HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Sági Gábor
gabor.sagi@yahoo.com

MEGVÉDHETŐEK-E A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK?

Absztrakt

A kritikus informatikai infrastruktúrák egyre nagyobb szerepet töltenek be mindennapi életünkben. Az újonnan felmerült igények megvalósítása miatt az infrastruktúrák komplexitása, integráltsága egyre nagyobb méreteket ölt. A kor követelményeinek való megfelelés érdekében a korábban zárt hálózatok fokozatosan megnyíltak először csak az adott vállalt belső informatikai hálózata felé, később - sok esetben - az internet felé is. Az architektúra nyílttá válása, a komplexitás növekedése magával hozta az infrastruktúrák fenyegetettségének növekedését és újszerű támadási technikák kialakulását, alkalmazhatóságát is. Napjainkban a legjelentősebb kihívást az olyan – sok esetben hosszabb előkészítést és végrehajtást igénylő – támadások jelentik, amelyek célzottan egy információs infrastruktúra, vállalat, kormányzati szerv ellen irányul. A megfelelő védelem kialakítása nehezíti, hogy sok esetben a támadás a korábbi tapasztalatoktól, ismerté vált eseménysorozattól eltérő módon kerül végrehajtásra, azaz nem ismert a fenyegetés karakterisztikája, és így a jelenlegi védelmi megoldások nem vagy csak korlátozottan alkalmasak ezen események észlelésére, kezelésére. A szerző a cikkben bemutatja, hogy információbiztonsági szempontból milyen nehézségeket hozott az informatikai infrastruktúrák fejlődése, milyen támadási vektorokkal kell számolni a védelem kialakítása során, illetve milyen nehézségekkel kell számolni, milyen kockázatot jelenthet egy képzett támadó, milyen veszélyt hordozhatnak a védelemre hivatott műszaki megoldások.

Critical information infrastructures play an increasingly important role in our daily lives. Due to the implementation of the new needs the infrastructures are becoming more complex, integrate. In order to meet the requirements of the nowadays, the previously closed networks gradually opened for the first time only to the internal network of a company's information technology, in many cases even later into the Internet. The increase in complexity brought increase of threats of infrastructures and appear new attack techniques. Today, the biggest challenge is - in many cases a longer preparation and implementation require - are the attacks that are directed specifically to an information infrastructure of company, government agency against. Developing good protection is complicated by the fact that in many cases the attack is carried out without past experience or known events, different way, ie not known to the threat characteristics, and so the current security solutions are not only limited use of these events to detect, defend. The author of the article shows from information security point of view,

what kind of difficulties for the development of the IT infrastructure, which attack vector can be expected in the development of protection, and what problems have been encountered, which kind of risks are carried by a skilled attacker, what kind of risks are carried by the protection of technical solutions.

Kulcsszavak: *kritikus információs infrastruktúrák védelme, fenyegetések, védelmi nehézségek ~- critical information infrastructure protection, threats, protection difficulties*

BEVEZETÉS

Az információs rendszerek használatának széles körű elterjedése, az információs rendszereket használók igényeinek változása, az információs rendszerekkel szemben támasztott – a korábbi funkcióktól eltérő igények szükségessé tettek új típusú rendszerek kifejlesztését, meglévő rendszerek továbbfejlesztését, amelyek a kor követelményeinek megfelelőin ki tudják szolgálni a megrendelők, felhasználók igényeit. Megnőtt az igény a rendszerek integrációjára, távolról történő menedzselésére, újfajta architektúrák (pl.: internet, web2, mobil eszközök, cloud) használatára, újfajta szolgáltatások (pl. mobil alkalmazások, netbank, BYOD, smart home, smart city, Internet of Things, vezető nélküli autó) igénybevételére. Az új szolgáltatások ugyanakkor korábban nem tapasztalt módon növelték az rendszerek komplexitását, s az egymással együttműködő rendszerek sebezhetőségét, illetve jelentősen nőtt a motiváció az információs infrastruktúrákból való információszerzésre, a rendszer működésének zavarására.

Az információs társadalom zavartalan működésének megbontására irányuló támadások tényleges célpontjai a kritikus infrastruktúrák - hiszen ezek adják működésének alapját -, azonban az ellenük irányuló információalapú támadások és fenyegetések a különböző szintű és fontosságú infokommunikációs rendszereket érintik. Ezek a rendszerek mára a fenyegetések stratégiai célpontjaivá váltak.[1]

Számos olyan kritikus infrastruktúránk van, amely sérülékeny információs (informatikai) rendszereket használ. Ezáltal a kritikus infrastruktúrák egyik legkritikusabb része maga az infrastruktúrát irányító, vagy az azt ellenőrző és vezérlő információs rendszer. [2]

Mind a hazai, mind a nemzetközi szakirodalomban számos szerző foglalkozik az információs infrastruktúrák védelmi kérdéseivel. Hazai vonatkozásban kiemelkedő a 2014-ben megjelent „Kritikus infrastruktúrák és kritikus információs infrastruktúrák” című tanulmány, amely részletesen taglalja a kritikus információs infrastruktúrák helyét szerepét a mindennapi életben, az infrastruktúrák támadási vektorait, valamint a lehetséges védelmi megoldásokat. A tanulmány részletesen bemutatja a kritikus információs infrastruktúrák civil és katonai vonatkozásait, valamint bemutatja a környező országok, az Egyesült Államok, Európai Unió és a NATO kritikus infrastruktúrákkal kapcsolatos tevékenységét, a tevékenységben résztvevő szervezetek szerepét, szabályozói környezetet. Ugyanakkor az elmúlt évben számos új fenyegetettség forrás, illetve védelmi megoldás látott napvilágot, amelyek lassan mindennapjaink részévé vállnak. A hazai szakirodalomban kevés cikk foglalkozik továbbá a már széles körben elterjedt védelmi megoldások, illetve a régi és az új védelmi megoldások hordozta kockázatokkal.

Jelen írás kívánja felhívni a figyelmet arra, hogy a jelenleg alkalmazott információvédelmi megoldások milyen kockázatokat hordoznak, az új védelmi elgondolások bevezetése során milyen új kockázatokkal kell számolni, illetve milyen nehézségekkel kell számolni a védelem működtetése során.

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME

Kritikus információ rendszerek, információk védelmének elve

Az információnak a tudásalapú információs társadalomban kitüntetett szerepe van. Az információs társadalom működése az információk és az az információs rendszerek támadásán keresztül jelentősen befolyásolható, károsítható, hatékonysága csökkenthető.[3]

A kritikus információs rendszerek megbízható működése, az információs rendszerekben kezelt információk a szervezetek számára a legfőbb értékek egyike, a hosszabb távon fenntartható fejlődés egyik legfontosabb alapja. Hatékonyan és biztonságosan működő

információs rendszer nélkül egy szervezet sem képes ellátni feladatát, nem képes megfelelni a tulajdonosi, irányító és szabályzói elvárásoknak.

