# A szoftver sérülékenységek kihasználási módozatai – Informatikai támadások, támadók és biztonság 2013-2016.

Dr. Horváth Attila
Kutató
Információs Társadalomért Alapítvány
e-mail: horvath.attila@infota.org

Erdősi Péter Máté
PhD hallgató
Nemzeti Közszolgálati Egyetem
Közigazgatás-tudományi Doktori Iskola
e-mail: erdosi.peter.kdi@office.uni-nke.hu

Dr. Kiss Ferenc
Kutató
Információs Társadalomért Alapítvány
e-mail: kiss.ferenc@infota.org

Benkő Zsanett
Kutató
Információs Társadalomért Alapítvány
e-mail: benko.zsanett@infota.org

Szanyi István
Kutató
Információs Társadalomért Alapítvány
e-mail: szanyi.istvan@infota.org

Török Marianna
Kutató
Információs Társadalomért Alapítvány
e-mail: torok.marianna@infota.org

**Absztrakt**

Az Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal – NKFIH által támogatott PD-109740 számú kutatási projekt keretében immár 3 éve vizsgáljuk az informatikai sérülékenységeket és azok lehetséges társadalmi, gazdasági hatásait. A kutatás három éve alatt az informatikai biztonság számos aspektusát vizsgáltuk meg, hiszen a szoftver sérülékenységek minden területen hatást gyakorolnak, lehetővé teszik a támadásokat.

A következő tanulmányban a kutatási évek során tapasztalt legfontosabb biztonsági trendeket foglaltuk össze. A tanulmányban először a dolgok internetével, majd a jelenleg legtöbb problémát okozó zsaroló vírusokkal foglalkozunk. Ezután megvizsgáljuk a célzott támadások természetét, a hagyományos kártékony kódok jelenlegi helyzetét, majd pedig a rendszerek feltörésének tudatos emberi tevékenységét a hekkelést és annak hatásait vizsgáljuk. Ezek után foglalkozom a mobil eszközök biztonságával, a kritikus infrastruktúrák védelmével, a jogi és iparági szabályozási környezettel, majd pedig a legkiszolgáltatottabb korosztály, a gyerekek és tinik helyzetével, az interneten rájuk leselkedő veszélyekkel foglalkozik.

***Kulcsszavak:*** *sérülékenység, biztonság, vírus, zsaroló, mobil biztonság, dolgok internete, célzott támadás, APT, okos eszközök, szabályozás, IKT, ipari vezérlő rendszer*

## 1. Bevezetés

Az elmúlt évek során a kutatók világosan bebizonyították, hogy a web vált a kártékony kódok fő terjedési csatornájává. A kifejezetten bűnelkövetési célú szoftverek (crimeware) terjedése és professzionalizálódása, a botnet hálózatok folyamatos növekedése és fenyegetése, a mobileszközöket célzó kártevők robbanásszerű terjedése azok a folyamatok, amelyek a legjobban fémjelzik a kutatás 3 évét. 2015 trendjei már világosan mutattak a vállalati és a kormányzati felhasználás egyre növekvő, kiterjedtebbé váló célkeresztbe kerülésére. (ESET, 2015)

Tisztán kivehetőek az összefüggések a hálózatra kapcsolat eszközök egyre növekvő száma, a gyors technológiai fejlődés, az adatbiztonság egyre növekvő jelentősége között, bármilyen távon vagy kontextusban is vizsgáljuk az eseményeket. 2013 volt a mobil kártékony kódok robbanásának éve (ESET, 2013), de ez csak az első fejezete volt az új technológiákat támadó, egyre kiterjedtebb biztonsági problémáknak, elég ha csak a dolgok internetére (IoT – Internet of Things), az okostévékre, okos otthonokra, a vezető nélküli járművek és a vezetést segítő rendszerek terjedésére vagy épp a viselhető technológiákra gondolunk. Az „egyszerű" felhasználók mellett, az ipar, az üzleti felhasználók és a közigazgatási szervek is folyamatosan kockázatoknak vannak kitéve.

## 2. A dolgok internete

Amikor a dolgok internetéről beszélünk, több millió berendezésről van szó, ami képes a hálózatra kapcsolódni, 2020-ra az előrejelzések szerint már 21 milliárd ilyen eszközzel kell számolni (Gartner, 2015c), amelyek mind adatokat generálnak és a fogadnak, rengeteg adatot éppen a felhasználók szokásairól, mozgásáról, biológiai működéséről, pl. az okos órák és más, viselhető eszközök esetében. Ez teljesen új biztonsági kihívásokat hoz a vállalati, kormányzati IT-osztályok számára is, hiszen ezek az eszközök napi szinten ki-be áramlanak a munkahelyi hálózatokba, jelentősen megnövelve az elvárt védelem szintjét és a biztonsági személyzet hozzáértését. (Horváth et.al., 2015)

**1. táblázat: IoT eszközök kategóriánként 2014-2020 (millió db)**

| Kategória | 2014 | 2015 | 2016 | 2020 |
|---|---|---|---|---|
| Végfelhasználó | 2.277 | 3.023 | 4.024 | 13.509 |
| Üzleti: általános | 632 | 815 | 1.092 | 4.408 |
| Üzleti: vertikális/specifikus | 898 | 1.065 | 1.276 | 2.880 |
| **Mindösszesen** | **3.807** | **4.902** | **6.392** | **20.797** |

**Forrás: Gartner, 2015c**

2015 koncentrált támadásokat hozott a vállalati szektor ellen, amelyben főleg célzottan a mobil eszközök illetve a dolgok internetéhez kapcsolódó megoldások voltak érintve. Ez a tanulmány áttekinti az elmúlt időszak legfontosabb eseményeit, trendjeit és megpróbálja előre jelezni azokat a jövőbeni trendeket és kihívásokat, amelyek az otthoni és üzleti környezetben meghatározóak lesznek a jövőben.

Áttekintésre kerülnek a kifejezetten bűnelkövetési céllal létrehozott megoldások (crimeware), a Folyamatosan Fennálló Fejlett Fenyegetések az APT-k (Advanced Persistent Threats), a zsaroló szoftverek hatásai a biztonságérzetre és a biztonság tudatosságra. Egy dolog bizonyos, az IT-biztonság egyre több és a több felhasználót érintő probléma, az intelligens eszközök terjedésével olyanok esetében is előkerül, akik néhány éve még egyáltalán nem számítottak bele a veszélyeztetett célcsoportba.

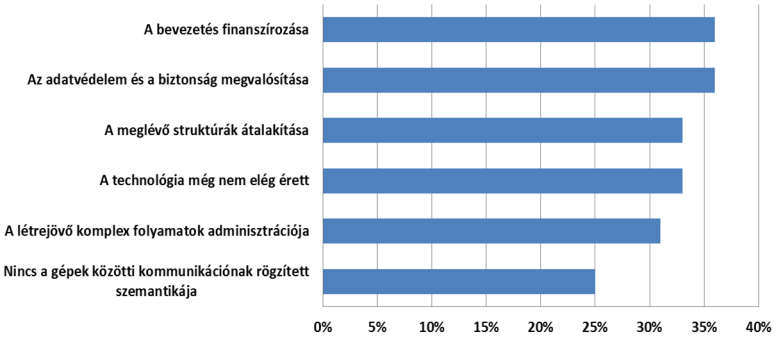
A dolgok internete (IoT), néhány éve a legnépszerűbb témák közözött szerepel a biztonsági világban, számos vitát generálva. De abban minden szakértő egyetért, hogy a jelen és jövő egyik legnagyobb biztonsági kihívását hordozzák a rohamosan terjedő, nem szakértő kezekbe szánt felokosított eszközök.

Már évekkel ezelőtt elkezdték felhívni a figyelmet a szakértők, az egyre „okosabb", így viszont támadhatóvá váló mindennapos eszközök elterjedésével járó kockázatokra. Három évvel később a technológiai fejlődés egyre csak gyorsul, sokszor messze megelőzve az eszközök védelmének, biztonsági tulajdonságainak fejlettségi szintjét. (Horváth, 2011b) Ahogy egyre több eszköz kapcsolódik az internethez, egyre több támadás is éri őket. Ma már senki nem lepődik meg egy routerek firmware-jét tömegesen támadó megoldáson, egy webkamerákból álló botnet hálózaton, vagy épp a hálózatra kapcsolódó egészségügyi eszközök elleni zsarolásos támadáson, amely egész kórházak működését lehetetlenítette el az elmúlt időszakban. Kutatói kísérletek bebizonyították, hogy a ma legforróbb témának számító önvezető autók és vezetéstámogató rendszerek, de akár az otthon automatizálási eszközök is a támadások célkeresztjébe kerülnek és elbuknak, biztonsági hiányosságaik miatt. Minél nyitottabban és minél könnyebben, egyszerűbben, történik a hálózatokhoz való kapcsolódás, annál nagyobb a támadási potenciál is.

A Gartner jelentése szerint 2015-ben majdnem 5 millió eszköz kapcsolódott már az internethez, és ez a szám 2020-ra 4-szeresére, 21 millióra nő majd az előrejelzések szerint. (Gartner, 2015c) A felhasználók egyre több olyan eszközt fognak használni, amely adatokat küld és fogad, azért, hogy növeljék a felhasználói élményt és egyszerűsítsék az elvégzendő feladatokat. A kulcsszó az egyszerűség, az egyre okosabb eszközök világában a felhasználók nem akarják tudni, mitől működnek az okos eszközök, egyszerűen csak használni akarják őket, úgy, ahogy kivették a dobozból, lehetőleg minél kevesebb beállítással, konfigurálással, ez pedig jelentős terhet ró a biztonsági szakemberekre, hogy ezen igények ellenére, már a dobozból kivéve is elfogadható biztonsági szintet

biztosítsanak ezen eszközöknek a teljesen laikus felhasználók kezében is. A túlzott egyszerűsítés a másik oldalon is megbosszulja magát, hiszen így a szakértő felhasználó kezébe viszont nem kerülnek azok a beállítási lehetőségek, amelyekkel az adott eszközt, egy egységes, testre szabott biztonsági rendszer részévé tehetné, így ezen eszközök egy vállalati környezetben, mindig is ki fognak lógni a többi közül, hiszen nem lehet esetükben ugyanazokat a biztonsági előírásokat és követelményeket alkalmazni, mint a hagyományos informatikai eszközök esetében.

Az IoT nem csak a felhasználókat érinti, az ipar, az üzlet és a kormányok is befektetnek és részt vesznek az ágazat bővítésében, hogy javítsák az emberek életminőségét és erősítsék saját pozícióikat. Ezt a folyamatot sokan, például a német Szövetségi Oktatási és Kutatási Hivatal (Zaske, 2015) a 4. ipari forradalomként jegyzi. Véleményük szerint okos eszközök kerülnek kifejlesztésre okos folyamatok által. Egy jelenlegi iparágat okos iparággá alakítani azzal jár, hogy IoT alapú megoldásokra és a kiegészítő szolgáltatásokra kell alapozni a további fejlesztéseket. A legfontosabb érintett iparágak az energiaszektor, az egészségügy és a fenntartható közlekedés.




**1. ábra: Az „ipar 4.0" koncepció bevezetésének legfőbb akadályai (McKinsey, 2015)**

Ha már a 4. ipari forradalomról (Castro, 2015) van szó, a robbanás gátja éppen azok a kérdések, azok a határok, amelyeket az üzleti szektor még vonakodik átlépni, ezek között az egyik legfontosabb az adatvédelem és biztonság kérdésköre. Ezen a területen ki kell dolgozni a megfelelő válaszokat, hogy a vállalatok tömegével merjenek a következő szintre lépni. A biztonság megtermése ezen a területen a következő évek legnagyobb kihívását fogja jelenteni.

## 2.1. Viselhető eszközök

Nagyon sok sérülékenység érinti ezeket az eszközöket, amelyeken keresztül a támadók adatokat lophatnak el akár a viselhető eszközről, akár az eszközön keresztül a kapcsolódott okostelefonról. (SC Magazine, 2015) Az általánosan alkalmazott Bluetooth smart protokoll a közös pontja minden ilyen eszköz csatlakoztatásának. A protokoll sérülékenységei minden csatlakoztatott eszközre kihatnak. Számos biztonsági incidens fordult már elő, mind Android, mind Apple alapú eszközök esetében. Az egyik legnevezetesebb eset az Apple Watch piacra kerülése után volt, egy szoftver sérülékenységnek köszönhetően (Woollaston, 2014) a támadó a bluetooth pinkódos védelme (Daws, 2014) ellenére leválaszthatta és egy másik IP-re csatlakoztathatta az órát minden nehézség nélkül.

## 2.2. Okos otthonok

Az IoT alapú technológia lehetővé teszi, hogy az egyes mindennapi eszközök a háztartásban összekapcsolódjanak egymással, az okostelefonokkal és a számítógépekkel. Ezáltal növekszik a technológiai élmény és az egyes eszközök hatékonysága is javul. A magas szintű kapcsolatok itt is adatvédelmi és IT-biztonsági kérdéseket vetnek fel, kombinálva akár a fizikai biztonság kérdéseivel, ha az intelligens zárakra, riasztó rendszerekre, tűzjelzőkre gondolunk. A személyes adatok mellett a kommunikációs protokollokat az alkalmazásokat és az operációs rendszereket is védeni és rendszeresen frissíteni szükséges.

2014 végén a HP jelentetett meg egy átfogó kutatást arról, hogy milyen okos eszközök jelenhetnek meg egy háztartásban és milyen típusú támadásoknak lehetnek ezek kitéve. (Oh, 2014) a kutatás sorra veszi az okos TV-ket, termosztátokat, IP-kamerákat és számos más eszközt, ezek az eszközök mind internetkapcsolattal rendelkeznek és egy biztonsági incidens esetén az egész család személyes adatai és műszaki megoldásai veszélynek lehetnek kitéve. (Thomas, 2015a) Egy okos hűtőn vagy televízión keresztül a támadók megszerezhetik a Google fiók hozzáférési adatait, de akár távolról vezérelhetnek egy bébi légzésfigyelő monitort, amin keresztül behatolhatnak az otthoni hálózatba. (Ellison, 2015)

Ahogy már korábban is említésre került a technológia rohamos fejlődésével, az eszközök okosodásával a biztonsági szintjük a legtöbb esetben nem tart lépést, különösen a kisebb értékű eszközök esetében, amelyek ugyanúgy kaput nyithatnak egy esetleges támadó számára. A válasz mégsem a technológiától való félelem kell, hogy legyen, hanem a biztonság tudatosság növelése, az otthoni hálózatok magas szintű, eszközök feletti védelme céleszközökkel (router, tűzfal, stb.) Az innováció most kezd el a biztonság irányába is fejlődni, a gyártók egyre inkább felismerik, hogy a tömegesen hálózati kapcsolattal

rendelkező eszközök világában, ma már a biztonsági kérdések, illetve az erre adandó megfelelő válaszok kihangsúlyozásával tudnak versenyelőnyhöz jutni.

### 2.3. Okos világ

Az összekapcsolt eszközök problémája természetesen nem szűnik meg az otthonok határain kívül. Az üzleti, ipari és kormányzati alkalmazások is az egyre erősebb összekapcsoltság felé fejlődnek, eszközök, rendszerek és szolgáltatások szintjén is. A közlekedésirányítástól a piackutatásig rengeteg megoldás épül ma az összekapcsolt eszközök hálózatára, de biztonsági téren sokszor itt sem jobb a helyzet, mint az otthoni felhasználók esetében. Az ipari IoT egyik célja, hogy olyan önirányító rendszereket hozzon létre, amelyek a technológiai interakciókból új információt és szolgáltatásokat képesek előállítani. (ESET, 2015) A cél elérése érdekében több vállalat tűzött ki díjakat biztonsági szakemberek számára, hogy keressenek hibákat, sérülékenységeket e rendszerekben. 2015 során számos törekvés indult el, hogy az IoT világában egységes szabványok és szabályozások jöjjenek létre, amelyek lehetővé teszik nagyobb területeken, az emberek tömegeinek életét befolyásoló alkalmazásukat (pl. okos városok). A német kormány Ipar 4.0 kezdeményezése mellett az Európai Információbiztonsági Ügynökség (ENISA) is adott ki ajánlásokat az okos infrastruktúrák fejlesztése és üzemeltetése tekintetében. (ENISA, 2015)

2016 még tovább lépett a kihívások területén: távolról vezérelhető autók, biztonsági rések a drónok rendszereiben, vagy épp az otthoni felhasználók hálózatainak egységesített védelme. Minden hálózatra kapcsolat eszköz ellenőrzése és megfelelő biztonsági szintjének biztosítása a következő évek iparági szabványainak és jogalkotásának legfontosabb feladatai közé tartozik.

Szét kell választani azokat az eszközöket, amelyekre a felhasználó is telepíthet célzott biztonsági megoldásokat (okostelefonok, tabletek, számítógépek) azoktól a céleszközöktől, amelyek zárt rendszerében a gyártóknak kell garantálni a megfelelő biztonságot (hálózati eszközök, viselhető eszközök, okos háztartási gépek). Különösen fontosak az otthoni hálózati kapcsolatokat létrehozó routerek, amelyek szoftverfrissítése, vagy akár a gyárilag beállított jelszó megváltoztatása nem kötelező a felhasználó számára, viszont ezek képviselik az otthoni hálózatok legmagasabb szintű védelmét, amely megfelelő erőssége esetén a csatlakoztatott eszközök biztonsági réseit is képes elfedni a külvilág elől. Így ezen eszközök biztonsági szintjének növelése, akár a felhasználók aktívabb bevonásával a következő évek egyik legfontosabb prioritása kell, hogy legyen.

