[154] Erdélyi Krisztina – Dr. Schubert Tamás (2011): i. m. 13.

Ezzel szemben a MOF (*Microsoft Operations Framework*), a Microsoft üzemeltetési keretrendszere azokat a kisebb szervezeteket célozza, amelyek nem szeretnék a teljes ITIL-t alkalmazni és megvásárolni. A MOF ingyenesen letölthető, a teljes informatikai életciklust felölelően közli a bevált gyakorlatok gyűjteményét kérdés alapú segédlettel támogatva. ITIL alapokon nyugszik, annak egyfajta korlátozott megvalósítása. Egységbe foglalja az informatikai tervezés, átadás, üzemeltetés közösségek által meghatározott folyamatait, az irányítással, kockázattal és megfelelőséggel kapcsolatos tevékenységeket, a vezetői jelentéseket és áttekintéseket.[155]

Jelen anyag szempontjából az ITIL a legfontosabb, amely az informatikai infrastruktúrák irányítására, fejlesztésére és üzemeltetésére alkalmas, nyilvános módszertan. Az ajánlások jelenleg a harmadik verziónál tartanak, amelyben a kettes verzió struktúráját alakították át, s a középpontba az életcikluson alapuló megközelítés került.[156]

Úgy tűnik, ez utóbbi módszertan a releváns minta ahhoz, hogy segítse az üzemeltetésben és fejlesztésben részt vevő munkatársakat, hogy egy incidens során melyek azok az eszközök vagy eszköztárak, amelyek biztosíthatják az informatikai rendszerek védelmét, és fenntartják az üzemeltetés folyamatosságát, vagy amelyek a kiesést gyorsabban helyreállítják.

Az említett három keretrendszerből az ITIL szabvány vált az informatikai szolgáltatás módszertanává. Az ITIL módszertant és annak verzióit a költséghatékonyság jegyében az informatikai szolgáltatások támogatása céljából fejlesztették ki. A módszertan azért is hatékony, mivel a szolgáltatások teljes életciklusára kiterjed, értve ez alatt a tervezést, a bevezetést, a működtetést és az újabb szolgáltatások lehetővé tételét is. A módszertan emellett tartalmazza az informatikai iparágban elfogadott eljárások és a legjobb gyakorlati metodikák gyűjteményét, az informatikai szolgáltatások menedzselésének területén. Továbbá leírja és definiálja a kulcsfolyamatokat és keretet ad az informatikai szolgáltatás irányítására.

A kilencvenes évek elején az IBM négy kötetet, az úgynevezett „Sárga könyveket” adta ki Management System for Information Systems néven, melynek szerzője Edward A. Van Schaik volt. Ezek az ITIL-könyvek eredeti szabálygyűjteményként váltak ismerté.

Az ITIL-nek három verziója van. Az ITILv1 a szervezeti funkciókkal foglakozik, az ITILv2 a horizontális folyamatokkal, az ITILv3 pedig a szolgáltatási életciklussal.

Amit most ITILv1-nek hívunk, az „Government Information Technology Infrastructure Management Methodology” (GITMM) volt, amely az évek alatt egy 40 kötetes módszertanná bővült.

Az ITILv2-nek pedig az volt az egyik célja, hogy az évek során 40 kötetben megjelent ITILv1 verziót 8 kötetben, egy logikus „állományba” csoportosítsa. Ennek az elképzelésnek annak idején szolgáltatásorientált megközelítése volt.[157]

Az angol kormányzati támogatással létrehozott módszertan neve arra utal, hogy kezdetben egy egységes szerkezetű könyvsorozatban dokumentálták a sikeres gyakorlati megoldásokat. Később ennek a sorozatnak a 10 legfontosabb témakörének a bevált gyakorlatát dokumentáló kötete lett a módszertan első változata. A mára nemzetközileg elterjedt, 2000-ben megújított módszertangyűjtemény 2 csoportban 11 témakört ölel fel:

- szolgáltatásbiztosítás:
    - szolgáltatási szintű menedzsment;
    - rendelkezésre állás menedzsmentje;
    - IT-szolgáltatás-folytonossági menedzsment;
    - kapacitásmenedzsment;
    - IT-szolgáltatások pénzügyi irányítása.

[155] Erdélyi Krisztina – Dr. Schubert Tamás (2011): i. m. 14.

[156] Erdélyi Krisztina – Dr. Schubert Tamás (2011): i. m. 15.

[157] Broczkó Péter (2011): *ITIL alapú szolgáltatásmenedzsment.* Budapest, Óbudai Egyetem, Neumann János Informatikai Kar. 13.

- Szolgáltatástámogatás:
    - ügyfélszolgálat;
    - incidensmenedzsment;
    - problémamenedzsment;
    - változáskezelés;
    - konfigurációkezelés;
    - kiadáskezelés – dokumentáció.

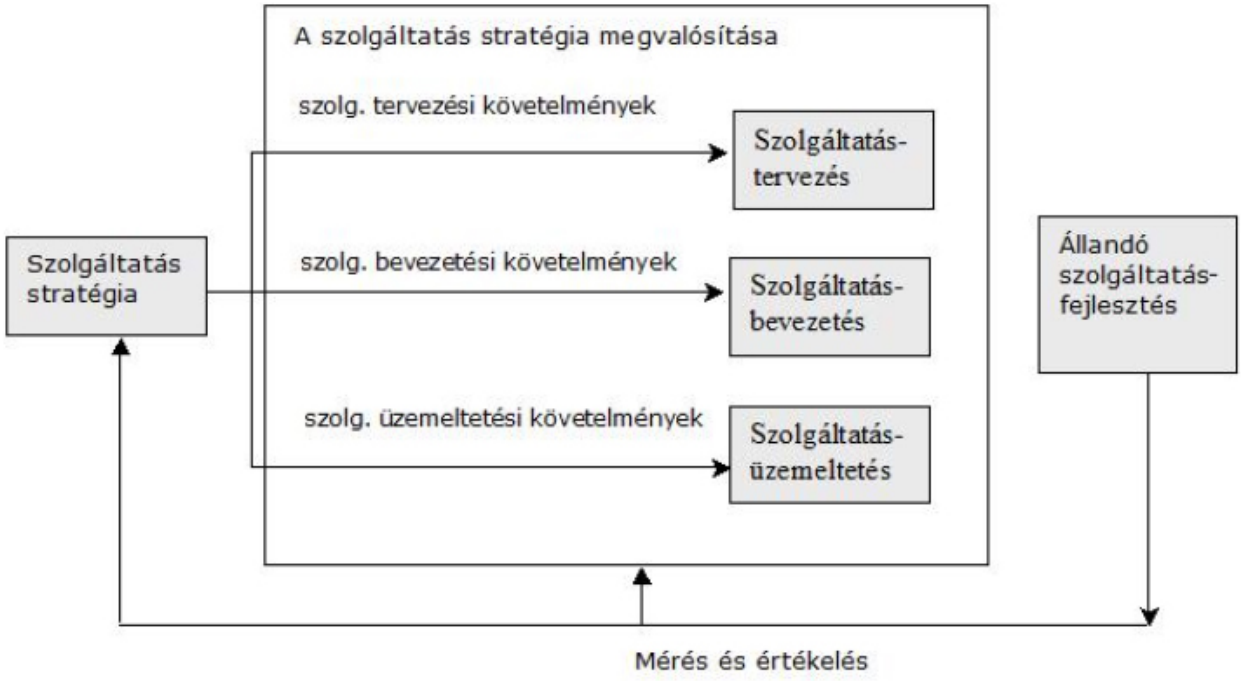
Az informatikai szolgáltatás irányítás módszertanát két kötetben adták ki: Service Delivery és Service Support. Ezek képezik az új dokumentáció alapját, illetve a nemzetközi vizsgák hivatalos anyagát is. A további megjelent kötetek a Security Management, amely az informatikai biztonság kérdéseivel foglalkozik, a Planning to implement Service Management, amely a bevezetés kérdéseit tárgyalja, az IT Service Management zsebkönyv pedig egy tömör, vázlatos összefoglalást ad a témáról. További tervezett kötetek az Application Management, az ICT Infrastructure Management és a The Business Perspective.[158]

Az ITILv3 szerepe:[159]

- általa előtérbe kerül a szolgáltatás értékteremtő (stratégiai) szerepe (a mérhető üzleti értékre fókuszál);
- SLA mint garancia a szolgáltatásminőségre (warranty);
- a szolgáltatások anyagi (erőforrások) és nem-anyagi jellegű eszközeinek (képességek) együttes kezelése;
- szolgáltatási életciklus: jól értelmezhető keret a szolgáltatásmenedzselés szervezéséhez;
- a szervezeti funkciók és a horizontális (együttműködést megvalósító) folyamatok egymást kiegészítő szerepe;
- gyakorlatiasabb „Hogyan csináljuk?” útmutatás;
- a szolgáltatásmenedzsment információigényének egységes rendszerbe foglalása (konfigurációmenedzsment-rendszer: CMS);
- modellek kiterjedt használata a szolgáltatásoknál és a szolgáltatásmenedzsmentnél.

ITILv3 az előző verzióktól megkülönböztető jellemzői közé tartozik egyrészt, hogy az üzletvitel, azaz a business szempontjából rajzolja meg az ITIL keretét, valamint, hogy az értékteremtés áll a középpontjában, mint az anyagi jellegű erőforrások és a nem anyagi jellegű képességek. A tárgyalási kerete az életciklus. Az ITILv3-életciklusszakaszok a következők: 0. Introduction to the ITIL Service Life Cycle, 1. Service Strategy, 2. Service Design, 3. Service Transition, 4. Service Operation, 5. Continual Service Improvement.

[158] *ITIL – az informatikaszolgáltatás módszertana* (2002). Budapest, KFKI Számítástechnikai Rt. 174.
[159] Broczkó (2011): i. m. 16–17.



26. ábra: A szolgáltatási életciklus működése (nem lineáris folyamatban)
Forrás: BROCZKÓ (2011): i. m. 22.

11.2. Az ITIL külföldön és itthon

Külföldi viszonylatban a módszertant legelőször az angol kormányzati és közigazgatási területen használták, ebből kiindulva vált kormányzati ajánlássá is. Minekután kedvező tapasztalatok voltak a gyakorlati alkalmazását illetően, piaci környezetben is alkalmazni kezdték. Végül „de facto" szabvánnyá vált.[160]

Ezt követően az ITIL módszertant egyre több országban elfogadták és „honosították", majd különböző országok fórumai „karolták fel", és járultak hozzá a terjedéséhez. A helyi fórumok összefogására jött létre például az IT Service Management Forum International [Az IT Service Management Forum (itSMF) az informatikai szolgáltatás-menedzsment területén nemzetközileg elismert és független szervezet, amelyet kizárólag a tagsága irányít]. A második nemzeti fórum Hollandiában alakult ki, ahol az EXIN informatikai oktató- és vizsgaközpont lett a módszertan hivatalos gazdája. Mivel az ITIL Hollandiában is „hivatalos, ajánlott" módszerré vált, az ITIL diplomákat itt is gyakran megkövetelik, sőt sok tenderfelhívásban az ITIL megfelelőséget pályázati feltételként írják elő.[161]

Magyarországon legelőször ITIL dokumentációt állítólag a KFKI Számítástechnikai Rt. (mai neve: KFKI Számítástechnikai Zrt.) készített, majd a MATÁV (mai neve: Magyar Telekom). Ezt követően fogadta el kormányzati ajánlásként a Magyar Informatikai Tárcaközi Bizottság (mai neve: Informatikai Tárcaközi Bizottság), 1996-ban.[162]

Miután Magyarországon mára elképzelhetetlenné vált, hogy egy vállalkozás, vállalat ne rendelkezzen informatikai támogatottsággal, egyre nagyobb szerephez jutott a működtetés megszervezése és menedzselése. Az ITIL elemei ennek következtében egyre jobban beépültek az IT-terület működésébe és szabályozásába.

---

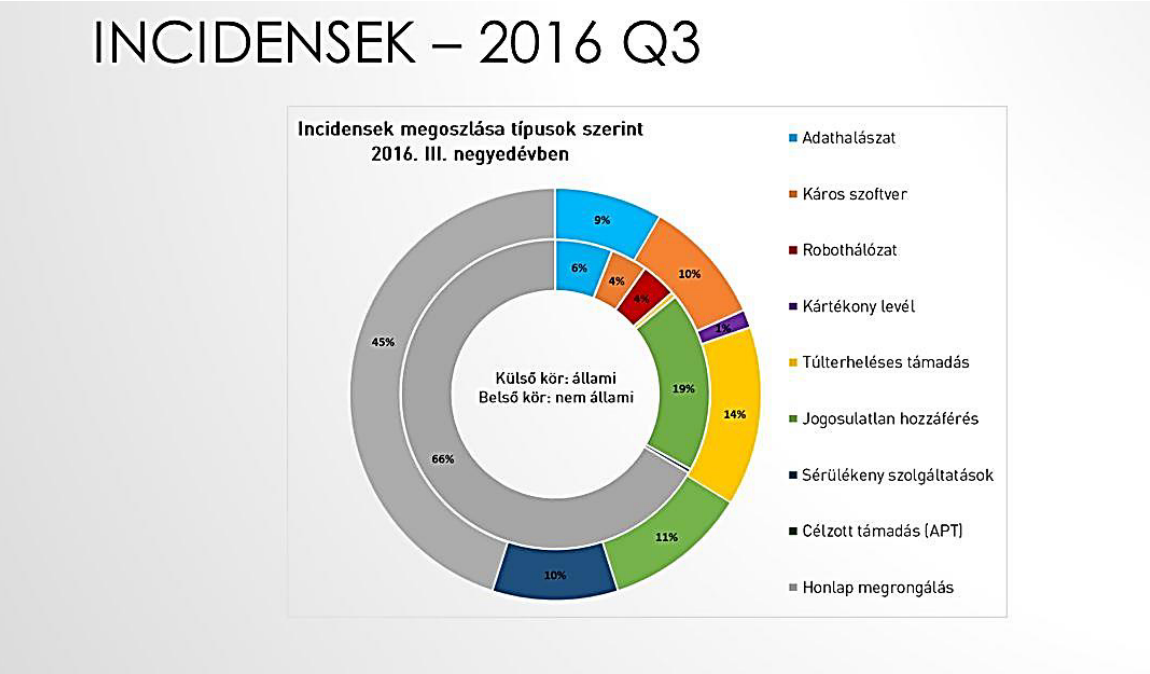
160 *ITIL – az informatikaszolgáltatás módszertana* (2002). Budapest, KFKI Számítástechnikai Rt. 3.
161 Uo.
162 Uo.

11.3. Az incidens és az incidenskezelés folyamata

Az ITIL módszertan lényegét a fogalmakon és az alkotóelemeken keresztül mutatjuk be. A kifejezések és rendszerelemek elemzése abban segíthet, hogy támogatást nyújtson, milyen támadásokra kell felkészülni, illetve milyen feladatokat kell elvégezni a biztonságos üzemeltetés vagy visszaállítás érdekében.

A következő, 27. ábrán látható, milyen összetett támadásoknak vannak kitéve az informatikai, s elsősorban a kritikus rendszerek. Mivel a támadók egyre fejlettebb technikával és kifinomultabb módszerekkel bombázzák az infrastruktúrát, ezért egy szervezet informatikai rendszerében különösen nagy hangsúlyt kell fektetni a kritikus információs rendszerek védelmére, hiszen ezen rendszerek tartalmazzák a bizalmas, titkos, személyes vagy pénzügyi adatokat, illetve rajtuk keresztül történik egy szolgáltatás (energia, közlekedésszervezés, kommunikáció) működtetése is.

Kritikus információs infrastruktúrák közé soroljuk például az energiaellátó rendszerek rendszerirányító számítógép-hálózatait, a kommunikációs hálózatokat (vezetékes, mobil, műholdas), a közlekedésszervezés és -irányítás számítógép-hálózatait, a pénzügyi-gazdasági rendszerek számítógép-hálózatait, a védelmi szféra riasztási, távközlési számítógép-hálózatait, az egészségügyi rendszer számítógép-hálózatait és a kormányzati, illetve az önkormányzati számítógép-hálózatokat.[163]



27. ábra: Az informatikai rendszereket érhető kiber incidensek
Forrás: http://images.slideplayer.hu/46/11640024/slides/slide_13.jpg *Nemzeti Kibervédelmi Intézet (utolsó letöltés: 2017. március 16.)*

Tehát akkor mire is kell figyelni egy rendszer kiesésekor? Mit is jelent az *incidens*? Az ITILv3 módszertanban használt meghatározás szerint, ha egy szolgáltatás nem az elvárt követelmények szerint működik most vagy a jövőben, az *incidensnek* tekintendő.[164]

---

[163] Haig Zsolt – Kovács László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest, Nemzeti Közszolgálati Egyetem. 49.

[164] Horváth Gergely Krisztián (2014): *Incidens-menedzsment, BCP, DRP integráció – A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez.* Budapest, Nemzeti Közszolgálati Egyetem, 8–11.

Ennek értelmében *incidens* (*incident*): egy IT-szolgáltatás be nem tervezett megszakadása, vagy az IT-szolgáltatás minőségének csökkenése. Egy konfigurációelem meghibásodása szintén incidensnek tekinthető, még ha nincs is hatással semmilyen szolgáltatásra (például a tükrözést végző diszkek közül az egyik meghibásodása).[165]

Az ITIL szerint az incidensre vonatkozó információ eredhet automatizált észlelésből *(detection),* felhasználói vagy rendszergazdai bejelentésből *(userlogging)* vagy felhasználói hívásból *(call).* Az észlelés *(detection)* a kiterjesztett incidens életciklus egy szakasza. Az észlelés hatására az incidens ismertté válik a szolgáltató számára. Ez lehet automatikus vagy annak eredménye, hogy egy felhasználó bejelenti az incidenst.[166] A *bejelentés (logging)* nincs külön definiálva, azonban értik alatta a hívást és a hibakezelő rendszerben való rögzítést is. A felhasználókat nem különböztetik meg. Idetartozhat az IT-üzemeltetők általi bejelentés is. A hívás *(call)* telefonhívás a felhasználótól az ügyfélszolgálatra. Egy hívás az incidens vagy szolgáltatáskérés rögzítését eredményezi.

Figyelembe kell venni, hogy nem minden hiba *(error),* meghibásodás *(failure)* vagy rendszeresemény *(event)* incidens. Például ha nem érinti az informatikai szolgáltatások minőségét, és az üzemeltetők képesek megoldani, akkor nem az. A *hiba (error/fault)* tervezési hiányosság vagy helytelen működés, amely meghibásodást okoz egy vagy több konfigurációelemben vagy IT-szolgáltatásban. Az olyan típusú emberi tévedés vagy hibás folyamat, amely valamilyen konfigurációelemre vagy IT-szolgáltatásra hatással van, szintén hiba.[167] A *meghibásodás (failure)* annak a képességnek az elvesztése, hogy a rendszer az előírás szerint működjön, vagy a kívánt eredmény előálljon. A kifejezést az IT-szolgáltatások, folyamatok, tevékenységek, konfigurációelemek s a többi esetében lehet használni. A meghibásodás gyakran incidenst okoz. Az esemény *(event)* olyan állapotváltozás, amelynek jelentősége van egy konfigurációs elemben vagy az IT szolgáltatás menedzsmentjében. A kifejezést bármilyen IT-szolgáltatás, konfigurációs elem vagy megfigyelő eszköz által keltett riasztásra vagy értesítésre használják. Az események általában az IT-üzemeltető személyzet beavatkozását igénylik, és gyakran vezetnek naplózandó incidensekhez.[168]

Az incidenskezelés folyamatában az elsődleges cél tehát a szolgáltatás helyreállítása *(restoration),* amely történhet ismert hiba *(knownerror)* esetén megkerülő megoldás *(workaround)* alkalmazásával vagy megoldással *(resolution).* Tehát nem a hibát javítjuk, hanem a felhasználó számára minél rövidebb időn belül a szolgáltatás igénybevételének képességét adjuk vissza.[169] A szolgáltatás helyreállítása *(restoration of service)* intézkedést jelent egy IT-szolgáltatás javítás és visszaállítás utáni visszaadásáról a felhasználóknak. Ez az incidensmenedzsment fő célja. Az ismert hiba *(knownerror)* olyan probléma, amelynek van dokumentált eredendő oka és megkerülő megoldása. Az ismert hibákat a problémamenedzsment hozza létre és kezeli, végig az élettörténetükön keresztül. Ismert hibákat a fejlesztők vagy a szállítók is azonosíthatnak. A megkerülő megoldás *(workaround)* olyan incidens vagy probléma hatásának csökkentése vagy kiküszöbölése, amelyre teljes megoldás még nincs (például egy meghibásodott konfigurációelem újraindítása). A problémák megkerüléseit ismert hibarekordokban dokumentálják. Azon incidensek megkerülő megoldásait, amelyeknek nincs kapcsolódó problémarekordjuk, az incidensrekordban dokumentálják. A megoldás *(resolution)* intézkedés egy

---

165 *ITIL® V3 HungarianGlossary® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5* (2008). itSMF Hungary. 40.

166 *ITIL® V3 HungarianGlossary® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5.* (2008) itSMF Hungary. 29.

167 *ITIL® V3 HungarianGlossary® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5.* (2008) itSMF Hungary. 33.

168 *ITIL® V3 HungarianGlossary® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5*. (2008) itSMF Hungary. 34.

