IT és hálózati sérülékenységek tovagyűrűző hatásai a gazdaságban

Dr. Horváth Attila
Főiskolai Docens
Dunaújvárosi Főiskola, Informatikai Intézet
E-mail: horvath.attila@mail.duf.hu

Összefoglalás: Az IT sérülékenységek, hálózati problémák, távközlési, műsorszórási gondokat leggyakrabban informatikai, műszaki problémaként kezeljük. Ezen események azonban sok áttételes hatást is generálnak, amelyek felderítésére egyelőre nincsenek egységes módszerek, megoldások. Az előadás egy újszerű kutatás első eredményeiről számol be, amely a CERT-Hungary közreműködésével, ezen események gazdasági-társadalmi hatásainak felmérését tűzte ki célul.

Kulcsszavak: IT sérülékenység, gazdaság, hálózat, műsorszórás

Abstract: IT vulnerablities and network failures, telecommunication and broadcasting problems are oftenly considered as an IT-based engineering problem. These events however have massive collateral effects on the economy and society, which are often neglected, and there is no uniform methodology to measure and describe this. The lecture covers the first outcomes of a novel research in association with CERT-Hungary dealing with these secondary effects of ICT affairs.

Keywords: IT vulnerablity, economy, network, broadcast

1. Bevezető

Az ICT egyre jobban áthatja életünket, a technológiák felhasználása kiterjedt mind az otthonokban, mind a gazdaságban. Jelenlétüket természetesnek vesszük, részei lettek a mindennapi infrastrukturális szolgáltatásoknak. Épp ezért meghibásodásuk, kiesésük ugyanolyan súlyosan tudja érinteni a gazdasági szereplőket vagy a háztartásokat, mint bármelyik más infrastrukturális erőforrás kiesése. Ha ehhez hozzávesszük azt, hogy ezek a technológiák tartalmazzák és őrzik szinte a teljes információvagyont, legyen szó akár céges, esetleg kormányzati adatokról, vagy épp a család fényképalbumáról, láthatjuk hibátlan, biztonságos működésük fenntartása közérdeknek tekinthető.

E területek problémáit, meghibásodásait mégis elsődlegesen technológiai oldalról közelítik, noha egy rendszersérülés, meghibásodás vagy épp szándékos támadás erőteljes tovagyűrűző hatásokkal rendelkezik a gazdaságban és a társadalomban.

Ezek a meghibásodások komoly károkat okozhatnak, mondhatnánk, hogy elhárításuk alapvetően technológiai, informatikai feladat. Ebben van is igazság, ám nem lehet figyelmen kívül hagyni néhány komoly kiegészítő körülményt. E hatások mérésére gyakorlatilag nem létezik egységes módszertan, noha nagyon fontos lenne számszerűsítésük. Egyrészt a technológiai beruházások, védekezési költségek megalapozásához, *hiszen sem kormányzati, sem vállalati szinten általában nem informatikai végzettségű szakemberek döntenek a keretszámokról,* így különösen fontos, hogy számukra is kézzelfoghatóvá tegyük e problémákat. Másrészt *az ICT-vel szembeni általános társadalmi bizalom is súlyos csorbákat szenvedhet* a nem megfelelő problémakezelés által, ami viszont a modernizációs, *digitális írástudás növelését célzó stratégiákat veszélyezteti.*

2. A kutatásról

A kutatás komoly összefogáson alapul. Alapvetően a Puskás Tivadar Közalapítvány Nemzeti Hálózatbiztonsági Központ (a továbbiakban PTA-CERT) és az Információs Társadalomért Alapítvány INFOTA kutatóintézet (a továbbiakban INFOTA) együttműködése indította el a vizsgálatokat. A kutatói kör pedig kiegészült a BellResearch Kutatóintézettel, akik már több mint 10 éve gyűjtenek adatokat az ICT-szektorban, illetve olyan gazdasági, műszaki területen jártas kutatókkal, akik az elemzésekben, vagy egy-egy speciális területen pl. hírközlési szolgáltatások, posta, stb. tudtak információkat beszállítani.

A sérülékenységek elemzésekor a nemzetgazdaságilag leginkább fenyegető, kritikus sérülékenységeket vettük figyelembe. Alapvetően három módszertan mentén történik az elemzés:

1. A kritikus sérülékenységek csoportosítása, gyártó, termék, esetleg verzió szerint és ezek összevetése a magyarországi szoftver és ICT-eszközhasználati adatokkal a lakossági és a vállalati szektorban, a szoftver és rendszerhasználati adatok forrása a kutatás első körében a BellResearch, Magyar Infokommunikációs Jelentés 2009. című kiadványa.
2. Ezután szekunder kutatások bevonásával, valamint szakértői becslésekkel kísérletet tettünk a sérülékenységek által előidézett potenciális károk, időkiesések, pénzben, munkaórában, egyéb, a gazdasági döntéshozók számára kézzelfogható formában való denominálására.
3. Ezen túl az egyes sérülékenységek mélyreható elemzésével, az adott sérülékenységet kihasználó támadás hatásainak bemutatása, ezáltal az IT-vezetők és döntéshozók figyelmét erőteljesebben sikerülhet felhívni a problémákra.

A kutatás 2010 nyarán indult el, ekkor 2010. első féléves adatai kerültek elemzésre, majd negyedévente bővült a feldolgozott adatok köre, 2011 elején pedig a teljes 2010-es év értékelése látott napvilágot. A kutatás gördülő módszerekkel folytatódik a 2011-es év során is, bővítve a módszertant és strukturálva a vizsgálatokat. A kutatás eredményei a tudományos/szakmai publikációk mellett felhasználásra kerülnek a PTA-CERT által megjelentetett negyedéves és éves jelentésekben, kiadványokban.