A probléma a vállalatok esetében is fennáll, hiszen a megfelelő konfigurációs lehetőségek hiánya, a biztonsági megoldások utólagos alkalmazhatatlansága a vállalati hálózatokat is

veszélybe sodorja, amikor a felhasználók a BYOD jelenségnek megfelelően a saját eszközeikkel jelennek meg a munkahelyi hálózatokban.

A támadások spektruma jelenleg a célzott támadásoktól a rosszindulatú kódok tömeges terjesztéséig bármilyen formát ölthet, egy azonban közös, minden esetben az eszközök, rendszerek valamilyen sérülékenységét használja ki a támadó.

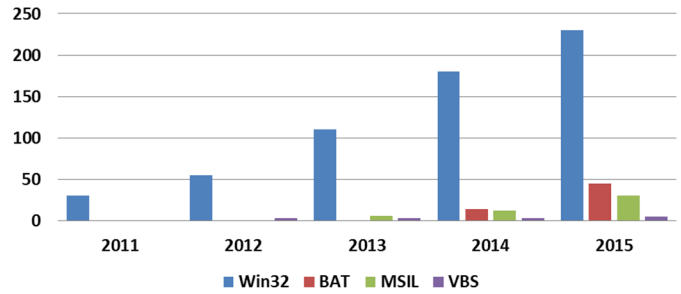
### 3. Zsaroló vírusok

Az egyik legfőbb informatikai biztonsági kockázatokat még a mai napig is a kártékony kódok jelentik, az 1986-ban megjelent első vírusoktól, a mai igen kifinomult és összetett malware-ekig. Ezek közül az egyik legújabb ágazat igen komoly problémákat okoz az utóbb időben, mind az otthoni, mind az üzleti és az állami intézmények felhasználóinak.

Az elmúlt év során a zsaroló vírusok szerepe különösen jelentősen megemelkedett, az érintett felhasználók számának ugrásszerű növekedésével egyetemben. Ez a támadási forma, mivel most került a sajtó nyilvánossága elé, innovatívnak tűnik, de valójában nem az, valójában az első zsaroló vírus több mint 25 éves, az „AIDS trójai" annak idején minden fájlnevet titkosított a C-meghajtón használhatatlanná téve ezzel a gépet, az érintettektől pedig 189 dolláros díjat követelt „licensz megújítás" címen. (Mendoza, 2015) Az azóta eltelt időben a titkosítási formák (szimmetrikus és aszimmetrikus kulcsú) és a kulcshosszok is folyamatosan változtak, fejlődtek, de az elv megmaradt, akár a 2005-ös Windows-os GP Coder-t, akár a 2013-as androidos CryptoLockert tekintjük. (Lipovsky, 2013)

A zsaroló szoftverek működési mechanizmusa egyszerű: állományokat titkosítanak a célgépen, amelyek feloldásáért a tulajdonosnak fizetnie kell, ez megakadályozhatja a hozzáférést bizonyos adatokhoz, de rendszerfájlok titkosítása esetén az egész rendszer működését ellehetetlenítheti. E kártékony szoftverek mögött mindig áll valamilyen bűnözői csoport, hiszen a váltságdíjat valakinek be kell szednie és a titkosítást fel kell oldania. Bár előfordulnak hibák, pl. hogy a váltságdíj ellenére sem tudta feloldani a kód tulajdonosa a titkosítást egy programhiba miatt, vagy épp a gyenge titkosítás miatt váltságdíjfizetés nélkül is visszaállíthatók a fájlok megfelelő szakértelemmel.

Ami jelentősen változott az a módszer és a szervezettség: szervezett bűnözői csoportok már szolgáltatásként kínálják a zsaroló vírusokat (Ransomware as a Service - RaaS). A konstrukció keretében olyan eszközöket kínálnak, amelyek segítségével automatikusan generálhatók zsaroló vírusok, technikai felkészültség sem kell hozzá. (Osborne, 2015) Ugyan csak a közelmúltban jelentek meg hírek a „Hidden Tear" nevű nyílt forráskódú zsaroló szoftverről, ahol az alap kódot szakértelemmel tetszőleges irányba lehet módosítani, végtelen számú mutációt létrehozva. (Paganini, 2015)




**2. ábra: A fájlkódoló malware változatok száma (ESET, 2015)**

Pontosan a variációk számának exponenciális növekedése teszi óriási problémává a zsaroló szoftverek kategóriáját az utóbbi időben. A legmagasabb éves növekedési ráta természetesen a Windows-hoz köthető variánsoknál mutatkozik, de egyre több kártékony kód jelenik meg OS X-re, Androidra, iOS-re, de a professzionális operációs rendszerek, mint a VBS, Python, BAT vagy a PowerShell sem maradnak ki, ami világosan mutatja, hogy a bűnözők az otthoni felhasználók mellett, a cégeket, szervezeteket is célba vették.

A mobil eszközökön sok esetben nem is a fájlok titkosítása a cél, az első androidos zsaroló vírusok végtelen ciklust idéztek elő a képernyőn, ami folyamatosan a váltságdíjkérő üzenetet mutatta, ez kis szakértelemmel könnyen megkerülhető volt, a következő generáció már a telefon saját biztonsági megoldásait, lezáró kódjait módosította, ami root jogok nélkül, vagy már a fertőzés előtt (!) telepített biztonsági szoftverek nélkül nagyon nehézzé tette a megkerülésüket. Végül elérkeztünk a jelenlegi generációhoz, ami ugyanúgy fájlokat is titkosít, mint a hagyományos számítógépek esetében, akár 2048 bites RSA nyilvános kulcsú algoritmusokkal, a TOR anonim hálózatán kommunikál és anonimizált kriptovalutában (bitcoin és variánsai) kéri a váltságdíjat.

2015-ben megjelentek a TrojanDownloader-ek és a Ransomware hibridek, ami világosan mutatja, hogy a kártevő fejlődése és a megfertőzött eszközök számának növekedése még korántsem ért véget

E kártevőtípus azonban nem áll meg az számítógépeknél és az okostelefonoknál, az utóbbi hónapokban számos esetbe kerültek a támadások célkeresztjébe az okosórák és televíziók, főleg az Android alapú szoftverrel rendelkezők. A zsarolóvírusok tehát elindultak az IoT világa felé, ami annak fényében, ami az okos otthonok, háztartási gépek, autók kapcsán előkerült az előző fejezetben, előrevetíti, hogy mekkorára is nőhet ez a probléma a jövőben, gyakorlatilag bármi, amiben CPU van és hálózatra kapcsolódik, valamint tartalmaz valamilyen szoftvert, vagy firmware-t, megfertőzhető, és így a támadások célpontjává

válhat. Ez esetben a támadó korlátozza az adott eszköz használhatóságát és váltságdíjat kér az eredeti állapot visszaállításáért.

Az is tendencia sajnos, hogy a támadók adott esetben visszatérnek. Ezek a szoftverek olyan maradványokat hagynak a rendszerekben, amivel egyéb járulékos károk (pl. adatlopás) is előidézhetők, valamint a zsaroló eszköz egy idő múlva visszatér, és újra zárolja a rendszert, hacsak nem sikerül gyökeresen, pl. egy teljes tiszta rendszer újratelepítéssel megszabadulni tőle.

A védelmi szoftverek mellett, a szigorú és átgondolt backup-politika lehet a legfőbb ellenszere annak, hogy ezek a típusú támadások túlzottan nagy károkat okozzanak a szervezetek, illetve a felhasználók számára.

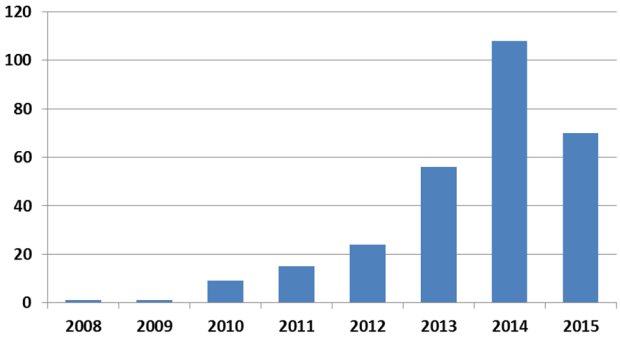
A célpontok közül természetesen a közművek, egészségügyi és kormányzati rendszerek sem maradnak ki. Több kórházban okozott már leállást külföldön, hogy a hálózatba kötött intelligens orvosi eszközök (CT, MR, szívpuma, stb.) lettek zárolva, míg a kórházi adminisztrációs rendszert már Magyarországon is érte sikeres támadás. A betegellátási protokollok miatt mind a hazai, mind a külföldi esetekben ez az ellátás teljes leállását jelentette az érintett osztályokon, bár közvetlen életveszélyt legalább nem idézett elő.

Ha komolyan vesszük a Gartner előrejelzését, hogy 2020-ra várhatóan 21 milliárd online eszközzel fogunk rendelkezni (Gartner, 2015c), akkor látható, hogy a bűnözésnek és az IT-biztonsági kockázatoknak ez a sajátos keverék területe, miért jeleni a jövő egyik legnagyobb kihívását IT-védelmi szempontból.

## 4. Célzott támadások

Az utóbbi években több olyan támadássorozat is megvalósult, amelyet a szakemberek APT (Advanced Persistent Threat) kategóriába soroltak. Amikor ezt a kategória elnevezést használják, akkor nem a hagyományos rosszindulatú kódokról beszélnek, amelyek célja, a minél szélesebb körben való elterjedés és fertőzés, hanem valami sokkal specifikusabbról. Az APT-k személyre szabott megoldásokat igényelnek a biztonsági cégek részéről is és az üzleti szféra előtt álló egyik legnagyobb kihívást jelentik. Hiszen testre szabottan, az adott rendszer feltérképezése után, annak gyenge pontjaira készítik fel őket a támadók, sokkal nehezebbé téve ez által a védekezést és a felderítést. (ESET, 2015)

2015-ben a GitHub összegyűjtötte a 2008 óta történt APT-ket, célzott támadásokat és „szponzorált malware”-eket (amikor kormányok támogatják a kártékony kódok elkészítését és alkalmazását). a 8 év során 291 célzott támadássorozatot gyűjtöttek össze, amelyek vállalatok, szervezetek vagy kormányok ellen irányultak. ebből 73 2015-ben zajlott, ami a 2014-es számokhoz képest 2×-es szorzót jelent. (Github, 2015)




**3. ábra: Az APT-k számának alakulása (Github, 2015)**

A támadások eredménye sok esetben széle körű vitákat eredményezett a biztonsági iparban a kiszivárgott információk jellege miatt. Az egyik legkomolyabb ilyen incidens a Hacking Team szervereinek meghekkelése volt, amikor is 400 Gb adat került nyilvánosságra a technológiákról és az ügyfelekről. A Hacking Team egy biztonsági vállalat, amely kormányoknak és vállalatoknak fejleszt elektronikus megfigyelési eszközöket, szoftvereket. (Albors, 2015) Az adatszivárgás azt eredményezte, hogy a Hacking Team által felfedezett és a megfigyelésekhez felhasznált sérülékenységeket, igen gyorsan beépítették a különböző kiberbűnözők támadási repertoárjukba, illetve kártékony szoftvereikbe.

Az Ashley Madison (társkereső házasoknak) mintegy 37 millió ügyféladatának kiszivárgása is óriási hatással volt ezen ügyfelek további életére. A támadók eredeti célja az volt, hogy a cég fejezze be a működését, miután ezt a követelést nem teljesítette, nyilvánosságra hozták az adatokat, amely kiterjedt zsarolási és fenyegetési hullámot indított el az áldozatok irányába a különböző bűnözői csoportok és ügyeskedők részéről. (Thomas, 2015c)

Ez csak két reprezentatív példa azokra a támadásokra, amelyek kifejezett, pontos céllal történtek és nagy ívű hatást értek el.

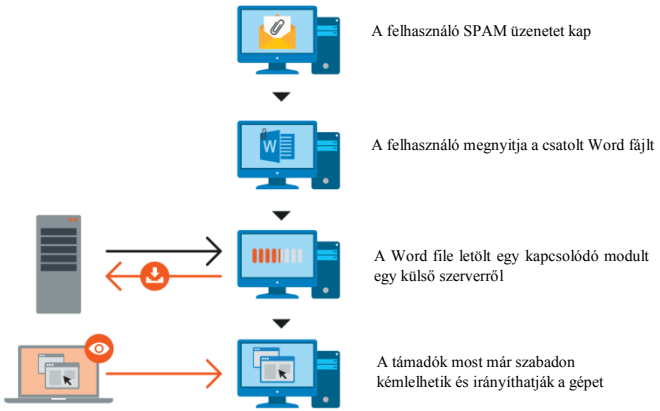
### 4.1. Kódkészletek kiberkémkedéshez

A Potao malware család 2011-ben jelent meg először, azóta komoly fejlődést, és több hasonló kezdeményezést (Babar, Bunny, Dino, Casper, …) is találunk. Itt már nem egyetlen célra kifejlesztett, jól definiálható kártékony eszközről van szó, hanem egy konfigurálható készletről, amelye a támadó céljainak (bizalmasság/sértetlenség/rendelkezésre állás) a támadás típusának (távoli/helyi) megfelelően ad különböző eszközöket a potenciális támadók kezébe. Megvannak a megfelelő eszközök az internetes terjesztéshez, de a pendrive-okon keresztül fertőző kódok elkészítéséhez is, az eredmény lehet egy keylogger, vagy épp bankkártya adatokra és belépési kódok lopására szakosított eszköz. Ukrajnában,

Iránban Szíriában, a Független Államok Közösségében gyakran felbukkannak ezek az eszközök bűnözők, de kormányzati ügynökségek eszköztárában is. (CSEC, 2011)

Rendszer-specifikus támadások

A támadások sok esetben egészen konkrét sérülékenységeket és réteget céloznak meg. Az egyik legemlékezetesebb ilyen fertőzés 2014-ben a Buhtrap (Paganini, 2016) volt, amely a Microsoft Word egy adott sérülékenységét (Microsoft, 2012) aknázta ki sikeresen mintegy 3 éven keresztül a felfedezéséig. A Célpontok kifejezetten az orosz bankok voltak, a kártevő csak a word orosz nyelvű verzióit fertőzte és kifejezetten netbanki rendszerek voltak és terjesztés teljesen legális weboldalak megfertőzésén keresztül történt. A mintázatból látható, hogy az ilyen típusú támadások egészen specifikus és kifinomult módon tudnak hatni a célpontjukra, jelentősen csökken az esély a felfedezésre, és ezáltal a lehető leghosszabb ideig tudnak működni. Különösen igaz ez, ha a támadások web-szerverek, vagy más hálózati szolgáltatások ellen irányulnak.




**4. ábra: Egy Buhtrap fertőzés felépítése (ESET, 2015 alapján)**

## 4.2. Az APT-k mint fegyverek

Egyetlen vállalat vagy kormány sem lehet biztos abban, hogy mikor válik egy ilyen célzott támadássorozat célpontjává, éppen ezért a folyamatos készültség a biztonsági eszközök alkalmazása elsődleges fontosságú, függetlenül attól, hogy a támadások célzottak vagy sem, a védelmi eszközök működnek. Nyilván egy jól előkészített célzott támadás már figyelembe veszi, feltérképezi a védelem főbb pontjait is és igyekszik ezzel együtt sikeres

lenni, de a megfelelően felépített biztonsági rendszer mindenképpen jelentősen megnehezíti a támadók dolgát és növeli a felfedezés valószínűségét.

Az IT-biztonság tehát egyre erősebben üzletmenet folytonossági kérdéssé válik, mind a vállalatok, mind az állami szolgáltatások esetében. Emiatt a megfelelő IT-biztonsági hozzáállás egyre inkább a proaktív megközelítés: a védelmi lehetőségek és a kockázatok gondos felmérése, a felhasználók megfelelő szintű felhatalmazása és a folyamatos képzés, néhány a legfontosabb intézkedés közül, amit meg kell tenni a hatékony IT-biztonság érdekében.

De hogyan lehet megvédeni egy szervezetet egy célzott támadástól, aminek a lehetőségéről sem tudunk addig, amíg be nem következik? A védekezés nem egy projekt, hanem egy folyamat. A védelmi megoldások, mind a végpontok, mind a szerverek és a fizikai biztonság területén folyamatos fejlesztésre és szakértői tesztelésre szorulnak. A titkosítás segít megőrizni az érzékeny adatokat, és nem túl gyakori, főleg a KKV-k szintjén, így a támadót meglepheti. Természetesen a menedzsment és az alkalmazottak folyamatos képzése, az IT-biztonsági kérdések saját szintjükön való tudatosítása szintén kulcsfontosságú része a feladatnak. Más szavakkal a menedzsmentnek meg kell értenie a biztonság szerepét és jelentőségét, hogy biztosítani tudja az üzletmenet folytonosságát és megfelelő döntéseket hozzon a biztonságba és a védekezésbe való befektetésekről. Ezzel együtt a felhasználók és az alkalmazottak biztonság tudatosságát is folyamatosan fenn kell tartani és a javítani kell, információs anyagok, képzések, workshopok, gyakorlatok keretében. Ez nem csak az incidensek elkerülésében segít, de egy esetleges incidens esetében jelentősen csökkenti a reakcióidőt, amely a támadás elhárításához szükséges.