A szervezet információs rendszerekkel szembeni folyamatosan növekvő kitettségének hatására az információs rendszerek és az azokban kezelt információk, a rendszerek által irányított folyamatok egyre kiemeltebb szerepet töltenek be a szervezet életében, olyannyira, hogy napjainkban számos ágazatban megfelelő szinten működő információs rendszerek nélkül elképzelhetetlen a működés. A kitettség növekedése magával hozta az igényt, hogy a szervezet által üzemeltetett, igénybe vett rendszereket egyre magasabb színvonalon kell védeni a nem kívánt, nem várt eseményekkel szemben.

A belső elvárások mellett ugyanakkor „társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme” [4]. Ahol:

- Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
- Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás megtörténtének bizonyosságát (letagadhatatlanság) is, illetve a rendszerelem tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható.
- Rendelkezésre állás: az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható.

A bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) hármasát szokták az angol kezdőbetűik alapján CIA-elvnek nevezni. [5]

A hazai szabályozásban, illetve nemzetközi szabványokban a hitelesség és a letagadhatatlanság nem minden esetben jelenik meg különálló követelményként, hanem része a sértetlenség követelményének.

A fentiek alapján a biztonság a rendszer olyan – az érintett számára kielégítő – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. [6]

A kockázatarányos védelem kialakítása során figyelembe kell venni a kezelt információk minősítését. Az adatminősítés jelenlegi rendjét figyelembe véve, a komplex információbiztonság szempontjából – a tárolt adatok minősítésétől függően – a vállalatoknál, intézményeknél, kormányzati és védelmi célú szervezeteknél biztonsági osztályokat kell kialakítani. [7]

Fontos megjegyezni azonban, hogy a kritikus információs infrastruktúrák védelmét szorosan koordinálni kell magával a kritikus infrastruktúrák védelemmel. [8]

Információs infrastruktúrák kialakulásának sajátosságai információbiztonsági aspektusból

A szervezetek megalakulása során ritkán adatik meg, hogy egy szervezet már induláskor tudatosan alakítsa ki információs rendszerét, információbiztonsági megoldásait. Ennek oka részben, hogy a szervezet indításakor – értelemszerűen – nem lehetnek meg azok a tervek, amelyek a szervezett hosszú távú céljait, feladatait tartalmaznák, s amelyből tervezetten ki lehet alakítani egy egységes információs rendszert, továbbá egy induló vállalkozás esetén általában nincsenek meg az egységes információs rendszer kialakításához szükséges emberi

és pénzügyi erőforrások sem. A szervezet fejlődése során jellemzően – főleg a kezdeti időben - egy adott feladatnak megfelelő alkalmazás kerül kiválasztásra, kifejlesztésre, az új rendszer általában nem kerül integrálásra a meglévő rendszerekkel. Az új rendszer tervezése során legtöbbször nem ismertek a hosszabb távú elképzelések, így csak később – az új igények megjelenésekor – válik láthatóvá, hogy szükség lehet különféle rendszerarchitektúrára épülő rendszerek összekapcsolása.

Másrészről a szervezet informatikai rendszerei számának növekedésével párhuzamosan nő az szervezett informatikai kitettsége, amely biztonságtudatos vállalati szemlélet esetén magával hozhatja a kockázatarányos védelem kialakítását. A kezdeti kezdetleges megoldásokat - a szervezet fejlődése során - felváltják a komplex – több szintű - védelmi megoldások, amelyek bevezetése általában magával hozza az üzleti folyamatok változását, így bevezetésük nem minden esetben könnyű feladat.

A több évtizede működő szervezetek esetén az adott pillanatban érvényes igény, szükséglet határozta meg, hogy mely folyamatok kerülnek információs rendszerekkel támogatásra, s jellemzően az adott időszak információbiztonsági technológiákat alkalmazva vagy – fenyegetettségek felismerésének és a jövőbeli elvárások ismeretének hiányába – mindenféle védelmi megoldás nélkül. A kezdeti időkben elsősorban a rendelkezésre állás volt a cél, kevesebb hangsúlyt helyeztek a bizalmasság, sértetlenség megőrzésére – ez a felfogás mai napig megtalálható – bár egyre kisebb mértékben - a különböző ipari irányító, mérési, stb. rendszereknél és sok esetben, az irodai környezetben is.

Ezen fejlődési utat járják be többek között a SCADA, PLC és egyéb ipari tevékenységet támogató informatikai rendszerek is. Információbiztonsági szempontból különösen aggasztó ezen rendszerekben alkalmazott technológiák védelmi megoldások gyengesége, védelmi mechanizmusok szinte teljes körű hiánya. Jelentős kockázatot hordoz, hogy ezen rendszerek közötti kommunikáció sok esetben nem titkos csatornán történik, mivel a fel nem ismert fenyegetések, a korábban nem ismert üzleti célok miatt az adatok titkosítása nem volt cél a protokollok fejlesztése során. Az egyedi megoldások miatt széles körben elterjedt a modem-es, hagyományos soros porton történő távoli rendszer elérés, de maga az master-slave architektúra is hordoz kockázatokat. [9]. Az ilyen rendszerekre is jellemző, hogy a kezdetben szeparált rendszer, összekötésre került a vállalat belső informatikai hálózatával, majd az internettel, s közben nem biztos, hogy kialakításra kerültek a megfelelő védelmi megoldások az infrastruktúra védelmének biztosítására.

A szélesebb körben elterjedt – nem speciális célra fejlesztett – rendszerek (pl.: ügyviteli-, banki-, vállalatirányítási-, pénzügyi rendszerek), vállalati belső információs rendszerek esetén a szervezetek a fenyegetettség érzetük alapján, illetve a szabályozói környezet szigorítása miatt vezették be védelmi megoldásaikat. A szervezet méretétől és az uralkodó információbiztonsági trendektől függően bevezetésre kerültek különféle egymással együttműködő, egymás működését támogató védelmi megoldások, többek között az IDM, IPS, IDS, DLP rendszerek, de fontos szerepet kaptak a különféle tűzfal és egyéb határvédelmi megoldások is.