169 Horváth Gergely Krisztián (2014): *Incidens-menedzsment, BCP, DRP integráció – A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez.* Budapest, Nemzeti Közszolgálati Egyetem, 8–11.

incidens vagy probléma eredendő okának kijavítására vagy egy megkerülő megoldás megvalósítására. Az eredendő ok *(rootcause)* pedig egy incidens vagy probléma mögöttes vagy eredeti oka.

Az incidenskezelés kulcsfogalmainak ismertetése után a *biztonság* fogalma kerül sorra. Ez azért érdekes, mivel az ITIL összekapcsolja az incidensmenedzsment és az információbiztonság-menedzsment folyamatokat. Itt tárgyalandó fogalom a *minőség*, az *információbiztonság-menedzsment* és a *biztonságmenedzsment információs rendszere*. A minőség *(quality)* egy termék, szolgáltatás vagy folyamat képessége arra vonatkozóan, hogy a tervezett értéket nyújtsa (például egy hardverkomponenst jó minőségűnek kell tekinteni, ha az elvárások szerint működik, és az elvárt megbízhatóságot nyújtja). A folyamatminőség szintén megköveteli a képességet az eredményesség és hatékonyság megfigyelésére, és ha szükséges, a javítására. Az Információbiztonság-menedzsment *(information-security management)* felelős azért, hogy egy szervezet eszközeinek, információinak, adatainak és IT-szolgáltatásainak bizalmassága, integritása és rendelkezésre állása megfeleljen a megállapodott üzleti igényeknek. Az információbiztonság-menedzsment támogatja az üzletbiztonságot és szélesebb a hatóköre, mint az IT-szolgáltatónak, mivel olyan dolgokra is kiterjed, mint például a papírdokumentumok, az épületbe való bejutás, a telefonhívások kezelése a teljes szervezetre vonatkozóan. A biztonságmenedzsment információs rendszere *(security management informationsystem)* azon segédeszközök, adatok és információk összessége, amelyet az információbiztonság-menedzsment támogatására használnak. A biztonságmenedzsment információs rendszere eleme az információbiztonság menedzsmentrendszerének.

11.3.1. Biztonság fogalma a magyar jogszabályokban[170]

Az alábbiakban a *biztonság* fogalmának meghatározhatóságáról lesz szó, a magyar jogszabályok kontextusában. A 2013. évi L. törvényben (információbiztonsági törvény, röviden: Ibtv)[171] határozzák meg a *biztonsági esemény* fogalmát. Utóbbi ezek alapján 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. A *biztonsági esemény kezelése* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálását jelenti, következményeinek felszámolását, a bekövetkezés okainak és felelőseinek megállapítását, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet.

Úgy tűnik, hogy nem egységes a hazai joganyag az *incidenskezelés* fogalomhasználatában.

Megjelenik még a létfontosságú rendszerek és létesítmények szabályozásáról szóló 2012. évi CLXVI. törvényben az *esemény* fogalma, a biztonságot veszélyeztető vagy sértő esemény értelmében külön definíció nélkül („rendkívüli esemény", a „hálózatbiztonsággal kapcsolatos események"). Ugyanakkor több helyen találkozhatunk az *incidens* kifejezéssel is, szintén konkrét definíció nélkül [például: 83/2012. (IV. 21.) Kormányrendeletben „biztonsági incidens" szerepel, 309/2011. (XII. 23.) Kormányrendeletben „felhasználói incidens" szerepel, és a 301/2013. (VII. 29.) Kormányrendeletben „incidens-kezelési munkacsoport" szerepel].

Korábban már használta a jogalkotó az *incidens* fogalmát *biztonsági eseményként,* különösen a légiközlekedés biztonságát szabályozó joganyagban [például 86/1997. (V. 28.) Kormányrendelet], továbbá megtalálható még banki területen [23/2013. (XI. 6.) MNB rendelet] és a honvédelemben [16/2013. (VIII. 30.) HM rendelet] is.

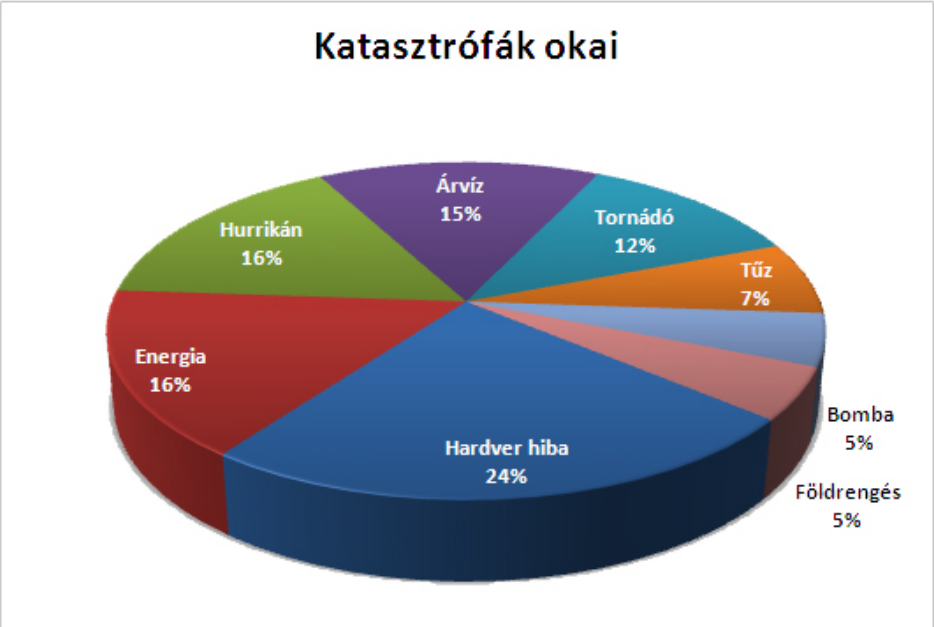
---

[170] Horváth Gergely Krisztián (2014): *Incidens-menedzsment, BCP, DRP integráció – A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez.* Budapest, Nemzeti Közszolgálati Egyetem, 10–11.

[171] További információk ezen anyag 1. mellékletében találhatók.

Folytatva a fogalmak elemzését, a *katasztrófa* és az *üzletmenet-folytonosság* meghatározásaihoz kapcsolódó témakörök következnek.

A 28. ábra a katasztrófák okait és bekövetkezési arányát mutatja. Az ábrából kiderül, hogy leginkább hardverhibák azok, amelyek kiesést okozhatnak egy informatikai rendszerben.



28. ábra: A katasztrófák lehetséges okai
Forrás: www.itsecure.hu/drp (utolsó letöltés: 2017. március 17.)

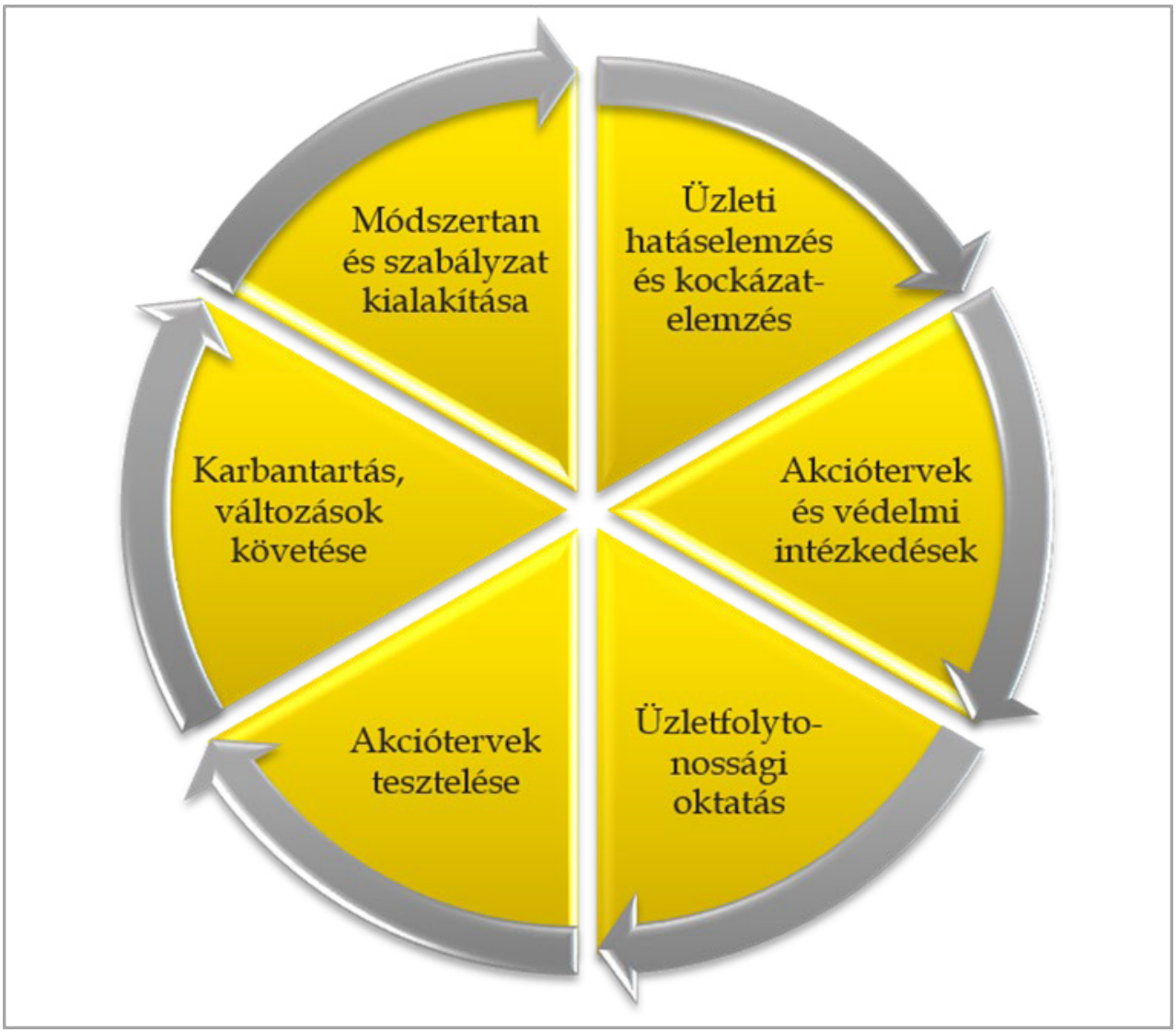
Az ITIL szerint a katasztrófa *(disaster)* olyan hirtelen, nem tervezett, szerencsétlen esemény, amely jelentős kárt vagy veszteséget okoz. Ez akkor jelentkezik, ha a szervezet egy előre meghatározott időn belül nem képes a kritikus folyamatait működtetni. A katasztrófát felelős vezetőnek kell deklarálnia. Az üzletmenet-folytonosság menedzsment *(Business Continuity Management – BCM)* az a folyamat, melynek során egy szervezet felkészül a kritikus üzleti folyamatok megszakadására, vagy kiesése esetén a folyamatok visszaállítására. Cél a kritikus szolgáltatások minimálisan szükséges szintjének fenntartása krízishelyzet esetén, és a folyamatok mielőbbi visszaállítása a normál üzemre.[172]

Az üzletmenet-folytonosság kialakításához az alábbi elemeket kell kidolgozni: működésfolytonossági terv *(MFT)*, katasztrófaelhárítási terv, üzleti hatáselemzés. A működésfolytonossági terv, *(Business Continiuty Plan – BCP)* azoknak az információknak és eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes váratlan káreseményekre hatékonyan reagálni és kritikus üzleti folyamatait egy elfogadható szinten fenntartani. MFT-nek nevezik azt a keretrendszert, amely átfogja a működésfolytonosság tervezési, megvalósítási és ellenőrzési fázisait. Ugyanakkor a normál működés megszakadása esetén alkalmazandó, az egyes kulcsfolyamatokhoz, szolgáltatásokhoz kapcsolódó konkrét tevékenységeket is MFT-nek hívják.

A katasztrófaelhárítási terv *(Disaster Recovery Plan – DRP)* azoknak az eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes a káresemények következtében kiesett szolgáltatásait a normál működési szintre visszaállítani. Működésfolytonossági terv készítése esetén a katasztrófaelhárítási terv az előbbi szerves részeként jelenik meg.

Az üzleti hatáselemzés *(Business Impact Analysis – BIA)* pedig olyan eljárás, amely során a szervezet meghatározza a kritikus üzleti folyamatok megszakadásának következményeit és a normál működési állapotra való visszaállás elvárásait.

[172] ITIL® V3 HungarianGlossary® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5. (2008) itSMF Hungary. 10.



29. ábra: Az üzletmenet-folytonossági rendszer elemei
Forrás: www.grid.hu/hu/megoldasaink-termekeink/uezletfolytonossagi-rendszer-kialakitasa
(utolsó letöltés: 2017. március 16.)

11.4. Az ITIL mint üzemeltetési keretrendszer[173]

A fogalmak elemzése után az üzemeltetési keretrendszer vizsgálata következik. A metodika leírja és definiálja a kulcsfolyamatokat és egyfajta keretet ad az informatikaszolgáltatás irányítására. Ez a keret segítheti egy informatikai szervezetben a folyamatok azonosítását és megvitatását. A keretrendszer támogatást ad, hogy az informatikaszolgáltatás minősége javulhasson, illetve hosszú távon a költségek csökkenhessenek.

Az üzemeltetéshez kapcsolódó folyamatokat az ITIL 5 fő kötete is magyarázza. A szolgáltatásstratégia *(Service Strategy)* során a folyamat azonosítja azokat a piaci lehetőségeket, amelyeket új szolgáltatások bevezetésével ki lehetne aknázni. Az eredmény egy stratégiai dokumentum, amely felvázolja az új szolgáltatás tervezésének, megvalósításának, üzembe helyezésének és folyamatosan

[173] ITIL – az informatikaszolgáltatás módszertana (2002). Budapest, KFKI Számítástechnikai Rt. 5-6.

javuló minőségben történő nyújtásának folyamatát. A kötet legfontosabb fejezetei a *Szolgáltatásportfólió kezelése* és *Pénzügyi menedzsment.*

A szolgáltatástervezés *(Service Design)* eredményeként projektterv készül az előző lépésben keletkezett stratégia által felvázolt szolgáltatás konkrét megvalósítására. A terv részletezi az új szolgáltatás bevezetésének minden vonatkozását, a bevezetéshez és üzemeltetéshez szükséges támogató folyamatokkal együtt. A kötet legfontosabb fejezetei az *Üzemeltetés és üzemvitel biztosítása, Kapacitástervezés,* valamint az *Informatikai- és üzembiztonság*.

A szolgáltatáslétesítés és -változtatás *(Service Transition)* a megtervezett szolgáltatás létesítéséhez és a környezet módosításához szükséges folyamatok leírása. Fontos fejezetek a *Változás- és verziókezelés,* a *Konfigurációmenedzsment* és a *Dokumentációkezelés.*

A szolgáltatásüzemeltetéssel *(Service Operation)* kapcsolatosan elmondható, hogy az előzővel szorosan összefüggő kötet tárgyalja a szolgáltatás folyamatos és hibamentes üzemeltetéséhez szükséges folyamatokat és szervezési kérdéseket. A folyamatok garantálják a szolgáltatási megállapodásokban *(Service LevelAgreement – SLA)* vállalt szolgáltatásminőséget. Legfontosabb fejezetek a Hiba- és igény- és incidenskezelés. Az állandó szolgáltatásfejlesztéssel *(Continual Service Improvement)* kapcsolatban a kötet tárgyalja a szolgáltatás folyamatosan javuló minőségben nyújtásának feltételeit. Kiemelt fejezetek a *Szolgáltatási szint mérése, riportolása (jelentése) és menedzsmentje* című fejezetek.

Az ITIL erejének titka valójában a szolgáltatási szintmenedzsment teljes, holisztikus megközelítése, amelynek során a szolgáltatási szintmenedzsmentet integrálja a támogató folyamatokkal. Az ITIL ennek értelmében egy integrált keretet biztosít, amelyen belül minden kulcsfolyamat definiálva van.

Bármely informatikai szervezet, amely elhatározza, hogy implementálni vagy javítani akarja a szolgáltatási szint menedzsmentjét és a szolgáltatási megállapodásait, annak ezen az integrált keretkörnyezeten belül kell a változásokat meglépnie.

Az ITIL keret gondosan definiálja az Incidens menedzsmentet *(Incident Management)* is.[174] Ebben az esetben az *incidens* egy olyan esemény, amely nem része a szolgáltatás normális működésének, és annak megszakadását vagy minőségének romlását okozhatja. Az incidens hátterében lévő ok a *probléma*. Az incidenskezelés célja, hogy a szolgáltatás normális állapotát a lehető leggyorsabban visszaállítsa úgy, hogy csökkentse az incidens üzletre gyakorolt hatását.

Az incidenskezelést szinte minden olyan vállalatnál alkalmazzák, ahol informatikai-üzemeltetői csapatot működtetnek házon belül. A felhasználóktól vagy ügyfelektől érkező kérdések, kérések, panaszok tekinthetők tehát incidenseknek.

Egy incidensnek különböző állapotai lehetnek, programtól, belső ügymenettől függően: az új igény, a módosítás, a javítás, az információ kérés, az ügyfélnek vissza-és/vagy leadott, tőle átvett, tesztelt, kiadott, lezárt, tervezett, félretett állapot.

Az *incidens* fogalmában leírtak mindig kapcsolhatók a felhasználóhoz vagy egy felhasználói csoporthoz (például fejlesztők, tanácsadók, ügyfél, vezetőség), ezért a feladatokat ki kell osztani *(eszkaláció).* Ennek célja, hogy az incidens az SLA-ban vállalt határidőn belül megoldódjon. Az SLA angol mozaikszó, jelentése: Service Level Agreement – Szolgáltatási Szint Megállapodás. Ez a gyakorlatban azt jelenti, hogy a megrendelő és a szolgáltató a szerződés megkötésekor megállapodnak abban, hogy a szolgáltatónak mit kell teljesítenie, a teljesítést a megrendelő milyen minőségi kritériumok mentén fogadja el, hogyan fogja a megrendelő ezeket a minőségi kritériumokat mérni, s az ezen mért minőségi mutatókkal arányosan mekkora számlát fog a szolgáltatótól elfogadni.)[175]

[174] Lásd: http://erp-blog.blog.hu/2010/08/24/itil_v3_foundation_szolgaltatas_uzemeltetes (utolsó letöltés: 2017. március 14.)

[175] Lásd www.sla.hu/sla-modszertan/sla-modszertan-tartalmi-elemei-9.html (utolsó letöltés: 2017. március 17.)

A problémamenedzsmentnek *(Problem Management)*[176] az incidenskezeléssel ellentétben nem az a feladata, hogy az elvárt, normális működés minél hamarabb visszaálljon, hanem a szolgáltatás üzemképtelenségének minimalizálása a fő célja. Vagyis megoldani a problémákat, amelyek incidenseket okozhatnak. A problémakezelés feladatai tehát a probléma azonosítása és a megoldás meghatározása, az előfordulás és az ismétlődés vizsgálata, az incidensek számának és a hatásoknak a csökkentése.

Továbbá még egy nagyon fontos terület tartozik a biztonságos üzemeltetés ismereteihez, mégpedig a hozzáférésmenedzsment *(Access Management)*.[177] Ennek lényege, hogy a megfelelő felhasználó csak a jogosult szolgáltatásokat, alkalmazásokat érhesse el. A *hozzáférés* a felhasználó szolgáltatási szintjét és mértékét határozza meg. Az *azonosító* egyedi, amely egy felhasználót, személyt vagy szerepkört határoz meg. Ehhez rendelődnek hozzá a *jogosultságok,* amelyek tehát a felhasználókhoz vagy szerepkörökhöz rendelt engedélyek, jogok. A *hozzáférési mátrix* a hozzáférések táblázatos ábrázolása.

Ennek értelmében a biztonsági eseménykezelési tevékenység akkor lehet sikeres, ha az informatikai szolgáltatások nyolcvan százalékának kiesésekor, és akár még a legfontosabb szolgáltatások minőségének romlása ellenére is a szervezet vezetője által meghatározott szolgáltatás legalább a minimálisan elvárt szolgáltatási szinten, a visszaállítási időablakon belül működik. Ezt úgy lehet megoldani, hogy akár ideiglenes, úgynevezett áthidaló megoldásokat léptetnek életbe a kritikus szolgáltatások minden körülmények közötti biztosítása érdekében. (Példának okáért gyakran helyettesítik a kiesett optikai hálózati kapcsolatot egy alternatív kapcsolattal, például mikrohullámú hálózatra állnak át a visszaállításig).

A biztonsági események kezelése során nem az összes szolgáltatás teljes helyreállítása a cél. Azaz, nem feltétel a felmerült hiba gyors javítása. A biztonsági eseménykezelés, továbbá a folyamatos működés fenntartására vonatkozó (BCM, ITSCM) módszerek ehhez biztosítják a szükséges szervezési hátteret.

12. Rendelkezésre állás menedzsmentje[178]

Ennek célja az üzleti igényeknek megfelelő rendelkezésre állás tervezése, figyelése és a szolgáltatások, informatikai infrastruktúra ilyen jellegű képességeinek folyamatos javítása.