## 5. Crimeware, malware – a „hagyományos" veszélyek

Minden felhasználó és szervezet legnagyobb és legáltalánosabb félelme, hogy kártékony kódok kompromittálják a rendszereiket, hozzáférnek, ellopják, vagy megsemmisítik értékes és/vagy érzékeny/bizalmas adataikat. Ez a félelem nem alaptalan, naponta jelentenek be újabb és újabb kártékony kódokat, amelyek működése és céljai egyértelműen a kiberbűnözés világához vezetnek, ezeket nevezzük crimeware-eknek. (Panda, 2011) A különböző IT-biztonsági cégek jelentéseiben naponta bukkannak rá újabb potenciális veszélyekre. Természetesen a támadások típusai folyamatosan változnak, fejlődnek, agresszivitásuk és hatásfokuk is egyre fejlődik. Például az Europol Internetes Szervezett Bűnözés Elleni egysége (IOCTA) fedezett fel olyan zombi gépekből álló hálózatokat, amelyek célja a zsaroló vírusok minél szélesebb körben való elterjesztése volt. (Europol, 2015) De történt olyan eset is amikor egy kiberbűnözői csoport klasszikus fizikai fenyegetéssel próbálta rávenni a biztonsági cégeket, hogy ne publikálják, az általuk készített kártevőkről szóló információkat. (KrebsonSecurity, 2015)

Amikor klasszikus malware járványokról beszélünk, akkor nem a célzott támadásokat értjük alatta. Ez esetben a rosszindulatú kód célja, hogy válogatás nélkül, minél szélesebb körben terjedjen és annyi információt lopjon el a felhasználóktól, amennyit csak lehetséges. Az ilyen járványok e-mailben, cserélhető meghajtókon, fertőzött, nagy forgalmú weboldalakon keresztül terjednek. A gyors, nagy volumenű terjedés és a kód folyamatos változása, mutációja teszi nehézzé az e fenyegetések elleni harcot.

A kiberbűnözői szektor is rétegződik, specializálódik, kialakulnak különböző csoportok, akik vagy az infrastruktúrát biztosítják, vagy programoznak, vagy épp más bűnözői csoportoknak értékesítik a kész eszközöket, mintegy szolgáltatásként. Szakosodnak, ki online bankokra, ki bankkártyákra, ki online játékok belépési kódjaira és így tovább… (Horváth, 2011b)

Bár a klasszikus fertőzések ellen nagyon sok biztonsági cég küzd, tulajdonképpen ez teszi ki a feladataik lényegét, a bűnözők mégis mindig újabb és újabb csatornákat találnak, amin keresztül elérhetik a felhasználókat.

Fontos hangsúlyozni, hogy ezek a járványok nem csak az otthoni felhasználókat érintik, a kis és közepes vállalatok ugyanúgy megfertőződhetnek, de még a nagyvállalatok sem teljesen mentesek a veszélytől. A Ponemon 2015-ös jelentése alapján ezeknek e biztonsági incidensek átlagköltsége mintegy 7,7 millió dollár volt, de volt olyan vállalat, amely mintegy 65 millió dollárt vesztett a 2015-ös incidensek során. (Ponemon, 2015c)

### 5.1. Botnetek, zombi hálózatok és világjárványok

Zombi számítógépes hálózatok, amit botneteknek neveznek évek óta a legfontosabb infrastrukturális alapot biztosítják a kiberbűnözői csoportok működéséhez. A különböző zsaroló vírusok, SPAM-ek, DoS támadások, adatlopások műszaki alapjait, terjesztik a kártékony kódokat, biztosítják a számítási kapacitásokat és erőforrásokat.

A biztonsági szolgáltatók legfontosabb feladata, hogy beazonosítsák a botnet hálózatok működésére utaló mintázatokat, felfedezzék az adott hálózatok kapcsolatait és blokkolják, leválasszák őket a tiszta hálózatokról. Fontos, hogy az ilyen hálózatokba irányuló kommunikáció is beazonosítható és blokkolható legyen a biztonsági szoftverek által.

Ha a kifejezetten adatlopásra szakosodott botnet hálózatokat vizsgáljuk, van olyan amely kifejezetten egy adott országot céloz, pl. a Liberpy, amely Dél-Amerikában, 96%-ban Venezuelában fertőzött. De vannak olyan hálózatok, amelyek nem állnak meg az országhatároknál, 2015-ben a Waski célja az volt, hogy világszerte annyi gépet fertőzzön meg, amennyit csak lehetséges és trójai vírusokkal fertőzött mellékletekkel ellátott e-maileket küldjön szét, amelyek semmi mást nem csinálnak, csak továbbterjesztik a

fertőzést. Az e-mail csak az egyik lehetséges csatorna a fertőzés terjesztésére, az elmúlt évek során a másik legfontosabb médium a káros makrókkal fertőzött Microsoft Office dokumentumok voltak.

Az olyan klasszikus fenyegetések, mint a trójai programok, amelyek banki adatokat lopnak a felhasználóktól, szintén jelen voltak. Azonban ezek a fenyegetések is folyamatosan fejlődnek, újabb funkciók és családok jelennek meg. Újabb eszközök fertőződnek meg, webkamerák, routerek, bármilyen hálózatba között, vezérlő szoftverrel rendelkező eszköz célpont lehet. 2015-ben a PoSeidon vírus a kártyaelfogadó PoS terminálokat fertőzte meg, a terminál memóriájából és kifelé irányuló kommunikációjából igyekezett kigyűjteni a kártya adatokat. A nagy kereskedelmi láncok, mint a UPS vagy a Home Depot sem maradtak le a fertőzöttek listájáról, a támadók hitelkártya adatok millióit szerezték meg ezen célpontoktól. Máskor a támadók weboldalak hibáit használták ki vagy épp maguk hoztak létre hamis játék-oldalakat a kártékony kódok terjesztésére. Sikeres támadások történtek CMS pluginek sérülékenységeit kihasználva, ami által a támadók több ezer weboldalt tudtak felhasználni a kártékony kódok terjesztésére.

### 5.2. A megoldás az összefogás

Ezeket a hálózatokat csak globális szintű összefogással lehet semlegesíteni. Az országhatárokon átívelő fertőzések megállítását csak több ország biztonsági cégeinek és nyomozó hatóságainak együttműködése tudja elérni, pl. a Darkode szervezet felgöngyölítésekor, ahol 18 országban 62 letartóztatásra került sor egy időben. (Cobb, 2015a)

A kiberbűnözés fejlődése folyamatosan fenyegeti a felhasználókat, a támadások egyre hatékonyabbá válnak. A bűnözők folyamatosan követik a legújabb sérülékenységeket, különösen a 0. napi fenyegetéseket, és igyekeznek kihasználni belőle annyit, amennyi lehetséges, mielőtt a javítások megérkeznek. A nemzetközi együttműködés, biztonsági cégek, kormányok, hatóságok között az egyetlen lehetőség a veszély visszaszorítására és az felhasználók internetbe vetett bizalmának helyreállítására. A vállalatok a kiberbűnözés állandó fenyegetésének hatására 4,7%-kal növelték biztonsági költéseiket 2015 során. (Gartner, 2015b) A védekezésnek legalább olyan szervezettnek kell lennie, mint a bűnözőknek, hogy eredményes legyen.

## 6. Tudatos aktív támadások

Az eddigiekben a különböző szoftverek, kártékony kódok által képviselt fenyegetést vettük górcső alá. Ezek, még ha tudatos, célzott támadások is, mégiscsak valamilyen szinten automatizáltak, miután a kártékony kód bejutott a célrendszerbe, annak kell elvégezni a feladatát. Léteznek azonban olyan támadások is, amelyek folyamatos személyes közreműködést igényelnek. Ezeket közkeletű néven gyakran hekkelésnek nevezik, a biztonsági terminológiában a hekkerek tevékenysége felé mutatott sebezhetőségeket a haxposure névvel illetik. Különösen akkor, ha rendszerfeltörés és adatlopás típusú bűnelkövetés, magas társadalmi kitettséggel, tovagyűrűző társadalmi, gazdasági, politikai következményekkel jár együtt. Olyan példák tartoznak ide, mint pl. az Ashley Madison eset, amikor a célzott adatlopásnak és az adatok nyilvánosságra hozatalának, súlyos, számos résztvevő életét, társadalmi státuszát, karrierjét negatívan befolyásoló következménye lett. Hasonló területet képviselnek a Wikileaks szivárogtatásai, ahol az alapanyag sok esetben hasonló kiberbűnözésből eredő forrásból származik, az adatok nyilvánosságra hozatala, pedig akár nemzetközi szintű politikai és gazdasági botrányokat, változásokat tud előidézni.

Mindezzel együtt a támadás célpontjául választott cég vagy szervezet jó hírneve is jelentősen csorbul, üzleti modellje ellehetetlenedik, vagy legalábbis jelentősen sérül, ami sok esetben az egész vállalat gazdasági ellehetetlenüléséhez vezet.

Az Ashley Madison mellett, a Hacking Team nevű biztonsági szervezet adatainak ellopása és nyilvánosságra hozatala, arra derített fényt, hogy az általuk forgalmazott hálózati megfigyelési eszközöket és technológiát elnyomó, diktatórikus kormányok és szervezetek számára is árusították, sőt célzott megrendelésre is dolgoztak, ilyen klienseknek. Természetesen ez az információ teljesen aláásta a szervezet piaci jó hírnevét. (Albors, 2015) Az Ashley Madison esetében pedig kiderült, hogy cég – ígérete ellenére – az adatbázisból soha nem törölte véglegesen a profiljuk törlését kérő felhasználók adatait, noha ezért a szolgáltatásért külön díjazást is beszedett tőlük. Ez természetesen teljes mértékben aláásta a cég szavahihetőségét és a felhasználó szerződés megsértése miatt számos per indult a vállalat ellen. (O'Brien, 2015)

Mindkét esetben a támadás célja látszólag az adott vállalat üzleti modelljének megtörése, működésének ellehetetlenítése volt olyanok által, akik az eredeti célokkal és a megoldásokkal nem értettek egyet. Hasonló motivációk érzékelhető a Sony Pictures évekkel korábbi feltörésekor is, amikor a cég belső levelezésre került napvilágra. Legyen bár politikai vagy morális oka a nevezett vállalatok megtámadásának, ez mindenképpen túlmutat a korábbi, egyszerű anyagi haszonszerzésen alapuló támadási kultúrának, amely együttműködés esetén legtöbbször diszkréten, a nagyközönség kizárásával zajlik. Itt a

szakma sok esetben a hacktivism, vagyis a hekker és az aktivista szavak összevonását használja, ezzel akarva utalni, hogy itt a támadásoknak valami magasabb rendű célja (is) van, mint az egyszerű anyagi haszonszerzés. (Cobb, 2015b)

Az egy teljesen más szint, amikor egyáltalán nincs anyagi jellegű követelés, csak tisztán az elvek mentén történi a szenzitív adatok nyilvánosságra hozatala, a támadók viszont ebben az esetben sem látják át, vagy egyszerűen nem érdekli őket, hogy a cég, az általa képviselt működési mód, az üzleti modell sikeres megtámadásával, hogy egyszerű alkalmazott vagy felhasználó életére lesznek erősen negatív befolyással.

Minden olyan cégnél, ami titkos és érzékeny adatok generálására, tárolására, gyűjtésére építi az üzleti modelljét, felmerül ez a kockázat. Az ilyen adatok napvilágra kerülése természetesen negatív hatással van a vállalat hírnevére, bevételére és értékére.

Az alábbi okok jelentősen növelték az utóbbi időben a kockázatát annak, hogy a hasonló üzleti modellt követő vállalatok ilyen támadások áldozatává váljanak:

- Hozzáférés a szolgáltatásokhoz

  A rendszerek feltörésének tudománya egyre jobban terjed, ma gyakorlatilag bárki felbérelhet egy hekkert. Gyakorlatilag mindenkinek rendelkezésre áll a hozzáférés a megfelelő tudású „szakemberekhez”.

- Nyílt működés

  Ha valaki digitális eszközökkel, tartalmakkal üzletel, és az internet mint csatorna jelen van az üzleti modellben, akkor előbb-utóbb annak részletei is ki fognak derülni. Ha kétes vagy kockázatos termékek és szolgáltatások tartoznak egy interneten működő cég portfoliójába, azokat hosszú távon szinte lehetetlen titokban tartani.

- Publikációs platformok

  Az olyan felületek, minta Wikileaks vagy a Pastebin szervezett teret adnak a kiszivárgott információk publikálásának. Ezek a platformok megfelelően védik forrásaikat, így a szivárogtatók kockázatai jelentősen csökkennek, ha ezeket választják.

- Szenzációéhség

  A közösségi média az elsődleges platform, hogy teret adjon – és fel is erősítse – a nyilvános felháborodásnak, ami vonzóvá teszi ezt a médiumot is a szivárogtatók számára, hiszen az adatok elterjedési sebessége és a kiváltott hatás is megtöbbszöröződhető általa.

- Az összetettség a titkosság és biztonság ellenfele

  Nagyon nehéz megtartani a digitális formában tárolt titkokat, különösen nehéz ezt megtenni, komplex, összetett, bonyolult informatikai rendszerek esetében, ahol a számos alkalmazott komponens többszörözi a feltáratlan, kijavítatlan sérülékenységek lehetőségét, ezáltal pedig a támadási potenciált. A digitális formában tárolt titkokat természetesen sokkal könnyebb is kimenteni a szervezet határain túlra, hiszen elég egyetlen kifelé irányuló kommunikációs szál, vagy egy aprócska fizikai adathordozó tetszőlegesen nagy tömegű adat továbbításához.

Ezzel párhuzamosan mik a védekezés lehetőségei:

- Itt sem lehet eléggé hangsúlyozni az erős védelmi rendszereket: **azonosítás, malware-védelem és titkosítás**, ezek a kulcsterületek
- **Biztonsági mentés** és **katasztrófa elhárítási tervek**
- **Azonnali reagálási tervek** biztonsági incidensek esetére
- **Belső ellenőrzés** (egy jól értesült és a rendszert ismerő belső ember veszélyesebb, mint sok ezer külső támadó, ld. pl. Showden-botrány)
- **Kockázatfelmérés**: a biztonsági politika tisztában van az üzletmenet, az üzleti modell ilyen irányú kitettségével, és vannak megfelelő válaszai erre?
- **Működési tudatosság**: tisztában van a szervezet azzal, hogy a folyamatok mely pontjain áll fenn a támadás veszélye?
- **Belső átláthatóság**: a titkos információkkal dolgozó szervezetek hajlamosak önmaguk előtt is titokban tartani sok mindent, természetesen ez csökkentheti a belső fenyegetéseket, viszont oda vezet, hogy senki nem látja át teljes egészében a belső működést. Így a kockázatokat sem, egy esetleges incidens esetén, pedig nem lesz senkinek teljes képe arról, mi is van veszélyben, mit, hogyan kellene megvédeni, hogyan kellene egyenszilárdságú védelmet létrehozni a teljes szervezet számára.

Ha néhány nagyvállalat, akiket hasonló támadás ér, és el tudják azt hárítani, és még a nyomózó hatóságokkal is együtt tudnak működni – ez esély adna arra, hogy néhány elrettentő példa visszafogja ezeket a támadásokat. Sajnos azonban a legtöbb vállalat, főleg, ha sikeresen visszaver egy támadást, a saját titoktartási politikájának köszönhetően ebből semmit sem hoz nyilvánosságra, nem oszt meg a hatóságokkal, és így esély sincsen arra, hogy az elkövetők valaha is felelősségre vonásra kerüljenek.

## 7. Mobil eszközök

Az okos mobileszközök nélkül mára elképzelhetetlen lenne az élet, ám ezek a technológiák sok olyan tulajdonsággal rendelkeznek, amelyek kiemelten vonzóvá teszik ezeket a kibertámadók számára. A két legnagyobb kockázat mindig is a készülék elvesztése, illetve a kártékony szoftverek installálása volt. Ám mindkét lehetőség következményei egyre súlyosabbak és a súlyosabbak, ahogyan ezek az eszközök egyre nagyobb szerepet kapnak életünkben, egyre mélyebben integrálódnak a magánéletbe és a vállalati működésbe egyaránt.

Hogy megérthessük, hogyan áll ma a társadalom a mobil eszközök biztonságához, érdemes visszatekinteni ennek a viszonylag új területnek a fejlődéstörténetére.

A támadók már 2013-14 során elkezdték kihasználni a népszerű mobil operációs rendszerek sérülékenységeit: például az iOS-ben megtalálták a módját, hogyan deaktiválják az iCloud azonosítást, a felhőplatformi kapcsolatot, ami blokkolja az iPhone-okoat, ha ellopják őket vagy elvesznek. Ugyanezen a sérülékenységen keresztül a támadók távolról is képesek voltak feloldani a telefonok belépési zárját.

Az Androidon a beépített böngésző sérülékenységeit kihasználva a támadók megkerülhették a böngésző biztonsági megoldásait, (Mitre, 2014) hozzáférhettek a megnyitott weboldalakhoz, megszerezhették az irányítást a böngésző fölött, ezzel a különböző weben megnyitott szolgáltatások belépési adataihoz (Facebook, stb.) is hozzáférhettek a támadók.

Ekkor jelentek meg az első zsaroló vírusok is platformra: a Simplocker a telefon beső memóriájában és az SD-kártyán keresett, kép és dokumentum fájlokat, majd pedig titkosította őket. A váltságdíjjal ezeket lehetett feloldani. (Lipovsky, 2014)

Az evolúció következő állomása az Android/Locker (Stefanko, 2015) volt, amely hamis antivírus alkalmazásként terjedt, adminisztrátori jogokat kért magának a rendszeren és épp ezért rendkívül nehéz volt eltávolítani. Más metodikát követett a „Porn Droid" (Gilbert, 2015), amely először gyermekpornográfiát mutatott a telefon tulajdonosának, majd pedig állítólagosan az FBI nevében zárolta a telefont, és börtönbüntetéssel és feljelentéssel fenyegette azokat, akik nem fizetnek.