A mobil eszközük elterjedése, a felhő alapú szolgáltatások igénybevétele azonban az eddigiektől eltérő, új szemléletet követelnek a biztonsági szakemberektől is, hiszen az addig jól körülbástyázott rendszerek hirtelen nyílttá váltak és a hatékonyságra törekvő üzleti igény lényegesen megelőzte ezen technológiák védelmét biztosító rendszerek kifejlesztését. Mobil eszközök védelmét biztosító MDM vagy EMM rendszerek még mindig nincsenek széles körben elterjedve, illetve a felhő alapú szolgáltatások esetén sem sikerült a biztonsági szakemberek számára megnyugtató védelmi megoldást találni.

Az informatikai rendszerek elterjedésével párhuzamosan alakultak ki az egyes rendszerekkel szemben megfogalmazott védelmi követelmények, amelyek segítettek a biztonsági szakembereknek megfelelő védelmi szint kialakításában. Később született meg a

felismerés, hogy hatékony információ védelem alapfeltétele - a különféle védelmi intézkedéseken túl - a megfelelő információ biztonsági irányítási rendszer működtetése (IBIR). Ma már természetesnek mondható, hogy egy szervezet rendelkezik az információbiztonsági irányítási rendszer területén külső, akkreditált tanúsítvánnyal (pl.: ISO 27001).

Információs infrastruktúrák fenyegetésének forrásai

Az információs infrastruktúrák megfelelő szintű működését számos külső és szervezeten belüli veszély fenyegeti. A támadások származhatnak egyes személyektől, jogosulatlan felhasználóktól, csoportoktól, terroristáktól valamint különböző nemzeti szervezetektől külföldi hírszerző szolgálatoktól, katonai szervezetetektől. Szakértők véleménye szerint a rendszerbetörések nagy többségében, mintegy 70–90%-ban belső munkatárs, vagy volt munkatárs is közreműködik. [10] Az információbiztonsági tevékenység része ezen fenyegetések kockázatainak csökkentése, a bekövetkezett esemény mielőbbi felismerése, hatékony kezelése, normál üzembe történő visszaállás megkönnyítése.

A fenyegetések eredete szempontjából megkülönböztethetünk emberi közreműködés nélküli (természeti eredetű) vagy közvetlen emberi közreműködés eredetű fenyegetéseket. Természeti eredetű fenyegetésnek tekintem azon fenyegetéseket, amelyeket kialakulását közvetlenül az ember nem tudja érdemben befolyásolni. Természeti jellegű fenyegetés az emberi tevékenység okozta természeti jelenségek (pl. erdőkivágások miatti árvíz, lokális időjárási események), az éghajlatváltozás és az időjárás szélsőségessé válása miatt kialakult fenyegetések, mivel ezen fenyegetések hosszú távú emberi tevékenységek következményei és befolyásolásukra rövid távon csak kis mértékben képes az emberiség, viselkedésük megegyezik a természeti jelenségek karakterisztikájával illetve ezen fenyegetések elleni védőintézkedések megegyeznek a természeti eredetű fenyegetések elleni védelmi intézkedésekkel.

Emberi tevékenység okozta fenyegetések közé sorolom azon fenyegetéseket, amelyeket közvetlen emberi tevékenység okoz, függetlenül attól, hogy annak mi a szándéka és oka. Az információs rendszer biztonságát lehet gondatlanul vagy szándékosan veszélyeztetni. A gondatlan veszélyeztetés elsősorban nem megfelelő szaktudásból, a biztonságtudatosság hiányából vagy a tevékenység következményeinek nem megfelelő felméréséből származik. Szándékos tevékenységek közé sorolandó azon tevékenységek, amelyek során egy személy vagy egy csoport célja az adott informatikai rendszer működésének megzavarása, a rendszerben tárolt információk kompromittálása (módosítása, törlése, információ megszerzése).

A belső veszélyeket elsősorban a saját alkalmazottak, munkatársak okozzák, akik a biztonsági rendszabályok be nem tartásával, képzetlenségükkel, hanyagságukkal, illetve vélt vagy valós sérelmeik megtorlásaként veszélyeztetik az adott szervezet, intézmény, vállalat stb. infokommunikációs rendszereit. Ezek a veszélyek, amennyiben felfedésükre és elhárításukra nem helyeznek hangsúlyt, komoly biztonsági problémák forrásai is lehetnek.

A külső veszélyek közé mindazon fenyegetések tartoznak, amelyek valamilyen külső forrásból származnak, és a támadás célja anyagi- politikai-, gazdasági- vagy katonai előnyszerzés. E támadásokat általában az információs technológiához kiválóan értők hajtják végre. E támadók köre az infokommunikációs rendszerek elterjedésével és fejlődésével egyenes arányban napról-napra növekszik és bővül. [1]

Az informatikai rendszerek tervezési, megvalósítási hibáiból adódó fenyegetések emberi tevékenység okozta fenyegetések közé soroltam, mivel közvetve véletlen vagy szándékos emberi tevékenység okozza a fenyegetést, illetve a fenyegetés kihasználásához is sokszor emberi tevékenység szükséges.

Az alábbi táblázatban összefoglaltam – a teljesség igénye nélkül - a leggyakoribb fenyegetéseket:

Természeti eredetű	Emberi közreműködés eredetű	
	gondatlan	szándékos
földrengés, árvíz, időjárás (pl.: vihar), kozmikus tevékenység (pl. napkitörés)	szoftverhiba, üzemeltetési folyamat megsértése, rossz döntés, ipari-, közlekedési-, nukleáris baleset	terrorizmus, hacking, bosszú, szabotázs, külső- vagy belső fegyveres konfliktus, információs hadviselés

1. táblázat Tipikus fenyegetések

A fenyegetés bekövetkezésének lehetséges hatása

A fenyegetés hathat közvetlen az infrastruktúra elemére vagy az infrastruktúra működését támogató egyéb – például információs – infrastruktúra elemre. Egy információ biztonsági esemény hatása azonban túlmutathat az információs infrastruktúra határain (pl. tartós áramszünet, szolgáltatás szünetelése miatti társadalmi, gazdasági hatás).

Az esemény hatását, kiterjedését többféle szempontból lehet csoportosítani.

Területi hatás alapján megkülönböztethetünk lokális, regionális, országos vagy akár több országon átívelő is eseményt. Jellemzően a kiterjedtség határozza meg, hogy az esemény kezelésében milyen szintű erőforrások bevonása szükséges. Jellemzően minél nagyobb a területi határ, annál nagyobb egy esetleges incidens bekövetkezésből adódó hatás, és annál komplexebb a védekezés.

Gazdasági hatás alapján az esemény bekövetkezésének közvetlen, illetve közvetett pénzügyi (gazdaság) hatás alapján lehet csoportosítani az eseményt. Alapvetően két fő csoportot lehet kialakítani: az esemény hatása az adott szervezeten belül kezelhető vagy az esemény kihatással van az adott megye, régió, ország gazdaságára. A szervezeten belül kezelhető hatás szélsőséges esetben akár a szervezet megszűnését is jelentheti.