A rendelkezésre állás *(availability)* az informatikai elem vagy szolgáltatás egy adott időpontban vagy időintervallumban normál működésre kész állapotát jelenti. Ez a jellemző adott időintervallumra vonatkoztatva a rendelkezésre állás tényleges és előírt értékének hányadosával jellemezhető. Ide tartozó kulcsfogalom a *megbízhatóság (reliability)*, ami jellemzi az informatikaszolgáltatás hibatűrő képességét. Ezt a jellemzőt a szolgáltatás komponenseinek megbízhatósága és a konfiguráció kialakítások (redundancia) határozzák meg. Az incidensek között eltelt átlagidővel számszerűsíthető. A karbantarthatóság *(maintainability)* az informatikai elem működőképes állapotban tartását és ebbe az állapotba történő visszaállítását jellemzi. Ezt több összetevő határozza meg: meghibásodások megelőzése, hibadetektálás, diagnosztizálás, hibaelhárítás, hibás komponens helyreállítása, adatok és szolgáltatások visszaállítása, megelőző karbantartási munkák. A szervizelhetőség *(serviceability)* külső fél által biztosított szolgáltatásokra vonatkozó, szerződés keretén belül biztosított rendelkezésre állási, megbízhatósági és karbantarthatósági jellemzőket foglal magában. A biztonság *(security)* a szolgáltatáshoz tartozó adatok bizalmassági, integritási és rendelkezésre állási jellemzője.

[176] Lásd: http://erp-blog.blog.hu/2010/08/24/itil_v3_foundation_szolgaltatas_uzemeltetes (utolsó letöltés: 2017. március 14.)

[177] Forrás: http://erp-blog.blog.hu/2010/08/24/itil_v3_foundation_szolgaltatas_uzemeltetes (utolsó letöltés: 2017. március 14.)

[178] *ITIL (IT Infrastructure Library) az informatikaszolgáltatás módszertana* (2002). KFKI. 66–73.

A rendelkezésreállás-menedzsment[179] tevékenységek két fő részre bonthatók. Az első a *kockázatanalízis*, mely során fel kell mérni az informatikai erőforrásokat, meg kell határozni az őket érintő szándékos és véletlen jellegű veszélyeket, és meg kell állapítani az erőforrások sebezhetőségi szintjét. Az informatikai erőforrásokba a hardver és szoftver elemeken kívül az adatok és a személyzet is bele tartozik. A kockázatanalízisnek több módszere is van. Az egyik a CCTA Risk Analysis and Management Method (CRAMM), amely olyan széles körben használható eszköz, amely a technikai és nem technikai kockázatokat képes felmérni. Alapszintű informatikai ismeretekkel is lehet használni, mivel tartalmazza a biztonsági szakemberek által összegyűjtött ismereteket. A kockázatelemzést az események különböző forgatókönyvek szerinti vizsgálatával segíti. Másik mód a Component Failure Impact Analysis (CFIA), amely egy egyszerű módszer, amelyben az informatikaszolgáltatás egyes elemeit lebontják komponensekre. Egy táblázatot kell létrehozni, az oszlopokban a szolgáltatásokkal, sorokban az eszközökkel. A táblázat celláiban az adott eszköz vagy komponens kiesését jelölik, azaz hogyan befolyásolja az adott szolgáltatást. Ilyen módon azonosíthatók a kritikus erőforrások és az összetett szolgáltatások is átláthatóvá tehetők. Harmadik kockázatelemző módszer a Fault Tree Analysis (FTA). Ezzel a módszerrel olyan események sora követhető, amelyek a szolgáltatás rendelkezésre állását befolyásolják. Az események együttes bekövetkezésének viszonyát logikai „és/vagy"-kapcsolattal jellemzik.

A rendelkezésre állás menedzsmentjének a kockázatanalízis melletti másik fő része a kockázatmenedzsment.[180] A kockázat kezelése során intézkedéseket kell tenni az eszközök sebezhetőségének csökkentésére. A kockázat számításakor figyelembe kell venni az esemény hatását és a bekövetkezés valószínűségét. A kockázatok kezelése olyan intézkedésekben nyilvánul meg, amelyek a tervezést és az infrastruktúra kialakítást is magában foglalják. A fizikai környezet kialakításánál a számítástechnikai központok elhelyezkedését, az infrastruktúra elrendezését és a környezeti paramétereket meghatározó tényezőket (klíma, áramellátás) kell figyelembe venni. Az elhelyezkedésnél a szabotázs, árvíz, robbanásveszély és egyéb katasztrófákat szükséges elkerülni, illetve fel kell készülni a hatás csökkentésére. Elrendezést tekintve a hardveregységek több helyszínen történő elhelyezésével lehet felkészülni. A kritikus hardver egységeknek megfelelő környezeti tényezőket biztosítanak klímaberendezés, szünetmentes tápegység és generátor alkalmazásával. A számítástechnikai központ környezetének kialakításánál a fizikai hozzáférést, az adatok biztonságos kezelését, tárolását, archiválását érdemes figyelembe venni. Az adattároló médiát tűzbiztos páncélszekrényekben, lehetőleg távoli helyen ajánlott tárolni. Hardver kiépítésnél javasolt a fürtözött megoldások, a komponensek – CPU, hálózati kártyák, diszkek – redundáns kialakítása. A hálózat kialakításánál fontos szempont az alternatív útvonalak, több csatlakozási pontok kialakítása. Az eszközök mellett a kulcsszerepet betöltő emberek helyettesíthetőségére is gondolni kell. Biztonsági szempontból érdemes figyelembe venni a szolgáltatáshoz tartozó adatok bizalmassági, integritási és rendelkezésre állási jellemzőit. Tehát csak a megfelelő jogosultsággal rendelkező személy férhessen hozzá az adott szolgáltatáshoz és adathoz. Az adatok módosítás nélkül, sértetlenül álljanak rendelkezésre, akár egy szolgáltatás kiesés után is. Emellett a szolgáltatási megállapodásban előírt időben hozzáférhetők legyenek az adatok.

A rendelkezésre állás menedzsmentjének tevékenységeinek sikeres megvalósításával elérhető, hogy kevesebb megszakítás történjen az informatikaszolgáltatásban. Amennyiben mégis bekövetkezik a leállás, a gyors helyreállítással minimalizálható az üzletmenetre gyakorolt kedvezőtlen hatás. A leállási idők csökkentésével közvetlenül a pénzügyi veszteségek is csökkenthetők vagy elkerülhetők. A karbantarthatósági és a szervizelhetőségi tevékenységek menedzselésével a kitűzött célok elérése mellett kézben tarthatók a kiadások. A szolgáltatási szint menedzsment tevékenységet nagymértékben támogatja a reális célok megállapításával, a szolgáltatások rendelkezésre állási jellemzőinek figyelésével, az adatok elemzésével és jelentésével, továbbá a kitűzött célok elérésében. A rendelkezésre állás menedzsmentje szorosan együttműködik a kapacitásmenedzsmenttel a szükséges

[179] Uo.
[180] Uo.

erőforrás-kapacitás tervezésével és a használat monitorozásával. Emellett az informatikaszolgáltatás-folytonosság menedzsment tevékenységet egészíti ki a hibatűrő rendszerek kialakításával, mert csökkenti a szolgáltatás kiesésének esélyét.

Ugyanakkor nehézséget jelenthet a kiadások igazolása, mivel a redundáns kialakítások kihasználatlan rendszereknek tűnnek. Akkor lehet a rendelkezésre állás menedzsment hatékony, ha léteznek az ezt támogató problémakezelés, incidensmenedzsment, szolgáltatási szintmenedzsment és egyéb támogató folyamatok. Megfelelő eszköz hiányában adatgyűjtési és feldolgozási nehézségek léphetnek fel. Például nincs információ a szolgáltatás kiesésének vagy komponens meghibásodásának kezdeti és végső időpontjáról, illetve nem tudjuk a rendelkezésre állás számítását automatizálni. Probléma lehet a külső szolgáltatóktól való függés, mivel az általuk vállalt elhárítási idők meghatározzák a vállalható szolgáltatási szintcélokat. Nehéz lehet az üzleti igények meghatározása a rendelkezésre állásra vonatkozóan. Emellett részletesen kell ismerni az informatikai infrastruktúra komponenseinek egymáshoz való kapcsolódását az egész szolgáltatásra számított rendelkezésre állás számításához. Ehhez a konfigurációs adatbázis nyújthat segítséget.

13. Informatikaszolgáltatás-folytonosság irányítása[181]

Az informatikaszolgáltatás-folytonosság irányítása a teljes körű üzletmenet-folytonosságot támogatja az informatikaszolgáltatás, infrastruktúra üzleti igényeknek megfelelő, elfogadott időn belül történő visszaállításával.

Három alapfogalom tárgyalása elengedhetetlen. A *tartalék elrendezés (stand-by arrangement)* az üzletmenet megszakadása esetén a használhatatlanná vált elsődleges eszközök helyettesítésére szolgáló tartalékeszközöket tartalmazó létesítmény vagy megoldás. Ez rendszerint az eszközök és a személyzet elhelyezésére szolgáló helyiségeket, informatikai és telekommunikációs rendszereket, hálózatokat és esetleg megfelelően képzett embereket jelent. A *hidegtartalék (cold start, coldstand-by)* olyan hordozható vagy helyhez kötött létesítmény, amelyben alapinfrastruktúrával (kábelezés, áramellátás) rendelkező számítógépközpont van. Szükséghelyzetben az ügyfél először a tartalékszervereket elhelyezi a létesítményben, majd a saját szoftvereit, archivált adatait erre az infrastruktúrára állítja vissza. A *forrótartalék (hot start, hot standby)* olyan létesítmény, amelyben az eszközök azonnal képesek a szoftverek, archivált adatot feltöltésére és futtatására.

Az informatikaszolgáltatás folytonosságát nem elszigetelten, hanem az üzletmenettel egységesen kell kezelni. A tevékenységek idő szerint négy részre bonthatók: kezdeti tervezésre, a követelmények meghatározására és stratégia kidolgozására, a megvalósításra és az üzemeltetési feladatok fázisára.

A kezdeti fázisban kell kidolgozni és nyilvánosságra hozni az informatikaszolgáltatás folytonosságára vonatkozó elvi szabályozást, amely az üzletmenet folytonossággal összhangban van. Definiálni kell a felelősségi köröket, a kockázatfelmérési és hatáselemzés tevékenységek terjedelmét, biztosítani a pénzügyi és emberi erőforrásokat. Mivel az informatikai szolgáltatásfolytonosság irányítása összetett feladatokat tartalmaz, amelyeket hatékonyan kell működtetni, ezért különös hangsúlyt kap a projektszervezet kialakítása. E fázis végén a változások hatékony kezelése érdekében és a minőségi célok eléréséhez projekttervet kell készíteni.

A követelmények meghatározása és stratégia kidolgozása során az üzleti hatáselemzéssel és a kockázatfelméréssel kell meghatározni a követelményeket és a kockázatcsökkentési lehetőségek vizsgálatával kidolgozni egy stratégiát. Az üzleti hatáselemzés *(Business Impact Analysis)* során a követelmények meghatározásában döntő, hogy az üzletmenet milyen mértékű szolgáltatáskiesést képes elviselni, illetve a veszteségek milyen gyorsan jelentkeznek a kiesések növekedésével. Az üzleti hatáselemzés célja e következmények felmérése. Az elemzés meghatározza a kritikus szolgáltatásokat és a szolgáltatások kiesése által okozott veszteségeket. Ezen kívül foglalkozik a közvetett hatásokkal

[181] *ITIL (IT Infrastructure Library) az informatikaszolgáltatás módszertana* (2002). KFKI. 66-73.

(elmaradt bevétel, járulékos kiadások, az ügyfelek bizalmának elvesztése). Meghatározza a kritikus szolgáltatások minimálisan elfogadható szintjéhez szükséges személyi, infrastrukturális és szolgáltatási előfeltételeit. Előírja a szolgáltatások, a személyzet minimálisan elfogadható, illetve a teljes szint biztosításának határidejét.

A követelmények meghatározásának másik fontos tényezője a kockázatok felmérése, vagyis a katasztrófa vagy szolgáltatáskiesés bekövetkezésének valószínűsége. A kockázatfelmérés – a rendelkezésreállás-menedzsment tevékenységnél ismertetett módon –, a kockázatanalízisből és a kockázatmenedzsmentből áll. A kockázatanalízis során fel kell mérni az informatikai erőforrásokat, meg kell határozni az őket érhető szándékos és véletlen veszélyeket, meg kell állapítani az erőforrások, szolgáltatások kiesésének valószínűségét és azt, hogy ezáltal a szervezet működése milyen mértékben érintett. A kockázat kezelése során intézkedéseket kell tenni az eszközök sebezhetőségének csökkentésére. A kockázat számításakor figyelembe kell venni az esemény hatását és a bekövetkezés valószínűségét. Általános értelemben a visszaállítási lehetőségeket az emberek, informatikai rendszerek, hálózatok, kritikus szolgáltatások, kritikus eszközök tekintetében kell megvizsgálni.

Az alábbiakban az informatikai visszaállítási lehetőségekről lesz szó. A fokozatos visszatérést lehetővé tévő hideg tartalékot olyan szervezetek választják, amelyek a szolgáltatás kiesése után legalább 72 órán keresztül képesek elviselni az informatikaszolgáltatás teljes vagy részleges hiányát. A hideg tartalékként szolgáló számítástechnikai létesítményt külső szolgáltatótól lehet igénybe venni, vagy belsőleg is kialakítható. Mivel a hardvereszközöket és a szoftvereket üzembe kell állítani, gondolni kell a beszerzés okozta késedelmekre. Fel kell mérni az egyedi hardverkiépítéseket, amelyek beszerzése nehézségekbe ütközhet, és meg kell határozni azokat az eszközöket, amelyekkel ezek helyettesíthetők. Ezzel szemben a közbenső visszatérést lehetővé tévő meleg tartalékot olyan szervezetek választják, amelyeknél az informatikaszolgáltatást meghatározott időn belül, jellemzően 24 és 72 óra között vissza kell állítani. Ennél a módozatnál a szolgáltató mobil vagy fix elhelyezkedésű számítástechnikai központot biztosít. A központ teljesen kiépített, szerverekkel, technikai személyzettel el van látva. A visszatérési időt befolyásolja, hogy a szervezet alkalmazásait telepíteni kell, az adatokat fel kell tölteni és az egyedi konfigurációnak megfelelően be kell állítani a tartalékrendszert. Az azonnali visszatérést támogatja a forrótartalék elrendezés, amelyet azok a szervezetek választanak, amelyeknél a szolgáltatás megszakítását követő legfeljebb 24 órán belül vissza kell állítani a teljes informatikaszolgáltatást. Az éles rendszernek megfelelő szerverek és alkalmazások futnak a tartalékrendszeren, és az adatokat replikálták. Így az éles rendszer kiesésekor a kritikus szolgáltatások kiesés nélkül elérhetők, a többi szolgáltatást pedig a 24 órás határon belül lehet visszaállítani.

A megvalósítási fázis lépései az alábbiak szerint alakulnak. A szervezetet alkalmassá kell tenni a katasztrófahelyzetek kezelésére. A vezetők feladata a jóváhagyások, egyes szervezeti egységek, média, szabályozó szervezetek, egyéb külső szervek közötti kapcsolat biztosítása. A koordináló csapat a szervezet egész tevékenységét hangolja össze. Az informatikaszolgáltatást visszaállító csapat a szolgáltatások és alkalmazások szerint tevődik össze. A katasztrófahelyzet esetén végrehajtott tevékenységek megtervezésekor létre kell hozni egy magas szintű tervet, amely az egész szervezetre vonatkozik. Ezután az egyes támogatást nyújtó területekre (mint például a számítástechnika, biztonság, telekommunikáció, elhelyezés, személyzet, pénzügy) létre kell hozni egy-egy specifikus tervet. Minden terület a saját tervéért felelős, kidolgozza a végrehajtandó eljárásokat és megvizsgálja, hogy az adott terület megfelelően van-e támogatva erőforrással és külső szolgáltatásokkal. A rendelkezésre állás menedzsment tevékenységgel karöltve kockázatcsökkentési lépéseket kell végrehajtani, amellyel a szolgáltatás kiesésének ideje és bekövetkezésének valószínűsége csökkenthető. Ki kell választani a szervezet számára legelőnyösebb visszatérési lehetőséget, meg kell kötni a szükséges szerződéseket, és elő kell készíteni a létesítményeket. Egy informatikaszolgáltatás-folytonossági tervet szükséges készíteni az üzleti szempontból kritikus szolgáltatásokra, amely nemcsak a visszaállítás módját adja meg, hanem leírja a szolgáltatások egymás közötti függőségi viszonyát, tesztelését és az adatok ellenőrzését is. A tervben olyan szinten kell az eljárásokat kidolgozni, hogy azt az adott feladathoz szükséges képzettséggel rendelkező bármilyen személy végre tudja hajtani. A terv tartalmazza a

hardver- és szoftverkövetelményeket, adatvisszatöltési pontokat, konfigurációs részleteket és (funkcionális, adatkonzisztencia) ellenőrzési pontokat az összes visszatérési pontra vonatkozóan.

Csak akkor lehetünk biztosak egy kiválasztott stratégia működőképességében, ha az elkészített tervet leteszteltük. A kezdeti elméleti szintű ellenőrzést követően a lehetőségekhez mérten érdemes minél életszerűbben végrehajtani azt, egy adott szituációnak megfelelően.

A tervezés és a megvalósítás után biztosítani kell, hogy az előírt folyamatok a mindennapi tevékenységek részévé váljanak. Figyelemfelkeltés, tájékoztatás vagy oktatás révén érhető el, hogy mindenki tisztában legyen az üzletmenet- és az informatikaszolgáltatás-folytonosság témakörével. A visszaállítási tevékenységet végző csapatot szakmailag fel kell készíteni a feladatok végrehajtására. Érdemes rendszeres időközönként felülvizsgálatot végezni az informatikai infrastruktúra jelentős változtatásakor vagy az üzleti tevékenység megváltozásakor. A kezdeti tesztelés után rendszeres időközönként a kritikus részekre koncentráló teszteket kell végrehajtani, amellyel biztosítható, hogy az időközben végrehajtott változtatásokat megfelelően figyelembe vettük-e. Az informatikaszolgáltatás-folytonossági tervet és a szolgáltatókkal kötött megállapodásokat a változáskezelés hatásköre alá kell vonni, így biztosítható a változtatások átvezetése.

Az informatikaszolgáltatás-folytonossági terv életbe léptetését egy kríziskezelési csoportnak kell jóváhagyni. Az egyes helyszíneken, csoporttagoknál kell lenni egy leírásnak, amelyben szerepel a tervek helye, értesítendő személyek elérhetőségi információja, kulcsfontosságú lépések, döntési pontok leírása.

Az informatikaszolgáltatás-folytonosság irányításának megvalósítása esetén a krízishelyzetek után a szolgáltatások visszaállítása ellenőrzött módon zajlik. Mivel az elvégzendő teendőket koordináltan és begyakoroltan hajtják végre, nagyobb esély van a sikeres visszatérésre. Az informatikaszolgáltatás-folytonossági terv és folyamat használatával a szolgáltatás kiesésének ideje csökkenthető, nagyobb szolgáltatásfolyamatosság érhető el. Az elvesztett adatok mennyisége minimalizálható, a biztonsági kérdések megválaszolása megfelelően kezelhető. Az üzleti tevékenységek kiesése minimalizálható és az üzlet által elfogadott szintre csökkenthető. Sokszor törvényben kötelezően előírt követelményeknek kell megfelelni, amelynek hiányában (ha nincs tesztelt megoldás a katasztrófahelyzetek kezelésére) büntetések, szankciók lépnek érvénybe. Az informatika és üzletmenet közötti kapcsolat javítható, az üzleti igényeket informatikai oldalról megközelítve jobban meg lehet érteni. Részletesen meg lehet ismerni az informatikaszolgáltatás kiesése által okozott veszteségeket, előre lehet számolni a kiesési idővel és a szolgáltatások átmeneti időszakra vonatkozó minőségi szintjeivel.

Problémát jelenthet ugyanakkor a felső vezetés elkötelezettségének hiánya, ezáltal az informatikaszolgáltatás-folytonosság irányításának tervezéséhez és karbantartásához szükséges pénzkeret, illetve emberi erőforrás nem biztosítható. A mindennapi tevékenységek elvégzése mellett külön időt kell biztosítani az ilyen jellegű feladatokra, különben nehéz megnyerni erre a felhasználókat. Az informatikaszolgáltatás-folytonosság irányításának tevékenysége a felső vezetés szempontjából nem megtérülő beruházást jelent, ezért sokszor jelentkezik a pénzügyi támogatás hiánya. Ezt olyan biztosítás jellegű befektetésnek kell tekinteni, amely az üzletmenet-folytonosság része.

A szolgáltatás-visszaállítási tervek kidolgozása után azokat rendszeresen tesztelni kell, ami az éles rendszer működtetése mellett erőforráshiányt eredményezhet. A tervek rendszeres frissítéséről is gondoskodni kell, a változásokat pedig át kell vezetni, mert módosulhat a szolgáltatások prioritása, technológiák, visszatérési lépések menete.

14. Fejlesztői tevékenységek az incidensmenedzsment támogatására

Az elektronikus információs rendszerek védelmi megoldási, naplózási és ezen keresztül incidensmenedzsmentet támogató képessége általában már a tervezési folyamat során eldől. Dobozos szoftverek, operációs rendszerek, egyéb rendszerkomponensek, hardvereszközök naplózási képessége általában

a rendszerelem konfigurációjának módosításával rugalmasan változtatható. Ugyanakkor, nem tervezett védelmi eszköz, a fejlesztett alkalmazások védelmi képességeinek utólagos módosítása általában nehézkes és költségigényes, ami egy újonnan üzembe helyezett rendszer esetében általában kevésbé elfogadható.