A trójai programok is megjelentek okostelefonokra, kifejezetten a mobilbanki alkalmazásokra és oldalakra specializálva.

2014-ben az iOS is elvesztette a csatát, hiszen eddig leginkább csak azok a készülékek voltak veszélyben, amelyet tulajdonosaik feltörtek (jailbreak) többletjogok szerzésének céljából, ám a WireLurker vírus (Donohue, 2014), már az érintetlen, teljesen hivatalos

szoftvert futtató Apple termékeket is meg tudta fertőzni (mintegy 400 appon keresztül, 350 ezer felhasználót érintett).

### 7.1. A jelen legfontosabb trendjei

A következő évek során a problémák megmaradtak, ám a rosszindulatú kódok folyamatosan fejlődtek, a támadások egyre szervezettebbé és összehangoltabbá váltak. A mobil operációs rendszerek számtalan sérülékenysége látott napvilágot. Ezek mind növelték a lehetőségek tárházát, hogy a támadók hogyan szerezhetik meg az irányítást a készülékek felett. Ez egyre nagyobb nyomás alá helyezi a gyártókat, hogy a biztonsági frissítéseket rendszeresebben és gyorsabban adják ki. Azonban az Android esetében, mivel a gyártókra van bízva a készülék specifikus frissítések kibocsátása, még ha a Google fel is gyorsítja a biztonsági frissítések ütemezését (mint ahogyan meg is tette), egyáltalán nem biztos, hogy ezek időben, vagy egyáltalán eljutnak a felhasználókhoz. Különösen igaz ez a régebbi készülékek esetében, hiszen ebbe a gyártóknak is fejlesztési és kommunikációs kapacitást kell befektetniük. Ez azonban ritkán fordul elő, hiszen a legtöbb gyártó a jövő, a jelen és a közelmúlt készülékeire koncentrál, a régebbieket teljesen támogatás nélkül hagyva. Így a régebbi szoftvert futtató készülékek a problémák melegágyává váltak az Androidos világban. Arról nem is beszélve, hogy számos felhasználó tudatosan nem frissít a legújabb főverzióra például, hiszen sok esetben rosszul optimalizált, hibásan működő verziók jelennek meg az 1-2 éves készülékekre, ezekre a gyártó nem fektet megfelelő hangsúlyt, a funkcionális hiányosságok miatt a legtöbb felhasználó nem is telepíti, vagy visszatér a régebbi verzióra, megőrizve ezzel a régi és jól kihasználható sérülékenységeket.

Jelenleg három fő trend figyelhető meg a mobil kockázatok tekintetésben:

1. Mivel a támadásokkal kapcsolatban komoly hírverés kezdődött és a gyártók is elkezdtek fellépni ellenük, a kártékony programok rejtőzködőbbé váltak, százával lappanganak az egyébként legális elosztó platformokban, letöltő központokban. Ez egyre komolyabb kihívás elé állítja a gyártókat és főleg a mobil operációs rendszerek fejlesztőit, hogy az egyes applikációk viselkedésében a kártékony, rendellenes működés mintázatait minél nagyobb hatékonysággal legyenek képesek azonosítani és a megfelelő ellenintézkedéseket megtenni.
2. A zsaroló programok váltak a mobil platformok leggyakoribb és a legveszélyesebb kártevőivé. Egyre kifinomultabb módszerekkel zárolják az eszközöket, fájlrendszereket, miközben a terjedési, fertőzési csatornák is folyamatosan változnak.
3. A támadók kihasználják a mobil platformokon hatalmas népszerűségnek örvendő csevegőprogramokat, mint a Messenger vagy a Whatsapp, hogy terjesszék a kártékony kódokat, akár platform és operációs rendszer független fertőzési

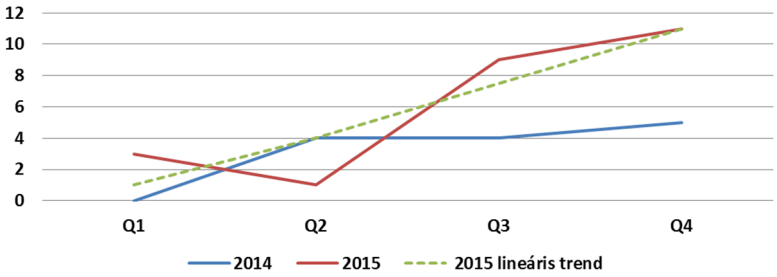
hullámokat elindítva, hiszen ezek a programok, desktop, laptop és mobil eszközökön egyaránt megtalálhatók.

A kiberbűnözők alapvetően két szempont alapján döntenek, amikor a megcélzott platformot, operációs rendszert kiválasztják: a felhasználói létszám és a kihasználható sérülékenységek száma. Ez mobil környezetben sincs másképp, ahogy egyre nagyobb tömegek használnak bizonyos verziókat és világszinten is elterjedt módon, folyamatosan növekszik a kártékony kódok megjelenésének esélye az adott környezetben. A platform elterjedtsége és a platformot célzó támadások száma lineáris kapcsolatban van egymással.

Épp ezért azonosítani kell a leginkább kitett rendszereket és ezek védelmére kell koncentrálni az erőforrásokat.

A Gartner kutatása szerint az Android platform 2015 végén 82,2%-os piaci részesedéssel rendelkezett, míg az iOS részesedése 14,6%, Windows Phone-é 2,5% és a Blackeberry-é 0,3% volt. Bár az Android részesedése csökkent valamit az elmúlt évhez képest, míg az Apple-é szignifikánsan növekedett, ennek ellenére továbbra is felhasználók millióira lehet kihatással világszerte minden új felfedezett Android sérülékenység.

Ezzel együtt felmerül a kérdés, ha az iOS részesedése nőtt, akkor több fenyegetés irányul az iPhone-ok és iPad-ek ellen? A válasz egyértelmű igen: 2014-ről 2015-re az Apple termékeit célzó kártevők száma mintegy megkétszereződött. (Gartner, 2015a)




**5. ábra: Új iOS malware variánsok (ESET, 2015 alapján)**

Ezek a kártevők sok esetben Social Engineering technikákkal, a közösségi és kommunikációs hálózatokon keresztül fertőznek, valamilyen trükkös módon rávéve az ügyfelet, hogy maga adja ki a szükséges adatokat. Sok esetben az ügyfelek nem telepítik a szükséges frissítéseket és ezért maradnak sérülékenyek bizonyos támadási típusokkal szemben. (Ez sok esetben nem csak az ügyfelek hibája: ahogy korábban is írtam, az Android frissítések kiadása a készülékgyártók kezében van, akik bizonyos generációs távolságból már egyáltalán nem adnak ki frissítéseket, ha igen is akkor is heterogén, hogy

mekkora késéssel, illetve milyen minőségben. Az ügyfelek biztonsági indokkal nem fognak frissíteni, ha a frissítés egyébként a készülék használhatóságát korlátozza, teljesítményét, a felhasználói élményt jelentősen csökkenti. Ugyanez a probléma az iOS esetében is: az új rendszerverziók sok esetben jelentős teljesítménycsökkenést jelentenek a régebbi készülékverziók tulajdonosainak, akik így még sok esetben az Apple kvázi kötelező frissítési politikája mellett is próbálnak kibújni az installálás alól.)

A harmadik lehetőség a root-olt illetve jailbreak-elt készülékek esete, amikor az ügyfelek többlet jogokért, magasabb felhasználói élményért cserébe tudatosan megkerülik a készülékek számos korlátozását, ezzel együtt a biztonsági korlátozásokat is, amely a fertőzések könnyebb bejutásához és elterjedéséhez vezethet.

A legutóbbi időszakban számos fontos sérülékenységre derült fény Android fronton:

- A CVE-2015-3860 (Mitre, 2015) például lehetővé tett a támadók számára, hogy megkerüljék a készülék zároló képernyős védelmét.
- Jelentős hibát találtak a számos gyártó által a saját operációs rendszer részévé tett SwiftKey billentyűzet-kezelő alkalmazásban, amely közbeékelődéses (man-in-the-middle) támadást tett lehetővé a saját frissítési protokollján keresztül. (Thomas, 2015b)
- 950 millió potenciális áldozattal a Stagefright az egyik legveszélyesebb fertőzés volt, amely adatlopásra szakosodott a megfertőzött készülékekről, amelyeket szöveges üzenetekben továbbított. (Gálffy, 2015)

Az iOS sem volt mentes a hibáktól

- Egy hibasorozat lehetővé tette a támadók számára, hogy átvegyék az irányítást a készülék fölött és hozzáférjenek az iCloud, valamint a Google Chrome jelszavaihoz (Xing et. al., 2015)
- Az iOS7 AirDrop közel-körzeti fájlmegosztó funkciójának hibáját kihasználva akkor is fájlokat küldhettek a készülékre, ha azt a felhasználó elutasította.

Épp ezért az Apple 2015 végén új biztonsági szabályokat vezetett be, ennek következtében a hirdető már nem férnek hozzá az app letöltési adatokhoz.

### 7.2. Mobil vírusok és kártékony kódok

A biztonsági cégek elemzői többször és alaposan átvizsgálták a két legnagyobb platformhoz tartozó alkalmazás-áruházakat: a Google Play-t és az Apple AppStore-t. Mindkét esetben számos veszélyes alkalmazást találtam megbújva a legális applikációk között.

A Play áruházban scareware (ijesztgető), phishing (adathalász), ransomware (zsaroló), trójai alkalmazások és bőségesen akadnak, amelyek főként játékoknak, játék kiegészítőknek, közösségi alkalmazásoknak álcázzák magukat. (Constantin, 2015) Sok esetben ezek a kódok már olyan fejlettek, hogy a telepítés után késleltetve, időzítetten változnak és teljesítik ki kártékony tevékenységüket, így tudnak átcsúszni a Google szűrőin, amivel az áruház tartalmát vizsgálja és védi.

Az AppleAppStore-ba 300 fertőzött alkalmazás került fel, miután a támadók sikeresen elterjesztették az XCode (Ducklin, 2015) fejlesztőeszköz fertőzött verzióit, ami az applikációk létrehozásához szükséges. Így a fejlesztők tudtukon kívül helyezték el a kártékony kódrészleteket a legkülönbözőbb alkalmazásokban és ezek az alkalmazások így átcsúsztak az Apple védelmén, mivel legális fejlesztői aláírással rendelkeztek.

Az Apple számára az egyetlen kiút az, hogy sokkal mélyebb kódvizsgálatot kell végeznie, mielőtt élesíteni engedi az alkalmazásokat az áruházában.

Emellett a szakértők még több mint 250 alkalmazást találtak az AppStore-ban (ESET, 2015), amely valamilyen módon megsérti az Apple adatvédelmi rendelkezéseit, vagyis e-mail címeket, bejelentkezési adatokat, kulcsokat, szériaszámokat gyűjtenek.

Megemlítendő még pl. a YiSpecter, egy új kártékony program, amely az iOS rendszer API hibáját kihasználva fertőz, letölthet, telepíthet és elindíthat külső forrásból származó iOS alkalmazásokat, sőt még képes lecserélni is a meglévő alkalmazásokat az általa letöltöttekkel.

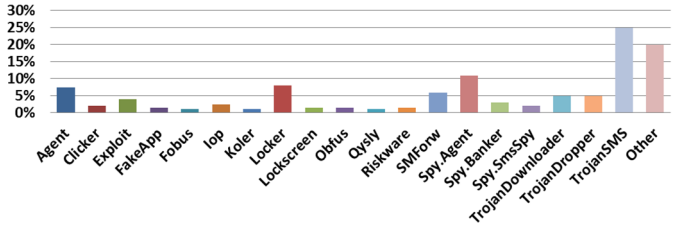
Platformtól függetlenül népszerűek azok a social engineering típusú csalások, amelyek a közösségi kommunikációs hálózatokon terjednek, nagy márkák (Zara, McDonalds, Starbucks, stb) képviselőinek adják ki magukat, hamis szervereken keresztül gyűjtenek adatokat, illetve szolgáltatnak fertőzött tartalmat és alkalmazásokat.

Eddig sok felhasználó és szervezet másodlagosként kezelte a mobil biztonságot. Ez vezetett el oda, hogy a mobil fenyegetettségek mára ennyire elterjedtek, és az otthoni és munkahelyi hálózatok egyik első számú fenyegetésévé váltak.

Emellett fontos kiemelni a kapcsolatot a dolgok internete és mobil biztonság világa között, hiszen nagyon sok intelligens eszköz futtat valamilyen mobil operációs rendszert: okosTV-

k, okosórák, Android Auto fedélzeti gépjármű rendszerek, stb. A zsaroló programok, illetve az eszközök feletti irányítás megszerzése ilyen esetekben még nagyobb áttételes károkat okozhat, mint az okostelefonok és tabletek esetében, különösen, hogy ezen eszközök jó részén nem tudunk külső biztonsági szoftverekkel növelni a védelem szintjén, ahogyan azt már korábban is kifejtettük.

Sok esetben a mobil válik a személyes hálózatok, profilok leggyengébb, támadható pontjává. A mobilon keresztül behatolva a felhő tárhelyekbe, profilokba a támadók több tokent, jelszót, felhasználói, bejelentkezési profilt kompromittálhatnak, amivel áttételesen sokkal több rendszert veszélyeztet egy-egy ilyen támadás, mint ahol a sérülékenységek vannak, akár teljesen eltérő platformokon.




**5. ábra: Az Android malware családok növekedési üteme 2015 (Schulze, 2016 alapján)**

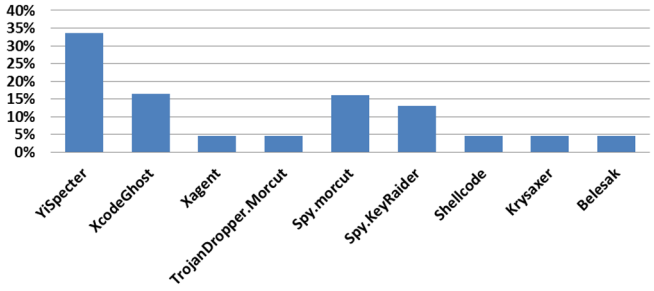
A jövőre nézve kijelenthető, hogy az eddigi körülbelül havi 200 újonnan felfedezett fenyegetettség számosságában a jövőben is fennmarad, folyamatosan várhatók egyre újabb és újabb kártékony kódok Android eszközökre. A legtöbb ilyen új kód valamiféle trójai program, ám a fertőzési, támadási módszerek egyre kifinomultabbá válnak.

Természetesen az alcsoportok között lehetnek átrendeződések, 2015 során például az SMS-trójai programok elterjedtsége nőtt meg jelentősen.

A netbanki és hitelkártya adatokra, de akár jelszavakra és kapcsolati adatokra vadászó kémprogramok száma szintén 2015 során mutatott egy jelentősebb ugrást.

Erőteljesen meglódult a zsaroló vírusok terjedése is, a következő évek egyik legnagyobb kihívását ez a csoport jelenti majd várhatóan, főleg, ahogy az okostelefon egyre több felhasználó magán és professzionális életének válik egyre szervesebb részévé. Különösen a lezáró képernyőt manipuláló változatuk terjedt el nagyon erőteljesen az utóbbi időszakban, a növekedés itt egy év alatt 600%-os volt.

Az iOS platformon lényegesen kevesebb kártevő jelenik meg, ám itt is erőteljes növekedés tapasztalható évről évre, nyilván alacsonyabb bázissal. Ezen a platformon főként a kémprogramok elterjedése jelentős.




**6. ábra: Az iOS malware családok növekedési üteme 2015 (Schulze, 2016 alapján)**

Mindkét platformon a legfőbb tanulság, hogy a fejlesztőknek biztonsági szempontból jóval kidolgozottabb, robusztusabb alkalmazásokkal kell előállniuk a jövőben. A biztonság megvalósítása nem lehet egy mellékes, utólagosan beépítendő szempont, hanem a tervezés első pillanatától kezdve központi irányelvnek kell lennie. A tesztelési eljárások javítása és szigorítása, a statikus és dinamikus tesztelés szintén hozzájárul a sérülékenységek korai felfedezéséhez.

### 7.3. Védekezési stratégiák

A fent említett problémák különböző válaszokat igényelnek attól függően, hogy otthoni vagy professzionális szervezeti környezetről beszélünk.

#### 7.3.1. Otthoni felhasználók

Amellett, hogy az okos eszközökre szükséges mobil biztonsági szoftvert installálni – ezek között ingyenesen elérhető módon is vannak rendkívül jól használható, minőségi eszközök, nagyon körültekintően kell eljárni, ha nem hivatalos alkalmazásboltokból származó szoftvereket telepítenek.

A felhasználóknak meg kell tanulni, hogyan azonosítsák be a nagy eséllyel hivatalos, biztonságos alkalmazásokat:

Netböngészés közben kerülni kell azokat az oldalakat, amelyek applikációk telepítésére és letöltésére szólítanak fel különböző gyanús weboldalakról.

Nem szabad letöltési az e-mailben, csevegő szoftverekben, sms-ben kapott letöltési linkekre előzetes ellenőrzés nélkül rákattintani, még akkor sem, ha látszólag jó ismerős küldte őket.

Láthattuk, hogy a kártékony kódok még a hivatalos alkalmazás áruházakon keresztül is terjednek, így egy-egy új alkalmazás telepítése előtt érdemes utána nézni a fejlesztőnek a

keresőkben, illetve a közösségi oldalakon, vajon előfordult –e már olyan eset korábban, amikor csalással vádolták őket. Ezzel együtt az alkalmazás áruházak üzemeltetőinek is folyamatosan szigorítani kell a feltételeket és a kódvizsgálati szempontokat, hogy minél kevesebb ilyen eset fordulhasson elő.