3. Sérülékenységek és eszközhasználat

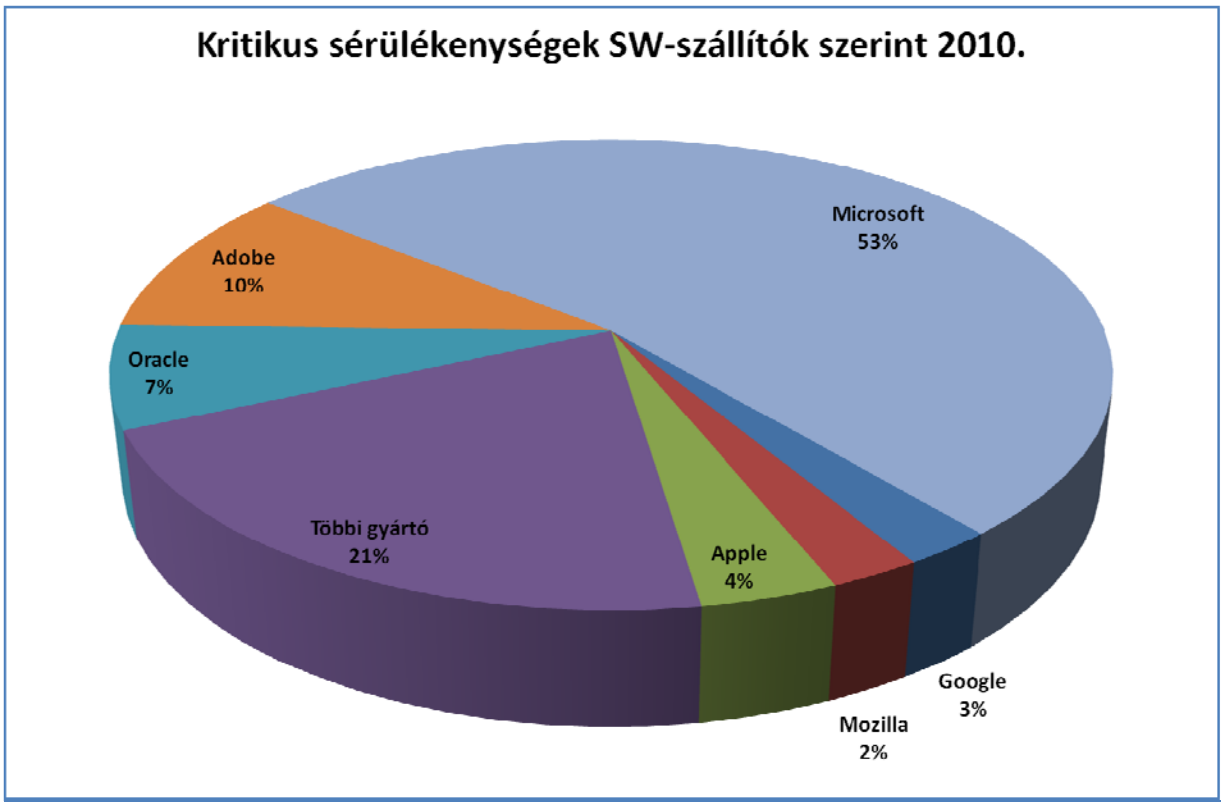
A 2010-es év a szoftver sérülékenységek szempontjából eléggé egyoldalú képet mutatott. összesen 252 kritikus sérülékenységre derült fény az év során. Ebből mintegy 235 az első féléves időszakban vált ismertté, a második félév lényegesen nyugodtabb volt mindössze 27 igazán kritikus eseménnyel, persze súlyos sérülékenységek ennél jóval nagyobb számban kerültek a látótérbe, ám az év végéig megfigyelhető volt egy folyamatosan javuló tendencia. Az érintett szoftverszállítókat tekintve nem meglepő, hogy igen szoros kapcsolat áll fenn egy-egy szoftver elterjedtsége és a kritikus, valódi kockázatot jelentő hibák mennyisége között.

- Ebből a szempontból az év két kiemeltje a **Microsoft,** amelynek különböző termékei (Windows, IE, Office) az év kritikus sebezhetőségeinek ¾-éért felelősek.
- A második szállító az **Adobe** volt, a harmadik helyezett az **Oracle**, amelynek termékei főként az első félévben szenvedtek kritikus biztonsági problémáktól.
- A lista további helyein, a nemzetgazdasági szempontból is kritikus sérülékenységek között található még a két vezető, Microsofttól független böngésző szállító a **Mozilla (Firefox)** és a **Google (Chrome)** termékei is, amelyek sérülékenységei széles körű és a nemzetgazdaság minden szintjén jellemző elterjedtsége szintén aggodalomra adhat

okot. Ezek a problémák főként az év második felében láttak napvilágot.

A Microsoft esetében különösen nagy veszélyt rejt magában, hogy a legszélesebb körben használt asztali operációs rendszerek és az Office termékcsalád a leginkább érintettek, A többi kiemelt szállítónak pedig főleg az internethasználathoz, böngészéshez köthető termékei a kockázathordozók. A Google, a Mozilla esetében is érintettek a böngészők; az Adobe esetében, pedig különösen nagy kockázatot jelent, hogy a szinte minden böngészőbe beépülő (Flash, Shockwawe), illetve a minden PC-n megtalálható dokumentumolvasó (Reader) alkalmazásokat érintették a legsúlyosabb hibák.