Az incidenskezeléssel kapcsolatos adminisztratív, illetve logikai kontrollokat az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) és a végrehajtására kiadott, 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 (továbbiakban: Vhr) határozza meg. A tervezés során célszerű figyelembe venni egyéb szabványokat előírásokat, mint például NIST publikációk, CCM,[182] ISO szabványok.

14.1. Az incidenskezelési tevékenység támogatása

A biztonsági események kezelésével (incidenskezeléssel) kapcsolatos előírások az adminisztratív védelmi intézkedések között jelennek meg 3. vagy magasabb biztonsági osztályba sorolt rendszerek esetén. Ezen követelmények a fejlesztési ciklusban csak akkor jelennek meg, ha az adott szervezet nem működteti a Vhr.-ben meghatározott védelmi intézkedéseket, és azt a fejlesztési projekt során ki kell dolgozni.

Az adminisztratív kontrollok teljesítése nem valósítható meg megfelelő műszaki támogatás nélkül, amelyek részben meg is jelennek a logikai kontrollok között egy-egy kontrollcsoportban.

14.2. Az elektronikus információs rendszer naplózási képességeivel szemben támasztott elvárások

A naplózással mint az elszámoltathatóság, illetve az incidensmenedzsment legfontosabb területével a Vhr. részletesen foglalkozik. Fontos, hogy az utólagos módosítások okozta nehézségek miatt a rendszer tervezése során a naplózási kérdések megfelelő súlyt kapjanak, és a szükséges tevékenységek, erőforrások tervezve legyenek.

A naplózási képesség megléte alapkövetelményként jelenik meg már a legalacsonyabb biztonsági osztályba sorolt rendszerek esetében is. A szervezetnek ki kell dolgoznia a naplózási eljárásrendet, meg kell határozni a naplózandó események körét és a naplótartalmat, és ezek alapján kell végeznie a naplózási tevékenységét.

A naplózás fejlesztésénél, beállításánál különösen oda kell figyelni, hogy a keletkezett naplóbejegyzések tárolhatók és feldolgozhatók legyenek. A túl sok és nem releváns naplóbejegyzés gyűjtése és a feldolgozás során keletkező események olyan terhelést jelenthetnek a szervezet számára, amelyet már nem képes elviselni, és aminek következtében – a naplózás háttérbe szorulása miatt – pont az elérni kívánt cél nem lesz teljesíthető. A releváns naplóbejegyzések hiánya pedig ellehetetlenítheti a hatékony vizsgálatot.

A naplózási célok teljesülését nagymértékben befolyásolja a naplók tartalma. Amennyiben lehetőség van a naplótartalom összeállítására, akkor törekedni kell arra, hogy bejegyzésben minden olyan információ szerepeljen, amely a naplózás céljainak megvalósításához szükséges, és ne tartalmazzon olyan információkat, amelyek később nem kerülnek felhasználásra. Minimálisan a naplóbejegyzésnek tartalmaznia kell az esemény időpontját, a rendszert, az eseményt és annak sikerességét.

[182] Cloud Controls Matrix: felhő alapú technológiák biztonsági mátrixa.

Az eszköz funkciójától függően további információknak kell a naplóbejegyzésben szerepelniük:

- hálózati eszközök esetében minimálisan a forgalmi adatok (forrás, cél, protokoll, port stb.), amennyiben lehetőség van, úgy hálózati csomagadatok, -tartalom;
- informatikai rendszerek esetében az esemény adatai, jellemzői, érintett felhasználó/rendszer stb.;
- egyéb infrastruktúraelemek esetében a tevékenységet végző felhasználó, a tevékenység leírása;
- üzleti alkalmazás esetében az érintett üzleti terület által meghatározott események felismeréséhez szükséges információk.

A naplózott, valamint az incidenskezelés során használt rendszerek időbeni szinkronizációja és egységes időformátum használata nélkül a korrelált eseményből generálódott incidenseket nem lehet feltárni; az esetleges nyomozás az eltérő időformátum, időfolyam-anomália miatt nehézkes.

Biztosítani kell a naplóállományok védelmét jogosulatlan megismerés ellen.

Biztosítani kell, hogy a naplóbejegyzések megőrzése a jogszabályokban, belső szabályzókban meghatározottak szerint történjen.

A 3. biztonsági osztályba sorolt rendszerek esetén gondoskodni kell a megfelelő tárkapacitás biztosításáról, a naplózási hibák kezeléséről, illetve vizsgálni kell a naplóbejegyzéseket, valamint jelentést kell készíteni meghatározott személyeknek.

A következő (4. biztonsági) osztályba sorolt rendszerek esetén jelenik meg követelményként az elemzési képesség javítása, a rendszer működésének további javítása, vagyis a naplótartalom kiegészítése, a naplóbejegyzések automatikus vizsgálata, jelentéskészítés, a korrelációs vizsgálat, a rendszeróra szinkronizálása és a naplófunkciók kezelésének korlátozása.

A Vhr. előírása alapján 5-ös szintre besorolt rendszerek esetén további követelmények jelennek meg, melyek közül a legfontosabbak a naplózandó események körének felülvizsgálata, a központi naplókezelés, a valós idejű riasztás, a naplóvizsgálat kiegészítése felügyeleti eszközökből érkező jelzésekkel, a fizikai hozzáférések korrelálása a rendszerben keletkező naplóbejegyzésekhez és a naplóbejegyzések kriptográfiai védeleme.

Ahhoz, hogy a Vhr. által a naplózás kapcsán megfogalmazott célok teljesüljenek, számos feltételnek kell megfelelni, amelyek közül a legfontosabbak, hogy:

- valamennyi biztonsági szempontból releváns informatikai eszközben keletkezzenek megfelelő tartamú naplóbejegyzések a rendszerben zajló tevékenységekről.
- a biztonsági szempontból releváns naplóbejegyzések jussanak el az elemzőhöz (legyen az automatikus elemző rendszer vagy emberi erőforrás);
- legyen meg az elemzési képesség, azaz kerüljön kialakításra olyan feltételrendszer (erőforrás), amely biztosítja a káros esemény feltárását;
- valós idejű riasztás esetén biztosítva legyen a válaszadáshoz szükséges képesség, mind szervezeti, mind technikai, mind személyi oldalról.

15. Mellékletek

1. melléklet

Módosították az információbiztonsági törvényt[183]

Az Országgyűlés az első két év tapasztalatai alapján felülvizsgálta az információbiztonsági törvényt, és az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. évi CXXX. törvény elfogadásával módosította azt. A módosítások 2015. július 16-án léptek hatályba. Az információbiztonsági törvény felülvizsgálatával párhuzamosan a kormány, valamint a Belügyminisztérium elvégezte a végrehajtási rendeletek felülvizsgálatát is.

Ennek eredményeként a következő új jogszabályok léptek hatályba:

- 187/2015. (VII. 13.) Kormányrendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról;
- 185/2015. (VII. 13.) Kormányrendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól; (hatályon kívül helyezte a 271/2018. (XII. 20.) Kormányrendelet)
- 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;
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről. (hatályon kívül helyezte a 44/2017. (XII. 29.) BM rendelet)

A fentiekkel párhuzamosan a következő jogszabályokat helyezték hatályon kívül:

- 233/2013. (VI. 30.) Kormányrendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről;
- 301/2013. (VII. 29.) Kormányrendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról;
- 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről;
- 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről.

[183] Lásd: http://informaciobiztonsagitv.blog.hu/2015/07/20/modositottak_az_informaciobiztonsagi_torvenyt_elso_benyomasok (utolsó letöltés: 2017. április 19.)

A következő szervezeti változások történtek:

- A 2014-es kormányzati átalakítás eredményeként már a korábbiakban a Belügyminisztériumhoz került a Nemzeti Biztonsági Felügyelet (korábbiakban: KIM), valamint a Nemzeti Elektronikus Információbiztonsági Hatóság (korábbiakban: NFM, továbbiakban: NEIH).
- Az információbiztonsági törvény és annak végrehajtási rendeleteinek módosításával a Nemzeti Biztonsági Felügyelet sérülékenység vizsgálati szakhatósági feladatköre megszűnt, azt a Nemzetbiztonsági Szakszolgálat vette át.
- A NEIH 2015. január 1-jétől a Belügyminisztérium főosztályaként tevékenykedett. Ezt a feladatkört 2015. október 1-jével szintén a Nemzetbiztonsági Szakszolgálat veszi át.

Az Ibtv. 2015. évi módosítása eredményeként az állami és önkormányzati szervezetek információs rendszerei tekintetében az információbiztonsági hatósági, a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó eseménykezelő központtal, valamint az informatikai rendszerek gyenge pontjainak feltárását, a rendszer védelmi képességek tesztelésével (sérülékenységvizsgálat) kapcsolatos feladatok ellátására a Nemzetbiztonsági Szakszolgálat (NBSZ) kerül kijelölésre, amelynek szervezetén belül 2015. október 1-jével létrehozásra került a Nemzeti Kibervédelmi Intézetet (NKI).

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet a 2019. január 1-jén hatályba lépett jogszabály-módosítások eredményeként ellátja

- az eseménykezelési feladatokat a létfontosságú információs rendszerek és rendszerelemek, valamint
- az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben meghatározott bejelentés-köteles szolgáltatást – úgymint online piactér, internetes keresőszolgáltatás, valamint felhőszolgáltatás – nyújtó szolgáltatók esetében az eseménykezelési, valamint a hatósági felügyeletet.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet jogszabályi feladatai közé tartozik továbbá az ún. „nemzeti kapcsolattartó pont" működtetése, amelynek feladata az Európai Unión belüli nagy hatású kiber-incidensek hazai koordinálása, az incidensekkel kapcsolatos jelentések fogadása, küldése a nemzetközi partner-szervezetek irányába.

Hatósági adatszolgáltatás változása

A korábbiakban lehetősége volt a szervezetnek az Ibtv. 15. § (3) bekezdése szerinti adatokat ÁNYK űrlapon, elektronikusan aláírt elektronikus levélben vagy postai úton is megküldeni a hatóság részére. Az új szabályozás értelmében erre csak a hatóság elektronikus adatbejelentő rendszerén keresztül elektronikusan, a hatóság által meghatározott és közzétett formátumban van lehetőség.[184]

Fontos változás, hogy idáig az Ibtv. 15. § (1) bekezdése szerinti, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatainak megküldésére vonatkozóan nem volt kötelezően meghatározott formai és tartalmi követelmény. A hatóság segédletet tett közzé a honlapján, mostantól ezeket az adatokat a hatóság által meghatározott formában kell megküldeni.

Változtatták a szervezeti regisztrációt is. Az új szabály szerint elsőként a szervezet regisztrálja be az elektronikus információs rendszerek biztonságáért felelős személyt (továbbiakban: IBF), majd az IBF jelenti be a szervezetet.

A szervezet vezetőjének feladata, hogy az így kapott regisztrációs űrlap hitelesített példányát biztonságos elektronikus kézbesítési szolgáltatás révén vagy postai úton megküldje a hatóság számára.

[184] 187/2015. (VII. 13.) Korm. rendelet10/D. §

Az új rendelet hatályba lépése előtt regisztrált szervezeteknek nem kell újra regisztrálniuk magukat. Az interneten fellelhető nem hivatalos információk szerint a mintegy 5000 érintett szervezet közül nagyságrendileg 1000 tett eleget a bejelentési kötelezettségének.

Biztonsági osztályba sorolás, biztonsági szintbe sorolás követelményeinek változása

Fontos megemlíteni, hogy megváltozott a szervezetek biztonsági szintbe sorolásának módja. A törvény alapján valamennyi hatálya alá tartozó szervezetnek biztonsági szintbe kell sorolnia szervezetét és a megállapított biztonsági szinttől függően adminisztratív és fizikai védelmi intézkedéseket kell bevezetni.

A korábbiakban az Ibtv. definiálta az egyes szervezetek minimális biztonsági szintjét, valamint azt, hogy legalább a legmagasabb biztonsági osztályba sorolt elektronikus információs rendszerével azonos biztonsági szinttel kell megegyeznie.

A módosítást követően a fenti módszertant megszüntették, mostantól az elektronikus információs rendszerek felhasználásának módja határozza meg egy szervezet biztonsági szintjét.

Változás továbbá, hogy az új szabály szerint nemcsak a szervezetet, hanem a következő szervezeti egységeket is biztonsági szintbe kell sorolni: az elektronikus információs rendszer fejlesztését és üzemeltetését végző, az üzemeltetéséért vagy az információbiztonságért felelős szervezeti egységek.

A besorolási útmutatót a technológiai Vhr. tartalmazza.

Ennek alapján 2-es a biztonsági szintje annak a szervezetnek, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.

Jogszabály alapján kijelölt szolgáltató lehet a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Kormányrendelet 1. § a) pontja alapján a Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban: NISZ), az IdomSoft Informatikai Zártkörűen Működő Részvénytársaság, valamint a KOPINT-DATORG Informatikai és Vagyonkezelő Kft.

3-as a biztonsági szintje annak a szervezetnek, amely a 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.

Az Ibtv. alapján *kritikus adatnak* minősül a személyes adat vagy valamely jogszabállyal védett adat. Az Infotv. szerint *különleges adat* pedig a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Jogszabály által *védett adat* lehet az adótitok, az üzleti titok, az orvosi, ügyvédi, biztosítási, banktitok stb.

4-es egy szervezet biztonsági szintje, ha az vagy egy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.

Az Ibtv. alapján zártcélú elektronikus információs rendszer a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja.

5-ös biztonsági szintbe kell sorolni azt a szervezetet, amely a 4. szinthez rendelt jellemzőkön túl európai és nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.

Az európai és a nemzeti létfontosságú rendszerelemekkel a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) foglalkozik.

Az új módszertan alapján javasolt minden szervezet számára a biztonsági szintjének felülvizsgálata, mivel más szempontrendszer alapján végzett vizsgálat vélhetően más eredményt ad.

A fentiek alapján megállapítható, hogy az a szervezet, amely központi szolgáltatótól veszi igénybe az elektronikus információs rendszerek szolgáltatásait, annak alacsonyabb lesz a biztonsági szintje, mint annak, aki önállóan üzemelteti azokat.

Hogy a fenti megoldás mennyire lesz hatékony, azt csak az elkövetkező évek tapasztalatai fogják tudni megmondani.

2. melléklet

ISO/IEC 27000 szabványcsalád[185]

Az ISO/IEC 27000-es szabványcsoport az információbiztonsági irányítási rendszerekkel kapcsolatos szabványokat tartalmazza, melyek egy része előkészítés, illetve korszerűsítés alatt áll, jelentős részük azonban már megjelent. Ezek közül az MSZT az ISO/IEC 27001-en kívül még két szabványt vezetett be magyar nemzeti szabványként, amelyek a következők: MSZ ISO/IEC 27002:2011: Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (magyar nyelvű) és az MSZ ISO/IEC 27006:2013: Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszereinek auditját és tanúsítását végző testületekre vonatkozó követelmények (angol nyelvű).

COBIT

Az Information Systems Audit and ControlAssociation (ISACA) és az IT Governance Institute (ITGI) hozta létre 1996-ban. Célja, hogy segítse az üzleti vezetők és auditorok mindennapi munkáját. Kutatja és fejleszti az általánosan elfogadott informatikai technológiák irányítási céljainak halmazát. A vezetőknek az informatikai döntések és befektetések alapjait nyújtja. Segíti a stratégiai tervek és az informatikai rendszerek felépítésének megalkotását. Tanácsot ad a folyamatos szolgáltatáshoz és a teljesítménymonitorozáshoz szükséges hardver és szoftver kiválasztásában. A COBIT által meghatározott kritériumok biztosítják az ügyfeleket az irányítás, a biztonság és a folyamatok kezelésének megfelelő szintjéről. Azonosítja az informatikai irányítás témáit a cég informatikai infrastruktúráján belül.

MOF (Microsoft Operations Framework)

A Microsoft üzemeltetési keretrendszere azokat a kisebb szervezeteket célozza, amelyek nem szeretnék a teljes ITIL-t alkalmazni és megvásárolni. A MOF ingyenesen letölthető, a teljes informatikai életciklust felölelően közli a bevált gyakorlatok gyűjteményét, kérdés alapú segédlettel támogatva. ITIL alapokon nyugszik, annak korlátozott megvalósítása. Egységbe foglalja az informatikai tervezés, átadás, üzemeltetés közösségek által meghatározott folyamatait, az irányítással, kockázattal és megfelelőséggel kapcsolatos tevékenységeket, a vezetői jelentéseket, áttekintéseket.

[185] Lásd: www.mszt.hu/web/guest/informaciobiztonsag1 (utolsó letöltés: 2017. április 24.)

A Code of practice for IT Service Management – PD0005

A Brit Szabványügyi Hivatal kiadványa, amely az ITIL elvein alapul, a szabványt magyarázó, annak alkalmazását elősegítő dokumentum. Az új ITIL modell a BSI modell kiterjesztésének tekinthető, amely még tovább fejleszti az informatikai szolgáltatásmenedzsmentet.

16. Felhasznált irodalom

- *Network Management System Database (NMSDB) – Üzemeltetés és dokumentáció kis költséggel, kis munkával.* T-Systems. Elérhető: www.t-systems.hu/static/sw/file/Network_management_system_database.pdf (utolsó letöltés: 2017. április 20.)
- Broczkó Péter (2011): *ITIL alapú szolgáltatásmenedzsment.* Budapest, Óbudai Egyetem, Neumann János Informatikai Kar. Elérhető: https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/12934/ITIL_alapu_szolgaltatas_menedzsment.pdf (utolsó letöltés: 2022. április 6.)
- Erdélyi Krisztina – Schubert Tamás (2011): *Informatikai Rendszerek Felügyelete.* Budapest, Óbudai Egyetem, Neumann János Informatikai Kar.
- Haig Zsolt – Kovács László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest, Nemzeti Közszolgálati Egyetem.
- *Útmutató a számítógépek felügyeletéhez – Üzleti célú asztali számítógépek* (2008). Harmadik kiadás. Hewlett-Packard Development Company, L.P.
- Horváth Gergely Krisztián, CISA CISM (2014): *Incidens-menedzsment, BCP, DRP integráció – A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez.* Budapest, Nemzeti Közszolgálati Egyetem.
- *ITIL® V3 Hungarian Glossary® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5* (2008). Elérhető: www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/ITIL/ITIL%20V3%20fogalomt%C3%A1r%20v2.5.pdf (utolsó letöltés: 2017. április 20.)
- *ITIL – az informatikaszolgáltatás módszertana (2002). KFKI Számítástechnikai Rt.* Elérhető: www.itsmf.hu/documents/itil2modszertan_osszefoglalo_v3.1.pdf (utolsó letöltés: 2017. április 20.)
- Spisák Andor (2006): Nyilvános kulcsú infrastruktúra architektúrák – Public Key Infrastructure Models. *Hadmérnök,* 1. évf. 1. sz. 31–46. Elérhető: http://hadmernok.hu/archivum/2006/1/2006_1_spisak.pdf (2017. április 20.)
- *Cisco Prime Infrastructure – Új generációs hálózatfelügyeleti megoldás.* T-System. Elérhető: www.t-systems.hu/static/sw/file/cisco_prime_infrastructure.pdf (utolsó letöltés: 2017. április 12.)
- 1139/2013. (III. 21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- ITILv3 Foundation – Szolgáltatás Üzemeltetés. Elérhető: http://erp-blog.blog.hu/2010/08/24/itil_v3_foundation_szolgaltatas_uzemeltetes
- (utolsó letöltés: 2017. március 14.)
- Incidensek – 2016. Elérhető: http://images.slideplayer.hu/46/11640024/slides/slide_13.jpg (utolsó letöltés: 2017. március 16.)
- Üzletfolytonossági rendszer kialakítása. Elérhető: www.grid.hu/hu/megoldasaink-termekeink/uezletfolytonossagi-rendszer-kialakitasa (utolsó letöltés: 2017. március 16.)
- Informatikai Katasztrófaterv. Elérhető: www.itsecure.hu/drp (utolsó letöltés: 2017. március 17.)
- Az SLA módszertan tartalmi elemei. Elérhető: www.sla.hu/sla-modszertan/sla-modszertan-tartalmi-elemei-9.html (utolsó letöltés: 2017. március 17.)

- Fejlesszen ki biztonsági irányelveket és kényszerítse ki az alkalmazásukat az IT alkalmazás-környezet egészében. Elérhető: www-03.ibm.com/software/products/hu/security-policy-manager (utolsó letöltés: 2017. április 10.)
- How does Azure VM replication work in Site Recovery? Online: https://docs.microsoft.com/hu-hu/azure/site-recovery/site-recovery-components (utolsó letöltés: 2017. április 10.)
- Áttekintés: Fájlok és mappák biztonsági mentése a Resource Manager-alapú üzemelő példányban. Elérhető: https://docs.microsoft.com/hu-hu/azure/backup/backup-try-azure-backup-in-10-mins (utolsó letöltés: 2017. április 10.)
- Az IBM InfoSphere eDiscovery Manager architektúra bemutatása. Elérhető: www.ibm.com/support/knowledgecenter/hu/SS8JHU_2.1.1/com.ibm.edc.doc/edcao001.htm (utolsó letöltés: 2017. április 12.)
- Megoldásarchitektúra: Kis- és középvállalati vészhelyreállítás az Azure Site Recovery segítségével. Elérhető: https://azure.microsoft.com/hu-hu/solutions/architecture/disaster-recovery-smb-azure-site-recovery/ (utolsó letöltés: 2017. április 20.)
- Microsoft Dynamic NAV. Elérhető: https://navision.hu/microsoft-dynamics-365-business-central/ (utolsó letöltés: 2022. április 6.)
- Microsoft Dynamic NAV termékleírás. Elérhető: www.karadi.hu/navision-modulok-reszletes-leirasa (utolsó letöltés: 2017. április 20.)
- Microsoft Dynamic NAV referenciák. Elérhető: https://navision.hu/microsoft-dynamics-nav-referenciak/ (utolsó letöltés: 2017. április 20.)
- Információbiztonság. Elérhető: www.mszt.hu/web/guest/informaciobiztonsag1 (utolsó letöltés: 2017. április 24.)