Időbeli hatás: amely megmutatja, hogy az adott infrastruktúra vagy egyes elemének vesztesége mennyi ideig fejti ki komoly hatását (azonnal, 24–48 óra, egy hét, hosszabb időtartam). [8]

Ugyanakkor sok esetben nem a területi, gazdasági hatás határozza meg a támadás hatékonyságát, hatását. Az elmúlt néhány évben napvilágra került számos olyan célzott támadás, amelynek célja egy jól irányzott tevékenység elvégzése és amelyek egy kormányzati szerv, szervezet vagy egymással kapcsolatban álló szervezetek ellen irányultak:

- Az első dokumentált kibertámadást 1997-ben egy Sri Lankai terrorszervezet követtel el, [3] amelyet számos egyéb (pl.: Észtország, Grúzia elleni) kibertámadás követett.
- a Stuxnet 2010. júniusi felfedezése volt az első olyan széles körben nyilvánosságra került biztonsági esemény, amely vélhetően kormányzati támogatással, vélhetően egy konkrét célpontra irányult és mellesleg rávilágított arra, hogy a SCADA rendszerek informatikai védelme nem megfelelő. A támadás célja vélhetően az iráni atomprogram késleltetése volt a natanzi centrifugáinák és bushehri atomerőmű berendezéseinek támadásán keresztül. A Stuxnet amellett, hogy talán a legismertebb malware, nagyon kifinomult technikát használ(t) működése során. A malware egyes szakértői vélemények alapján 2-3 évig működött észrevétlenül, hozzávetőlegesen 100 ezer (egyes vélemények szerint 150 ezer) számítógépet fertőzött meg a világon, készítőiről bizonyíthatóan a ma napig nem derült ki, hogy kik voltak [11].
- vélhetően a Stuxnet fejlesztője, vagy a forráskódot ismerő személy készítette a magyar Crysys Lab által 2011-ben felfedezett Doqut [12], amely vezérlőrendszerekkel kapcsolatos információszerzésre lett vélhetően készítve és

ellentétben a Stuxnettel – az előzetes vizsgálatok alapján – nem tartalmaz romboló jellegű kódot.
- Európában az első – 2012. decemberében – nyilvánosságra hozott célzott kibertámadás a német 50 Hz elleni támadás volt, ami ugyan nem érintette a tényleges szolgáltatást, de több órára lebénította a cég informatikai rendszerét és rávilágított az informatikai rendszerek védelem fontosságára az M2M (machine to machine) rendszerek vonatkozásában [13].
- 2012-es felfedezésekor a legszofisztikáltabb káros program [14] Flame volt. A megfertőzött hozzávetőlegesen 1000 számítógépet fertőzött meg Közel-Keleten. A támadás célpontjai között oktatási, egészségügyi, kormányzati intézmények is voltak és a program gyakorlatilag bármilyen forrásból, csatornáról képes volt adatot lopni.
- Ugyanakkor 2014-ben is több 10 millió esetben történ például bankkártya vagy személyes adat lopás csak az Egyesült Államokban [15].

A támadások jellemzően a kibertérben maradnak, azaz közvetlen fizikai pusztító hatásuk nincs a fizikai környezetre. Ez alól kivételt képeznek az irányító rendszerek elleni támadások, amelyek – a különféle érzékelők, a technológiai folyamatok manipulánsán keresztül – sikeresen akadályozták a technológiai folyamatokat, illetve akár komoly fizikai pusztítással járó incidenst is okozhattak volna.

A támadásoknak azonban van egy közös tulajdonságuk: nem lehetett minden kétséget kizáróan bizonyítani, hogy kik voltak az elkövetők. Közvetlen bizonyítékok, szakértői vélekedések alapján azonban mindig volt feltételezett elkövető. Az egyetlen ismertté vált ítélet az orosz-észt konfliktus után született, ahol a 20 éves egyetemista 850 fontnyi büntetést kapott. [16]

Biztonsági esemény előre jelezhetősége

Az információs rendszerek globális jellegéből adódóan e rendszerek bárhonnan, bármikor elérhetők, és az információtechnológia vívmányait ellenük fordítva támadhatók. [1]

Az incidensek bekövetkezését minden esetben valamilyen eseménysorozat előzi meg. A támadó a támadás sikeres végrehajtásának érdekében számos tevékenység közül választhat. Ezen tevékenységek egy része a megtámadott számára nem észrevehető (pl.: publikus információ források elemzése), más része látható lehet, ugyanakkor megfelelő védelem hiányában nem biztos, hogy látható, a látható jelekből pedig nem biztos, hogy felfedezhetőek a támadás nyomai. Sok esetben az utólagos vizsgálat során derül ki, hogy jobban szervezett védelmi megoldással a támadási kísérlet felfedezhető lett volna.

Meghatározott események sorozata utalhat egy incidens várható bekövetkezésére, de nem feltétlenül jelenti azt, hogy a biztonsági esemény be is következik, illetve, hogy az esemény biztonsági eseménnyé válik-e. Ilyen események lehetnek például az elektronikus – pl.: elektronikus levélben beküldött káros kódok, amelyek megfertőzhetik a számítógépet és ott adatot gyűjthetnek vagy egyéb káros tevékenységet végezhetnek, de ilyen esemény lehet sikertelen bejelentkezések után egy sikeres, vagy akár egy IP cím lekérdezése is.

Az információ biztonsági incidens megelőző esemény sorozat definiáltságától függően megkülönböztethetünk:
- előre jól definiált eseménysorozat követő incidens: az eseményt egy időben, viselkedésében előre jól definiálható eseménysorozat előzi meg, amelyet a jelző, figyelmeztető rendszerek nagy biztonsággal jelezni fognak. Ezen eseménytípusok esetén jól tervezhetőek a különféle védelmi megoldások, legyenek azok fizikai, logikai vagy folyamati jellegűek. A korszerű információs technológiáknak köszönhetően számos olyan figyelmeztető mechanizmus került bevezetésre, ami képes előre jelezni az egyes infrastruktúra elemek várható fizikai hibáit, és ezzel

jelentős mértékben tudja támogatni a rendszereket üzemeltető szervezeteket. A kiforrott információbiztonsági védelmi megoldásoknak köszönhetően sok lehetőség van automatikus beavatkozásra is. Ilyen védelmi lehetőségek lehetnek hálózati forgalom átirányítások, vírus eltávolítás egy állományból, IDS rendszer jelzése, beavatkozása, riasztás küldése központi monitoring, riasztási rendszernek, DDoS védelem.