Meg kell említeni, hogy a hibák nem csak windows platformot érintik, az év sérülékenységei között előkelő helyre futottak be az Apple operációs rendszereit (iOS, MacOS), böngészőit (Safari), valamint az Apple hardverek és a PC együttműködését biztosító iTunes alkalmazás.



Ez azt jelenti, hogy ezen széles körben elterjedt szoftverek sérülékenységeinek kihasználása az egész nemzetgazdaság szintjén súlyos és nehezen elháríthatóproblémákat eredményezhet.

3.1. Lakosság

Az adat-információ biztonságnak nem a műszaki-technikai feltételek, hanem a műszaki-technikai eszközöket üzemeltető, a dokumentumokat, adatokat, információkat kezelő személyzet, az ember a legnagyobb kockázata. A mai munkavégzés, szervezés, irányítás, végrehajtás és ellenőrzés jelentős része elektronikusan zajlik, számítógépeken illetve távközlő, számítógépes hálózatokon.

Ezek az emberek különböző szerepkörökben vesznek részt az infokommunikációs rendszerekhez való hozzáférésben. Például: tulajdonosi kör; menedzsment, felső vezetés; középvezetők; alsószintű vezetés; ügyintézők; távközlési-informatikai üzemeltetők; karbantartók, takarítók, őrző-védő szolgálat munkatársai; a cég ingatlanjának, ingóságainak kezelését, tervezését, építését, fejlesztését, üzemeltetését, biztonságvédelmét végzők, stb. A

felsorolt csoportoknak és tagjainak érdekei, tevékenységei, motivációi, szerepei, felelősségei és kockázati vonatkozásai eltérőek. Az emberi tényezőnek, mint a legjelentősebb biztonsági kockázati elemnek az ellenőrizhetősége is megszervezhető bizonyos kereteken belül jelentős, de nem végezhető el mindenre kiterjedően, azaz a teljes kockázatmentességet nem lehet elérni.

Az alapvető probléma, hogy egy ember gondolkodó, okos lény, miközben azonban szubjektum, érzelmi lény is egyben, azaz az élete egy változó folyamat, ami ismeretlenül-láthatatlanul és kiszámíthatatlanul is befolyásolhatja egyéniségét, tulajdonságait, érdekviszonyait. Az adat-információvadászok számára ennek kihasználása a legegyszerűbb és legolcsóbb, mert egy vagy több személy megvásárlása sokkal kevésbé kockázatos, mint egy bizonyos fokig védett műszaki-technikai rendszer megcsapolása, lehallgatása és sokkal olcsóbb is.

Figyelembe véve a magyarországi IT-eszköz használat sajátosságait, hogy a lakossági területen a számítógéppel ellátott háztartások 87%-ban használják valamelyik Windows verziót operációs rendszerként, ebből is a sérülékenységekkel leginkább érintett két típust az XP-t és a 2000-t.

Az irodai programcsomagok esetében hasonló a helyzet, az irodai programokat használó háztartások mintegy 83%-a használ Office-t, az adatokból kitűnik, hogy az Office verziók sérülékenységei nagyjából kiegyenlítik egymást, egyik sem emelkedik ki biztonságosságban jelentősen a többi közül.

Emellett aggasztó, hogy potenciális veszélyek ellenére csak a felhasználók mintegy ¾-énél alkalmazzák az informatikai biztonság alapszintjének tekinthető vírusvédelmi megoldásokat, sok esetben ezek sem megfelelően frissítettek, amely lényegesen rontja hatékonyságukat. Tűzfal a felhasználók felét védi, kémprogramok elleni (anti spyware) szoftver pedig mindössze a PC-vel rendelkező háztartások tizedében található meg. (Az adatok forrása a Bellresearch [1])

Figyelembe véve a lakosság szoftverhasználati szokásait látható, hogy a hibákat hordozó Microsoft termékek széles körű használata, amely ráadásul a biztonsági eszközök nem megfelelő elterjedtségével jár együtt, így komolyan veszélyezteti az állampolgárok elektronikus ügyintézési lehetőségeit, adatbiztonságát és személyes adatainak védelmét, valamint az információs társadalom lehetőségeibe vetett bizalmát.

3.2. Vállalti szféra

A vállaltokat méret szerint csoportosítva vizsgáltuk, ugyanis a nagyobb anyagi erőforrásokkal rendelkező társas vállalkozások alapvető eltéréseket mutatnak az egyéni, vagy néhány főt foglalkoztató szektortól, ahol sok esetben inkább a lakossági szektorral való hasonlatosság tűnik ki, mind az informatikai eszközök felhasználási szokásaiban, mind pedig a szakértő karbantartás hiányában és a védelmi megoldások alkalmazásában.

A védelmi megoldásokat tekintve a Bellresearch [1] és a KSH [3] adatai szerint a 10 főnél nagyobb vállalkozások 97%-a rendelkezik az alapvető vírus védelmi eszközökkel, 83%-uk tűzfallal és 72%-uk spam szűrővel. Sajnos korántsem ilyen jó a helyzet a kémprogram szűréssel (36%), a behatolásvédelmi és -jelző eszközökkel (23%), rendszeres naplózást pedig a vállalatok mindössze 15%-a alkalmaz. Ennek fényében talán jobban érzékelhetők a 4. fejezetben bemutatott támadási potenciálok, ugyanis látható, hogy a vállalati szféra igen csekély mértékben van felkészülve egy komoly informatikai biztonsági támadás kezelésére és szakszerű, gyors elhárítására. Amint azt a második fejezet konklúziója is mutatja a

komplexebb kockázatokat leginkább az informatikai tevékenység megfigyelésével, naplózással lehet kiszűrni, amelynek a részesedése aggasztóan alacsony.