4. KAPITÁNY SÁNDOR: INCIDENSKEZELÉS FELHASZNÁLÓI SZEMMEL

Az incidenskezelés és a „hagyományos” problémamegoldás folyamatai, ha kellő elvonatkoztatással vizsgáljuk őket, sok ponton mutatnak hasonlóságot. Mivel a végfelhasználók számára az incidenskezelés elsőre ijesztően hangozhat, nézzük meg, hogy ezek a hasonlóságok miként segítik a megértést. Ezek felderítésével láthatóvá válik, hogy egyszerű, logikus lépéseket követve miként tudjuk az incidenseket is a hagyományos problémamegoldás eszközeivel kezelni.

1. Általános problémamegoldó folyamat lépései és a felhasználók szerepe

Minden szervezeti működésben megvan annak a lehetősége, hogy egy folyamat, tevékenység nem a megfelelő, megszokott vagy éppen az előírások által definiált módon működik, illetve kezd el működni. Az ilyen eltérést az általános szóhasználat szerint *problémának* szoktuk definiálni. A későbbiekben látni fogjuk, hogy az informatikai folyamatok szabályozásának egyik legelterjedtebb követelményrendszere a *probléma* fogalmát részben másként értelmezi, de az egyszerűség kedvéért egyelőre maradjunk az iménti általános szóhasználatnál.

Mivel probléma minden folyamat, termék vagy szolgáltatás kapcsán előfordulhat, nagyon sokféle problémafeltáró, problémamegoldó technika érhető el. Ezek egy része valamilyen szakterület egyedi igényeihez igazodik, míg mások általános megoldásokat kínálnak a normál elvárások szerinti működéshez való visszatérésre.

Jelen jegyzet az informatikai, információbiztonsági problémák kezelésével foglalkozik – amelyet ezen szakterületen jellemzően *incidensnek* neveznek –, a következőkben bemutatandó problémamegoldó módszertan azt kívánja szemléltetni, hogy valójában az általános vagy néhány szakterületen használt módszertanok ismerete sokszor segítségünkre lehet az információbiztonsági incidensek kezelésének mikéntjében is. A későbbi fejezetekben megismerkedünk majd azokkal a folyamatokkal, feladatokkal, melyek az információbiztonsági incidensek felismerését, feldolgozását, kezelését és ismétlődésük megakadályozását segítik, teszik egyszerűbbé azok számára is, akik a rendszereket „csak” használják, és nem rendelkeznek érdemi ismeretekkel azok működéséről, működtetéséről.

Egy probléma megoldásának lépéseit az autóiparból indult, és azóta széleskörűen elterjedt úgynevezett 8D technika írja le. Megjegyzendő, hogy az eredeti 8D módszertan ezen lépések megtételére időkorlátokat is meghatároz, azaz bizonyos lépéseknek adott időn belül meg kell történniük. Ez egy különösen fontos kérdésre hívja fel a figyelmet az incidensek kezelése kapcsán, ami nem más, mint az időtényező. Nyilván az senki számára nem kérdés, hogy egy incidens minél gyorsabb megoldása a cél. Ugyanakkor egy olyan szituációban, amikor a normál működéstől eltérőt tapasztalunk, amely ráadásul biztonsági, illetve működési vagy pénzügyi kockázatokat vet fel, még nagyobb nyomás kerül a munkatársakra. Ezt a nyomást növeli az az igény, hogy a lehető leghamarabb hárítsuk el a hibás működést, csökkentsük a kockázatot. Ahhoz, hogy az ilyen helyzetekben megfelelő magatartást tanúsítsanak a munkatársak, szükséges, hogy jól kidolgozott, és általánosan ismer megoldásokat vezessünk be a szervezetnél az incidensek jelzésére, kezelésére. Értelmezzük tehát első körben a 8+1 lépést az információbiztonsági incidensek kapcsán. Hogyan valósul ez meg egy incidens esetén, és mit tehet az egyes lépésekben a felhasználó, mi az ő felelőssége.

Az úgynevezett 0. pont az elemzendő probléma kijelölése.

Csak olyan incidensekre tudunk reagálni, amelyek ténylegesen azonosításra kerültek. Sok más szakmával ellentétben – ahol egy hibás termék vagy nem jól elvégzett tevékenység egyértelműen jelzi a problémát – az információbiztonság területén ez a lépés lehet akár az egyik legnehezebb. Aki informatikai eszközök felhasználója, az rendszeresen találkozik olyan „jelenségekkel", melyek nem egyértelműen a jó működéshez tartoznak, mégsem jelentenek a hagyományos értelemben információbiztonsági incidenst. A felhasználók felelőssége tehát jelentős, hiszen a fel nem ismert biztonsági incidens komoly következményekkel jár(hat), ugyanakkor könnyen előfordulhat, hogy nehéz megkülönböztetni a normál működést az incidens jeleitől.

A szervezeti működés szabályozásait kialakítók elsődleges felelőssége, hogy egyrészt támpontot adjanak a felhasználóknak arra vonatkozóan, hogy – az egyértelmű szituációkon kívül – mikor érdemes incidensre gyanakodni. Másrészt olyan könnyen működtethető utakat kell biztosítani, amivel a felhasználók – gyanú esetén – egyszerűen jelezhetik, hogy incidenst észleltek. Adott esetben olyan köztes pontokat kell beépíteni, ahol megfelelő kompetenciával rendelkező személyek dönteni tudnak arról, hogy az észlelt jelenség tényleg incidens-e, vagy a működés normál része.

Egy probléma megoldása során a 8D technika szerinti tényleges első lépés a problémamegoldó csoport alakítása, a „mozgósítás".

Az informatikai, információbiztonsági incidensek esetén különböző módszertanok másként határozzák meg az ilyen csoportok, teamek összehívásának módszerét, rendjét. Mind az előre definiált reagálócsoportok, mind az adott incidens kapcsán ad hoc megalakított teamek jó megoldást jelenthetnek. A felhasználók felelőssége, illetve szerepe ebben a lépésben általában kevesebb, talán arra érdemes ilyenkor figyelni, hogy az incidens további terjedését ne segítsük, illetve a későbbi kivizsgálást ne akadályozzuk.

Jellemző feladatok ebben a fázisban az eredeti 8D technika szerint:

- csoportmunkát igénylő hiba hibaként való megjelölése, és az érintettek körének kijelölése;
- akciócsoport összehívása;
- a hiba definiálása;
- érintett (technológiai) terület megjelölése.

A második lépés a 8D-ben a probléma leírása, az elemzésre alkalmas tényrögzítés (a helyszínen).

Ebben a lépésben alapozzuk meg a későbbi okkeresés sikerének lehetőségét. A kellően alapos tényrögzítés segítheti az incidenshez vezető okok feltárását és az incidens megszűntetését, illetve ismétlődésének megakadályozását.

A felhasználó elsődleges felelőssége, hogy minden lehetséges körülményt rögzítsen, illetve elmondjon a feltárást végző(k)nek. Itt meg kell jegyezni, hogy, ha az incidens gondatlan (vagy netán szándékos) magatartásra vezethető vissza, gyakran a felhasználók, illetve azok, akik magatartásukkal az incidenst okozták, megpróbálnak bizonyos tényeket elhallgatni, a kivizsgálást segítő adatokat eltüntetni, esetleg megváltoztatni. A szervezeti működést kialakítók felelőssége, hogy ilyen hozzáállást a szabályozások megfelelő kialakításával, illetve a tudatosság növelésével mérsékeljék. Hasznos eszköz lehet, ha a tudatosítás és az esetleges retorziók szintjén egyaránt kihirdetik, hogy a gondatlan magatartás kisebb következménnyel jár, mint az incidens vizsgálatának és megszűntetésének akadályozása.

A tényrögzítés fázisában jellemzően az alábbiak vizsgálatára lehet célszerű kitérni:

- A hiba hol merült fel a térben?
- A közvetlen környezet jellegzetességei, állapotok leírása (logok).
- A hiba hol merült fel a rendszerben/technológiai sorban?
- Visszakövetés és vizsgálat a dokumentációban.
- Milyen, a hibával időben összekapcsolható környezeti események történtek (logok)?
- Fényképek, screenshotok, rajzok készítése, helyszíni interjúk.

A harmadik lépés során elvégzendők az azonnali elhárító és kárenyhítő intézkedések.

Ennek a lépésnek az egyik lényege, hogy minden olyan tevékenységet, működést megakadályozzunk, amely az incidens további terjedését, illetve újabb incidensek kialakulását okozná. Ez gyakran a legegyszerűbb megoldásokat kívánja, például a számítógép hálózatról való leválasztását, de előfordulhat, hogy ellentétes a tények felmérésével, hiszen egy megszűnt kapcsolat nem biztos, hogy kinyomozható.

A másik kulcselem, hogy hozzunk meg minden olyan (meghozható) döntést, amely a további normális (közeli) működést támogatni tudja. Vagyis a nem érintett területek működjenek tovább, és ha van azonnali javító intézkedésre lehetőség, akkor tegyük meg, hogy az incidens okozta közvetett kár minél kisebb lehessen.

A felhasználók ekkor leginkább a működés rugalmas támogatásával, illetve az alternatívák értékelésének segítésével tudják előmozdítani a hatékony incidenskezelést.

Az általánosan megfogalmazott feladatok jellemzően:

- alternatívák keresése, majd döntés és akcióterv a hiba terjedésének megakadályozásáról;
- elhárító intézkedés bevezetése;
- döntés és akcióterv a károk megakadályozására és enyhítésére;
- kárenyhítő intézkedés bevezetése.

Az 1–3. lépések, bár az eredeti módszertanban egyfajta logikai sorrendben kerülnek leírásra, könnyen előfordulhat, hogy időben párhuzamosan kerülnek elvégzésre. Ennek egyik oka, hogy az egyes tevékenységek azonos szakembereket igényelnek, a másik, hogy egy incidens hatékony kezelése nem teszi lehetővé, hogy sorrendet állítsunk fel a körülmények felmérése, és az átmeneti intézkedések bevezetése között. Egy incidenskezelés időnyomása valamelyest akkor csökken, ha a harmadik lépést sikeresen végrehajtottuk.

A negyedik lépés a vizsgálatok, az okok meghatározása, és a kapcsolatok elemzése.

Ettől a lépéstől kezdve jellemzően már csak az incidenst kivizsgáló team tagjai végeznek tevékenységet, a felhasználók ebben pusztán annyi felelősséget kapnak, hogy a vizsgálódás közben felmerülő esetleges kérdésekre a legjobb tudásuk szerint megadják a válaszokat. Ugyanakkor a kivizsgálás egyik leglényegesebb lépése ez. Mivel az időnyomás már enyhült, teret kaphat a kellően megalapozott, szakmai munka, hogy az incidens összefüggéseit, okozati viszonyait, forrásait felderítsék.

A tipikusan ebben a lépésben megvalósítandó feladatok általánosságban:

- részletes elemző vizsgálatok: a hibás objektum/működés vizsgálata, a beszámolók feljegyzéseinek elemzése, a technikai környezet vizsgálata, a berendezés funkciópróbája, logok elemzése;
- lehetséges okok összegyűjtése;
- okok csoportosítása;
- ok-okozati összefüggések elemzése;
- okok súlyosság szerinti rangsorolása.

Az ötödik lépés a javító intézkedések végleges változatának kiválasztása és tesztelése.

Sokszor nehéz elkülöníteni a megoldási javaslatok kidolgozását, és az azokról való döntések meghozatalát. Mivel a működésünket a harmadik lépésben már – valamilyen szinten – biztosítottuk, most arra kell megfelelő választ találnunk, miként tudjuk elhárítani teljes mértékben az incidenst (vagy legalább amennyire a körülmények lehetővé teszik), és miként tudunk olyan megoldást bevezetni, amely a hasonló incidens bekövetkezésének valószínűségét elfogadható szintűre csökkenti. Ehhez a rendelkezésre álló oksági elemzések alapján kell kidolgozni alternatívákat, melyekből a megfelelő szintű vezetői döntés után végrehajtandó intézkedések születnek.

Ebben a lépésben a felhasználók közreműködése minimális, leginkább az alternatívák értékelésére szorítkozik, amennyiben ebbe bevonásra kerülnek.

A jellemző feladatok:

- a javító intézkedésváltozatok hatásainak elemzése (kockázatelemzési módszerekkel);
- az okok és a megoldásváltozatok ismeretében a leghatékonyabb javító intézkedés meghatározása;
- a harmadik lépésben kijelölt azonnali elhárító intézkedés és hatásainak értékelése, korrekciók végrehajtása;
- a kijelölt javító intézkedés elvi és gyakorlati tesztelése;
- az intézkedés elfogadása és igazolása.

Hatodik lépés a bevezetés és a folyamatos ellenőrzés.

A kiválasztott megoldási alternatíva bevezetése, amely a szervezet több területének együttműködését is igényelheti. Itt a feladatok jelentős része már nem korlátozódik az incidens kezelőire, hanem a szervezet nagyobb részét, adott esetben egészét érintő változtatások bevezetése is lehetséges. A felhasználók ebben a fázisban már nem mint az incidens által érintettek, hanem a változások alanyaiként jelennek meg. Egy kellően átgondolt intézkedés esetén, megfelelő tesztelések után, ekkor már csak a változások elfogadása a szerepük, illetve azon észrevételeik jelzése, melyek a működéshatékonyságot befolyásolják, vagy esetleges incidensekhez vezethetnek.

A lépések az alábbiak lehetnek:

- bevezetési terv készítése (sarokpontokhoz határidő rendelése; felelősök kijelölése; erőforrások megadása; sarokpontokon az igazolás formájának meghatározása);
- a harmadik lépésben jelölt (átmeneti) intézkedések megszűntetése vagy állandósítása;
- a működtetés kritikus elemeinek megjelölése és az ellenőrzés módszerének kidolgozása (számszerűsítés; elfogadhatósági határértékek meghatározása; ellenőrzést végzők kijelölése; teendők meghatározása eltérés esetén);
- a határértékek figyelése, a tények igazolása, eltérések esetén helyesbítő beavatkozások.

Hetedik lépés a visszacsatolás, az újbóli előfordulás megakadályozása.

Egy kellően alapos incidenskezelés, illetve problémamegoldás nem áll meg ott, hogy az adott incidensre reagál. Ha az erőforrások engedik, célszerű a működés más elemeit is megvizsgálva annak a felderítése, milyen más folyamatokban van lehetőség hasonló incidens bekövetkezésének. Amit azonban mindenképpen a bevezetés részévé kell tegyünk, hogy az incidensre adott válasz eredményét (ha az nem maga a szabályozás módosítása) átvezessük a szervezet működését rögzítő eljárásokba, szabályzatokba, leírásokba. Ekkor ne feledkezzünk el arról, hogy a módosított szabályozókat kellő alapossággal megismertessük az érintettekkel. A felhasználók felelőssége innentől a módosított elvárásoknak, szabályzatoknak megfelelő működés.

A szabályozásba integrálás lehetséges lépései:

- a probléma megoldását követően az intézkedéseket integráljuk a rendszerbe;
- az új megoldások és a „régi” működési forma kölcsönhatásainak elemzése;
- dokumentáció aktualizálása;
- felelősségi körök rendezése az új viszonyokra;
- monitoring rendszer kiterjesztése az új intézkedések elemeire.

Az utolsó, nyolcadik lépés a csoport munkájának értékelése.

Amennyiben egy szervezet kellő komolysággal kezeli a saját működését támogató folyamatokat, nem tekinthet el attól, hogy – mint minden más munkának az eredményét – az incidenskezelés sikerességét és hatékonyságát is értékelje. Az utolsó lépése a 8D technikának ennek megfelelően a munka értékelése. Ennek lényege, hogy tárják fel mindazon fejlesztési lehetőségeket, melyek egy következő incidens esetén gyorsabbá, hatékonyabbá, eredményesebbé tehetik a csoport működését. Mivel ez egyfajta belső értékelés, a felhasználók ekkor jellemzően nem kell részt vegyenek a feladatokban, arra azonban lehetőséget kaphatnak, hogy egyes kérdésekben elmondják tapasztalataikat.

A jellemző lépések:

- a probléma megoldását követő dokumentumok összegyűjtése;
- a csoport tagjainak összefoglaló értékelése a munkáról;
- vezetői értékelés a munkáról;
- jelentés készítése (cél – folyamat – eredmény);
- az eredmények kommunikálása a csoporton kívülre.

Áttekintve a problémamegoldás lépéseit, melyeket az autóipar – és mára sok más terület – használ, jól láthatjuk, hogy egy kis kreativitással az informatikai, információbiztonsági incidensek kezelésére is jól használhatjuk, illetve szükség szerint felépíthetjük rá a szervezeti módszereinket. Azt azonban ne feledjük, hogy IT és információbiztonság területén vannak olyan követelményrendszerek, melyek elvárásokat fogalmaznak meg az incidensek kezelésével kapcsolatban. Sőt jó gyakorlatot összefoglaló módszertani segédletek egész konkrét értelmezéseket adnak az incidensek kezelése kapcsán. A következőkben ezeket az elvárásrendeket, jó gyakorlati útmutatókat ismertetjük.

2. Az incidenskezeléssel kapcsolatos elvárások

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

Röviden tekintsük át, hogy mely általánosan elterjedt követelményrendszerek definiálnak elvárásokat az incidenskezeléssel kapcsolatban.

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

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

Az Information Technology Infrastructure Library (ITIL) leginkább a szolgáltatásmenedzsment jól bevált gyakorlatának gyűjteményeként definiálható. Az ebben definiált szolgáltatási életciklusmodell keretrendszert biztosít a szolgáltatásmenedzsment megvalósítására. Az ITIL az Egyesült Királyság

kormányzati beszerzésekért felelős hivatalának (Office of Government Commerce) egységesítésre törekvő gondolkozásmódjának az eredménye. Elsődleges célja az üzemeltetés részletes leszabályozásának eredményeként a szolgáltatás minőségének javítása. Első elődjeként említhető a nyolcvanas évek elején az IBM által kiadott 4-kötetes „Sárga könyvek": A Management System for Information Systems. Szerzője: Edward A. Van Schaik. Ezek az ITIL-könyvek eredeti szabálygyűjteményének a kulcsbemenetét képezték.

Amikor manapság incidenskezelésről beszélünk, sokaknak az ITIL által definiált logika jut az eszébe. Ahol IT-területen alkalmaznak szabályozott incidenskezelést, ott a legtöbb esetben (legalább részben) ITIL alapokon teszik ezt. Azt azonban nem szabad figyelmen kívül hagyni, hogy ez informatikai incidensekre vonatkozik, nem kifejezetten információbiztonsági incidensekre. Ennek részleteire később még visszatérünk.

Az Országgyűlés 2013. április 15-én fogadta el az állami és önkormányzati szervezetek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.) és rendeleteit. Ezen jogszabály megalkotása elsődlegesen az állami és önkormányzati elektronikus adatkezelés biztonságának megteremtését tűzte ki célul. Egyebek mellett azonban kijelölték az információbiztonsággal foglalkozó szervezeteket, valamint azok együttműködésének szabályait. Definíciós hátterében, fogalmi rendszerében a jogszabályok igazodnak az információbiztonságot hosszabb ideje meghatározó nemzetközi szabványokhoz, követelményekhez, mint a már említett ISO/IEC 27001, vagy a Common Criteria (CC – Közös Követelmények).

Mint azt az előzőekben említettük, fontos megkülönböztetni, hogy valamely követelmény az *információbiztonsági incidensekről* beszél, mint teszi ezt az ISO/IEC 27001 szabvány, vagy az *informatikai incidensekről,* mint ahogy azt az ITIL fogalmazza meg. Ahhoz, hogy a szervezetek által jellemzően használt incidenskezelési megoldásokat megértsük, először nézzük meg a két (részben) eltérő szemléletű követelményrendszert valamivel részletesebben.

Az ITILv3 struktúrája igen összetett, megkülönböztet szolgáltatási életciklusszakaszokat, melyek további elemekre, „menedzsmentekre" (folyamatokra) bonthatók. Ezen menedzsmentek megfelelő alkalmazása biztosítja, hogy az IT a szolgáltatásait az üzleti érdekeknek megfelelően, kellően jó minőségben biztosítsa. A teljes struktúra bemutatása meghaladja ezen jegyzet kereteit, így csak az incidensmenedzsment vonatkozásaira szorítkozunk.

Az ITILv3 a szolgáltatásmenedzsment alapjaként öt szolgáltatási életciklusszakaszt különböztet meg: szolgáltatásstratégia (service strategy); szolgáltatás tervezése (service design); szolgáltatás bevezetése (service transition); szolgáltatás üzemeltetése (service operation) szolgáltatás állandó fejlesztése (continual service improvement).