- nem vagy gyengén definiált eseménysorozatot követő incidens: ez eseményt nem előzi meg olyan – időben behatárolható - konkrét ismert eseménysorozat, tevékenység, amely egyértelműen előre jelzi a bekövetkezendő incidenst. Az időben elhúzódó és a jelző rendszerek által - az időbeni elhúzódás miatt - nem érzékelt eseménysorozatot is ebbe a kategóriába soroltam, mivel ilyen események felismerése is csak korlátozottan alkalmasak a jelenlegi védelmi megoldások. Definíció szerint ebbe a csoportba tartoznak továbbá azon eseményeket is, amelyek észlelése nem vagy csak hosszú idejű tevékenység után történik meg. Ezen csoportba jellemzően az információs rendszert érintő támadások tartoznak, amelyek előkészítése jellemzően hosszabb ideig tart és komolyabb erőforrást, szaktudást igényel. Ezen támadások elleni védekezés nehézkes, a jelenlegi információbiztonsági védelmi rendszerekkel szinte lehetetlen.

Vizsgálva a különböző veszély típusokat könnyen belátható, hogy a természeti katasztrófák elleni felkészülés többnyire gondos tervezéssel biztosítható, és ezáltal a kár bekövetkezése jó eséllyel a lehetőségekhez képest a legkisebbre csökkenthető. A mégis bekövetkező eseményeknél a kárelhárítás – elsősorban itt is a jó tervezhetőség miatt – gyorsan és hatékonyan véghezvihető.[5]

Az emberi közreműködés eredetű fenyegetések jelentős részének bekövetkezési valószínűsége – hasonlóan a természeti eredetű fenyegetésekhez – gondos tervezéssel, előre definiált eljárásokkal, megfelelő képzéssel jelentős mértékben csökkenthető. A kárelhárítás az esemény nagyságától függően hatékonyan végrehajtható. Ugyanakkor a védekezés a szándékos károkozás, illetve nem ismert támadási technika (pl. nulladik napi sérülékenység) kihasználása esetén jelentős nehézséget okozhat.

Szándékos emberi tevékenységből fakadó fenyegetések nagymértékben függenek a támadó fél szakmai tudásától, motivációjától, illetve a rendszer védelmi képességeitől. A napvilágra került sikeres kritikus infrastruktúrákkal szembeni támadások szinte mindegyikéről elmondható, hogy a támadás előre jól megtervezett módon, korábban nem ismert technikákkal történt, a támadók kihasználták a támadott rendszerek nulladik napi (0-day) sérülékenységeit és azon keresztül bejutva az információs rendszerbe végezték tevékenységüket. Jól jellemzi a támadások kifinomultságát, hogy például a Stuxnet az atomreaktornak csak a dúsító berendezéseit (centrifugákat) támadta, magát az erőművet nem, a Flame számos különböző modullal rendelkezik (kb. 20 megabájt méretben) és a vezérlő szerver parancsára képes volt magát eltávolítani a fertőzött rendszerből, a Doqu pedig célirányosan csak releváns információt gyűjtött.

Az előző fejezetekben említett és vélhetően még számos egyéb fertőzés további közös jellemzője, hogy a fejlesztés során kiemelt figyelmet fordítottak arra, hogy a káros tevékenységek minél hosszabb ideig – akár évekig is – rejtve maradjanak.

Az információs rendszerek „intézményesített” védelme

A fenyegetés eredetétől, illetve méretétől függetlenül léteznek olyan eljárások, védelmi mechanizmusok, amelyek jelentősen tudják csökkenteni az információbiztonsági incidens bekövetkezésének valószínűségét, segíteni tudnak az esemény bekövetkezésének korai felismerésében, az incidens bekövetkezése esetén az információs infrastruktúrák

működésének zavarásából eredő károk csökkentésében, illetve segítenek az elvárt működés mihamarabbi visszaállításában.

Hatékony információvédelmi rendszer kialakítását sok esetben jogszabályok írják elő, követelik meg. A hazai szabályozásban a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapozta meg a kritikus infrastruktúrák védelemének rendszerét. A törvény végrehajtásának érdekében számos kormányrendelet született, ugyanakkor kormányrendeletek kiadása még sok ágazat esetén nem történt meg, így az infrastruktúrák kijelölése több ágazatban nem kezdődött el.

A kritikus információs infrastruktúrák információvédelem alapjait a hazai szabályozási rendszerben az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, illetve a végrehajtására kiadott 77/2013. NFM. rendelet, majd a rendeletet hatályon kívül helyező, de tartalmában közel megegyező 41/2015. BM. rendelet alapozta meg. A kormányrendelet konkrét követelménylistát tartalmaz, figyelembe veszi az informatikai rendszer kieséséből, az informatikai rendszerben kezelt adatok bizalmasságának, sértetlenségének, rendelkezésre állásának elvesztése esetén bekövetkező közvetlen, közvetett kár nagyságát, társadalmi-, politikai hatását. A fentebb említett rendelet mellet számos olyan követelményrendszer létezik, amely szintén használhatóak az információvédelmi rendszerének kialakításában: például ISO/IEC 27002, NIST 800-53, BSI IT-Grundschutz-Kataloge, stb.

Fontos kiemelni azonban, hogy a védelem kialakításának kockázatarányosnak kell lennie, azaz a védelmi költség nem haladhatja meg a lehetséges kár maximális értékét, illetve a védelmi tevékenységek aránytalanul nem csökkenthetik a rendszer használhatóságát. Ezen egyensúly megtalálása sok esetben nem könnyű feladat.

A szervezeten belül kialakított információvédelmi képességének nagymértékben függnek továbbá a szervezett információbiztonsági érettségétől, a munkavállalók, szerződéses partnerek biztonság tudatától, illetve az alkalmazott konkrét fizikai, logikai védelmi megoldásoktól.

Mindazonáltal egy szervezet működtetheti a legfejlettebb információvédelmi rendszert, ha a szervezet dolgozói nem rendelkeznek megfelelő ismeretekkel, biztonság tudattal, a bevezetett védelmi megoldásokat nem tudják hatékonyan használni, akkor az információvédelem nem tud, nem képes hatékonyan működni.

Információs infrastruktúrák védelmének nehézségei

Az információs infrastruktúrák működtetése során egyre nehezebb biztosítani az infrastruktúra elemek megfelelő szintű védelmét, biztonságos – elfogadható szintű - működését az egyre komplexebb rendszerek, az integrált elemek sokszínűsége, az egyre nagyobb hatékonyságra való törekvés, valamint a pénzügyi és technikai korlátok miatt.