A Microsoft, mint szoftverszállító (vendor) jelenléte még erőteljesebb, hiszen a vállalatok több mint 98%-ánál alkalmazzák valamely Windows verziót (itt is kiemelten elterjedt az XP és a 2000), a Szerver oldali arány valamivel alacsonyabb, de itt is kétharmad körüli a termékeket alkalmazó vállalatok aránya. Az irodai programcsomagok között az Office verziók részesedése nagyjából 90%-os.

Az adatbáziskezelési területen a magyarországi, legalább 10 főt foglalkoztató vállalatok mintegy 45%-a használ valamiféle adatbázis kezelő megoldást, a nagyvállalati szektorban azonban ez az érték 90% körüli. Adatbáziskezelő rendszerek szintjén a Microsoft SQL 2005 és 2000 vannak túlsúlyban, ám rátekintve a nemzetgazdasági szempontból legkritikusabb nagyvállalati értékekre látható, hogy ott az Oracle 40%-körüli részesedésével igen jelentős szereplő és támadhatósága ezt a szektort veszélyezteti leginkább.

Fontos kiemelni, hogy az Internet Explorer régebbi 5-ös és 6-os verziói szintén kiemelkedően sok súlyos sérülékenységet hordoznak magukban. Mivel a statisztikákból látható, hogy a régebbi operációs rendszerek alkalmazása, amelyeknek ezek a verziók szerves részét képezik, még mindig igen nagy arányú, ezért jelentős kockázatot hordoznak. A verziófrissítés a nagyvállalati szektorban jelentős részt végbe ment, ám a közszférában és a kisebb vállalatoknál az esetek döntő többségében még mindig az eredeti verziókat alkalmazzák a felhasználók. A vállalati szférában, bár a biztonságtudatosság és a biztonsági eszközök használata jóval elterjedtebb, szintén komoly kockázatok rejlenek, hiszen itt is széles körben alkalmazzák a legkritikusabb sérülékenységeket hordozó szoftvereket, operációs rendszerként, a napi irodai munkához és a vállalat legfontosabb vagyonát jelentő adatbázisok kezelésére is.

A vállalati szférában, bár a biztonságtudatosság és a biztonsági eszközök használata jóval elterjedtebb, szintén komoly kockázatok rejlenek, hiszen itt is széles körben alkalmazzák a legkritikusabb sérülékenységeket hordozó szoftvereket, operációs rendszerként, a napi irodai munkához és a vállalat legfontosabb vagyonát jelentő adatbázisok kezelésére is.

A vállalati biztonsági politikák nem egyenszilárdságú alkalmazása, a védelmi eszközök alkalmazásának túlsúlya az integrált, és sokszor egyszerűbb, szervezési intézkedéssel szemben, nemzetgazdasági szintű kitettséget jelent, veszélyezteti a vállalati szektor működését és adatainak bizalmasságát, integritását.

Az utóbbi évek során, ahogy a vállalatok mind több kritikus üzleti folyamat támogatására alkalmaznak különböző informatikai megoldásokat, mind nagyobb adatvagyonnal gazdálkodnak, a rendszerekkel szembeni kitettségük is fokozódott. Így még abban az esetben is nagyobb kockázattal néznének szembe, ha mindeközben az IT-biztonsági fenyegetések nem nőttek volna.

A mobilitás iránti igény erősödése és a hordozható eszközök terjedése szintén növeli a kockázatokat. A notebookok, amelyek a tolvajok kedvelt célpontjának számítanak, a vállalati pc-állomány mind nagyobb hányadát adják. Megfelelő óvintézkedések nélkül egy ingzsebben elférő pendrive-on vagy egy mobiltelefon memóriájában ma több adatot lehet szinte észrevétlenül kicsempészni a vállalattól, mint amennyit egy évtizeddel ezelőtt egy közepes méretű cég fájlszerverein összesen tároltak.

Az informatikai biztonság kérdése messze túlmutat a sebezhetőséget csökkentő szoftver- és hardverkomponenseken. Több azoknál. Stratégiai szemléletben előkészített terven alapuló

döntések sorozata, rendszeresen felülvizsgált és következetesen betartatott szabályok összessége, amelyek megvalósítási eszközei között találunk hardver- és szoftvereszközöket is.

A biztonsági incidensek gazdasági hatásinak kutatásában a Sagesecure kutatóintézet elemzéséből indultunk ki, amely elemezte a biztonsági incidensekből fakadó leállások nagyságát. Ezt vetettük össze a KSH adataiból [3] származó, számításokkal, amelyek segítségével a kiesett idő értékét próbáltuk meghatározni. Számításaink alapja a munkaidő értéke, vagyis, egységnyi időre jutó GDP-termelő képesség volt.