A Root és a jailbreak az operációs rendszerekbe épített védelmi mechanizmusokat is megkerüli, így javasolt kerülni ezek alkalmazását.

Nagyon fontos, hogy az operációs rendszerek és az alkalmazások is folyamatosan frissítve legyenek, mindig alkalmazni kellene a legfrissebben hozzáférhető biztonsági frissítéseket és patcheket.

Mivel az Android alapú eszközöknél a gyártókra van bízva milyen gyakorisággal és milyen frissítéseket adnak ki, és erre sem az operációs rendszerek gyártóinak, sem a felhasználóknak nincs közvetlen ráhatása, a készüléktípus kiválasztásánál a készülék tulajdonságai mellett ezt is figyelembe kell venni szempontként, és azon gyártók készülékeit előnyben részesíteni, amelyek kiemelten figyelnek a frissítési ütemtervek betartására. Ezen belül a Google Nexus eszközök és a módosítatlan Android szoftvert futtató eszközök járnak legelöl, hiszen ezek rögtön megkapják a frissítéseket, amint a Google publikálja azokat.

Hogy az adatvédelem ellopott vagy elvesztett eszköz esetén is megmaradjon, nagyon fontos, hogy zároljuk az eszközt, lehetőleg minél erősebb, kód, vagy az újabb generációknál biometrikus (ujjlenyomat, írisz) azonosítást használva. Megfelelő biztonsági szoftverek segítségével a telefon távoli lokalizálása, zárolása, adattörlése is megoldható.

Mivel a zsaroló vírusok jelentik az egyik legfontosabb fenyegetést, nagyon fontos, hogy rendszeresen készüljön biztonsági mentés a készülékeken tárolt adatokról, akár felhőbe, akár lokálisan, így egy esetleges fertőzés esetén a váltságdíj kifizetése helyett egy egyszerű gyári visszaállítás/újratelepítés megoldja a problémát.

A mobil számlák, mobil fizetési elszámolások tüzetes átvizsgálásakor esetlegesen beazonosított rendellenes tételek pedig hozzásegítenek a gyanús alkalmazások felderítéséhez.

### 7.3.2. Vállalati környezet

Egészen bizonyos, hogy mindazok a trendek, problémák, amelyek az otthoni felhasználóknál megjelennek, a vállalatokat is érintik, hiszen a felhasználók magukkal viszik eszközeiket a vállalati környezetbe. Egy emeltdíjas SMS trójai a vállalati telefonszámlát növeli, egy adatlopó kód pedig a vállalati bejelentkezési adatokat, kontaktokat szivárogtatja ki, egy mobil zsaroló vírusból fakadó adatvesztés is érzékenyen érintheti a vállalati költségvetést.

Fontos tudatosítani a felhasználókban, hogy a mobileszközök különösen alkalmasak arra, hogy rajtuk keresztül valósítsanak meg támadást a vállalati belső rendszerek ellen. A védekezés első lépése ennek tudatosítása a felhasználókon kívül a vállalati IT-biztonsági szakemberekben is, akik a belső biztonsági intézkedéseket, valamint a boyod-szabályzatokat ehhez a tapasztalathoz alakítják.

A kockázatcsökkentés egyik kiváló eszköze lehet tisztán vállalati célú eszközök esetében a távoli menedzsment eszközök telepítése. Ezeknek erős titkosítást kell alkalmazni, és a vállalati hálózathoz VPN-kapcsolaton keresztül csatlakozni. Fontos továbbá leválasztani a mobil adatforgalmat a vállalat normál tranzakciós forgalmáról, ennek külön monitorozása, valamint a megfelelő biztonsági szoftverek alkalmazása jelentősen növeli a biztonsági szintet.

Ezeket a monitoring eszközöket hozzá kell kapcsolni az adatvesztés ellenes (DLP – Data Loss Prevention) és a tartalomszűrő és ellenőrző (CMF – Content Monitoring and Filtering) rendszerekhez, és létrehozni a mobil alkalmazásokra vonatkozó menedzsment szabályokat és biztonságos rendszerkonfigurációt.

Mint mindenhol, itt is meg kell követelni a megfelelő hosszúságú, összetettségű jelszavak használatát, fix élettartammal és a rendszeres csere kényszerével.

Ezeknek a politikáknak kell meghatározni, hogy mely gyártók, platformok és verziók engedélyezettek vállalati környezetben és melyek nem. Meg kell követelni a digitálisan aláírt szoftver komponensek használatát, valamint szigorúan tiltani az adminisztrátori jogokat megszerző átalakítások alkalmazását.

A fenti technológiai megoldásokkal egyetemben biztonsági képzéseket is kell tartani a felhasználóknak, amelyek során megismertetik a felhasználókat a fentiekben említett veszélyekkel és biztonsági trendekkel, valamint felkészítik őket a főbb kockázatok elkerülésére.

## 8. Kritikus infrastruktúrák

Az ipari rendszerek (ICS – Industrial Control Systems) biztonsága már évek óta a figyelem középpontjában van, különösen a 2010-es Stuxnet féreg támadás (Matrosov, 2011) óta, ami megmutatta, hogy mennyire védtelenek lehetnek ezek a rendszerek egy külső támadással szemben, még akkor is, ha a régi iskola szerinti leválasztott működési modellt képviselik. 5 évvel a Stuxnet után, olyan új fenyegetések fényében, mint a Falme vagy a Duqu, az informatikai biztonsági szakemberek olyan támadásokkal találják szemben magukat, melyek nem válogatnak a különböző iparágak között, kontrollálatlanul fertőznek a különböző ipari rendszerekben. A kérdés, hogy erre az új kihívásra felkészültek-e megfelelően a biztonsági szervezetek?

A kritikus rendszerek (energiatermelés és ellátás, közművek, közlekedés, stb.) már évekkel ezelőtt felismerték, ám a szükséges biztonsági fejlesztések nagyon egyenetlen mértékben történtek meg valójában.

Nagyon lényeges megérteni, hogy az ipari rendszerek jelentős változásokon mennek keresztül napjaink fejlődési trendjeit követve. Egy ICS rendszer esetében egy rendszerhibából életet veszélyeztető esemény lehet, épp ezért korábban céleszközökből álló sziget rendszerben működtek, a kommunikációs eljárások egyediek voltak, alapelvárás volt a megbízható működés és az elválasztás.

Az IKT rendszerek korábban biztonsági szempontból nem veszélyezettek közvetlenül emberéletet. Ezek a rendszerek egységesített, szabvány elemekből állnak, nyilvános hálózatokra kapcsolódnak, külön kifejlesztett és bevezetett biztonsági megoldások és eljárások segítségével lehet megvédeni ezeket.

A két kategória viszont a dolgok internete és a távoli üzemeltetés, a virtualizált, felhő alapú megoldások egyértelmű rövid távú költség és technológiai előnyei miatt kezd teljesen összekeveredni. Az ICS rendszerek is szabványosodnak, a korábbi szigetrendszerek, amelyek fejlesztésénél még az elválasztott üzemeltetés volt a koncepció, összekapcsolásra kerülnek, az IKT-val és a hálózatokkal, noha sokkal gyengébb ellenállóképességgel rendelkeznek, eltérő tervezési koncepciójuk miatt, és az ilyen összekapcsolási projektekben a biztonság gyakran csak látszólagos. Az ICS és az IKT teljes koncepciója között ellentét feszül, míg az IKT szerint az ICS a túlzott biztonság és elzárkózás oltárán hasznos üzleti és kényelmi lehetőségeket, funkciókat áldoz fel, addig az ICS szerint az IKT túlságosan előtérbe helyezi az üzleti szempontokat, a trendkövetést, a technológiai fejlődés maximalizált kihasználását és a felhasználói/üzemeltetői kényelmet, elfelejtkezve olyan alapértékekről, amelyek a jó informatikai rendszerek sajátjai.

A kiterjedt sérülékenységek egyik legfontosabb oka, hogy az ICS platformok gyártói sok esetben nem engednek semmilyen külső fejlesztést, beavatkozást a kritikus infrastruktúra részét képező hardver komponensek vezérlő rendszereibe. Összegezve tehát a kritikus infrastruktúrát kezelő vállalatok gyakran elavult, sérülékeny operációs rendszereket alkalmaznak, amelyek mindennek ellenére csatlakoznak az internetre, és ez jelentősen megnöveli a biztonsági incidensek valószínűségét. A biztonság megteremtése itt nem csak a biztonsági cégeken és a szervezetek biztonsággal foglakozó szakemberein múlik, hanem szoros együttműködés szükséges a gyártókkal, hogy rendszeresen frissítsék az infrastruktúrához tartozó vezérléseket, és ezáltal csökkentsék a támadásoknak való kitettséget.

A vitában egyébként véleményem szerint mindkét félnek igaza van. A kritikus infrastruktúrákat továbbra is lehetne szigetrendszerként, leválasztva üzemeltetni, az is igaz, hogy lényegesen drágábban, saját hálózatot, nem nyilvános protokollokat használva nem kellene lemondani a rendszer okosságáról, pl. a külső szenzorinformációk feldolgozásáról sem. Az is igaz, hogy egy szigetrendszerben viszont nagyon nehézkesen lehet a mai okostechnológiák egyik alapelemét, a crowdsourcing-ot beépíteni. Eszerint a felhasználók a saját eszközeikkel nagy tömegű adatokat gyűjtenek, ezt dolgozza fel egy központi rendszer és változtatja az infrastruktúra működését. Ezt úgy kell elképzelni, mintha a népszerű Waze közösségi navigáció adatai nem csak az útvonaltervezést végző szerverre, hanem a közlekedést vezérlő intelligens központokba is befutnának, amelyek utána ez alapján hoznának forgalomszervezési döntéseket (pl. jelzőlámpa ciklusok változtatása) az anomáliák kezelésére, a közlekedés optimalizálására. Ehhez hasonló projektek már léteznek szerte a világban, és ilyen esetekben természetesen nem lehet megúszni a nyilvános infrastruktúra használatát, ám természetesen itt is lehetséges volna egy biztonságos kapcsolat (VPN, https, SSL stb.) alkalmazása, amely nyilvánvalóan erőforrás igényesebb, ám képes jelentősen csökkenteni a nyíltsággal kapcsolatos hátrányokat. Ésszerű költségek mellett, bizonyos területeken ma már elképzelhetetlen, hogy egy leválasztott rendszer ennyi adathoz juthasson és ilyen komplex döntéseket hozhasson, más területeken viszont nem szabad korlátlanul a trendek után menni és csak azért enyhíteni a biztonságon, hogy illeszkedjünk a mai elvárásokhoz, a rendszer okossága és biztonsága között ma még sajnos sokszor tradeoff feszül, amit a kritikusság fényében kell optimalizálni. Mindazonáltal ez valós trend, több mint divat, egyre több adatból, egyre automatizáltabb módon, egyre komplexebb módon kell a rendszereknek reagálni a környezetükre, ezt visszafejleszteni, visszaállítani nem lehet, a biztonság fejlesztési üteme, viszont nem lehet lassabb az általános technológiai fejlődésnél és a követelmények átalakulási üteménél, a biztonsági komponensek alkalmazása pedig nem lehet a költségcsökkentés első számú forrása egy egyre újabb és okosabb technológiák árának racionális szinten tartásakor.

## 8.1. Információmenedzsment mint kulcstényező

A probléma tehát nem csak az, hogy nagyon sok ipari rendszer elavult operációs rendszereket alkalmaz, és a gyártók nem frissítik, teszik kompatibilisség a vezérlő programokat az új változatokkal. Itt a felhasználóknak nincs sok választása: több 100 millió forintos berendezéseket nem fognak azért lecserélni az újabb, ismét drága, akár milliárdos beruházási költségű változatokra, mert a régihez nincsen driver és vezérlő program Windows 7 vagy 10 alá és még mindig XP, rosszabb esetben Win2000, 98 vagy épp 3.1 (!) alól kell vezérelni. Természetesen ezen elavult operációs rendszerek alatt az is probléma, hogy a legújabb biztonsági szoftverek sok esetben már nem is kompatibilisek velük, így a kiegészítő biztonság lehetőségek is nagyban limitáltak. (Ilyen esetekben gyakran a megfelelő vezérlő hardver beszerzése, vagyis olyan régi komponensekből álló számítógép összeállítása, ami képes fogadni ezeket az abszolút elavult operációs rendszereket, sokszor a legnagyobb fejtörés az üzemeltetés számára.) Mindez nem lenne akkora kockázat, ha e rendszerek sziget üzemben, elszigetelten működnének.

Azonban a második nagy probléma éppen az, hogy minden elavultságuk ellenére ezek a vezérlő berendezések el vannak látva nyilvános internet kapcsolattal karbantartási és kívülről történő menedzsment célokra. Ez természetesen állandó kockázatot jelent, hiszen kizárólag nagyon gondos és folyamatos menedzsment esetén lehet hatékonyan meggátolni, hogy illetéktelen külső felhasználók csatlakozzanak a rendszerekhez. A megfelelő szoftvermenedzsment szabályoknak le kell korlátozni a hálózati hozzáférést a valódi karbantartási feladatokra, illetve biztonságos kapcsolaton (VPN) keresztül kell megvalósítani az adatok küldését és fogadását.

Ezen felül, mivel a belső komponensek sok esetben elavultak, szükségessé válik a teljes hálózat védelmére nagyobb hangsúlyt fektetni. Ilyen például a tűzfalak alkalmazása, vagy általános szabályok és irányelvek meghatározása arra nézve, hogy mely eszközök, komponensek kommunikálhatnak egyáltalán a hálózaton, és milyen esetekben cserélhet két eszköz adatokat távolról.

Sok esetben viszont ezek a vezérlő rendszerek speciális kommunikációs protokollokat használnak, amelyek ismeretlenek a sokkal általánosabb célra tervezett tűzfalak számára, így akár egyedi fejlesztésekre, módosításokra is szükség lehet a rendszerben, pontosan „betanítva” a védelmi rendszereket az adott vezérlési megoldások működésére, és ezáltal a rendellenes forgalom kiszűrésére. Így pontos kontroll szerezhető az ipari rendszerek felett is, és elérhető, hogy csak a speciális protokollok és azok is ellenőrzötten tudjanak kommunikálni.

Bár megjelent a közelmúltban néhány gyártó, akik kifejezetten az ipar igényeire szabott tűzfalakat készítenek, e speciális komponensek fejlődése és elterjedése igen lassú, és nagyon sok feladat van még hátra.

További szervezési veszélyforrás, hogy a távoli eszközmenedzsmentet és a hálózati és informatikai biztonságot teljesen elkülönített feladatként kezeli a legtöbb vállalat. A két terület között ezért sokszor kommunikációs problémák és a késleltetések vannak. Sok esetben az üzemeltetéssel foglalkozó szakemberek bizonyos biztonsági feladatokra és a komponensekre mint a hatékonyságot csökkentő tényezőkre gondolnak és igyekeznek megkerülni vagy legalábbis csak a legszükségesebb mértékben alkalmazni azokat, ezáltal sok veszélynek teszik ki a vállalatot, aminek direkt anyagi következményei is jelentősek lehetnek.

A rendelkezésre állás az ipari kritikus szolgáltatások, a magán és állami kritikus infrastruktúrák esetében mindenek felett álló szempont, ami bizonyos esetekben még a biztonságot is felülírja, kitéve a rendszereket a potenciális távoli támadásoknak az interneten keresztüli elérhetőség biztosításával.

Bár a rendelkezésre állás kétségtelenül az elsődleges szempont ezekben az esetekben, azért a bizalmasságot és a sértetlenséget sem szabad teljesen háttérbe szorítani.

Végül ezen elavult rendszerek esetében gyakran az a határozott üzleti hozzáállás is felfedezhető, hogy ha valami éppen működik, akkor véletlenül se nyúljunk hozzá (frissítés, biztonsági komponensek beépítése, hálózati adatforgalom változtatása), hiszen nem lehet tudni, mi „romolhat el" a beavatkozás során, és hogy egy ilyen, minden szempontból elavult és sokszor már nem is közismert megoldásokat alkalmazó rendszer esetében visszaállítható lesz-e egyáltalán a normális működés, ha egyszer valami balul sül el. Ebből a hozzáállásból rengeteg biztonsági probléma fakad: elavult, soha nem frissített operációs rendszerek és böngésző változatok, amelyek könnyen engednek nem engedélyezett hozzáférést a támadók számára. Ha ma valami stabilan működik, az még nem biztos, hogy ok arra, hogy ne próbáljuk felkészíteni a jövő veszélyeire.

### 8.2. Közös fenyegetések

Az ipari rendszereket nem csak az olyan célzott és kifinomult támadási formák fenyegetik, mint amilyen a Stuxnet, a Duqu vagy a Flame voltak. 2015 folyamán több jelentés érkezett a Laziok nevű kártékony program tevékenykedéséről ipari rendszerekben. Ez a program adatokat gyűjt és továbbít a támadók számára a rendszerben található hardverkomponensekről, szoftverekről és verziókról, a telepített vírusirtó és más biztonsági megoldások meglétéről, és típusáról. Ezek az adatok remekül felhasználhatóak a későbbiekben egy célzott támadás megtervezéséhez. A legrosszabb a dologban, hogy a

Laziok egy olyan Windows sérülékenységet használ ki e-mailes terjedése és fertőzött csatolmányok útján való települése során, amelyre 2012. áprilisában már megjelent a javítás, ám ezt számos rendszerben a mai napig nem telepítették.