Az információs infrastruktúrák komplexitásának növekedésével párhuzamosan jelentős mértékben nőtt az egyes elemek sérülékenységéből adódó eredendő kockázat, az integrációknak köszönhetően az addig védettnek és zártnak hitt rendszerek biztonsági szempontból védtelenné válhatnak. A hiányosságokat jól mutatja, hogy például az elmúlt években is több esetben külső partneren keresztül sikerült kritikus információs infrastruktúra védelmi rendszerin áthatolni és ott jogosulatlan műveletet végezni.

Sok esetben nem biztosított a kritikus információs infrastruktúra kiszolgálását biztosító infrastruktúra védelme. Nem megfelelő a közműellátás, illetve nagyon sérülékenyek a telephelyek közötti kommunikációs csatornák: hiányzó tartalék közmű hálózatok, könnyen hozzáférhető hálózati kábelek. Ugyanakkor számos egyéb tényező veszélyezteti a biztonságos működést.

Motivációs – emberi - tényezők

Az informatikai rendszerekben kezelt adatok biztonsága a különböző rendszerelemeken megvalósított védelemtől függ, ezért a védelmi rendszer kialakításánál mindenkor számításba kell venni az embert, amely az egész védelmi rendszerben a legnagyobb bizonytalansági tényezőt jelenti. [17] Az emberi tényező több szempontból is biztonsági kockázatnak mondható, a felhasználók tudatlansága, szakképzetlensége, valamint az ezekből adódó emberi mulasztások aggasztó hatással vannak az informatikai biztonságra, de nem szabad megfeledkezni az emberi segítőkészség, befolyásolhatóság és naivság kihasználhatóságáról sem [18]. Különösen jelentős a kockázat, ha a munkavállaló tudásánál, képességénél magasabb szintű jogosultsággal rendelkezik az adott rendszerben. A nem kellő tudatosság, az adminisztratív szabályok hiánya sok esetben biztosít lehetőséget az emberi viselkedés támadó általi befolyásolására, azaz social engineering-re.

Az emberi tényező megjelenhet a támadó oldalon is. A támadónak a céljainak elérésére számos lehetőség kínálkozik. Minél komolyabb a támadó szándéka, annál szerteágazóbb eszközöket használhat információszerzésre, a támadás kivitelezésére. A támadás hatékonysága jelentősen javulhat, ha a támadó speciális szaktudással rendelkezik, vagy olyan csoport tagja, amely érdemi információval rendelkezik a cél rendszerről, illetve megfelelő erőforrást tud biztosítani a támadás megtervezéséhez végrehajtásához. Ilyen csoportok lehetnek hektivisták, de akár egy állam (vagy annak titkosszolgálatának) dolgozói. Fontos megemlíteni azt a tényt is, hogy a biztonsági incidensek legtöbbjét a vállalat belső munkatársai követik el, vagy legalábbis belső alkalmazottak segítsége, közreműködése is szükséges a sikeres támadás végrehajtásához [19]. A támadó szaktudása, lehetőségei és a támadás sikerességének esélye alapján a támadót az alábbi főbb csoportok egyikébe lehet besorolni:

- script kiddie, lamer, noob: olyan informatikában kevésbé jártas személy, aki mások által készített megoldásokat használ, nem képes újításokra, szofisztikált támadások végrehajtására. Információit hasonló tudással rendelkező társaitól szerez, velük oszt meg. Széles körű ismeret hiánya miatt igazán komoly károkat nem tudnak okozni, célja inkább a figyelemfelhívás. Az általános védelmi megoldások általában hatékony védelmet nyújtanak ellenük, ugyanakkor az ismert sebezhetőségek javításának hiánya nagymértékben növelhetik a támadás sikerességének esélyét.
- egyéni, kis szervezettségű támadók (hacker, cracker): több szintje létezik, jellemzően elegendően magas szintű informatikai, információ biztonsági tudással rendelkezik ahhoz, hogy önállóan vagy csoportosan meg tudjanak tervezni és végre tudjanak hajtani egyedi támadást. Általában nem rendelkeznek korlátlan erőforrással, így a támadás bár jól tervezett lehet, de nem szofisztikált. Célok között lehet a pénzszerzés, információszerzés, károkozás, de lehet, hogy csak szociális, társadalmi, ideológiai, vallási ok miatti figyelemfelkeltés. Nem megfelelően kialakított és üzemeltetett információ védelmi rendszer hiányosságait kihasználva komoly károkozásra képesek. Védekezés megfelelően kialakított és üzemeltetett információvédelmi rendszerrel lehetséges, amelynek része a többszintű védelem (pl.: intelligens tűzfalak, DLP, IPS, IDS megoldások), biztonsági monitorozás, naplóelemzés is.
- „hivatásos támadók”: általában szervezetekhez – nagyvállalatokhoz, kormányokhoz, terrorszervezetekhez, jelentősebb társadalmi csoportokhoz köthető személyek, akik megfelelő anyagi hátteret, akár titkosszolgálati úton szerzett, gyártóktól, fejlesztőktől ellopott információt kapnak a „megrendelőktől” a támadás sikeres végrehajtásának érdekében. Munkájuk során fontos, hogy észrevétlenek maradjanak, felfedésük ne történjen meg. Ez alól kivétel, amikor a támadó kiléte szándékosan nem mered rejtve (pl.: terrorszervezetek). Mélyreható ismeretük és megfelelő háttér miatt a védekezés

ellenük nehéz. A támadások során a rendelkezésre álló eszközök széles spektrumát alkalmazzák. Támadási módszerek a social engineeringtől, nem ismert sebezhetőségeken át, új támadási technikák kialakításáig terjedhet. A támadások nehezen felismerhetőek, nem egy esetben éveken keresztül maradt rejtve a támadó tevékenysége. A támadás jelentős költsége (Stuxnet esetén 10 és 50 millió dollár közötti összeg) miatt ezen támadási forma nem elterjedt, és csak akkor „éri meg", ha a sikeres támadásnak komoly pénzügyi, politikai hozadéka van (például Stuxnet).

Műszaki kockázatok

Napjainkban használt védelmi megoldások – néhány kivételtől eltekintve – nem képesek olyan eseménysorozatokat, jelsorozatokat felismerni, amelyek korábban nem lettek az adott rendszerben megadva. A rendszerek tanulása múltbéli események elemzésének eredményeként, manuális úton – frissítések által – kerül be a rendszerbe, nem tanulással.