A Sagesecure [5] kutatásai szerint a különböző biztonsági incidensekből fakadó problémák naponta akár 240 percnyi hasznos munkaidő kihasználhatóságát korlátozzák, vagy teszik teljesen lehetetlenné a vállalati szférában. Ez az idő látszólagosan rövid, 10-15 perces kiesésekből áll össze és a különböző kártékony programokkal (vírus spyware, keylogger, féreg, stb.), konkrét támadásokkal kapcsolatos események mellett leginkább az ezek ellen való szakszerűtlen és átgondolatlan védekezési megoldások okoznak kiesést. Gyakori az üzemidőben futtatott teljes biztonsági ellenőrzés, amely kapacitás kieséseket okoz, a rosszul menedzselt sávszélesség és hálózati topológiák, a frissítések és biztonsági patchek munkaidőben való telepítése, valamint az ezekből gyakran adódó kompatibilitási problémák megoldása. Látható, hogy a hatékony és jól végrehajtott biztonsági politika mennyire fontos, hiszen a nem kellően szervezett védekezés legalább akkora kieséseket tud okozni, mint a valódi támadások. (A fenti 240-ből 100 percnyi kiesés teljes egészében az IT-biztonsági politika végrehajtásának tudható be.) Ide sorolhatók egyébként a túlbonyolított, túl szigorú biztonsági ellenőrzési, jogosultsági és beléptetési rutinok is, amelyek rendszerhasználati nehézségekhez vezetnek az alkalmazottak körében.

Probléma	**Átlagos időveszteség (perc)**
Alkalmazáshoz és rendszerhez kötődő leállások	10
Email szűrés és SPAM	15
Sávszélesség hatékony kihasználása. Áteresztőképesség	10
Nem hatékony és hatástalan biztonsági politikák	10
Biztonsági politikák szigorúsága	10
Rendszerhez kötődő kiesések és frissítések az IT részéről	10
OS és alkalmazások biztonsági javításai	10
Nem biztonságos és nem hatékony hálózati topológia	15
Vírusok, vírus ellenőrzés	10
Férgek	10
Trójai, keylogger	10
Kémprogramok	10
Felugró hirdetések	10
Kompatibilitási problémák	15

Engedély alapú biztonsági problémák (felhasználónév/jelszó)	15
Fájlrendszer rendezetlensége	10
Sérült vagy elérhetetlen adatok	15
Rendszerinformációk és adatok illetéktelen elérése vagy eltulajdonítása	15
Biztonsági mentések visszaállítása	15
Alkalmazás használati problémák	15
Teljes idő	**240**

A KSH adatok alapján az egy percre jutó kiesett GDP nagysága a leginformatika-intenzívebb iparágakban, mint amilyen a közigazgatás, a pénzügyi közvetítés, az oktatás vagy az energetikai ipar, 7-17 millió forint között szór, átlagosan 10 millió Ft körül van. Ezek az ágazatok az átlagnál valamivel magasabb munkaerő költségekkel is bírnak, így a kiesések hatásai még súlyosabbak. Pozitív irányba korrigálja az összefüggéseket a pótlás és az IT-biztonsági, különösen a backup megoldások megléte, bár a Sagesecure kutatói ezt többnyire már figyelembe vették.

A vállalati hatékonyság mindenképpen romlik, és naponta akár 100 millió Ft-os nagyságrendű GDP csökkenéssel lehet számolni egy informatikailag nem kellőképpen felkészült szervezetnél. Nem feledkezhetünk meg az **áttételes hatásokról** sem**, főként a közhivatalok és az államigazgatási rendszerek esetében,** hiszen ez esetben **nem csak a munkavégzés elmaradása vagy lassulása a probléma, hanem az ügyfélkiszolgálás lassulása/kimaradása miatt, a nemzetgazdaság többi részéből is elvonja a munkára fordítható időt.**

3.3 A kormányzati szektor

A Bellresearch kutatásai [1] alapján a védettség érdekében megtett lépések gyakorta csak antivírus-szoftverek és tűzfalmegoldások használatára korlátozódnak, amelyek a teljes intézményi szektor 88, illetve 80 százalékánál találhatók meg. A szervezetek hat százaléka ugyanakkor semmilyen IT-biztonsági megoldást nem alkalmaz, azaz számítógépek ezrei minden védelmet nélkülöznek a közszférában.

Az alkalmazott IT-biztonsági eszközök állománya az előző évekhez képest némi előrelépést mutat: növekedett többek között a spamszűrők használatának elterjedtsége (38-ról 52 százalékra), miközben a kifinomultabb védelmi megoldások elterjedtsége is emelkedett valamelyest. Áttörésre azonban mégsem lehet számítani a közeljövőben. Az olyan, szofisztikáltabb védelmi megoldások, mint a rendszerhasználat és a hozzáférés naplózása vagy a behatolás-érzékelés, még az intézmények egyötödében sem terjedtek el.

Gyakran hallani olyan külföldi példákat (Németország, USA, stb), ahol értékes - akár kormányzati - adatok gigabájtjai kerültek illetéktelen kezekbe mulasztás, szándékos károkozás vagy véletlen hiba következtében. A veszély mértékét nem könnyű becsülni, de léte bizonyosan belátható.

Ennek ellenére az IT-biztonságot stratégiai szintre emelő tudatos gondolkodás csak a

hazai intézmények kis hányadára jellemző. Erre utal, hogy például katasztrófa-elhárítási terve csak minden tizedik intézménynek van, de informatikai szabályzatot is csak az érintett döntéshozók egyötöde követelt meg, biztonsági auditnak pedig kevesebb mint 3 százalék vetette alá magát. Pedig a szabályozási keretek és a cselekvési tervek pontos és részletes definiálása nélkül nehezebb a számonkérés, nem beszélve arról, hogy nehezebb előre vetíteni, mi történik, ha bekövetkezik a baj.

A magyarországi intézmények jellemzően csak a védelem legalapvetőbb elemeit alkalmazzák, míg a szervezet mélyebb rétegeit is átható stratégiai szemlélet igen ritka. Az intézményi szféra szereplőire kevés kivételtől eltekintve jellemző, hogy IT-biztonsági tudatosságuk sokkal inkább az alkalmazott eszközök halmazaiban ölt testet, mint hogy a szervezet működésének egészét befolyásoló filozófiában csúcsosodna ki.