Ezek értelmezésére a következő rövid leírásokat adhatjuk.

Szolgáltatás stratégia: az ITIL szerint szolgáltatásokat üzleti szempontból kell megközelíteni. Ennek értelmében az üzlet az elsődleges, azaz az üzletet szolgálja ki az informatika, informatikai rendszer. A szolgáltatásstratégiának kell tartalmaznia, hogy a szervezet által kijelölt (üzleti) célokat hogyan lehet elérni. Továbbá fontos szerepet tölt be a szolgáltatásstratégia abban, hogyan lehet az üzleti stratégiát informatikai stratégiába átfordítani.

Szolgáltatás tervezése: az IT szolgáltatási megoldástervezés az IT policy és architektúra létrehozási és kezelési alapelveit tartalmazza. Ide tartozik például, hogy adott feladatok saját vagy külső erőforrásból (esetleg vegyesen), legyenek megvalósítva (például mi legyen kiszervezve).

Szolgáltatás bevezetése: a szolgáltatás bevezetése tartalmazza a hosszú távú változáskezelés és a verziókkal kapcsolatos gyakorlatot. Ezen túl fontos, hogy egy adott szolgáltatást le kell képezni egy konkrét üzleti (termelési) környezetbe.

Szolgáltatás üzemeltetése: nagyon leegyszerűsítve az IT-szolgáltatások biztosításával, azok stabilitásával foglalkozik. Többek között ennek a része az incidensmenedzsment is.

Szolgáltatás állandó fejlesztése: az üzleti szolgáltatás menedzsment fejlesztésével foglalkozik. Ezen kívül a bevezetett szolgáltatások tökéletesítésével.

A szolgáltatásüzemeltetés célja, hogy koordinálja és megvalósítsa azokat a tevékenységeket és folyamatokat, amelyek az üzleti felhasználók számára lehetővé teszik, hogy az elvárt szolgáltatási szintnek megfelelően igénybe vegyék az IT által nyújtott szolgáltatásokat.

A szolgáltatásüzemeltetés folyamatában megkülönböztetjük az eseménymenedzsmentet (event management), incidensmenedzsmentet (incident management), problémamenedzsmentet (problem management), szolgáltatási kérések teljesítését (request fulfilment), hozzáférés-menedzsmentet (access management).

A felsorolt folyamatok önmagukban persze nem feltétlenül jelentik egy szolgáltatás hatékony üzemeltetés, működését. A kellően stabil infrastruktúrára és képzett személyzetre is szükség van. A személyzet esetében különböző feladatokra különböző csoportokat definiál az ITIL.

Ezek mindegyike szükséges a megfelelő üzemeltetéséhez: ügyfélszolgálat (Service desk vagy Helpdesk); technikai menedzsment (Technical management); IT-műveletek menedzsmentje (IT operations management); alkalmazásmenedzsment (Application management).

A szolgáltatás üzemeltetésének ezen kívül kapcsolódnia kell a szolgáltatási életciklus más elemeihez, mint a változásmenedzsment (Change Management), illetve a kapacitás- és hozzáférés-menedzsment (Capacity and Availability management)

Mindezt azért definiáltuk, hogy megértsük azt az összetett logikát, ahogy az ITIL az esemény, incidens, probléma hármasságát kezeli.

A hétköznapi nyelvhasználatban ezen fogalmak gyakorlatilag szinonimaként vannak jelen. Fontos azonban megjegyezni, hogy az ITIL működésében ezek egymástól eltérő folyamatokat jelentenek, melyek szoros összefüggésben vannak egymással.

Az ITIL felfogásában informatikai szolgáltatás üzemeltetésre egyrészt tekinthetünk a szolgáltató (IT), másrészt pedig az ügyfél, azaz az igénybe vevő üzleti terület szempontjából. A két fél más-más szempontból közelíti meg a szolgáltatásüzemeltetést.

A szolgáltató szempontjából nézve ez egy olyan folyamat, amelynek célja, hogy a szolgáltatásmenedzsment-életciklus során az ügyfelét kiszolgálja úgy, hogy optimalizálja a költségeket és a szolgáltatási minőséget.

Az ügyfél számára a legkisebb ráfordítás mellet megvalósított lehető legmagasabb szintű igénykielégítés a célja.

Amennyiben a szolgáltatásnyújtás közben minőségi hiba történik, az kihatással van ezekre a célokra. Ilyenkor bekövetkezik egy úgynevezett *esemény,* amely tehát egy hatás (külső vagy belső), amely miatt a szolgáltatás minőségében változás történik.

Természetesen az informatikai szolgáltatásnyújtást is lehet monitorozni. Például, ha egy adott időpontban többen hívták az ügyfélszolgálatot, ezt hívjuk eseménynek, az ezen területtel foglalkozó feladatokat összefoglalóan pedig eseménymenedzsmentnek (event management).

Az események bekövetkezésekor a következő tevékenységek mennek végbe:

- Esemény észlelése. Cél, hogy észlelni tudjuk az eseményeket. Ezt szolgálja szolgáltatás monitorozása.
- Események csoportosítása. Fontos tudni, hogy nem minden eseményből lesz incidens vagy probléma. Egyes események csak informatív jellegűek, elegendő, ha tudunk róluk.
- Eseményt kiváltó okok vizsgálata.
- Események közti összefüggések vizsgálata.
- Intézkedés, válaszadás.

Az események hátterében gyakran valamilyen incidensek állnak. Az incidens az ITIL gondolatiságában lehet hiba, kérdés vagy új kérés is. Tehát fontos, hogy nem csak hibát soroljuk az incidensek közé ebben az értelmezésben. Az incidens azonnali beavatkozást igényel, mivel ebben az összefüggésben ez azt jelenti, hogy olyan mértékben megváltozott a szolgáltatás minősége, hogy azt a lehető

legrövidebb időn belül vissza kell állítani a korábbi szintre. Ez az incidensmenedzsment (incident management).

Amikor incidensmenedzsmentről beszélünk, a folyamatok már különböznek a korábban bemutatott eseménymenedzsmenthez képest:

- az incidens azonosítása;
- az incidens rögzítése írásban (hibajegy);
- osztályozás (hiba, kérdés, új kérés stb.);
- fontossági rangsorolás (normál, sürgős);
- előzetes diagnózis;
- feladatok kiosztása, eszkaláció;
- megoldás és lezárás;
- post-mortem analízis.

A *probléma* az incidens mögötti ok, amit egy incidensből közvetlenül nem is biztos, hogy ki lehet deríteni. A szolgáltatás nyújtása során fellép egy hiba, amelyet az ügyfélszolgálat meg is old, de ettől még nem tudják garantálni, hogy nem fog megismétlődni. Sőt, ha a hiba javítása az okának sikeres felderítése nélkül megtörténik, az nagy eséllyel meg tud ismétlődni. Egy adott probléma felderítéséhez ismerni kell a körülményeket, és közel sem biztos, hogy a probléma teljesen feltárható. A problémák feltárásának van egy további haszna is. Az eredményeként létrejön egy olyan adatbázis, amely az ismert hibákat tartalmazza. Ez segítséget nyújthat abban, hogy az incidensekre még gyorsabb választ tudjanak adni.

A fentieknek megfelelően tehát az incidensmenedzsment folyamata az összes incidenssel foglalkozik: hardver/szoftver hibák; az ügyfél kérdése/kérése; a technikai személyzet kérései, kérdései; az automatikusan érzékelt események, melyek az monitoring eszközökről érkeznek.

Fontos megérteni, hogy ebben az összefüggésben egy hardverelem meghibásodása akkor is incidensnek tekinthető, ha az nincsen hatással a szolgáltatásra.

Az ITIL tehát nagyon sok eseményt sorol az incidensek közé, amelyeket a „hétköznapi" értelemben nem tekintünk annak. Ezért fontos megjegyezni, hogy jelen jegyzet alapvetően nem az ITIL fogalommeghatározása szerint értelmezi az *incidenst*.

Az információbiztonsági incidensek olyan nem kívánt vagy nem várt egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik az üzleti tevékenységet, és fenyegetik az információbiztonságot.

Az ISO/IEC 27001 szabvány A) melléklete – mely a technikai kontrollokat tartalmazza – kiemelten foglalkozik az incidensekkel kapcsolatos tevékenységekkel. A célkitűzésével kapcsolatban úgy fogalmaz: biztosítani kell egy konzisztens és hatásos megközelítési módot az információbiztonsági incidensek kezelésére, beleértve a biztonsági események és gyengeségek kommunikációját is.

Mint azt korábban már taglaltuk, az ISO/IEC 27001 egy menedzsmentszabvány, így nem tartalmaz olyan konkrét elvárásokat, melyek megmondanák, hogy az incidenskezelést – vagy bármely más követelménynek való megfelelést – hogyan kell megvalósítani. Arra viszont kitér, hogy milyen szempontokat kell figyelembe venni egy incidenskezelési módszertan kialakításánál.

A főbb pontokat, melyekre elvárások találhatók a szabványban, most vesszük sorra.

Felelősségek és eljárások

Mint menedzsment szabvány, az elsődleges elvárás, hogy a szervezet alakítson ki olyan eljárásokat, amelyekben a folyamatok, tevékenységek és a felelősségek definiáltak arra az esetre vonatkozóan, ha információbiztonsági esemény következne be. Itt kell megjegyezni, hogy az *incidens* fogalmát az aktuális szabvány *információbiztonsági eseményként* nevezi meg.

Információbiztonsági események jelentése

Felismerve az incidenskezelés egyik kulcskérdését, a szabvány elvárja, hogy legyen kidolgozott folyamata a szervezetnek, melyben meghatározza, miként kerülnek az információbiztonsági események felismerésre, és hogyan jelzik a munkatársak, ha ilyet észlelnek.

Információbiztonsági gyengeségek jelentése

Tartalmában megegyezik az elvárás az események jelzésével, de egy olyan fogalomról rendelkezik itt, melyet az eddigiek során még nem említettünk. Többek között a szabványcsalád folyamatos fejlesztési logikája és a tudatosság, illetve a megelőzésre koncentrálás eredményeként azokról az „eseményekről" van itt szó, amelyek nem következtek be, de a rendszer vagy működés alapján potenciálisan incidensek forrásai lehetnek.

Értékelés és döntés az információbiztonsági eseményekről

Az események bejelentését követő folyamatokkal kapcsolatos elvárásokat definiál a szabvány. Az eseményekről megfelelően kialakított működés alapján kell döntéseket hozni, illetve ezek alapján kell a reagálni.

Válaszadás az információbiztonsági incidensekre

Továbbra is az egyetlen vezetővonal, hogy a szervezet kellően alapos működést dolgozzon ki az incidensekre adott válaszokhoz.

Tanulás az információbiztonsági incidensekből

Fontos eleme a menedzsmentszabványoknak, hogy az események, a begyűjtött adatok időről időre a fejlődést szolgálják. Így ez a szabvány itt is elvárja, hogy mind az információbiztonsági eseményekből, mind a gyengeségekből olyan fejlesztések szülessenek, amelyek túlmutatnak az adott incidens kezelésén, és a későbbi incidensek bekövetkezési valószínűségének csökkentése érdekében használják fel a megszerzett tapasztalatokat.

Bizonyítékok gyűjtése

Kettős célt szolgáló elvárás. Egyrészt a tényeken alapuló döntéshozatalt segítendő elvárja, hogy az incidensekről megfelelő bizonyítékokat gyűjtsenek be. Másrészt fontos szempont, hogy bármilyen későbbi jogi következményekhez álljanak rendelkezésre olyan bizonyítékok, melyek felhasználhatók egy jogi folyamat során.

3. Incidenskezelés a felhasználó szemszögéből

A biztonsági események kezelésének kulcsfontosságú momentuma a lehetséges problémák felismerése. Ezt számos esetben, például célzott támadásoknál műszaki eszközökkel nehezen és csak a

támadás egy viszonylag késői fázisában lehet megtenni. Célszerű ezért a szervezet munkavállalóival is megismertetni a fenyegetések felismerésének és jelentésének folyamatát. Jelen jegyzet célja bemutatni a felhasználók számára ezt. Ehhez azonban elsőként azt kell tisztázni, hogy a felhasználói oldalról nézve mit is kell *incidens* alatt érteni. Bár a korábbiakban több követelményrendszer is adott valamiféle megfogalmazást, a szervezet és a felhasználó viszonylatában ezt még nem – vagy legalábbis nem kellő összefoglaltsággal – tisztáztuk.

Ezek alapján próbáljuk meg egy rövid mondatba tömöríteni, hogy mit is értünk ez alatt. *Biztonsági esemény* minden esemény, mely a biztonságra nézve fenyegetés (lehet). Bár a megfogalmazás rövidségéből adódóan hagy kívánnivalót maga után, de könnyen megérthető és felhasználói oldalról talán a leginkább alkalmazható.

Miként is jelenhet meg ezek után a felhasználó életében a biztonsági esemény, vagyis az incidens? Erre nem lehet egyértelmű és minden potenciális esemény felölelő választ vagy felsorolást adni, hiszen egy szemetesbe dobott okirat ugyanúgy lehet incidens, mint egy hacker támadás. Minden esetben azt kell mérlegelnünk, hogy az adott történés ténylegesen vagy potenciálisan veszélyeztette-e a(z információ) biztonságot.

A legtöbb incidens forrásaként három fő csoportot tudunk meghatározni. Egyrész az incidensek bekövetkezhetnek valamilyen szabályozás nem megfelelő betartásából, másrészt valamilyen technikai gyengeségből vagy hibából, harmadrészt külső hatás eredményeként. Mint ahogy a jegyzet elején láthattuk, ezek felismerése és incidensként történő azonosítása minden esetben azt első lépés ahhoz, hogy megfelelő eljárással tudjuk kezelni őket.

Az incidensek felfedezésének a legmeghatározóbb eleme, ha ismerjük a működést mind annak szabályozását, mind pedig szokásos módját tekintve. Az iménti csoportosítást segítségül hívva, azt mondhatjuk, hogy első körben mindenképpen incidensre utal, ha valami a szabályozásoktól eltérőt észlelünk. Ez lehet egy beléptetési folyamat vagy egy nem a szabály szerint kért hozzáférés, vagy ha bárki olyan tevékenységre kér bennünket, amely a lefektetett szabályokkal ellentétes. Az ilyen tevékenységek önmagukban vagy valósan veszélyeztetik a biztonságot, vagy esélyt adnak a biztonság veszélyeztetésére, így mindenképpen úgy tekinthetünk rájuk, mint incidensekre. Bár nem lehet minden részletre kiterjedő listát felállítani, az incidensek jelentős része az adathordozók használatával, iratok átadásával vagy megsemmisítésivel, hálózati csatlakozásokkal kapcsolatos, illetve az adattárolásra, titkosításra vonatkozó szabályok megsértésével hozhatók összefüggésbe.

Incidensre gyanakodhatunk azokban az esetekben is, amikor egy tevékenységfolyamat hirtelen megváltozott, vagy az eddig megszokottakhoz képes érdemben gyorsabb, lassabb, egyszerűbb, bonyolultabb lett. A lényeg ilyen esetekben mindig, hogy a változás oka nem ismert. Nem arról van szó, hogy valamilyen fejlesztés eredményeként újabb szoftververziót használunk, aminek köszönhetően a rendszer terhelése megnőtt, hanem látszólag indokolatlan az eltérés az eddig megszokottaktól. Az ilyen incidensek felismerésének fontos része a tudatosság, az odafigyelés.

Szintén incidensre utalhat, ha olyan kommunikációt tapasztalunk, amely szokatlan vagy ismeretlen eredetű. Ez megvalósulhat akár elektronikusan, akár telefonon, de még személyesen is. Az ismeretlen feladótól, ismeretlen témában, látszólag ok nélkül érkezett levelek, üzenetek mindig fel kell keltsék a gyanút, különösen, ha ezek csatolmányokat vagy hivatkozásokat tartalmaznak, vagy olyan adatokra kérdeznek rá, melyek átruházása visszaélésre adhat lehetőséget (például jelszavak, bejelentkezési azonosítók, személyes adatok, bankkártya adatok stb.). Az ilyen információkérések ritkábban, de érkezhetnek telefonon, vagy akár személyesen. Gyakran a jóindulatunkat kihasználva segítségkérésnek álcázva.

Az incidensek kezelésének egyik legfontosabb tényezője, az időben történő reakció. Ahhoz, hogy egy szervezet kellő gyorsasággal tudjon reagálni, a legfontosabb, hogy időben értesüljön az incidensről, illetve, hogy a munkatársak a kompetenciáiknak megfelelően reagáljanak. Adott esetben próbálják, vagy ne próbálják meg az incidens elhárítását. Nyilvánvaló, hogy egy az iratmegsemmisítő helyett a kommunális kukába dobott irat esetében nincs szükség speciális tudásra, hogy az incidenst kezeljük. Egy informatikai rendszerben tapasztalt incidens (vagy annak gyanúja) esetén ez már nem

ennyire egyértelmű. Az ilyen esetekre vonatkozóan a legtöbb szervezet belső szabályozása azt mondja ki, hogy haladéktalanul értesíteni kell vagy egy definiált vezetőt vagy a biztonsági, illetve üzemeltetési szervezet munkatársát. Annyi kiegészítésre azért szorul az ilyen irányú gyakorlat, hogy ha egyértelműen azonosított, hogy az incidens a szakszerű segítség érkezéséig jelentős károkat okozhat, akkor célszerű lehet az alapvető beavatkozásokat elvégezni. Ez többnyire azt jelenti, hogy az eszközt a legalább szervezet hálózatáról érdemes lecsatlakoztatni. Jó tudni azonban, hogy azonnali lecsatlakozás a hálózatról általában jó ötlet, de egy célzott támadás esetén a támadó rájöhet, hogy felismerték a támadását, amelynek következtében azonnal tud reagálni, például a nyomainak eltüntetésével.

Az időnyomás hatása lehet, hogy az egyébként megfelelő tudással rendelkező kollégák, akiknek egyébként nem tartozik a munkaköréhez az incidensek kezelése, ilyen körülmények között nem a megfelelő döntéseket hozzák.

Az egész incidenskezelést értelmezzük olyan módon, mint amikor tüzet látunk. Elsőre el kell döntenünk, hogy az a tűz egy folyamat része (például kijelölt helyen, felügyelet mellett, bográcsalatt), vagy egy nem kívánt esemény. Ha ezt feltártuk, azt kell eldöntenünk, képesek vagyunk-e magunk megfékezni az akkor és ott rendelkezésre álló eszközeinkkel. Van-e nálunk a tűz méretének és fajtájának megfelelő oltóanyag abban a mennyiségben, amely elegendő a tűz eloltásához, vagy legalább a terjedésének megakadályozásához. Illetve kell-e, és ha igen, milyen segítség szükséges. Elegendő-e néhány velünk azonos tudással rendelkező ember, vagy hivatásos tűzoltókra van szükség. Ha a helyzet úgy kívánja, az oltás megkezdése, vagy épp a segítség kérése során azt is figyelembe kell venni, hogy egy szakszerűtlen oltással milyen további károkat okozhatunk, illetve, hogy a beavatkozásunk milyen mértékben nehezít(het)i majd meg a tűz keletkezésének okát vizsgálók munkáját.

Mint látható, ebben a folyamatban is igen sok helyen elbizonytalanodhatunk, hiszen, ha egy kijelölt helyen lobogó tüzet találunk, de körülötte nem látunk senkit, felmerül a kérdés, hogy ez most egy normál működés része vagy egy nem kívánt esemény. Ugyanígy egy lassú rendszerműködés lehet egy háttérben futó normál művelet eredménye, de utalhat incidensre is. Ha tovább nézzük a példát, olykor igencsak nehéz eldönteni, képesek vagyunk-e a tüzet megfékezni saját eszközeinkkel, vagy segítségre van szükségünk. Ugyanígy sokszor a tapasztalattal rendelkezők számára is kérdés lehet, hogy egy nem szokványos működést egy számítógép újraindítása megszűntet, vagy éppen ezzel okozzuk egy rosszindulatú kód további terjedését. A legjobb, amit ilyenkor tehetünk – mint ahogy a tűz oltásánál is –, hogy segítséget kérünk a probléma mértékének függvényében kellő gyorsasággal elérhető, megfelelő szakember(ek)től.

A szakszerű beavatkozás is jelentős hatással lehet egy szervezet működésére. Ennek szemléltetésére szolgál az alábbi szabályozás, mely egy valós szervezet információbiztonsági eljárásából kiemelt részlet, és jól szemlélteti, hogy akár a működés átmeneti kárára is szükséges lehet az incidensek tovább terjedésének megakadályozása.

„Az információbiztonság megsértése vagy veszélyeztetése esetén a további károk megelőzése, illetve elhárítása érdekében az informatikai rendszer üzemeltetéséért felelős munkatársak a szervezet feladata ellátásának számítógépes támogatását csökkenthetik vagy felfüggeszthetik azon eszközök leállításával, illetve rendszerből való kizárásával, amelyek az információbiztonság szempontjából sérültnek tekinthetők, illetve melyekkel szemben az információbiztonság szempontjából a bizalom megrendült.”

Az információbiztonsági incidensek olyan nem kívánt vagy nem várt egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik az üzleti tevékenységet, és fenyegetik az információbiztonságot.