### 8.3. Az egyik leginkább érintett szektor az egészségügy

Az ipar mellett az egészségügy bizonyult az IT-biztonság szempontjából leginkább fenyegetett kritikus infrastruktúrának az elmúlt időszakban. Csak 2015-ben mintegy 234 biztonsági incidens és 141 adatvesztéssel vagy szivárgással járó támadás történt az egészségügyben. Ez esetek 20%-ában hibás felhasználói magatartás vagy hibás folyamatok vezettek az incidenshez. Ami nyugtalanító, hogy ezen arány 2014-ben még csak 15% volt, tehát nem hogy növekedne az egészségügyben dolgozók és az egészségügy intézmények biztonság tudatossága, hanem a számok egyenesen romló tendenciákról árulkodnak. (Verzion, 2016)

Az egészségügyi intézmények kiemelten érzékenyek a web applikáció alapú támadásokra, illetve a szolgáltatásmegtagadással járó DDoS támadásokra. Az egészségügyben 4%-kal több ilyen támadás történt, mint az összes többi iparágban együttvéve.

A Ponemon Intézet jelentése (Ponemon, 2015a) egy másik nyugtalanító trendet is kiemel: az egészségügyi intézmények biztonsági eseményei korábban a véletlen kategóriába tartoztak leginkább, vagyis valamilyen nagyobb volumenű válogatás nélkül fertőző támadó kampány szórásába estek bele. Az utóbbi időben viszont ez megváltozott. a biztonsági események szándékos, célzott támadásokhoz köthetők. A kifejezetten bűnelkövetés hátterű támadások száma 125%-kal nőtt az elmúlt 5 év során, és már nem az elhagyott céges laptopok az első számú okai az adatszivárgásoknak.

Egy másik tanulmány (Ponemon, 2015b) kimutatta, hogy az egészségügyi intézmények általában igen felkészületlenek a biztonsági kihívásokkal szemben és nincsenek is meg a megfelelő eszközeik, hogy megvédjék a betegek szenzitív adatait. 2015-ben az intézmények 45% jelentette ki, hogy az adatvesztések elsőszámú oka kibertámadás volt, míg ez az arány mindössze 40% volt egy évvel korábban.

### 8.4. Sérülékeny egészségügyi berendezések

A fenti szervezési veszélyforrásokon kívül, az ipari rendszerekhez hasonlóan, maguk a hálózatra kapcsolt egészségügyi, diagnosztikai és kezelésekhez szükséges berendezések és műszerek is jelentős kockázatot jelentenek az intézmények számára. A modern egészségügy eszközök nagyon sokszor kapcsolódnak a hálózatra, ami áldás és átok egyszerre. Természetesen sokkal hatékonyabb a menedzsment, a vezérlés, szakemberek

távolról is elvégezhetnek bonyolult beavatkozásokat, személyes jelenlét nélkül, illetve részt vehetnek az eredmények értékelésében. Ám a külső beavatkozás ezen berendezések működésébe súlyos, akár halálos következményekkel is járhat a páciensre nézve. CT és MR berendezések, szív-tüdő gépek, levegő- és gyógyszeradagoló pumpák – mind vezérelhetők hálózati kapcsolatokon keresztül, de nem kell nagy képzelőerő ahhoz, hogy egy beavatkozás, vizsgálat közbeni illetéktelen beavatkozás a berendezés működésébe milyen kockázatokkal járhat.

A fenyegetés nagyon is valós, csak 2014 több mint 300 sérülékenységet azonosítottak intelligens sebészeti eszközök vezérlő szoftvereiben, amely lehetővé tette a külső behatoló számára, hogy hozzáférjen az eszköz működését vezérlő beállításokhoz. (Rios-McCorkle, 2014)

A probléma gyökere itt is azonos azzal, amit az ipari rendszerek esetében láthattunk: a könnyű hálózatban kapcsolhatóság, a plug&play működés sokkal fontosabb tervezési szempont, mint a biztonság. Az egészségügyi intézményekben gyakran hiányzik, vagy nem elégséges a szakértő informatikai csapat, az orvosok és a szakdolgozók, kezelik és konfigurálják ezeket a berendezéseket, számukra pedig minden alá rendelődik a könnyű és erőfeszítés minimalizáló használatnak. Az orvosi berendezések tehát szintén elavult vezérlő programokkal és komoly biztonsági résekkel terhesen üzemelnek éveken keresztül, általában semmi, vagy minimális frissítést és javítást végezve rajtuk. A hálózatba köthető egészségügyi eszközök nagy részénél nem is lehet a biztonsági beállításokat szigorítani, még szakértő kezelőszemélyzet számára sem, és természetesen semmilyen harmadik féltől származó biztonsági eszköz telepítését, hozzájuk kapcsolását sem támogatják. Így a böngészőn keresztüli elérhetőség óriási biztonsági réseket hordoz.

2015-ben egy nevezetes kutatási kísérlet során a szakemberek fél évig monitorozták egy amerikai egészségügyi intézmény belső hálózatát csali eszközöket elhelyezve benne, a fél év alatt, mintegy 68.000 különböző sérülékenységekkel rendelkező eszközt és rendszert azonosítottak egyetlen (!) intézmény hálózatában. (Erven-Collao, 2015)

Az egészségügyi szektor üzemeltetésébe is fel kellene vennie az informatikai kockázatkezelési szempontokat és periodikusan újra értékelni az eszközöket és rendszereket, mielőtt még súlyosabb következményekkel kell szembe nézni. A kockázatelemzés eredményeinek megfelelően itt is megfelelő katasztrófa elhárítási és incidens válaszlépés tervezeteket kell kidolgozni és szükség esetén végrehajtani. 2015 során már megtörténtek az első, nagyobb visszhangot kiváltó incidensek, mind az Egyesült Államokban, mind Magyarországon, ahol kórházi informatikai rendszerek váltak zsaroló vírusok áldozatává.

A sérülékenységeket kihasználó sikeres támadások legtöbbször adatlopási célzattal történnek, különösen az egészségügyben, ahol nevek, TAJ-számok, telefonszámok, otthoni és e-mail címek szerezhetők meg több más személyes, akár szenzitív egészségügyi adat mellett. Ez az információ nagyon értékes lehet a támadók számára, specializált ajánlatok keretében nagyon jó pénzt lehet kapni érte a feketepiacon. Függetlenül attól, hogy hol szerezték meg a személyes adatokat, ha túl sok halmozódik fel ezekből a szervezett bűnözői csoportok kezében, akkor az a digitális bűnelkövetés egy teljesen új, tömeges korszakát hozhatja, hiszen ennyi adatból komplett személyazonosság-profilok rekonstruálhatók, amelyekkel aztán vissza lehet élni a legkülönfélébb formákban: hamis azonosító okmányok előállítása, hamis bankszámlák megnyitása, hamis hitelkártyák előállítása, internetes profilok biztonsági kérdéseinek megválaszolása, stb.

Az internet a hálózatba kapcsoltság természetesen nagyon vonzó opció és mérföldkő az egészségügy fejlődésében, ám nem szabad elfelejtkezni arról, hogy ezeken a hálózatokon keresztül milyen komplex és érzékeny adatokhoz lehet hozzáférni, és azon túl hogy megfelelően biztonságos környezetben, biztonságos hálózati elemekkel körülvéve kell ezeket tárolni, olyan különleges biztonsági intézkedések is szükségesek lennének, mint a titkosított adattovábbítás, a többfaktoros azonosítás, hálózatok szétválasztása tűzfalakkal és használható válasz stratégiák incidensek esetére.

### 8.5. Behatolás ellenőrző rendszerek

A fenti esetekből világosan látszik, hogyha maradnak nyitott lehetőségek, sérülékenységek egy rendszerben, akkor a támadók ezeket kíméletlenül ki fogják használni. Ezért nagyban szükséges, hogy mind a magán, mind a közszférában növekedjen a tudatosság és az információ biztonsági oktatás a mindennapi továbbképzés részévé váljon. A támadók nem csak adatokat szerezhetnek meg, de fel is tölthetnek oda nem illő tartalmakat, és a saját céljaikra használhatják a szervezet informatikai erőforrásait.

Hogy mennyire súlyos kérdés ez a kritikus infrastruktúrák esetében, azt mi sem mutatja jobban, minthogy az Egyesült Államok Nemzeti Tudományos Alapja 250 ezer dollárral támogatta 2015-ben a Texasi Egyetemet, ahol az egészségügyi rendszerek védelmét szolgáló megoldásokat dolgoznak ki ebből a forrásból. (Purba, 2015) Az Európai Hálózat- és Informatikai Biztonsági Ügynökség (ENISA) pedig 2016-os kutatásaink fókuszába az okos kritikus infrastruktúrák előretörését és ennek kockázati vizsgálatait állította. (ENISA, 2015)

A kritikus infrastruktúrák valóban jelentős áttételes hatásokat képesek generálni a teljes gazdaságban és társadalomban, hiszen az energia, a víz, a fűtés, vagy épp az egészségügy sikeres megbénítása jelentősen hat a többi iparágra is, valamint exponenciálisan csökkenti a

társadalmi biztonságérzetet. Bár néhány biztonsági intézkedés már kezd elterjedni ezeken a területeken is, az bizonyos, hogy a kritikus infrastruktúrákat megcélzó támadások száma jelentősen növekedni fog, és bizonyosan várható egy-két súlyos hatású incidens, mielőtt a biztonság ezen a területen valódi politikai-gazdasági súlyt és prioritást kap. A kritikus infrastruktúrák elleni kiberhadviselés jelentős szerepet kaphat a jövő háborúiban is.

## 9. Állam, politika és jog

A jogi szabályozás kiemelt fontosságú az informatikai biztonsági fenyegetések elleni hatékony küzdelemben. A követelmények részletesen szabályozhatók az egyes üzleti, szolgáltatási területek jellemzőinek, igényeinek megfelelően. A szabályozó eszközök között lehetnek törvények, szabványok, szabályzatok és politikák.

Az IT-biztonság törvényi szabályozásában a személyes adatok védelmének területe az egyik legfontosabb és legegységesebb. Az ügyfelek adatainak kezelését védelmét legtöbb esetben magas szintű jogszabályok írják elő. A saját adataikat és a velük szerződésben álló partnerek adatait pedig önként felvállalt tanúsítványok, szabályrendszerek segítenek megvédeni.

Nem számít a vállalati méret, hogy magán vagy állami tulajdonról beszélünk: ha egy vállalat érzékeny adatokat dolgoz fel, továbbít vagy tárol, akkor az biztonsági intézkedéseket igényel, amelynek kereteit meghatározhatják maguk a vállalatok, de a beszállítók, partnerek, ügyfelek és az állam elvárásai is érvényesítésre kerülhetnek.

A megfelelő adatvédelmi szabályok hiánya minden esetben fontos szerepet játszott az utóbbi évek nagy adatszivárgási botrányaiban: Sony, Ashley Madison, Hacking Team – csak néhány az előző fejezetekben feldolgozott, legkomolyabb esetek közül. E terület fontossága várhatóan nem is fog csökkenni a jövőben, sőt, még tovább emelkedhet, ahogy az információ értéke egyre nő.

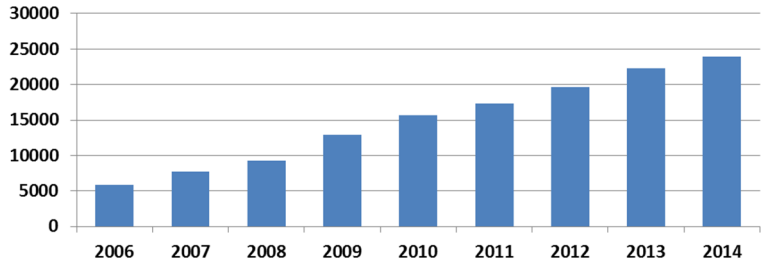
### 9.1. Szabványkövetés

A vállalatok tehát alkalmazkodhatnak a saját belső követelményrendszerükhöz, vagy valamilyen a partnerek és/vagy a szabályozó hatóságok által rájuk kényszerített rendszerhez. Bárhogy is a kiválasztott rendszer dokumentálni, rendszeresen monitorozni, és auditálni kell, hogy a megfelelő biztonsági szint fenntartása biztosított legyen.

IT-biztonság szervezési kérdésekben az egyik alappont az ISO/IEC 27001 szabvány (ISO/IEC, 2013), ami az Információbiztonság Menedzsment Rendszerek (Information Security Management System - ISMS) kialakítást és fenntartását támogatja. Ez egy nyílt dokumentum, amely az azt megalkotó szakemberek tudásán és tapasztalatain alapul.

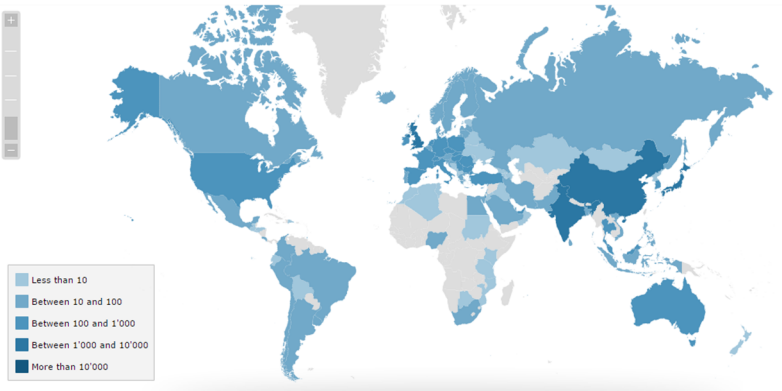
Nyíltsága miatt a szervezetek szabadon a saját igényeikre, működésükre szabhatják a benne foglaltakat.

Alapvetően két fő területet fed le: meghatározza azokat a szervezeti kereteket, követelményeket, amelyek egy ISMS rendszert fenntartó szervezettől elvárhatók, a második része pedig sorra veszi a legfontosabb biztonságirányítási célokat, amelyeket a szervezetnek meg kell valósítania. Teszi mindezt irányvonalak és jó gyakorlatok bemutatásával. Az alapverzió 2005-ből való, 2013-ban pedig kapott egy teljes körű frissítést. Egyre több szervezet szerzi meg a tanúsítványt világszerte, a tanúsított szervezetek száma évi 7-10%-kal nő az elmúlt évek tapasztalatai alapján. (ISO/IEC, 2014)




**7. ábra: Kiadott ISO/IEC 27001 tanúsítványok száma világszerte (ISO/IEC, 2014 alapján)**

A legnagyobb növekedést Japán, az Egyesült Királyság és India mutatta a kiadott tanúsítványok tekintetében.




**8. ábra: Kiadott ISO/IEC 27001 tanúsítványok száma országok szerint (ISO/IEC Stat 2014)**

Természetesen a tanúsítvány megléte nem garantálja, hogy a szervezet ennek szellemében is működik a való életben, de azt bizonyítja, hogy tett olyan tudatos lépéseket, amelyek végül elvezethetnek az információbiztonság kívánt szintjéhez három kiemelt területen:

- Vállalatirányítás
- Kockázatkezelés
- Compliance (jogi megfelelőség)

### 9.2. Adatvédelem

Az adatvédelem már az Emberi Jogok Nyilatkozatának 12. pontjában is megjelenik:

„Senkinek magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez.” (ENSZ, 1948)

Az elmúlt évek során egyre komolyabb szerepet tölt be, mint a modern társadalom és gazdaság egyik sarokköve. A technológia korszakában, ahol az adatok, köztük a személyes adatok áramlása és áramoltatása olyan könnyű, mint még soha korábban, egy nemzetközileg egységes szabályozás az egyetlen, ami segíthet gátak közé szorítani az emberi jogok és az üzleti/politikai érdekek konfliktusát.

Mint az ismeretes, a személyes adatok fogalma egészen tág: „meghatározott természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés.” (Info Tv. 2011)

Vagyis a szűken vett személyes adatokon kívül az adott személy családjára, munkájára, kapcsolatrendszerére, időtöltéseire, csoporthoz tartozására, meggyőződésére, véleményére vonatkozó adatok mind ide tartoznak, mindaddig, amíg a kapcsolódó természetes személy bármilyen módon beazonosítható.

Nem véletlen tehát, hogy sokan sürgetnek egységes nemzetközi jogi megoldást a kérdésben. 2014 végén több mint 100 ország rendelkezett a világon valamiféle adatvédelmi jogi szabályozással, amely az állami, illetve a vállalati adatkezeléseket is szabályozta, jó néhány országban pedig jelenleg is folyamatban van terület jogi védelmének rendezése. (Banisar, 2016)

Bár az adatvédelemhez való jog univerzálisnak tűnik, az egyes országok mégis merőben eltérő szabályozást alkalmaznak, az európai modell erős állami kontrollt, még sok más szabály, pl. az USA-ban inkább az iparági önszabályozást helyezi előtérbe.

Ennek az egyik legnagyobb vívmány az utóbbi időkből a 2016. április 14-én megszavazott egységes Európai Uniós Adatvédelmi Rendelet (EU, 2016), ami hatályba lépésekor (az egyes országokban legkésőbb 2018 tavaszán kötelező bevezetni a helyi jogi szabályozásba) még szigorúbban és még egységesebben fogja meghatározni a követelményeket az európai országokban. Az új direktíva már tartalmazza, az új okos eszközökön alapuló információs korszakra alkalmazható részletszabályokat is. Az Európai Bíróság egyúttal véget vetett a Safe Harbour (Biztonságos Kikötő) egyezményeknek, amely lehetővé tette az Európai Direktívának meg nem felelő amerikai kormányzati szervek felé történő adatcserét.