Ugyanakkor az elmúlt időszakban ismertté vált incidensek rávilágítottak arra, hogy az információ védelemre hivatott megoldások magukban is jelentős kockázatot hordoznak, amivel az információbiztonsági szakma nem vagy csak kevésbé számolt:

- a biztonságosnak hitt biztonsági rendszerek belátnak mindenhova, azaz bizonyos körülmények között bármilyen műveletet el tudnak végezni a kritikus információs infrastruktúrában, így a biztonsági rendszerek sérülékenységei fokozott veszélyt jelentenek,
- a széles körben elterjedt szignatúra alapú megoldások nem képesek követni a támadások során alkalmazott folyamatosan változó technikákat,
- a biztonság szavatolására hivatott rendszerek is számos hibát, sérülékenységet tartalmaznak,
- a felvásárlásoknak köszönhetően jelentősen csökkent a védelmi megoldásokat szállító vállalatok száma, ami sok esetben hasonló biztonsági megközelítést jelent a különféle termékeikben, megkönnyítve az integrációt és az üzemeltetést, de csökkentve a rendszer védelmi képességét,
- az egymástól függetlennek tűnő megoldások sok esetben hasonló alapokon működnek, így párhuzamos használatuk sem hozza meg az elvárt eredményt, ezzel hamis biztonságérzetet nyújtanak a szakemberek és a döntéshozók számára,
- a különböző szállítók által készített megoldások mindenki számára elérhetőek, így lehetőség van az egyes védelmi megoldások gyenge pontjainak megkeresésére,
- költséghatékonyság miatt a szervezetek általában nem használnak ugyanarra a feladatra több szállítótól is beszerzett terméket,
- a termékek fejlesztése során a kormányzati, titkosszolgálati szervek nyomására backdoorok kerülnek a rendszerekbe, amelyekről előbb-utóbb információt szerez a hacker társadalom is,
- hosszabb távon komoly kockázatot jelent a nem hazai, EU-n belül készített védelmi rendszerek, technológiák használata. A jelenleg baráti országok viszonya változhat, ami magában hordozhatja a fenyegetés jelentős növekedését,
- pozitív kockázatként jelent meg, hogy az elmúlt időszak eseményei következtében a biztonsági megoldást szállító cégek, kutató laborok egyre nagyobb figyelmet fordítanak saját nemzetük által használt rendszerek védelmére, ami rövid távon is jelentősen javíthatja biztonságunkat.

Ezen kockázatok meglétét bizonyítja, az elmúlt időszakban napvilágra került lehallgatási ügyek (többek között NSA – winchester firmware manipuláció, titkosszolgálati lehallgatások), számos kiemelt, magas kockázatú sérülékenység biztonsági megoldásokban

(például SSL, SYMANTEC Endpoint Protection, CISCO ASA sérülékenység [20]), illetve a korábban említett káros kódok éveken keresztül tartó észrevétlen működése is.

Hatékony információvédelem megteremtésének lehetőségei

A védelmet, mint tevékenységet modellezve egy egyszerűsített helyzetet képzeljünk el, amelyben a támadókat és a védőket egyszerűsítéssel egy-egy személy, a védő és a támadó testesíti meg. A támadó az egyik oldalról támad, és ez a támadás mindig valamilyen, a támadás végső célját képező értékre, a védett értékre irányul. A támadás legtöbbször nem közvetlenül éri a védett értéket, hanem a körülményektől függő támadási útvonalon zajlik le, amelyen különböző természetes vagy művi védelmi akadályokat kell legyőzni. A másik oldalon a védő a védett értéket védi, vagyis a támadásokat igyekszik megakadályozni, elhárítani. Mivel a védő és a támadó egymás szándékairól, módszereiről semmilyen információval nem rendelkezik, ezért elmondhatjuk, hogy mindkét fél egymástól független és egymás számára ismeretlen stratégiával igyekszik megvalósítani támadási, illetve védelmi szándékait. [21]

Az előző fejezetekben említett okok és kockázatok miatt nyilvánvaló, hogy a jelenleg széles körben alkalmazott védelmi megoldások nem vagy csak részben jelentenek megoldást megfelelő információbiztonság kialakításához. Fokozott figyelmet kell fordítani a korábbi években - a biztonságos rendszerfejlesztés érdekében megfogalmazott - alapelvek betartására, ugyanakkor az új kihívások egyben újszerű gondolkodásmódot, újszerű megoldásokat is követelnek az információbiztonság területén tevékenykedő vállalatoktól, szakemberektől.

Másrészről pedig fokozott figyelmet kell fordítani az információs rendszer tervezésére, a fejlesztési, tesztelési feladatok magasabb színvonalú, biztonságos üzletmenetet garantáló végrehajtására. Egy rendszer vagy szolgáltatás gyorsabb bevezetése nem járhat a rendszer implementációs idejének csökkentésével.

Újszerű gondolkodás részeként lehetséges megoldásként látom az eddig alkalmazott technológiák kiegészítését, olyam védelmi rendszerekkel, amelynek működési paraméterei részben vagy egészben egyediek, a támadó számára nehezen vagy egyáltalán nem megismerhetőek.

Napjainkban rendelkezésre álló nagy számítási kapacitásnak köszönhetően már széles körben elterjedtek azok a megoldások is, amelyek a felhasználó, rendszer viselkedésében vagy a hálózati adatforgalomban bekövetkező szokatlan tevékenységet vizsgálják.

Részleges megoldást jelenthet a – nem feltétlenül publikus - felhő alapú technológia, amely segítségével a világ számos pontjáról lehet gyűjteni az információbiztonsági szempontból releváns információkat, a begyűjtött információkat rövid idő alatt fel lehet dolgozni és el lehet küldeni a szolgáltatást igénybe vevő szervezeteknek, így a hatékony információ megosztás segíthet az incidens megelőzésében, kezelésében. Ugyanakkor számos szakmai vita zajlik a felhő alapú szolgáltatások biztonságával kapcsolatban, aminek következtében a különböző hatóságok sem ajánlják, támogatják a publikus felhő alapú szolgáltatások igénybevételét.

A kutatások során előtérbe kerülhet a mesterséges intelligencia alapú technológiák alkalmazási lehetőségeinek vizsgálata, alkalmazása. [3] Várhatóan jelentős előrelépést fog jelenteni a tanuló rendszerek szélesebb körű elterjedése, függetlenül attól, hogy az helyi vagy felhőszolgáltatás alapú védelmi megoldásban kerül kialakításra. Ugyanakkor a tanuló rendszerek sem fognak tudni teljes védelmet biztosítani, mivel a tanulási folyamat manipulálható, illetve az incidensek felismerésére a mai rendszerekben figyelt paraméterek széles körű kiterjesztésére lenne szükség, amelyhez jelenleg még nincs elegendő számítási kapacitás és a vizsgálat, rendszer fenntartásának költsége már nem biztos, hogy

kockázatarányos. A tanulásra képes rendszerek – jó definiált esetekben – akár képesek lehetnek önálló döntésre, beavatkozásra is.