Az informatikai rendszerekben a kapcsolódó adatokkal és eszközökkel való műveletek során előforduló incidensek fajtáinak feltárása, a körülmények tisztázása, az előfordulási gyakoriságok statisztikai elemzése, a felelősségi körök pontos tisztázása hozzájárul ahhoz, hogy a szervezet informatikai rendszerei minél magasabb szinten elláthassák alapvető feladataikat. Az előforduló incidensek elemzése, a rendszeres felülvizsgálatok és biztonsági elemzések lehetővé teszik, hogy az esetekből tanulva a rendszerek működése még biztonságosabb legyen.

Kiemelkedő jelentőségű, hogy az *incidens* (és ezen belül az *információbiztonsági incidens*) fogalma mindenki számára egyértelmű legyen. Mivel az incidensek igen sokfélék lehetnek, nézzünk néhány példát az információbiztonsági incidensekre, illetve arra, hogy ezeket a felhasználók miként azonosíthatják és kezelhetik.

- ***Szolgáltatás, berendezés vagy eszközök elvesztése.***
  A felhasználók ezt viszonylag könnyen tudják azonosítani, mivel valamilyen tevékenységükhöz szükséges rendszerelem – akár szoftveres, akár hardveres – nem áll a rendelkezésükre. Ilyenkor az incidensek elhárítása érdekében az egyetlen út a felhasználó számára a megfelelő szintű jelzés.
- ***A rendszer hibás működése vagy túlterhelések (DDos-támadás).***
  Hibás működés észlelése a felhasználó oldalon általában jól azonosítható, és incidensként könnyen jelezhető, ahogy a túlterhelés (illetve a túlterheléses támadás) azonosítása is. Ilyenkor azonban a felhasználó nem feltétlenül tud különbséget tenni egy szolgáltatás elvesztése, illetve túlterhelés miatti elérhetetlensége között. Az incidens kezelése itt is a megfelelő szintű eszkalációval valósítható meg.
- ***Emberi hibák.***
  Az emberi hibák sokfélesége miatt nem minden esetben egyértelmű, hogy ténylegesen incidensről van-e szó. A felhasználók általában az ilyen eredetű eseményeket csak késve jelzik, amelynek gyakran az is oka, hogy a hibát elkövető igyekszik az incidenst saját hatáskörében kezelni, s csak ennek sikertelensége esetén eszkalálja a megfelelő szintre.
- ***Szabályzatoknak vagy irányelveknek való nem megfelelés.***
  Az ilyen jellegű incidensek felismerése nagyban függ a szabályozások általános ismeretétől. Sok esetben nem önmagukban jelentenek kockázatot az információbiztonságra, hanem az eltérések következtében valamilyen más esemény bekövetkezésén keresztül. Az ilyen incidensek gyakran a felhasználók által kezelhetők, de ehhez megfelelő szintű tudatosság szükséges.
- ***Fizikai biztonsági rendelkezések megsértése.***
  Többnyire a belépési szabályok, illetve a biztonsági területeken tartózkodás szabályai sérülnek. Mind a felismerésben, mind a kezelésben nagyban hasonlítanak az előző pontban leírtakhoz.
- ***Szoftver vagy hardver hibás működése.***
  Alapesetben a felhasználó könnyen érzékeli, hogy a működés eltér a normálistól. Igazi kockázatot rejt azonban magában, hogy akár az incidens kezelésével is megpróbálkozik, amelyhez hiányzik a jogosultsága, illetve a megfelelő képzettsége, így az incidens kezelése során komolyabb problémákat is okozhat.
- ***Hozzáférési sértések.***
  A felhasználó – ha nem szándékosan követi el – gyakran észre sem veszi, hogy ilyen jellegű incidens történt. Gyakori, hogy csak utólagosan, a logokból, vagy más független eseményekből derül ki az esemény. Az ilyen helyzetek kezelése a felhasználó részéről csak az eszkaláció lehet.
- ***Rosszindulatú kód.***
  Minden technikai felkészültség ellenére még mindig gyakori ok az incidensek között, amelynek okai között gyakran a felhasználó nem kellően tudatos magatartása található. A jelzésen túl a felhasználók sikeresen tehetnek kísérletet az ilyen incidensek kezelésére, de a manapság terjedő vírusok esetében legalább a hálózatról történő leválasztás jelentősen csökkentheti az okozott kár nagyságát.

Az incidensek lehetnek véletlen események, illetve szándékos károkozás eredményei. Soha ne feledjük el, hogy az incidensek vélt forrása mögött sokkal súlyosabb szándék is meghúzódhat (például szándékos hackertámadás, vagy olyan esemény, mely átlépheti a szervezeti vagy akár a nemzeti határokat), ezért önkényesen soha ne kezdjük hozzá az incidens kezeléséhez vagy felfedéséhez, hanem csakis a szervezetnél kidolgozott módszertan szerint szabad eljárni.

Szabályalkotói oldalról ennek fontos elelme, hogy kellően részletes és általánosan ismertetett szabályozásokat dolgozzunk ki, amely alapján a felhasználók tisztában lehetnek az incidensek során tanúsítandó magatartással.

Szándékos vagy véletlen biztonsági incidensek bekövetkezhetnek alkalmazottak vagy a vállalaton kívül álló személyek cselekedeteinek hatására, informatikai eszközökben, hálózatokban és rendszerekben rejlő gyengeségek miatt, valamint harmadik fél által nyújtott szolgáltatások (elektromosság, telekommunikáció, külső beszállítók) kiesése esetén.

4. Biztonsági incidensek fokozatai

A szervezetnél előforduló biztonsági incidenseket célszerű súlyosságuk alapján besorolni. Minden szervezet a méretétől, az általa kezelt adatok mennyiségétől, érzékenységétől függően maga határozhatja meg, hogy a besorolás mennyi fokozatot tartalmazzon. Minél több fokozatot használ a szervezet, annál biztosabb ismeretek szükségesek a besoroláshoz, viszont annál pontosabban meg lehet határozni, és előzetesen ki lehet dolgozni a követendő magatartásokat. Egy átlagos szervezet számára jellemzően elegendő, ha két fokozatot különböztet meg. Lényeges követelmény, hogy a fokozatok definíciója egyértelmű, és a besorolást végzők számára könnyen érthető, illetve könnyen alkalmazható legyen. Nem szerencsés olyan besorolási kritériumok meghatározása, amelyek nem pontosak, illetve olyan, például számításos módszer kialakítása, amely a besorolást időigényessé teszi.

Súlyos biztonsági incidens

Minden olyan biztonsági esemény súlyosnak minősül, amelynek hatása és következményei, közvetlen vagy közvetett mértékben, jelentős mértékben megkárosíthatják a szervezetet, partnereit, ügyfeleit vagy az alkalmazottakat. Ennek értelmében jelentős biztonsági incidensnek minősülnek (például) a nagy mennyiségű vagy nagy értékű információk, informatikai felszerelések eltulajdonítása; az ügyfelek, partnerek vagy a szervezet tulajdonában lévő információk engedély nélküli kiadása, nyilvánosságra hozatala; sikeres számítógépes behatolási kísérlet (hackelés).

Azt, hogy egy szervezeten belül pontosan mi minősül súlyos biztonsági incidensnek, minden esetben a saját szabályozás határozza meg. Minden jelentős biztonsági incidenst azonnal jelenteni kell az incidens által érintett főosztály, osztály vagy osztályok vezetőjének, illetve a kijelölt illetékes(ek)nek.

Enyhébb fokozatú biztonsági incidens

Enyhe fokozatúnak minősül minden olyan biztonsági incidens, amelynek hatása a szervezetre és belső rendszereire korlátozódik, és a vizsgálat következményeként csak belső fegyelmi eljárás várható. Enyhe biztonsági incidens például a belső előírások, szabályzatok és eljárások gondatlanságból elkövetett megsértése.

Ezeket az eseteket gyakran a biztonsági incidens által érintett terület vagy területek vezetői vizsgálják ki, és saját hatáskörükben teszik meg a szükséges lépéseket.

5. Információbiztonsági incidensek kezelése

Mivel minden szervezet egyedi adottságokkal rendelkezik, nem lehet általánosan jó szabályozási mintát kialakítani. Azt azonban meg lehet határozni, hogy melyek a legfontosabb elemek, melyeket

célszerű a szabályozások részévé tenni. A következők az incidensek kezelésének főbb szabályai, melyek szinte minden szervezet szabályzatának alapját képezhetik.

Bármilyen biztonsági incidens észlelése esetén minden alkalmazottnak:

- azonnal jelentenie kell az incidenst közvetlen munkahelyi vezetőjének;
- biztosítania kell az incidens bekövetkezésének helyszínét;
- gondoskodnia kell a további károk bekövetkezésének megelőzéséről;
- gondoskodnia kell bármely (tárgyi vagy egyéb) bizonyíték megőrzéséről;
- a lehető leghamarabb írásban rögzítenie kell a biztonsági incidens bekövetkezésének körülményeit.

Az információbiztonsági incidensek kezelésének lépései:

1. az incidens okának elemzése és azonosítása;
2. behatárolás;
3. a szükséges, helyesbítő tevékenység tervezése és bevezetése az újbóli előfordulás megakadályozására;
4. adatközlés azoknak, akiket érint az incidens-helyreállítás, vagy abba be vannak vonva;
5. a tevékenység jelentése az illetékes testületnek.

Nulladik lépés

Mindenekelőtt szükséges az információs rendszerekhez kapcsolódó információbiztonsági események és gyenge pontok azonosítása, illetve közzététele, hogy lehetőség legyen helyesbítő tevékenységek időben való megtételére. Szükséges, hogy eseményjelentési és kiterjesztési eljárások álljanak rendelkezésre. Szükséges az információbiztonsági tudatosság oktatása egyaránt az alkalmazottak, illetve a szerződő partnerek, harmadik felek felé, melynek egyik pontja éppen az ilyen információbiztonsági események jelentésének kötelezettségét írja elő, illetve kijelöli, hogy mely vezetőt kell értesíteni az esemény bekövetkeztéről. A jelentéseket a lehető leggyorsabban kell közzétenni bármely információbiztonsági incidensről. A jelentő mechanizmus a lehető legkönnyebben, legjobban hozzáférhető és rendelkezésre állónak kell lennie. Tájékoztatni kell az érintett alkalmazottakat, szerződő partnereket, harmadik feleket, hogy semmilyen körülmények között ne kíséreljék meg ellenőrizni a gyanított gyenge pontot.

Hasznos segítség lehet a munkatársak számára összeállított rövid (maximum 1 oldalas) tájékoztató, hogy mit tegyenek olyan esetekben, ha incidenst észlelnek. Ilyenre jó példa a cert.hu által közzétett 9 lépéses segítség incidenskezelésre:

„Incidens kezelés

Lépésről lépésre

Ha incidenst észlelsz, és nem tudod, mit tegyél, kövesd ezeket a lépéseket!

1. lépés:	*Maradj nyugodt!* Még egy egészen apró kis incidens is mindenkit stresszes állapotba hoz. Ilyenkor a kommunikáció és az együttműködés nehézkessé válhat. De a nyugodtságod segít abban, hogy súlyos hibát ne kövess el. Különben is, a legtöbb incidens nem olyan, mint amilyennek első látásra tűnik.
2. lépés:	*Vedd elő a jegyzeteidet!* Vegyél elő kézikönyvet! Nyisd ki az incidensek azonosításánál! Ezek után gondold végig a lényeges tennivalókat. Miközben ezt teszed, ne felejtkezz meg arról sem, hogy a feljegyzéseid bizonyítékként is szolgálhatnak. Válaszolj a négy kérdésre: ki, mit, mikor, hol és a további kettőre: miért és hogyan! Egy kis magnetofon hasznos lehet.

3. lépés:	*Értesítsd a megfelelő embereket* és kérj segítséget! Szólj a biztonsági felelősnek és a főnöködnek! Kérd meg a munkatársaidat, hogy segítsenek az incidenskezelés folyamatában! Kérd meg a kollégáidat, hogy készítsenek pontos feljegyzést arról, hogy kivel beszélgetettek és partnereik mit mondtak! Ellenőrizd, hogy valóban azt teszik-e!
4. lépés:	Juttasd érvényre azt az elvet, hogy *„csak az tudjon az incidensről, akinek tudnia kell”*. A lehető legkevesebb embert szólj az esetről. Emlékeztesd kollégáidat, hogy őket megbízhatóknak tartod, és ezért számítasz a diszkréciójukra. Kerüld a spekulációkat, kivéve, ha éppen döntened kell, hogy mit tegyél. Nagyon gyakori, hogy az incidensről szóló kezdeti információ megtévesztő, és a kidolgozott munkatervedet menetközben el kell dobnod.
5. lépés:	*Használj független kommunikációs eszközt!* Ha a számítógépeket érte az incidens, akkor az incidenskezelés során kerüld azt! Inkább telefont vagy faxot használj! Ne küldj az incidensről semmilyen információt elektronikus levélben, talk vagy chat formában, vagy news-on keresztül: az üzenetet a támadó elfoghatja és akár a helyzetedet is tovább ronthatja. Ha mégis számítógépet használsz, kódolj minden elektronikus levelet!
6. lépés:	*Elemezd a helyzetet!* Tedd meg a szükséges lépéseket, nehogy a probléma súlyosabbá váljon! Általában ez azt jelenti, hogy a rendszert húzd le a hálózatról, bár a vezetőséggel való egyeztetés után az a döntés is születhet, hogy maradjon meg a kapcsolat, hogy a támadót elfoghassátok.
7. lépés:	*Azonnal készíts másolatot az érintett rendszerről,* ha úgy véled, hogy incidens történt. Új médiát használj! Ha lehet, bináris vagy „bitről bitre” másolatot készíts.
8. lépés:	*Véglegesen old meg a problémát!* Azonosítsd, mi ment tönkre, ha tudod. Javítsd ki azokat a hibákat, ami lehetővé tette az incidens bekövetkeztét.
9. lépés:	*Állítsd vissza a normális menetet!* Miután ellenőrizted, hogy a korábbi mentésed még ép, incidens nyomai azon még nincsenek, állítsd vissza erről a rendszert és figyeld, hogy helyesen működik-e. Tanulj a tapasztalatokból, hogy legközelebb n(s)e érjen felkészületlenül az incidens.”

Elérhetőség: www.cert.hu/sites/default/files/incidens_kezeles_refcard.pdf
(utolsó letöltés: 2017. május 2.)

Jelzési eljárások

A jelzési eljárások magukba kell foglalják a következőket:

- alkalmas visszajelzési folyamatok, biztosítva, hogy azok, akik jelentést adnak az információbiztonsági eseményekről, értesítve legyenek az eredményekről, miután a kérdéssel foglalkoztak, és azt lezárták;
- az információbiztonsági eseményt jelentő „formanyomtatványok”, segítik a jelentési tevékenységet és a jelentő személyt, hogy emlékezzék az összes szükséges tevékenységre egy információbiztonsági esemény esetén;
- a helyes viselkedés, amelyet egy információbiztonsági esemény esetén tanúsítani kell, azaz:
    - minden lényeges részlet azonnali feljegyzése (például a nemmegfelelőség vagy sértés fajtája, az előforduló helytelen működés, üzenet a képernyőn, különleges viselkedés),
    - nem hajtanak végre semmilyen saját tevékenységet, hanem azonnal jelentenek a kapcsolati helynek;
- utalás egy kidolgozott, hivatalos fegyelmi folyamatra, amely olyan alkalmazottakkal, szerződő felekkel és használó harmadik féllel foglalkozik, akik biztonsági sértést követnek el.

Hibás működés vagy más rendellenes rendszerviselkedés jele lehet egy biztonsági támadásnak vagy tényleges biztonsági sértésnek, ezért mindig információbiztonsági eseményként kell jelenteni.

Nagy kockázatú környezetben kényszervészjelzést lehet alkalmazni, ezáltal egy kényszer alatt álló személy jelezhet ilyen problémákat (például banki betörés során). A kényszervészjelzésekre válaszoló eljárások tükrözzék azt a nagy kockázatú helyzetet, amelyet az ilyen vészjelek mutatnak.

Biztonsági incidensek kivizsgálása

A biztonsági incidensekkel kapcsolatos vizsgálatok információit és eredményeit bizalmasan kell kezelni, azokról csak a szükséges mértékben lehet tájékoztatást nyújtani.

A biztonsági incidensek kivizsgálása esetén a következő területeket kell vizsgálni:

- a biztonsági incidens típusa, súlyossága, következményei *(Mi történt? Mik a következmények?);*
- az incidens bekövetkezésének közvetett és közvetlen okai *(Miért történt?);*
- az incidens bekövetkezésének körülményei *(Hogyan történt?);*
- a további károk keletkezésének megakadályozása és kezdeti felszámolásuk megkönnyítése érdekében szükséges teendők;
- hasonló biztonsági incidensek bekövetkezésének hosszabb távú megelőzése érdekében szükséges intézkedések;
- az esetleges felelősök, illetve a személyi felelősségre vonás szükségességének meghatározása.

A vizsgálat folyamán szükséges lehet audit információk és hasonló bizonyítékok begyűjtésére, amelyek:

- lehetővé teszik a belső problémaelemzést;
- szerződésszegéssel, vagy jogszabálysértéssel kapcsolatos eljárásokban bizonyítékként felhasználhatók;
- az informatikai eszközök, szoftverek beszállítóival, külső szolgáltatókkal folytatott kártérítési tárgyalásokban felhasználhatók;
- adatvédelmi, vagy számítógéppel elkövetett visszaélésekről szóló jogszabályok hatálya eső jogi eljárásban bizonyítékként felhasználhatók.

Ilyen jellegű információk, tárgyi bizonyítékok begyűjtésével kapcsolatban a területért vagy az információbiztonságért felelős vezető nyújt felvilágosítást.

6. Biztonsági incidensek nyilvántartása

A biztonsági incidensek kivizsgálásáról, a vizsgálat eredményéről minden esetben jelentést kell készíteni, és ezt a dokumentumot a biztonsági incidensek nyilvántartásában kell őrizni. Minden jelentés bizalmas (vagy ennek megfelelő) minősítésű dokumentum, és ennek megfelelően kell kezelni.

Súlyos biztonsági incidens esetén célszerű, ha a jelentést az információbiztonságért felelős vezető készíti, akit a vizsgálat folyamatáról és eredményeiről teljes mértékben informálni kell.

A biztonsági incidens észlelése során megállapítják az incidens típusát; azt, hogy ki és mikor jelentette az incidens észlelését; kit és mikor értesítettek az incidensről; illetve kinek és mikor továbbították az incidens tényét (illetve annak kezelését).

Az incidens kivizsgálása érinti a vizsgálat során végrehajtott műveletek, cselekedetek részletei, a végrehajtók személye, a végrehajtás ideje, valamint az eredmények.

Az incidens következményeinek felszámolása során definiálódnak a következmények behatárolása, újabb károk keletkezésének megakadályozása érdekében tett rendkívüli és szükségintézkedések részletei; a biztonsági incidens következményeinek felszámolása, újabb incidensek bekövetkezésének megelőzése érdekében elfogadott, állandó jellegű intézkedések és megoldások részletei.

Az incidenssel kapcsolatos felelősségre vonás a személyi felelősségre vonással járó intézkedések részleteit jelenti.

Az elemzés kiterjedhet az incidens anyagi és eszmei következményeire, a biztonsági incidensből és felszámolásából eredő költségekkel együtt.

Kellően fejlett informatikai háttérrel és tudatos működéssel rendelkező szervezetek az incidenskezelés teljes folyamatát támogathatják akár erre a célra kifejlesztett szoftverekkel. Ezek nagy előnye, hogy a teljes folyamatot képesek lehetnek kezelni, az első bejelentéstől a lezárást követő statisztikák elkészítéséig. Az ilyen szoftverek alkalmazása ott ajánlott különösen, ahol a jelentős mértékű a kiszervezés, így az incidensek kivizsgálása külső feleket is érint, illetve adott esetben az ő feladatuk.

Összegzésképp elmondható, hogy legyenek kész mechanizmusok, hogy lehetővé tegyék az információbiztonsági incidensek fajtái, mennyiségei és költségei számszerűsítését és figyelemmel kísérését, a kinyert információt használják fel, hogy azonosítsák az ismétlődő vagy nagy hatású incidenseket.

Az információbiztonsági incidensek kiértékelése jelezheti az igényt a fokozott vagy kiegészítő ellenőrzésekre, hogy korlátozzák a jövőbeli előfordulások gyakoriságát, a belőle származó kárt és költséget, vagy amelyeket számításba kell venni a biztonsági szabályozások átvizsgálási folyamatában.

A titoktartási szempontokra megfelelően gondolva, az információbiztonsági incidensek felhasználhatók a munkatársak tudatossági oktatásában példaként, hogy mi történhet, hogyan válaszoljanak az ilyen incidensekre, és hogyan kerüljék el azokat a jövőben.

Szükséges lehet, hogy képesek legyenek az információbiztonsági események és incidensek megfelelő kezelésére, hogy bizonyítékot gyűjtsenek az előfordulás után, amint csak lehet.