### 9.3. A szabályozás haszna

Közhely, hogy minden szabályozás csak annyit ér, amennyi érvényesíthető belőle, amennyit betartanak. Fel kell azonban ismerni azt, hogy a hatékony információbiztonság csak az állam a vállaltok és a felhasználók közös erősfeszítéseivel, együttműködésével lehet létrehozni. Lehet mindenféle szabályokat és szabványokat létrehozni, ám valójában csak az ezek mentén elinduló önszabályozás, megfelelő magatartásminták kialakulása, tudatosodás azok, amelyek a gyakorlati biztonsághoz vezetnek. Ezen túl pedig az állandó képzés és odafigyelés, hiszen minden nap újabb és újabb sérülékenységek kerülnek fel az adatbázisokban, napi szinten jelennek meg új kártevők, a biztonság művelése tehát egy dinamikus folyamat, amelyet a szükségszerűen jóval lassabban változni képes szabályoknak való megfelelési kényszeren túl, a biztonságra való valódi belső igény határoz meg.

Érdemes ebbe fektetni, hiszen az adatvédelem, a privacy folyamatosan, dinamikusan fejlődő területek, ahol a maximális biztonság garantálása az üzletileg elvárt magatartás a felhasználók részéről a szervezetek, intézmények irányában, az ennek való megfelelőség pedig valódi üzleti hasznot, illetve általános biztonságérzetet és elégedettséget képes generálni.

Természetesen az állam feladata az hogy kirostálj a piacot, megkövetelje és ellenőrizze az információbiztonság minimálisan elvárható szintjét a megfelelő ágazatokban, ez azonban csak az alapvonal, még nem biztosít valód versenyelőnyt az adott szervezet számára, ezt csak belülről a kötelező szabályozás internalizálásával, akár az azon való pozitív irányú túllépéssel lehet elérni.

## 10. Gyerekek a weben

Ahogyan a Z-generáció felnövekszik, a gyerekek egyre korábban kerülnek kapcsolatba a modern technikai eszközökkel, ezek nagy részének pedig alapvető működéséhez tartozik az internetkapcsolat kihasználása. Az élet egyre több területével kapcsolatban (kapcsolattartás, információgyűjtés, tanulás, szórakozás, játék, navigáció, fizetés, stb.) kapcsolatban alakul ki függőség a technológiától, ami azt eredményezi, hogy a mai gyerekek tulajdonképpen életünk jelentős részét online élik le. A tabletek, okostelefonok könnyű és intuitív kezelhetősége még lejjebb szállítja azt az életkort, amikor a gyerekek szó szerint a kezükbe vehetik az irányítást a hálón. A szociális életük is párhuzamosan fejlődik online és offline. A fiatalok 95%-a közösségi hálózatokon keresztül (is) használja az internetet. Itt osztják meg az információkat és kommunikálnak a „barátaikkal" és sajnos sokszor a „nem barátaikkal" is. (Lenhart, 2015)

A közösségi hálózatok mellett az olyan eszközök, mint a WhatsApp, online játékok és más portálok kitágítják az internet kommunikációs célú alkalmazását, és a továbbításra és megosztásra kerülő adatok körét. Számos portál és szolgáltatás alakult ki a gyerekek, fiatalok igényeit kiszolgálandó, és több ezek közül fizetős funkciókat és szolgáltatásokat is alkalmaz, tehát jelentős pénzügyi kockázat is fellép, hiszen gyerekek és tinik használják a szülők hitelkártya adatait.

Mennyire vannak felkészülve a felnőttek, hogy kezeljék ezt a helyzetet? A digitális szakadék a szülők és a gyerekek között csak növekedett az elmúlt évek során. Kutatások azt mutatják, hogy a szülők 50%-a egyáltalán nincs tisztában azzal, hogy a gyerekeik mit csinálnak az interneten, és minden 10. gyerek azt állítja, hogy a szüleik egyáltalán nem ismerik azokat a technológiákat, amiket használnak. (Duggan et.al., 2015)

Azzal együtt tehát, hogy a fiatalok elleni kibertámadások határozottan növekvő trendet képviselnek az IT-biztonsági területen, mindez zömében szülői kontroll és beavatkozási lehetőség nélkül folyik. A fiatalok privát szférája elleni támadások alapvetően három dolog köré csoportosulnak: személyes adatok, pénzügyi adatok és szexualitás…

### 10.1. Adatvédelem és sexting

Az internetes adatvédelem egyik leglényegesebb pontja, hogy a adatalanyok kontrollálni tudják a hozzáférést az információkhoz, annak és ahhoz engednek hozzáférést, akinek és amihez ők szeretnének. Ez vonatkozik a személyes adatokra, fotókra, fájlokra, stb. Amikor viszont fiatalokról, gyerekekről van szó, ők még nem rendelkeznek a fenti döntések meghozatalához szükséges belátással, megalapozott döntésképességgel. Az ehhez

szükséges szociális és kognitív készségek csak a serdülő, majd a felnőttkor során alakulnak ki.

Mind a közösségi hálózatok, mind a közösségi funkciókkal (chat, interakció, ismerősök stb.) rendelkező játékok, amelyek a gyerekeket célozzák, lehetőséget adnak arra, hogy az idősebbek átverjék a fiatalokat és adatokhoz jussanak hozzá rajtuk keresztül, manipulálva őket social engineering támadásokon keresztül.

Másrészt a gyerekek nagyon gyakran osztják meg az információkat az ismerőseikkel oly módon, hogy nem veszik figyelembe, ki máshoz juthat még el a hálózatban. Kiváló példa az utóbbira a sexting jelensége, amikor a fiatalok önkéntesen küldenek szexuális töltetű tartalmat magukról, digitális csatornákon keresztül. Ez általános gyakorlattá vált a kamaszok között, függetlenül attól, hogy nagyobb közösségekhez (baráti kör, osztály, iskola) is eljuthat az ilyen módon megosztott tartalom. A fent bemutatott kutatások szerint a válaszadó 18 év alattiak 25%-a küldött már meztelen vagy félmeztelen fotót magáról, emellett a fiatalok 50%-a nyilatkozta azt, hogy látott már ilyen fotót úgy, hogy az eredetileg nem neki volt szánva.

Ezek a tartalmak eredetileg úgy készülnek, hogy két ember között kellene maradniuk, ám először egy kisebb csoportban válnak nyilvánossá, majd terjedésük vitálissá válhat. Az ilyen tartalmak terjesztésének fő csatornái az olyan okostelefonos applikációk, mint az WhatsApp, a Kik, a SnapChat vagy a Twitter.

### 10.2. Becserkészés (grooming)

A becserkészés egy olyan bűncselekmény típus, amely az utóbbi időszakban vált igazán elterjedtté. A becserkészés egy fiatal felnőtt általi, interneten keresztül történő manipulálását jelenti, amely valamilyen szexuális tartalmú tevékenységben csúcsosodik ki: pl. meztelen képek küldetése vagy különböző szexuális tartalmú tevékenységek végeztetése webkamera előtt. Az esetek egy részében a zaklató fizikai kontaktust, valódi találkozót, is kezdeményez az internetes kommunikáció során. A felnőtt sokszor szintén egykorú fiatalnak adja ki magát, hogy megszerezze a célpont bizalmát és érzelmi kapcsolatot alakítson ki vele. Így tudnak elég szimpátiát összegyűjteni ahhoz, hogy legyőzzék a gyermek természetes ellenállását.

Ha már hozzájutott a tartalomhoz, a bűnelkövető az esetek egy részében zsarolni kezdi áldozatát, azzal, hogy megosztja az elhamarkodottan elküldött tartalmat annak barátaival, iskolatársaival, családjával, ha a továbbiakban nem teljesíti a zaklató kívánságait.

Ez az offline világban egy tipikus bűncselekmény volt, ám az online világban az elmúlt időszakban öltött igazán nagy méreteket. Itt a támadóknak könnyű anonimnek maradni,

identitást lopni, egyszerre több áldozatot „cserkészni". Az esetek nagy részében a kapcsolat a közösségi hálózatokon indul és időnként kiterjed a fizikai világra is, ahol rossz esetben pedofília vagy nemi erőszak, gyermekbántalmazás is lehet dolog vége.

A kutatásokban rendre megjelenik, hogy a szexuális gyermekbántalmazás online elkövetői tipikusan jól képzett, munkahellyel rendelkező, főleg európai és észak-amerikai, különböző korú férfiak, de női elkövetőket is derítettek már fel. Arról azonban egyáltalán nincsenek adatok, mennyien is lehetnek azok, akik az interneten környékezik meg a gyerekeket. A grooming ugyanis sok országban nem minősül bűncselekménynek – ahogyan Magyarországon sem –, ezért nem is vezetnek róla nyilvántartást. (UNICEF, 2011) Az esetek menete általában azonos sémát követ: bizalomépítés, gyorsan változó személyazonosságok, ajándékok, vagy egyszerűen csak közös időtöltés egy virtuális közösségben vagy online játéktérben.

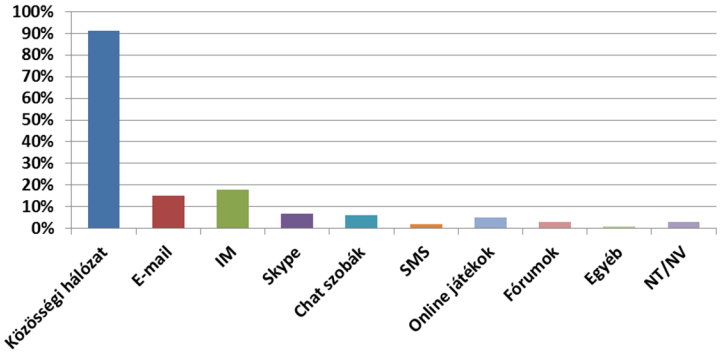
### 10.3. Virtuális bántalmazás (cyberbullying)

A fiatalok esetében a józan belátás hiánya nem csak a személyes adataik könnyebb kiadásában, terjesztésében nyilvánulhat meg, de az agresszív, erőszakos tartalmak kontrollálatlan terjesztésében is.

A virtuális bántalmazás színterei szintén a közösségi hálózatok, az üzenetküldő chat programok, az e-mail és a weboldalak, fórumok. Bosszantó, fenyegető, megalázó tartalmak publikálását jelenti, amelyek egy konkrét személyt céloznak, ezzel őt zaklatják, akár el is lehetetlenítik. A leggyakoribb formái a rémhírterjesztés, hamis pletykák, megalázó fotók és videók, és az áldozat elleni fizikai és/vagy pszichológiai erőszakra buzdító tartalmak, profilok, weboldalak létrehozása. A zaklatók sokszor más személyek identitása mögé bújva végzik cselekményüket, terjesztik a hazugságokat, vagy fenyegetik az áldozatot érzékeny, kínos személyes információk, adatok kisziárogtatásával.

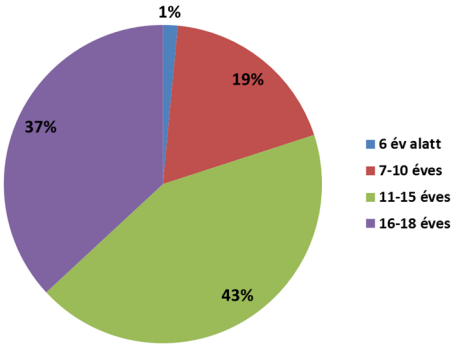
Az áldozatok általában érzékeny, sérülékeny személyiségek, akik mások, mint az őket zaklató közeg. A virtuális bántalmazás sajnos exponenciálisan terjed a weben és nagyon nehéz gátat szabni neki. Éppen ezért különösen veszélyes és ártalmas.

Évekig a zaklatás egy konkrét helyre, pl. az iskolára korlátozódott, onnan kiszabadulva az áldozat megszabadult zaklatóitól, ám mióta a folyamat a virtuális térbe költözött, a 24 órás online jelenlétnek köszönhetően nincs menekvés, éppen ezért az ilyen, állandó zaklatás sokkal traumatikusabb a gyerekek számára, mert folyamatosan jelen van az életükben, ráadásul egyre terjed, teljesen ellehetetlenítve őket a számukra oly fontos virtuális terekben.




**9. ábra: A virtuális zaklatás (cyberbullying) legfőbb színterei (ESET, 2015 alapján)**

Bár a jelenség nem újkeletű, és ismert is a szakemberek körében, a zaklatás nagyon sokáig lappanghat a virtuális térben, mielőtt fizikai formában manifesztálódna, így nagyon sokáig gyötörheti az áldozatot, a digitális szakadék miatt a felnőtt, szülői, tanári segítségtől jórészt elválasztva. A kutatások szerint a zaklatás első számú helyszínei a közösségi hálózatok, majd az azonnali üzenetküldő – főként mobilos – szolgáltatások következnek a sorban. Egy kutatásban a megkérdezettek 42%-a ismert olyan embert, aki áldozata volt hasonlóknak, és ezek között jócskán voltak 14 év alattiak is, noha hivatalosan nekik nem is lehetne a szabályzat szerint pl. Facebook profiljuk.




**10. ábra: A virtuális zaklatás (cyberbullying) célpontjai korcsoport szerint (ESET, 2015 alapján)**

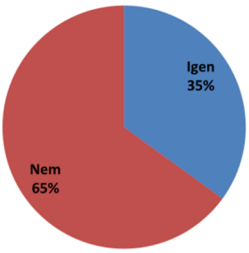
A fiatalok számára ez a digitális korszak egyik legnagyobb fenyegetése és elterjedtsége várhatóan folyamatosan növekedni fog a következő évek során.

### 10.4. Megelőzés

Bármilyen, a gyerekekre leselkedő digitális fenyegetésről is legyen szó első sorban a kommunikáció, a szülők, felnőttek iránti bizalom, a megfelelő otthoni légkör megteremtése a fontos, amelyben a gyerek a digitális szakadék ellenére hajlandó beszélni a problémáiról. A szülők részéről viszont nem lehet az a válasz, hogy túlreagálva eltiltják a technológiától, abban látva minden baj okozóját. Ha ez a veszély fenyeget a gyerekek sosem fognak megnyílni, hiszen a Z-generáció életének annyira részévé válik a technika, hogy nem tudnak, nem is akarnak lemondani róla, bármilyen veszélyekkel vagy atrocitásokkal kell is szembenézniük ebben a közegben. A felnőttek felelőssége tehát az, hogy ennek tudatában legyenek képesek hatékonyan segíteni, megerősíteni a fiatalt.

Mindezzel együtt hasznos lehet, ha gyerekek nem tudják kontrollálatlanul fogyasztani a technológiát, a tartalmat és a szolgáltatásokat. A különböző szűrők, korlátozások, szülői zárak egy darabig hatékony segítséget tudnak nyújtani. Ezek esetében fontos az, hogy a digitálisan elmaradottabb szülők is képesek legyenek kezelni, alapvető dolgokat beállítani rajta, felületük és vezérlésük a digitálisan gyengébb képességű felhasználók számára is használható kell, hogy maradjon.

A másik lehetőség természetesen a törvényi védelem, és annak tudatosítása már egészen fiatal korban, hogy a digitális zaklatás bűncselekmény, ami ugyanolyan büntetési tételeket von maga után, mint ugyanennek a fizikai világban való elkövetése. Mind az áldozatoknak, mind a potenciális elkövetőknek tudniuk kell, hogy vannak törvényi keretek ezen a területen, amelyeket be kell tartani, és amelyek valós büntetéssel fenyegetnek. Természetesen a törvényeket mindig ki kell, hogy egészítsék házirendek: akár otthon, akár az iskolában vagy egyéb közösségekben. A család, az iskola is fel kell hogy hívja a figyelmet a veszélyekre, bemutatva, hogy hol lehet segítséget kérni és a segítségkérést valóban komolyan venni, az eseteket megfelelően kivizsgálni, az esetleges beazonosított elkövetők számára pedig példa értékű következményeket támasztani.




**11. ábra: A törvényi védelem ismerete hiányzik (ESET, 2015 alapján)**

Különösen a közösségi oldalak és az online játékokban végzett tevékenységek kerülnek ki a felnőtt környezet látóköréből, ezekben a közösségekben a felnőttek nem mindig tudnak és nem is akarnak jelen lenni, ám a helyes fizikai világban történő kommunikációval, annak tudatosításával a gyerekekben, hogy bárki bármit állíthat magáról a profiljában, de az nem feltétlenül valós, nagyon sokat tehet a környezet ezen esetek megelőzéséért.

## 11. Összefoglalás: A legfontosabb trendek, a legnagyobb kihívások

Mindenek előtt egyértelműen leszögezhető, hogy a támadások egyre kifinomultabbá válnak. Az adat- és információbiztonság egyre drágább és komplexebb intézkedéseket kíván, még a jól képzett személyzet is egyre nehezebb helyzetben van. A biztonság megteremtése, a szükséges költségek (Ponemon, 2015c) fedezése sziszifuszi küzdelemnek tűnik, ám a felhasználó az állam és az üzleti szféra összefogása, az irányítás, az oktatás és a technológia együtt sikeres védelmet teremthet.

Mivel a technológia egyre inkább átszövi életünket, különösen az okoseszközök, a dolgok internete korában, el kell fogadni, hogy a biztonsági rések, a támadási felület akárhol lehet, olyan helyeken is amire korábban nem is gondoltunk volna. Ez nagyon nagy kihívást jelent a biztonság-menedzsmentnek, a kockázatok teljes körű felmérésének.