És ez az éremnek csupán az egyik oldala. Az IT-biztonság ugyanis elsősorban nem az eszközök meglétének, hanem a stratégiai gondolkodásnak, a tudatosságnak és a jártasságnak a függvénye.

Az adatok számos ponton rávilágítanak a közszféra hiányosságaira. A szervezetek hiába védik adataikat a külső támadásoktól, ha a jogosultságok hézagos szabályozása miatt bármely alkalmazott engedély nélkül is hozzáférhet a legféltettebb információkhoz, és a legegyszerűbb adattárolón kiviheti a szervezetből.

Katasztrófa-elhárítási terve például az intézmények egytizedének van, IT-szabályzatot is csak az érintett döntéshozók 22 százaléka dolgoztatott ki, míg biztonsági auditot csupán 4 százalékuk végeztetett.

A rögzített szabályok, a megvalósítási lépések és az ellenőrzési eljárások hiánya megnehezíti vagy akár lehetetlenné is teszi a potenciális veszélyekre való tudatos és következetes felkészülést. Nincs a teljes államigazgatást átfogó, egyenszilárdságú és menedzselt kockázatú koncepción alapuló irányelv (szabvány csomag), emiatt nincsenek adekvát egységes biztonsági szempontokkal kézben tartható infokommunikációs (távközlési és számítástechnikai) védelmi rendszerek sem.

A biztonságtudatosság témakörében nem hagyható figyelmen kívül egy alapvető tényező, a működési folyamatok pontos definiálása, valamint azok lefordítása az informatikai rendszerek „nyelvére” – ennek hiányában ugyanis elképzelhetetlen a részletes, írásos biztonsági stratégia kidolgozása. A Jelentés adatai azt mutatják, hogy a hazai intézményi szektor ezen a területen is jelentős problémákkal küzd. További jellegzetességként említhető, hogy **a közszféra szervezeteinek közel 60 százaléka nem von be külső kompetenciát IT-biztonsági rendszerének kidolgozásába és működtetésébe**, hanem kizárólag saját maga, belső erőforrásaira támaszkodva alakítja ki és menedzseli azokat.

Az üzleti területen dolgozó jó kvalitású szakemberek bérezése 2-3-szorosa az állami szférában dolgozókénak. Ezért a közigazgatásban csak közepes képzettségű informatikai szakembereket lehet alapvetően alkalmazni. Tudomásul kell venni, ezért, hogy nagy rendszerek fejlesztéséhez szükséges professzionális és gazdaságosan működtethető informatikai fejlesztő és szolgáltató üzemeltető gárdával nem rendelkezhet.

A közigazgatás alkalmazó, ezért fontos, hogy a megrendelő - szolgáltató szerep szétválasztása megtörténjen. A továbbiakban a közigazgatáson belül köztisztviselőként, közalkalmazottként is csak a megrendelői szándékot képviselők maradnak, az informatikai szolgáltatások a szolgáltatás jellegéhez jobban illő alkalmazási struktúrában történjenek (szolgáltatásvásárlás

külső cégtől, vagy saját szolgáltatási szervezet gazdasági társaság létrehozásával.

A piaci viszonyok között előnyösebben megszerezhető szolgáltatásoknál határozottabban kell a kormányzaton kívüli szférára támaszkodni. Ez a megközelítés megfelel a fejlett EU országok fejlődési trendjének. A nemzetközi tapasztalatok alapján azonban ez a megközelítés nem vonatkozhat az informatikai biztonsággal kapcsolatos kulcspozíciókra és a szükséges belső szakemberekre.

4. Sérülékenységi elemzések

2010 során számos súlyos és kritikus sérülékenység került a szakemberek látóterébe:

- Az első félév során 48 kritikus sérülékenységet detektáltak (a kutatás ezen szakaszában csak erre a súlyossági fokra koncentráltunk, a súlyos sérülékenységek ekkor még nem képezték a vizsgálat tárgyát), melyek közül egy-egy sebezhetőség több terméket is érintett, összesen 225 alesetben, 127 különböző termék-érintettség mellett.
- A harmadik negyedévben 6 kritikus és 141 súlyos sérülékenység jelent meg, melyek közül egy-egy sebezhetőség több terméket is érintett, összesen 13 alesetben, 130 különböző termék-érintettség mellett.
- Az év utolsó negyede 22 kritikus és 93 súlyos sérülékenységet hozott, melyek közül egy-egy sebezhetőség több terméket is érintett, összesen 3*4 alesetben (vagyis összesen 124 esetben), 163 terméknek a 238 különböző termékverzió érintettsége mellett.

Elviekben a sebezhetőségek három típusát különböztethetjük meg:

1. a rendszer nyilvánosan elérhető felületének hibáját kihasználó támadási forma („kapuhiba”), vagy
2. a rendszer hibáját kihasználó távoli forma („falhiba”), vagy
3. a rendszerbe bejuttatott kód futtatásával végrehajtott támadási forma („trójai”).

A gyakorlatban minden sebezhetőség valamelyik elvi osztályba tartozott a 2010-es év során.

A sérülékenységek gyártók szerinti megoszlását az első fejezet elején mutattuk be. A sebezhetőségek száma és a szoftverek elterjedtsége között szignifikáns összefüggés mutatható ki.