5. táblázat: Jellemző szerepek, felelősségek

Szerepek:	Felelősségek:	Idő tényezők:
Minden munkatárs	A tudomására jutott ténylegesen bekövetkezett vagy feltételezett biztonsági incidensek jelzése a közvetlen vezetőnek, illetve a kijelölt munkatársnak/vezetőnek.	Azonnal
Területi vezetők	• A tudomásukra jutott tényleges, vagy feltételezett súlyos biztonsági incidenseket közvetlen vezetőjének, illetve az információbiztonságért felelős vezetőnek azonnal jelenteni. • Az enyhébb biztonsági incidenseket kivizsgálni, az incidens következményeit megfelelően kezelni, és amennyiben lehetséges, felszámolni. • A vizsgálat eredményeit és az incidensről összegyűjtött információkat az információbiztonságért felelős vezetőnek továbbítani. • Közreműködni a biztonsági incidensek következményeinek felmérésében és felszámolásában.	Azonnal
Információbiztonsági felelős	• A területi vezetők által jelzett, vagy közvetlenül felmerülő súlyos biztonsági incidensek hatásainak, következményeinek felmérése. • További károk keletkezésének megakadályozása. • A következmények felszámolásának megszervezése. • A megfelelő szintek tájékoztatása.	Azonnal, illetve a lehető legrövidebb időn belül
Információbiztonsági felelős	• Nyilvántartást vezet minden biztonsági incidensről. • Segítséget nyújt az egyes vezetőknek a bekövetkezett biztonsági incidensek kivizsgálásában, illetve a szükséges teendők, megoldások meghatározásában. • A vezetés tájékoztatása minden biztonsági incidensről, a vizsgálat folyamatáról és eredményeiről. • Éves jelentés elkészítése a szervezetet érintő biztonsági incidensekről.	Rendszeresen

Forrás: A szerző saját szerkesztése

7. Jogszabálytár

- A jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről szóló 23/2013. (XI. 6.) MNB rendelet
  www.mnb.hu/letoltes/23-2013-xi-6-mnbrendelet.pdf
- Az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet
  https://net.jogtar.hu/jogszabaly?docid=a1800271.kor
- A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. tv.
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv
- A Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 16/2013. (VIII. 30.) HM rendelet
  http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/9.pdf[186]
- A Magyar Köztársaság Kormánya és a Németországi Szövetségi Köztársaság Kormánya között Budapesten, 1989. december 18-án aláírt légiközlekedési egyezmény kihirdetéséről szóló 86/1997. (V. 28.) Kormányrendelet
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99700086.KOR
- A minősített adat védelméről szóló 2009. évi CLV. törvény
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131
- Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 187/2015. (VII. 13.) Korm. rendelet
  https://net.jogtar.hu/jogszabaly?docid=a1500187.kor[187]
- A pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Kormányrendelet módosításáról szóló 157/2016. (VI. 13.) Kormányrendelet
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- A pénzügyi intézmények, a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről 535/2013. (XII. 30.) Kormányrendelet
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300535.KOR&txtreferer=A1300235.TV
- Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Kormányrendelet
  https://net.jogtar.hu/jogszabaly?docid=a1600451.kor
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158
- Az elektronikus hírközlésről szóló 2003. évi C. törvény
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV
- Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Kormányrendelet
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR

[186] Hatályos: 2015. július 15-ig
[187] Letöltve: 2022.02.14.

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
- Az állami szervek informatikai fejlesztéseinek koordinációjáról szóló 228/2016. (VII. 29.) Kormányrendelet
  https://net.jogtar.hu/jogszabaly?docid=A1600228.KOR&timeshift=20170102&txtreferer=A1500222.TV
- Az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló 42/2015. (VII. 15.) BM rendelet
  https://net.jogtar.hu/jogszabaly?docid=A1500042.BM&txtreferer=A1500041.BM
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 95/46/EK irányelv
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU
- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU
- Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU
- Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Kormányhatározat
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845
- Az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet
  https://net.jogtar.hu/jogszabaly?docid=A1800271.KOR

FOGALOMTÁR

Fogalom	Definíció
(FIRST) CSIRT	Forum of Incident response and Security teams Számítógép biztonsági incidenskezelő csoport – Computer Security Incident Response Team.
(TI) CSIRT	Trusted Introducer Számítógép biztonsági incidens kezelő csoport – Computer Security Incident Response Team.
ACPI	Advanced Configuration and Power Interface, az APM felváltására készült energiagazdálkodási rendszer. Az utóbbival ellentétben nem a BIOS irányítja a folyamatokat, hanem az operációs rendszer.
ACT	Allied Command Transformation – Szövetséges Transzformációs Parancsnokság.
adatbiztonság	Az adatok fizikai biztonságát szolgáló eljárások.
adatvédelem	A személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.
adatvédelmi incidens	Az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
advise	Tanácsadás.
AMT	Intel – Active Management Technology.
APWG	Anti Phishing Working Group.
ASF	Advanced Streaming Format – a Microsoft által szabadalmazott digitális audio/digitális videó csomagoló (konténer), amit különösen a média folyamok továbbítására szántak.
ATP	Advanced Persistent Threat: fejlett támadás.
BAH	Booz-Allen Hamilton.
bejelentés (logging)	A hívást és a hibakezelő rendszerben való rögzítést is jelenti, és nem különböztetik meg a felhasználókat.
BfV	A német Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz).
bizalmasság	Az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.
biztonsági esemény	Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
biztonsági esemény kezelése	Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

Fogalom	Definíció
biztonságmenedzsment információs rendszere (security management information system):	Azon segédeszközök, adatok és információk összessége, amelyet az információbiztonság-menedzsment támogatására használnak.
CA	Certification Authority – hitelesítésszolgáltató.
CC	Common Criteria – Közös Követelmények.
CCD CoE	Cooperative Cyber Defence Centre of Excellence – 1.2.8 KOOPERATÍV KIBERVÉDELMI KIVÁLÓSÁGI KÖZPONT.
CDMA	Cyber Defence Management Authority.
CDMB	Cyber Defence Management Board.
CECSP	közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform).
CERT	számítógép vészhelyzet kezelő csoport – Computer Emergency Response Team.
CERT/CC	számítógép vészhelyzet kezelő csoport /koordinációs központ – Computer Emergency Response Team/ Coordination Center.
CERT/CC	CERT Competence Center.
CFIA	Component Failure Impact Analysis.
címtár	Azonosítja és hitelesíti a szervezet felhasználóit meghatározva alapvető jogosultságukat, a felhasználók és munkaállomások tevékenysége központilag korlátozható, a biztonsági házirendek központilag definiálhatók.
CIP CSIRT	Kritikus infrastruktúra védelméért felelős.
CIS	Center of Internet Security.
CMS	Content Management System.
COBIT	Control Objectives for Information and Related Technologies.
COBIT	Control Objectives for IT and Related Technology.
Code of Practice	Magatartási kódex.
cookie	Egy információcsomag, amelyet a szerver küld a böngészőnek, majd a böngésző vissza-küld a szervernek minden, a szerver felé irányított kérés alkalmával. Segíti a böngészést, biztonsági kockázata is van.
COSI	Európai Unió Belső Biztonsági Állandó Bizottsága.
CRAMM	Risk Analysis and Management Method.
CVSS	Common Vulnerability Scoring System.
cyberbullying	Elektronikus zaklatás.
CSA	Cloud Security Alliance.
CSIRT	Számítógép-biztonsági incidenskezelő csoport – Computer Security Incident Response Team.
CSIS	Stratégiai és Nemzetközi Tanulmányok Központ (Center for Strategic and International Studies).
DDoS	Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás.
dead analízis	A lefoglalt anyagokat (disk image, memória image, számítógép) analizál.

Fogalom	Definíció
DENSEK projekt	Distributed Energy Security Knowledge.
disaster recovery site	Egy olyan része az informatikai rendszernek, mely attól fizikailag elkülönülő helyen üzemel, az éles rendszer minden elemét és adatát tartalmazza.
DLP	Adatszivárgást megelőz eszköz.
DMZ	A demilitarizált zóna a hálózat egy olyan része, melyet mind az internet irányából, mind pedig a munkahelyi hálózatról csak speciális tűzfalszabályokon keresztül érhető el.
DNS szerver	Domain Name System.
DoD	Department of Defense.
DoS	Denial of Service – szolgáltatás megtagadással járó támadás.
dump file	Egy pillanatfelvétel az alkalmazásról.
EC3	European Cybercrime Centre – 1.2.7.1 EUROPOL-SZÁMÍTÁSTECHNIKAI BŰNÖZÉS ELLENI KÖZPONT.
EDR	Endpoint Detection and Response.
EE-ISAC	European Energy – Information Sharing Analysis Centre.
EMPACT Program	Európai Multidiszciplináris Platform a bűnügyi fenyegetés ellen – European Multidisciplinary Platform against Criminal Threats.
ENISA	Európai Uniós Hálózat- és Információbiztonsági Ügynökség – European Union Agency for Network and Information Security.
eredendő ok (root cause)	Egy incidens vagy probléma mögöttes vagy eredeti oka.
esemény (event)	Olyan állapotváltozás, amelynek jelentősége van egy konfigurációs elemben vagy az IT-szolgáltatás menedzsmentjében.
észlelés (detection)	A kiterjesztett incidens-életciklus egy szakasza. A biztonsági esemény bekövetkezésének felismerése.
európai digitális menetrend	Célja a digitális technológia előnyei az európai polgárok és vállalkozások számára minél szélesebb körben elérhetőek legyenek.
EUROPOL	Európai Rendőrségi Hivatal.
failover	Az eszközöknek egy olyan felhasználása, amikor az informatikai rendszer azonos funkciójú elemeiből két vagy több példány folyamatosan működik a rendszerben, de egy időben mindig csak egy érhető el belőle.
FAIR	Fejlesztéspolitikai Adatbázis és Információs Rendszer.
FancyBear	Hacker csoport.
FI-ISAC	European Financial Institutes – Information Sharing and Analysis Centre.
forensics	A bizonyítékokat olyan minőségben, és azoknak az alapelveknek a betartásával gyűjtsük össze és analizáljuk, amik garantálják, hogy akár egy bírósági tárgyaláson is elfogadhatók lesznek.
forrótartalék (hot start, hot standby)	Olyan létesítmény, amelyben az eszközök azonnal képesek a szoftverek, archivált adatot feltöltésére és futtatására.
FTA	Fault Tree Analysis – Hibafaelemzés.
FTK	The Forensic Toolkit képes többek között disk, és memória imagelésre is.

Fogalom	Definíció
GAO	U.S. Government Accountability Office.
GDPR	Európai Unió Általános Adatvédelmi Rendelete – General Data Protection Regulation.
GovCERT	Kormányzati Eseménykezelő Központ.
GPT	Guid Partition Table – partíció eloszlás táblázat.
hálózati szegmentáció	A különböző funkciójú infrastruktúra elemeket egymástól hálózati eszközök segítségével elválasztják.
hash függvény	Olyan informatikában használt eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le.
hiba (error/fault)	Tervezési hiányosság vagy helytelen működés, amely meghibásodást okoz egy vagy több konfigurációelemben vagy IT-szolgáltatásban.
hidegtartalék (cold start, cold standby)	Olyan hordozható vagy helyhez kötött létesítmény, amelyben alap infrastruktúrával (kábelezés, áramellátás) rendelkező számítógép központ van.
hívás (call)	Telefonhívás a felhasználótól az ügyfélszolgálatra.
HSAC	Homeland Security Advisory Council – Belbiztonsági tanácsadó testület (USA).
Hun-CERT	Két önkéntes alapon működő CSIRT.
Iaas	Azonnal elérhető számítási infrastruktúra.
IBSZ	Informatikai biztonsági szabályzat.
IDC	International Data Corporation.
IDF	Behatolás detektáló rendszer.
incidens	Egy IT-szolgáltatás be nem tervezett megszakadása, vagy az IT szolgáltatás minőségének csökkenése.
információbizton-ság-menedzsment (information security management)	Ez a folyamat felelős azért, hogy egy szervezet eszközeinek, információinak, adatainak és IT-szolgáltatásainak bizalmassága, integritása, és rendelkezésre állása megfeleljen a megállapodott üzleti igényeknek.
IoC	Indicator of Compromise.
IPS	Behatolás megelőző rendszer.
IPS/IDS rendszer	A külső támadások elleni védelem eszközei, a forgalom folyamatos elemzését végzik, és szükség esetén riasztanak képesek az adott folyamatot letiltani.
IRT	Incidenskezelő csapat.
ISACA	Információrendszer-menedzserek és ellenőrök nemzetközi szakmai szervezete.
ismert hiba (known error)	Olyan probléma, amelynek van dokumentált eredendő oka és megkerülő megoldása.
ITGI	IT Governance Institute.
ITIL	Nemzetközi szabvány – informatikai rendszerek üzemeltetésére és fejlesztésére vonatkozó ajánlás, módszertan.
ITIL	Information Technology Infrastructure Library.
ITILv3	legfrissebb szabvány verzió.
IWWN	nemzetközi kiberbiztonsági fórum.

Fogalom	Definíció
katasztrófa (disaster)	Olyan hirtelen, nem tervezett, szerencsétlen esemény, amely jelentős kárt vagy veszteséget okoz.
Katasztrófa-elhárítási Terv (Disaster Recovery Plan – DRP)	Azoknak az eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes a káresemények következtében kiesett szolgáltatásait a normál működési szintre visszaállítani.
KEF	Közbeszerzési és Ellátási Főigazgatóság.
kibertér	A számítógéprendszerek és -hálózatok által alkotott metaforikus tér, amelyben elektronikus adatok tárolódnak és online adatforgalom, valamint kommunikáció zajlik.
KNBSZ	Katonai Nemzetbiztonsági Szolgálat.
különleges személyes adat	A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
live analízis	A futó számítógépet vizsgáljuk meg.
LMS	Learning Management System.
load ballancing	Az eszközöknek egy olyan felhasználása, amikor az informatikai rendszer azonos funkciójú elemeiből két vagy több példány folyamatosan működik a rendszerben, és folyamatosan elérhetők a felhasználók számára.
LRLIBEK	Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ.
malware	Rosszindulatú program.
meghibásodás (failure)	Annak a képességnek az elvesztése, hogy előírás szerint működjön, vagy a kívánt eredmény előálljon.
megkerülő megoldás (workaround)	Olyan incidens vagy probléma hatásának csökkentése vagy kiküszöbölése, amelyre teljes megoldás még nincs (például egy meghibásodott konfigurációelem újraindítása).
megoldás (resolution)	Intézkedés egy incidens vagy probléma eredendő okának kijavítására vagy egy megkerülő megoldás megvalósítására.
Microsoft Event log	Microsoft naplózási protokoll.
MILCERT	Honvédelmi/katonai CERT.
minőség (quality)	Egy termék, szolgáltatás vagy folyamat képessége arra vonatkozóan, hogy a tervezett értéket nyújtsa (például egy hardverkomponenst jó minőségűnek kell tekinteni, ha az elvárások szerint működik, és nyújtja az elvárt megbízhatóságot).
MOF	Microsoft Operations Framework.
MTA SZTAKI	Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézet.
Működésfolytonossági Terv (MFT), (Business Continiuty Plan – BCP)	Azoknak az információknak és eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes váratlan káreseményekre hatékonyan reagálni, és a kritikus üzleti folyamatait egy elfogadható szinten fenntartani. MFT-nek nevezik azt a keretrendszert, amely átfogja a működésfolytonosság tervezési, megvalósítási és ellenőrzési fázisait.
NAC	Network Access Control – Hálózati hozzáférés felügyelet.
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság.

Fogalom	Definíció
NCSC	Nemzeti Kiberbiztonsági Központok – National cyber Security Center.
NEIH	Nemzeti Elektronikus Információbiztonsági Hatóságra.
nemzeti adatvagyon	A közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.
NIIF-CSIRT	Nemzeti Információs Infrastruktúra Fejlesztés.
NIIFI-CSIRT	két önkéntes alapon működő CSIRT.
NIST	Nemzeti Szabvány és Technológiai Intézete – National Institute of Standards and Technology.
NKI	Nemzeti Kibervédelmi Intézet.
NMHH	Nemzeti Média- és Hírközlési Hatóságon.
NMHH-OIHF	Országos Informatikai és Hírközlési Főügyelettel.
NMSDB	Network Management System Database.
nulladik napi fenyegetés	Egy biztonsági fenyegetés, ami valamely számítógépes alkalmazás olyan sebezhetőségét használja ki, ami még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el azt foltozó biztonsági javítás.
OECD	Gazdasági Együttműködési és Fejlesztési Szervezet.
ORFK NEBEK	Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központ.
OSCE	Organization for Security and Co-operation in Europe – Európai Biztonsági és Együttműködési Szervezet (EBESZ).
PaaS	Azonnal elérhető platform.
PDCA elv	Plan – Do – Check – Act = Tervezés – Végrehajtás – Ellenőrzés – Beavatkozás.
PKI	Public key infrastructure – közösségi kulcs infrastruktúra.
PreDeCo elv	Preventive – Detective – Corrective = Megelőzés – felderítés – korrigálás.
Problémamenedzsment (Problem Management)	A szolgáltatás üzemképtelenségének minimalizálása a fő célja.
proxy	Helyettesítő/kiváltó.
ransomware	Zsarolóvírus.
rendelkezésre állás	Az elektronikus információs rendszerek az arra jogosult személy számára elérhetők, és az abban kezelt adatok felhasználhatók.
reporting	Gyakorlatok megosztása.
rootkit	Olyan szoftvereszközök, amelyek segítségével egy cracker könnyen visszatérhet a „tett színhelyére”, ha már korábban beférkőzött a rendszerbe, hogy bizalmas adatokat gyűjtsön a fertőzött számítógépről.
SaaS	Azonnal elérhető szoftver.
sandbox	Olyan ellenőrzött – valós világhoz közeli – informatikai környezet, ahol megfigyelhető egy állomány futtatása során annak tevékenysége úgy, hogy az ne jelentsen veszélyt a teljes informatikai rendszerre.
SECaaS	Azonnal elérhető biztonsági szolgáltatás.
SEM	Security Event Management – Biztonsági eseménykezelő

Fogalom	Definíció
SERT	Security Emergency Response Team – Sörgosségi regáló biztonsági csapat
sértetlenség	Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles és származása ellenőrizhető.
SIEM	Security Information and Event Management – Biztonsági információ és eseménykezelő csoport.
SIM	Security Information Management – Biztonsági információ kezelés.
SLA	Service Level Agreement – Szolgáltatási szint megállapodás.
SNMP	Simple Network Management Protocol – Egyszerű hálózatkezelő protokoll.
SOA	Szolgáltatásorientált architektúra (Service Oriented Architecture).
SOAR	Biztonsági eseménykezelő rendszer.
SOC	Biztonsági Üzemeltetési Központok – Secrity Operation központok.
social engineering	Támadási forma, ahol a hozzáféréssel rendelkezőket zsarolják vagy befolyásolják, esetleg bizalmukba férkőzve kihasználják hiszékenységüket.
SSO	Single Sign-On – egyszeri bejelentkezési módszer.
Stuxnet	Annak a rosszindulatú programnak a neve, amelyet célzottan csak az iráni urándúsító létesítmény ellen terveztek, és amely csak azt támadta meg, annak ellenére, hogy több százezer számítógépen is megtalálták később.
SWOT analízis	A stratégiaalkotás folyamatának egyik lépése. Strengths – erősségek; Weaknesses – gyengeségek; Opportunities – lehetőségek; Threats – veszélyek.
SYN Flood	Elárasztásos támadás.
syslog	Linux naplózási protokoll.
szolgáltatás helyreállítása (Restoration of Service)	Intézkedés egy IT-szolgáltatás javítás és visszaállítás utáni visszaadásáról a felhasználóknak.
szolgáltatásstratégia (Service Strategy)	A folyamat azonosítja azokat a piaci lehetőségeket, amelyeket új szolgáltatások bevezetésével ki lehetne aknázni.
Szolgáltatástervezés (Service Design)	A folyamat eredményeként projektterv készül az előző lépésben keletkezett stratégia által felvázolt szolgáltatás konkrét megvalósítására.
TARANSITS	Egy európai projekt, amelynek célja az új CSIRT-ek létrehozásának és a már működő CSIRT-ek bővítésének, fejlesztésének támogatása speciális tanfolyamok által.
TCO	Total Cost of Ownership –Teljes Bekerülési Érték
TI	Fenyegetettségi információ szolgáltatást.
Tivoli Security Policy Manager	Leválasztja a biztonsági irányelveket az alkalmazásokról, lehetővé téve az alkalmazásjogosítványok központosítását és leegyszerűsítését, valamint az adathozzáférés részletes szabályozását.
TPM	Trusted Platform Module.
Tűzfal	A külső támadások ellen védik a szervezeti infrastruktúra elemeit.
üzleti hatáselemzés (Business Impact Analysis – BIA)	Eljárás, amely során a szervezet meghatározza a kritikus üzleti folyamatok megszakadásának következményeit és a normál működési állapotra való visszaállás elvárásait.

Fogalom	Definíció
Üzletmenet-folyto-nosság menedzsment (Business Continuity Management – BCM)	Az a folyamat, melynek során egy szervezet felkészül a kritikus üzleti folyamatok megszakadására, vagy kiesése esetén a folyamatok visszaállítására.
vis major	Váratlan, nem befolyásolható esemény.
volatility	Változékonyság.
volatility	Memória dump analizáló eszköz.
VPN	Virtual private network – virtuális magánhálózat.
warning	Riasztás.
WARP	Warning, Advise and Reporting Points.
WBEM	Web-Based Enterprise Management.
WMI	Windows Management Interface.
worm attack	Féregtámadás.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

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

Kiadói szerkesztő:
Császár-Biró Anna

Tördelőszerkesztő:
Vörösss Ferenc

ISBN 978-963-498-488-7 (elektronikus)

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