A jövő kihívása egyértelmű: 5 év múlva várhatóan mintegy 21 milliárd eszköz fog kapcsolódni a világhálóra a Gartner szerint (Gartner, 2015c), de ez nem azt jelenti, hogy a felhasználóknak paranoiássá kell válniuk, mindenhol ellenséget kutatva. A biztonságba való tudatos befektetés viszont továbbra sem maradhat el. A vállalatoknak hozzá kell jutniuk a legfrissebb technológiákhoz, amelyekkel megvédelmezhetik üzleti érdekeiket. A védelmi rétegek, az előjelző és felderítő rendszerek tudatos és szisztematikus elhelyezése és karban tartása kiemelt feladat az adatszivárgások és kibertámadások megelőzéséhez.

Ha az alkalmazottak képesek felismerni a veszélyt, a támadást, ami többnyire e-mailben érkezik, az jelentősen csökkenti a reakcióidőt és sokszorosára növeli a sikeres védekezés esélyét. Ezt a képességet természetesen csak állandó biztonság-tudatosítás és megfelelő képzések segítségével lehet elérni. Ez a képesség sosem fog kifejlődni, ha a felhasználót, a felhasználók bevonódását a szervezet nem kezeli a biztonsági rendszer integráns részeként, fontos üzleti területként. Megfelelően képzett alkalmazottak hiányában egy szervezet sokkal sebezhetőbb a kibertámadásokkal szemben.

A kiemelkedően sikeres, nagy kárt okozó támadások legtöbbször nem a támadási módszerek, az innováció miatt lesznek kiemelkedően sikeresek, hanem a felhasználói nemtörődömség, tudatlanság, óvatlanság vezet el oda. Az államnak, a vállalatoknak, de az otthoni felhasználóknak is aktívan kell cselekedniük, ha infrastruktúrájukat és adataikat meg akarják védeni.

A felhasználók egyre magasabb szintű biztonságot és adatvédelmet kívánnak, biztonságban akarják tudni gyermekeiket és elvárják, hogy az állam és a biztonsági cégek tegyenek meg mindent, hogy az a sok millió új eszköz, ami összeköttetést teremt az életünkben, biztonságosan működhessen és kommunikálhasson.

Bár a biztonsági cégek, a vállalatok és az állam szerepe jelentős, az IT-biztonságban az egyén szerepe egyre inkább felértékelődik. A rengeteg adat és szolgáltatás,amit felhasználunk, már mind digitálisan tárolódik, valahol, nem lehetünk benne biztosak, hogy hol, pontosan milyen rendszeren és egyáltalán melyik országban, minden esetre a saját, közvetlen befolyásunk alatt álló rendszereken kívül, ahol persze dönthetünk a sorsáról, amennyire a felhasználói megállapodások, ÁSZF-ek megengedik, de fizikailag sosem lesz már nálunk.

A vállalati stratégiák három pillére a menedzsment, a technológia és a képzés. (Chaffey – White, 2010) Az állam és a biztonsági cégek szerepét is hangsúlyozni kell, hiszen megfelelő jogi keretek között lehet csak hatékony védelmet kialakítani, meg kell határozni azokat a szabványokat, amiket a biztonságnak, a technológiának, a fejlesztésnek alkalmazkodnia kell. Fenn kell tartani az emberek biztonságérzetét, az adataik védelmét, valamint a közszolgáltatások és a kritikus infrastruktúra folyamatos működését. Az új technológiai irányokat kutató R&D projektek esetében a biztonság, mint szempont, meg kell hogy jelenjen már az ötletnél, a tervezés legelső lépéseinél, csak így tud majd integráns részévé válni a végleges terméknek, szolgáltatásnak.

Egyre több sérülékenység válik ismertté és ilyen körülmények között kell a jövőben fenntartani a hálózatokat, a hozzáférést az internethez és azokat a megoldásokat, amelyekkel az egyes eszközök képesek összekapcsolódni. A routerektől, amelyek az otthoni internet-hozzáférés kapui, az okos városokig minden szinten ki kell emelni a biztonság szerepét, amely csak a megfelelő együttműködés során érhető el.

Az itt bemutatott szempontokat tükröző proaktív, együttműködő, stratégiai-, taktikai- és egyedi akciók szintjén megtervezett, jogilag támogatott informatikai biztonság az egyetlen, amely képes az állandóan megjelenő új sérülékenységek, és a napi szinten érkező új technológiai eszközök tengerében megvédelmezni a mindennapi életnek, működésnek, létezésnek egyre inkább elválaszthatatlan részét képező informatikai szolgáltatásokat és rendszereket.

**Köszönetnyilvánítás**

Jelen tanulmány elkészítését a PD-109740 számú „IT és hálózati sérülékenységek tovagyűrűző társadalmi-gazdasági hatásai” című projekt támogatta a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal – NKFIH finanszírozásával.

**Irodalomjegyzék**


[1] Albors, Josep 2015: 400GB of info leaked from Hacking Team. welivesecurity, 2015.07.06., http://www.welivesecurity.com/2015/07/06/400gb-info-leaked-hacking-team/

[2] Banisar, David 2016: National Comprehensive Data Protection/Privacy Laws and Bills 2016 Map, SSRN, 2016.04.30. http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2776621_code1573110.pdf?abstractid=1951416&mirid=1

[3] Castro, Raphael Labaca 2015: Germany's Industrie 4.0 – the challenges in IT-Security, welivesecurity.com 2015.11.03. http://www.welivesecurity.com/2015/11/03/what-is-industry-4-0/

[4] Chaffey, Dave – White, Gareth, 2010: Business Information Management - Improving Performance Using Information Systems, 2nd Edition, Pearson, 2010.

[5] Cobb, Stephen 2015a: Cybercrime update: take downs, arrests, convictions, and sentences, welivesecurity.com, 2013.07.27. http://www.welivesecurity.com/2015/07/27/cybercrime-take-downs-arrests-convictions-sentences/

[6] Cobb, Stephen 2015b: Hacking Team and other breaches as security lessons learned, welivesecurity.com, 2013.08.01. http://www.welivesecurity.com/2015/08/01/security-lessons-hacking-breaches/

[7] Constantin, Lucian: Scareware found hidden in Google Play apps downloaded by millions, IDG - PCWorld, 2015.02.04. http://www.pcworld.com/article/2879952/scareware-found-hidden-in-google-play-apps-downloaded-by-millions.html

[8] CSEC, 2011: SNOWGLOBE - From Discovery to Attribution, Communications Security Establishment Canada, Der Spiegel, http://www.spiegel.de/media/media-35683.pdf

[9] Daws, Ryan 2014: Bitdefender proves Bluetooth wearables' vulnerability, WearableTech, 2014.12.15., http://www.wearabletechnology-news.com/news/2014/dec/15/bitdefender-proves-bluetooth-wearables-vulnerability/

[10] Donohue, Brian 2014: WireLurker Apple Malware Targets Mac OS X Then iOS, Kaspersky Lab, 2014.11.06. https://blog.kaspersky.com/wirelurker-ios-osx-malware/6563/

[11] Ducklin, Paul 2015: Apple's App Store hit by the XCodeGhost of malware present, SOPHOS, 2015.09.22. https://nakedsecurity.sophos.com/2015/09/22/apples-app-store-hit-by-the-xcodeghost-of-malware-present/

[12] Duggan, Maeve et. al. 2015: Parents and social media, Pew Research Center, 2015.06.16. http://www.pewinternet.org/files/2015/07/Parents-and-Social-Media-FIN-DRAFT-071515.pdf

[13] Ellison, Kyle 2015: Hacked nanny cam plays mysterious music to sleeping baby, Welivesecurity, 2015.04.07., http://www.welivesecurity.com/2015/04/07/hacked-nanny-cam-plays-mysterious-music-sleeping-baby/

[14] ENISA, 2015: ENISA Work programme 2016, European Union Agency for Network and Information Security, https://www.enisa.europa.eu/publications/corporate/enisa-work-programme-2016

[15] ENSZ, 1948: Az Emberi Jogok Egyetemes Nyilatkozata, Egyesült Nemzetek Szervezete, 1948, http://www.menszt.hu/layout/set/print/content/view/full/201

[16] Erven, Scott – Collao, Mark, 2015: Medical Devices: Pwnage and Honeypots, DefCon 2015 Conference, 2015.08.06-09. https://www.youtube.com/watch?v=qX_dV6LUTdo

[17] ESET, 2013: TRENDS FOR 2013 – Astounding growth of mobile malware, ESET Latin America's Lab, http://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf

[18] ESET, 2015a: TRENDS FOR 2015 – Targeting the Corporate World, ESET LATAM Research Lab, http://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf

[19] ESET, 2016: TRENDS 2016 – In Security Everywhere, ESET, http://www.welivesecurity.com/wp-content/uploads/2016/01/eset-trends-2016-insecurity-everywhere.pdf

[20] EU, 2016: Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg), Európai Unió, 2016.04.27. http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=HU

[21] Europol, 2015: The Internet Organised Crime Threat Assessment (IOCTA) 2015, Europol, 2015.09.30. https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf

[22] Gálffy, Csaba 2015: Stagefright: mit kell tudni az új Android-horrorról?, hwsw.hu 2015.07.28. http://www.hwsw.hu/hirek/54313/android-stagefright-sebezhetoseg-biztonsag-worm-tamadas.html

[23] Gartner, 2015a: Gartner Says Worldwide Smartphone Sales Recorded Slowest Growth Rate Since 2013, Gartner, 2015.08.20. http://www.gartner.com/newsroom/id/3115517

[24] Gartner, 2015b: Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015, Gartner – Stamford, Conn 2015.09.23., http://www.gartner.com/newsroom/id/3135617

[25] Gartner, 2015c: Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner – Stamford, Conn 2015.11.10., http://www.gartner.com/newsroom/id/3165317

[26] Gilbert, David 2015: Porn Droid Android App Revealed As LockerPIN Ransomware Locking Your Smartphone, ibttimes.com, 2015.09.10. http://www.ibtimes.com/porn-droid-android-app-revealed-lockerpin-ransomware-locking-your-smartphone-2090926

[27] Github, 2015: APT Notes, https://github.com/kbandla/APTnotes

[28] Horváth, Attila Dr. – Kiss, Ferenc Dr. – Szanyi, István – Török, Marianna, 2015: Modern ICT technologies – situation and trends, In: Ferenc Kiss (ed.): Tourism and ICT Aspects of Balkan Wellbeing - A Balkán Jóllét Turisztikai és IKT Vonatkozásai, 155-186. old., ISBN 978-615-80061-2-5, Információs Társadalomért Alapítvány, Komlóska

[29] Horváth, Attila Dr., 2011a: IT és hálózati sérülékenységek tovagyűrűző hatásai a gazdaságban, NETWORKSHOP 2011. konferencia, Kaposvári Egyetem, 2011. április 27-29.

[30] Horváth, Attila Dr., 2011b: Informatikai sérülékenységek és kockázatok – a társadalmi-gazdasági hatások tükrében (A második év eredményei), 8. Országos Gazdaság-informatikai Konferencia OGIK'2011, Szent István Egyetem, Győr, 2011. november 11-12.

[31] Info Tv, 2011: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, Magyarország Kormánya, 2011. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV

[32] ISO/IEC 2013: ISO/IEC 27001 - Information security management, International Standards Organization, 2013 http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[33] ISO/IEC, 2014: The ISO Survey of Management System Standard Certifications – 2014, International Standards Organization, 2014 http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2014

[34] ISO/IEC Stat 2014: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=#standardpick

[35] KrebsonSecurity, 2015: ATM Skimmer Gang Firebombed Antivirus Firm, 2015.09.15. http://krebsonsecurity.com/2015/09/atm-skimmer-gang-firebombed-antivirus-firm/

[36] Lenhart, Amanda 2015: Teens, Social Media & Technology Overview 2015, Pew Research Center, 2015.04.09. http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf

[37] Lipovsky, Robert 2014: ESET Analyzes Simplocker – First Android File-Encrypting, TOR-enabled Ransomware, welivesecurity.com, 2014.06.04. http://www.welivesecurity.com/2014/06/04/simplocker/

[38] Lipovsky, Robert, 2013: Cryptolocker 2.0 – new version, or copycat?, welivesecurity, 2013.12.19., http://www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/

[39] McKinsey 2015: Industry 4.0 - How to navigate digitization of the manufacturing sector, McKinsey Digital, 2015, https://www.mckinsey.de/files/mck_industry_40_report.pdf

[40] Mendoza, Miguel Ángel, 2015: The evolution of ransomware: From PC Cyborg to a service for sale, welivesecurity, 2015.09.18., http://www.welivesecurity.com/2015/09/18/evolution-ransomware-pc-cyborg-service-sale/

[41] Microsoft 2012: Microsoft Security Bulletin MS12-027 – Critical, Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258), Microsoft, 2012.04.10. https://technet.microsoft.com/en-us/library/security/ms12-027.aspx

[42] Mitre, 2014: CVE-2014-6041, Mitre.org - Common Vulnerabilities and Exposures, 2014., https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6041

[43] Mitre, 2015: CVE-2015-3860, Mitre.org - Common Vulnerabilities and Exposures, 2015., https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3860

[44] O'Brien, Dick 2015: Scammers quick to capitalize on Ashley Madison breach, Symantec, 2015.08.27. http://www.symantec.com/connect/blogs/scammers-quick-capitalize-ashley-madison-breach

[45] Oh, Jeong Wook: Smart Home Appliance Security and Malware, Virus Bulletin Conference, 2014. szeptember, https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Oh.pdf

[46] Osborne, Charlie 2015: Tox ransomware owner 'screws up,' offers platform for sale, ZDNet, 2015.06.05., http://www.zdnet.com/article/tox-ransomware-owner-screws-up-offers-platform-for-sale/

[47] Paganini, Pierluigi 2015: Hidden Tear Ransomware is now open Source and available on GitHub, Securityaffairs, 2015.08.18., http://securityaffairs.co/wordpress/39419/cyber-crime/ransomware-open-source.html

[48] Paganini, Pierluigi 2016: From August 2015 to February 2016 Buhtrap group managed to conduct 13 successful attacks against Russian banks for a total amount of $25.7 mln., Securityaffairs, 2016.03.18., http://securityaffairs.co/wordpress/45405/cyber-crime/buhtrap-group-attacks.html

[49] Panda, 2011: Crimeware: the silent epidemic, Panda Security, http://www.pandasecurity.com/homeusers/security-info/types-malware/crimeware/

[50] Ponemon 2015a: 2015 Cost of Data Breach Study: Global Analysis , Ponemon Institute LLC, 2015. május, https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF

[51] Ponemon 2015b: Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data , Ponemon Institute LLC, 2015. május, http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf

[52] Ponemon, 2015c: 2015 Cost of Cyber Crime Study: Global, Ponemon Institute LLC, 2015. október https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

[53] Purba, Narinder, 2015: Cybersecurity research boost for medical devices, welivesecurity.com 2015.11.03., http://www.welivesecurity.com/2015/11/03/medical-device-cybersecurity-research-boost/

[54] Rios, Billy – McCorkle, Terry, 2014: Medical Devices Hard-Coded Passwords, ICS-CERT, 2014.06.13., https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01

[55] SC Magazine, 2015: Fitness wearables vulnerable to data exfiltration, Sc Magazine UK editorial staff, 2015.03.27. http://www.scmagazineuk.com/fitness-wearables-vulnerable-to-data-exfiltration/article/405909/

[56] Schulze, Holger 2016: BYOD & MOBILE SECURITY SPOTLIGHT REPORT, LinkedIn Informtion Security Community, 2016, http://www.gyartastrend.hu/download.php?id=27070

[57] Matrosov, Aleksandr et.al. 2011: Stuxnet Under the Microscope Revision 1.1 , ESET 2011, https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf

[58] Stefanko, Lukas 2015: Aggressive Android ransomware spreading in the USA, welivesecurity.com, 2015.09.10. http://www.welivesecurity.com/2015/09/10/aggressive-android-ransomware-spreading-in-the-usa/

[59] Symantec, 2011: Advanced Persistent Threats: A Symantec Perspective, Symantec, 2011. november, http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

[60] Thomas, Karl 2015a: How secure is your smartwatch?, welivesecurity, 2015.04.15. http://www.welivesecurity.com/2015/04/15/secure-smartwatch/http://www.welivesecurity.com/2015/04/15/secure-smartwatch/

[61] Thomas, Karl 2015b: New exploit compromises Samsung Galaxy phones, welivesecurity.com, 2015.06.17. http://www.welivesecurity.com/2015/06/17/new-exploit-compromises-samsung-galaxy-phones/

[62] Thomas, Karl 2015c: Security of Ashley Madison breached sooner than you think, welivesecurity.com, 2015.08.27. http://www.welivesecurity.com/2015/08/27/ashley-madison-timeline-events/

[63] UNICEF, 2011: Child Safety Online – Global Challenges and strategies, UNICEF Innocenti Research Centre, 2011. december, https://www.unicef-irc.org/publications/pdf/ict_eng.pdf

[64] Verzion, 2016: 2016 Data Breach Investigations Report, Verzion, 2016, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

[65] Woollaston, Victoria 2015: Apple Watch security flaw leaves it vulnerable to thieves: Device can be reset and paired with ANY phone within minutes, DailyMail Online, 2015.05.14., http://www.dailymail.co.uk/sciencetech/article-3081478/Apple-Watch-security-flaw-leaves-vulnerable-thieves-Device-reset-paired-phone-minutes.html

[66] Xing, Luyi et.al. 2015: Cracking App Isolation on Apple: Unauthorized Cross-App Resource Access on MAC OS X and iOS, ACM, 2015, http://www.informatics.indiana.edu/xw7/papers/xara-ready.pdf

[67] Zaske, Sara 2015: Germany's vision for Industrie 4.0: The revolution will be digitised, ZDNet 2015.02.23., http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised/#!