A sebezhetőségek és a javítások közötti összefüggést szemlélteti az alábbi táblázat. A javítások lehetnek javítócsomag, új verzió vagy egyéb – például egy beállítás vagy különös biztonsági rendszabályok életbe léptetése.

Érdekes lehet megvizsgálni a javítások terjedelmének a változását is. Látható, hogy a fenyegetésekkel szemben megalkotott javítások aránya az év során folyamatosan romlott, vagyis a nulladik napi támadások kockázata jelentősen nőtt 2010. év során.

Javítási forma	Százalékos megoszlás		
	2010. I-II. né.	2010. III. né.	2010. IV. né.
Nincs javítás	46%	47%	63%
Van javítás	0,2%	2%	7%
Van frissítés	20,8%	5%	6%

Egyéb javítás	25%	46%	24%

Az eredmény magyarázatához hozzáfűzzük, hogy vélhetően a szoftvergyártók fejlesztési kapacitása szűkösnek bizonyult a sebezhetőségek kezelésére, hiszen 2010-ben minden bizonnyal a gazdasági kilábalásra, a 2008-2009-ben elmaradt bevételek kompenzálására, pótlására fókuszáltak. Ez okozhatja ezt a szignifikáns eltérést a javított és a nem javított sebezhetőségek éven belüli arányában. Ezt a véleményt egyébként jól alátámasztja a patchek és a javított verziók számának jelentős csökkenése és az egyéb javítások részarányának változatlansága is. Ez az eredmény felértékeli a sebezhetőségek javítása helyett azok elfedését célzó védelmi intézkedéseket, melyek védelmi vonalat alkotnak a rövid időn belül javíthatatlan sebezhetőségekkel rendelkező rendszerek számára.

A tapasztalat az, hogy az új sebezhetőségeket a biztonsági portálok nyilvántartják és ez a javítócsomagok gyors megjelenését is elősegíti. A legtöbb sebezhetőség esetében előbb-utóbb a javító patch is közkinccsé lesz, de ez a folyamat nem mindig következik be a kellő gyorsasággal. Az, hogy 63%-nál nincs még javítás a felfedett sérülékenységekre, óvatosságra kell, hogy intse a biztonsági szakembereket – különösen azért, mert az elmúlt negyedévben ez az arány még csak 46% volt – és a preventív kontrollok mellett a detektív kontrollok erősítését is javasolt napirendre tűzni, hogy az események a lehető leghamarabb kiderülhessenek. Ennek elmulasztása esetén a rendszerek kitettsége sokáig fennállhat.

Így tehát az informatikai biztonsági ellenőrzések, és kontrollok életciklusának fenntartása (tervezés, implementálás, működtetés, ellenőrzés) továbbra is erősen javasolható minden informatikát használó és informatika-függő szervezetnek, az adott szoftver-érintettség függvényében.

A sebezhetőségek értékelésénél fontos az, hogy a biztonságon belül melyik biztonsági követelményt fenyegeti.

A *bizalmasság – sértetlenség – rendelkezésre állás* hármasságából az év nagy része kiegyensúlyozott volt, az utolsó negyedévben volt megfigyelhető markáns eltolódás a bizalmasságot fenyegető támadások felé. Ezért az ellenőrzéseket a bizalmasság területére javasolt fókuszálni az elkövetkezendő időszakban, az életbe léptetett kontrollok hatékonyságát és megelőző képességét javasolt mindenhol megvizsgálni. Ez természetesen nem azt jelenti, hogy a rendelkezésre állás és a sértetlenség megvalósítását szolgáló védelmi intézkedések működését érintően a követő auditok feleslegesek lennének a továbbiakban. Összehasonlítva a korábbi negyedévek adataival megállapítható, hogy nem a bizalmasságot érintő fenyegetések számossága növekedett, hanem a sértetlenségre és rendelkezésre állásra vonatkozó sebezhetőségek száma csökkent a kétharmadára.

Ez utalhat a szervezetek információ-éhségére, ami válságban illetve a válság utáni kilábalás időszakában összefügghet a talpon maradt vállalatok tudása iránti érdeklődéssel, hiszen ennek másolása megkönnyíti a válságban lemaradók gyors felzárkózását. Érdekes jelenség volt a közelmúltban a Wikileaks portál, melynek híreit több nagy újság szerkesztősége is érdemesnek találta a közlésre – ez szintén megerősíti az információk iránti erős érdeklődést, ami maga után vonja az informatikai rendszerek megtámadását információszerzési céllal – ezt a DOS-támadásokat realizáló sebezhetőségek nullára csökkenése és a rendszerhozzáférést célzó támadási formák jelentős növekedése is alátámasztja, a távoli támadások több mint 90%-os részaránya mellett.