A fejlődés ezen lehetséges útjai azonban számos új kockázatot hordoznak, amelynek feltérképezése még nem történt meg teljes körűen, a kockázatok kezelésére ma még nincsenek meg a válaszok. Várhatóan azonban az újszerű technológiák szélesebb elterjedése ki fogja kényszeríteni ezen kockázatok részletes feltárását, valamint az ügyfelek, hatóságok számára megfelelő megoldás biztosítását.

Megítélésem szerint igazi áttörést és megoldást a korábban lefektetett tervezési, fejlesztési alapelvek figyelembe vétele mellett, a jelenlegi alkalmazott védelmi megoldások az új technológiákkal történő hatékony ötvözése, valamint a tudásmegosztás hozhat.

ÖSSZEGZÉS

A kritikus infrastruktúrák és kritikus információs infrastruktúrák megfelelő szintű védelme elengedhetetlen a társadalom, a gazdaság, a védelmi szektor működéséhez. A kritikus infrastruktúrák működése manapság szinte elképzelhetetlen hatékony informatikai támogatás nélkül. Az infrastruktúrák fejlődésével párhuzamosan kerültek új informatikai támogató rendszerek bevezetésre, kerültek a meglévő rendszerek integrálásra. A fenyegetettségek felismerése magával hozta az infrastruktúrát védeni hivatott védelmi megoldások bevezetését. Meghatározása kerültek a rendszerekkel szemben támasztott fizikai, logikai követelmények és kialakultak az információbiztonsági irányítási rendszerek.

Az informatikai rendszerek komplexitása, sokszínűsége ugyanakkor magával hozta az emberi és technikai fenyegetettségek jelentős növekedését, amelyre az információ biztonsági szakma csak részben tudott válaszolni.

Az információs rendszerek és az azokban tárolt információk egyre nagyobb értéket képviselnek, így a rendszerek működésének zavarására, valamint az információk megszerzésére is egyre nagyobb a motiváció. Nem egy információbiztonsági incidens mögött vélhetően állami szereplők állnak, aminek bizonyítása ugyan nehézkes, de a támadás célja és a támadáshoz felhasznált anyagi-, emberi erőforrások valószínűsítik a támadó hátterét.

Ugyanakkor az elmúlt időszak eseményei rávilágítottak arra is, hogy nem csak közvetlenül az emberi tényező jelent komoly kockázatot, hanem a védelem biztosítására hivatott rendszerek is. A jelenleg széles körben elterjedt védelmi eszközök csak akkor tudják hatékonyan ellátni feladataikat, ha a támadás karakterisztikája ismert, azaz korábban sikerült azonosítani egy biztonsági incidens előzményeit. Számos esetben azonban – a rendelkezésre álló erőforrások miatt – megjelennek olyan tevékenységek, amelyek nem utalnak támadásra, így a védelmi rendszerek nem jeleznek, sokszor akár több éven keresztül sem.

Az újszerű megoldások – hasonlóan a korábbi évekhez – várhatóan nem fognak önmagukban megoldást hozni a folyamatosan növekvő kockázatok elviselhető mértékű szintre csökkentésében.

Hatékony információvédelem kialakításához újfajta technikai megoldások bevezetése, új gondolkodásmód szükséges, amely magával hozhatja az elmúlt években megjelent korszerűnek tekinthető információvédelmi megoldások integrációját, a már széles körben alkalmazott megoldásokkal. Új szerepet kaphat a felhő alapú szolgáltatás, a viselkedés alapú esemény felismerés, illetve a mesterséges intelligencia is a hatékony védelem megteremtésében.

Felhasznált irodalom

[1] Haig Zsolt: Az információs társadalmat fenyegető információalapú-veszélyforrások:

http://www.zmne.hu/kulso/mhtt/hadtudomany/2007/3/2007_3_4.html (letöltve: 2015.szeptember 3.)

[2] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van II.: Célok és teendők http://www.hadmernok.hu/2011_1_kovacs_sipos.pdf (letöltve: 2015.szeptember 3.)

[3] Haig Zsolt – Kovács László: Fenyegetés a cybertérből http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (letöltve: 2015.szeptember 6.)

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény

[5] Muha Lajos: A MAGYAR KÖZTÁRSASÁG KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁINAK VÉDELME Doktori (PhD) értekezés Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem 2007.

[6] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008

[7] Haig Zsolt – Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák tanulmány 2012 http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf (letöltve: 2015. július 10.)

[8] Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nádor: A kritikus információs infrastruktúrák meghatározásának módszertana 2009. http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf (letöltve 2015. július 10.)

[9] Eric J. Byres - Matthew Franz - Darrin Miller: The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf (letöltve: 2014.03.10.)

[10] Haig Zsolt: Számítógép-hálózatok hadviselés rendszere az információs műveletekben. http://uni-nke.hu/downloads/bsz/bszemle2006/1/06_Haig_Zsolt.pdf (letöltve 2015. július 10.)

[11] Nicolas Falliere, Liam O Murchu, and Eric Chien: W32.Stuxnet Dossier https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (letöltve: 2015.04.30)

[12] Steven Cherry: Sons of Stuxnet http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet (letöltve: 2015.04.30)

[13] Pelle Neroth: Germany's 50Hertz hit by cyber attack in European first http://eandt.theiet.org/blog/blogpost.cfm?threadid=49719&catid=390 (letöltve: 2015.04.30)

[14] sKyWIper Analysis Team: A complex malware for targeted attacks http://www.crysys.hu/skywiper/skywiper.pdf (letöltve: 2015.04.30)

[15] Bill Hardekopf:The Big Data Breaches of 2014 http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/ (letöltve: 2015.04.30)

[16] Estonia fines man for 'cyber war' http://news.bbc.co.uk/2/hi/technology/7208511.stm (letöltve: 2015.09.10)

[17]Muha Lajos – Krasznay Csaba Az elektronikus információs rendszerek biztonságának menedzselése https://opac.uni-nke.hu/webview?infile=&sobj=9696&source=webvd&cgimime=application.pdf (letöltve: 2014.03.10.)

[18] Thapar, 2007 Thapar, A. (2007): Social Engineering - An attack vector most intricate to tackle!, http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf letöltve: 2015. március 10)

[19] Oroszi Eszter: Social Engineering Az emberi erőforrás, mint az információbiztonság kritikus tényezője http://krasznay.hu/presentation/diploma_oroszi.pdf (letöltve: 2015.03.20)

[20] Kormányzati Eseménykezelő Központ (GOV CERT Magyarország) sérülékenységek: http://tech.cert-hungary.hu/taxonomy/term/22 (letöltve: 2015.05.04)

[21] Muha Lajos: Az informatikai biztonság meghatározása (3.3. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2004., ISBN:963 9313