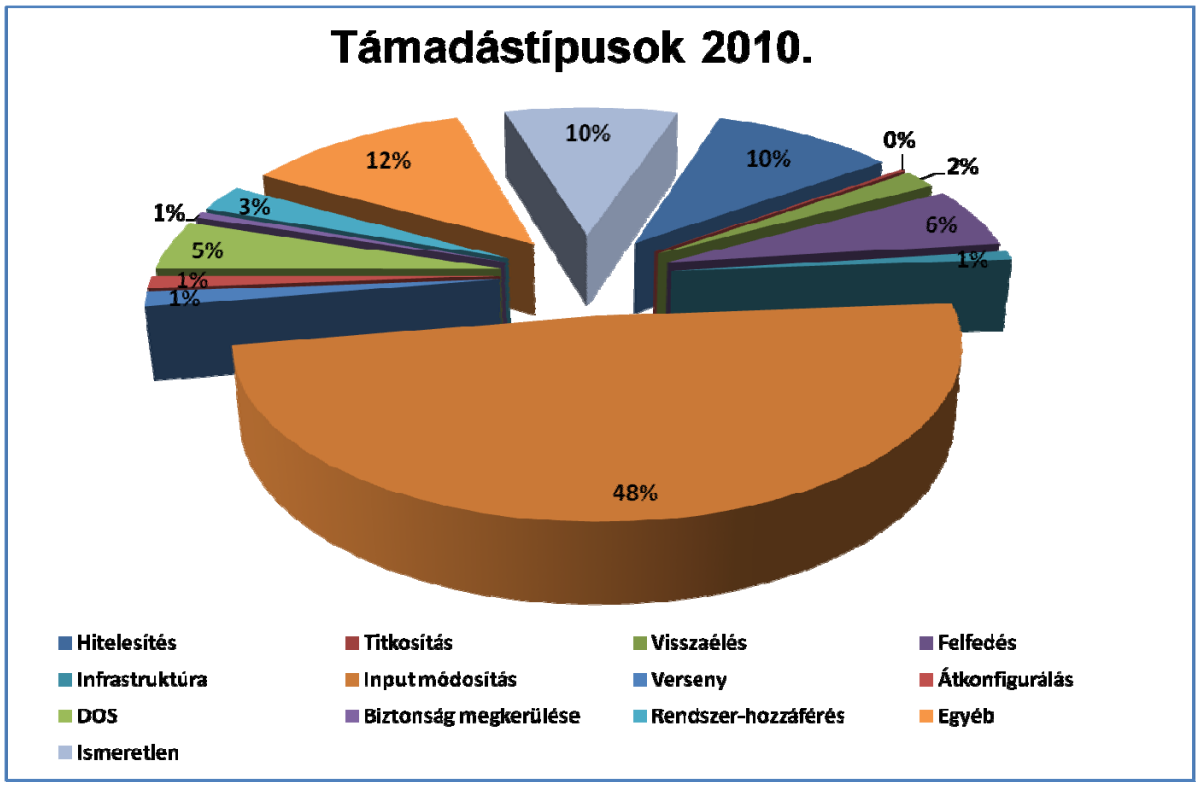
Az eredmény másik olvasata az, hogy a rendszerek 2010-ben fejlődést a sértetlenséget és rendelkezésre állást biztosító intézkedések terén mutattak, ezért ezeken a területeken

kevesebb működő sebezhetőséget tudtak megtalálni, ami a bizalmasság területére még nem igaz.

Feltételezésünk szerint a következő negyedévek eredményei megerősítik az információ-éhség hipotézist, és várhatóan marad a távolból viszonylag egyszerű eszközökkel végrehajtható, információszerzést célzó sebezhetőségek részaránya a teljes sebezhetőségeken belül.

A távoli, interneten keresztül végrehajtható támadások lényeges súlyponteltolódása (98,6%), ez azt jelzi, hogy továbbra sem lehet az IDS-ektől és a tűzfalaktól eltekinteni, működésük és szabályrendszereik ellenőrzése ajánlatos minden szervezet számára, a fizikai biztonságot megvalósító intézkedések további fenntartása mellett.

A támadások típus-megoszlását az alábbi diagram mutatja részleteiben.



Az input-adatok módosítása továbbra is sláger, a 27 egyéb és 24 ismeretlennek címkézett fenyegetés mellett. A bemenő adatok ellenőrzése a tehát továbbiakban is igen fontos, az általános biztonsági intézkedések végrehajtása mellett.

Az input-adatok módosítása egész évben kiemelt területnek számított. A bemenő adatok ellenőrzése a tehát továbbiakban is igen fontos, az általános biztonsági intézkedések végrehajtása mellett.

Látható a táblázatból, hogy a hitelesítési sebezhetőségek erős csökkenést mutatnak, ezt okozhatja a PKI-technológia egyre szélesebb körű elterjedése és alkalmazása weblapoknál és kódaláírásoknál is.

Szintén jelentős változást mutat, de a növekedés irányába, a rendszerhozzáférést eredményező sebezhetőségek száma. Jelzi, hogy a támadók ma már nem elégednek meg az adatok és a szolgáltatások támadásával, a rendszerek felett akarják átvenni az irányítást. Talán ennek a jele az input-módosítások számának csökkenése is, de erre csak a következő 2-3 negyedév adatai jelenthetnek megerősítést.

Irodalomjegyzék

[1] Bellresearch: *Magyar Infokommunikációs Jelentés 2009.* adatai, http://www.ictreport.hu/ .

[2] IT Governance Institute: *Enterpride Value: Governanceof IT investments - The Val IT Framework 2.0, IT Governance Institute, Rolling Meadows. IL 60008 USA, 2008.,* http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT 1.aspx

[3] KSH: Adattáblák az egyes nemzetgazdasági ágak jövedelemtermelő képességéről, és az IT-eszközök használatáról regionális bontásban; www.ksh.hu 2011. jan.

[4] Puskás Tivadar Közalapítvány: *PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ szoftver sérülékenységi adatai. 2010. jan-dec.*

[5] Sonnenreich, Wes: *Return On Security Investment (ROSI): A Practical Quantitative Model,* Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006

[6] Várhalmi A. Miklós: *Az infokommunikációs közművek biztonsági kockázatai és az információs hadviselés*, „Társadalom és gazdaság – új trendek és kihívások" c. tudományos konferencia, Baja (2008), www.varhalmi.hu/cucc/361433.rtf; 2010.okt.