Az információbiztonsági törvény által előírt biztonsági besorolások és kapcsolódó intézkedések lehetséges hatásainak vizsgálata a szoftveres sérülékenységek szempontjából

Erdősi Péter Máté

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

Dr. Horváth Attila

Vezető kutató
Információs Társadalomért Alapítvány
e-mail: horvath.attila@infota.org

Dr. Kiss Ferenc

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

Absztrakt

A 2013. évi L. törvény hatályba lépését követően az állami és önkormányzati szervezetek számára kötelező az információbiztonsággal foglalkozni, rendszeres védelmi tevékenységeket végezni a vonatkozó jogszabályokban foglalt előírások végrehajtásával. Kutatásunkban arra a kérdésre kerestük a választ, hogy az előírt biztonsági besorolásoknak a szervezetek és a rendszerek vonatkozásában és a hozzájuk tartozó védelmi intézkedéseknek milyen hatása lehetséges a szoftveres sérülékenységek által jelentett információbiztonsági kockázatok csökkentése aspektusából. Kimutattuk, hogy nem létezik olyan szoftverkombináció, melyhez a vizsgált sérülékenységi adatbázisból nem tartozik sérülékenység, másrészről azt is megállapítottuk, hogy az egyes sérülékenység kihasználásából adódó következmények az információbiztonságot hasonló módon érintik. Más szóval ezt azt jelenti, hogy a szoftvereket használó szervezetek az információbiztonsági kockázataikat nem tudják jelentősen befolyásolni a termékek megválasztásával és a sérülékenységek kihasználhatósága lényegében független a szervezet biztonsági besorolásától. Következésképpen a biztonsági besorolások hatása a feltáró és a javító védelmi intézkedések létezésében jelentkezik, preventív hatás – a kiváltó okok függetlensége miatt – korlátozottan érhető csupán el.

Kulcsszavak: *sérülékenység, 2013. évi L. törvény, biztonsági szint, védelmi intézkedés*

Bevezetés

A hazai állami és önkormányzati szervezetek komoly előírásokkal szembesültek 2013-ban, az információbiztonsági törvény hatályba lépését követően. A védelem megvalósításának alapvető kérdése, hogy elérte-e vagy el fogja-e érni a célját valaha is? Tekintettel arra, hogy az információbiztonsági események, sérülékenységek megjelenése nem mutat érdemi csökkenést, másrészről a bekövetkezett események regisztrálását, feltárását, elemzését és a következtetések levonását a tanulmány írásának idején a Nemzetbiztonsági Szakszolgálat részeként működő Kormányzati Eseménykezelő Központ végzi, aki– jogszabályi tilalom következtében – az incidensekről nem adhat ki információkat, vizsgálatunk a kérdés második felének a tárgyalására fókuszálhat, vagyis azt a kérdést kívánjuk a középpontba helyezni, hogy a feltárt ismert sérülékenységek tükrében megvalósítható-e az elvárt biztonsági szint a jogszabályban a törvény erejénél fogva erre kötelezett szervezeteknél.

A sérülékenységek létezése minden szektorban problémát okoz, melyről egy kiterjedt forrásokra alapozott sérülékenység-vizsgálati kutatás eredményeként ezeket fogalmazták meg 2011-ben [3]:

- **Lakossági megállapítás:** „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."
- **Vállalati megállapítás:** „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.„ Megjegyezhető, hogy az ismert vállalati információbiztonsági módszerek, kockázatok és esettanulmányok megállapításai összecsengenek ezzel [12].
- **Kormányzati megállapítás:** „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."

Nem túlzás tehát a sérülékenységek létezését, de még inkább az ezek kihasználására irányuló törekvéseket nem csupán technológiai, hanem társadalmi problémának is tekinteni.

A vizsgálati kérdés megközelítésmódjának a kialakításakor megfontoltuk a témát tudományos igénnyel tárgyalni kívánók számára a terület kutatói által megfogalmazott javaslatot:

> *„(...) azt tudjuk javasolni tudományos pályára készülő vagy ott már aktívan dolgozó kollégáknak, hogy munkájuk során folyamatosan vegyék figyelembe azt a széles körben hangoztatott nézetet, miszerint a kiberbiztonság közös felelősség. A kibertér szereplőinek együttműködése nélkül a kiberbiztonság nem megvalósítható, az egész láncolat pontosan annyira erős, mint benne a leggyengébb láncszem."* [4].

Ezt a közös felelősséget fogalmazta meg az Amerikai Egyesült Államok Nemzeti Kibertér-védelmi Stratégiája 2003-ban, az előszó világossá tette, hogy a fejlett világok működése függ a kibertér működésétől, így minden érintett szereplőnek kötelessége védeni azt [11].

> *„Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people."*

Magyarországon a jelenleg hatályos jogszabályok nem írják elő minden érintett szereplő számára a védelmi kötelezettséget, habár 2009-ben az akkori törvény-előkészítő munka még úgy gondolta, hogy minden szereplőt be kell vonni a készülő törvény hatálya alá (állampolgár, mint felhasználó és az állam, mint felhasználó, üzemeltető és szolgáltatásnyújtó). Négy évvel később megszületett az információbiztonságról szóló törvény jelenleg is érvényes szűkített, de még így is az alkalmazók számára értelmezési problémákat felvető hatállyal. Az állampolgárok első körben kimaradtak a védelemre való jogszabály által előírt elkötelezettségből.

A 2013. évi L. törvény (Ibtv.)

A 2013. évi L. törvény tehát hosszas előkészítő munka után jött létre. Az információ-biztonság iránti igény a számítógépek terjedésével együtt járó információbiztonsági incidensekkel együtt fejlődött. Különböző rész-szabályozások korábban is megjelentek, a terület átfogó szabályozása azonban 2013-ig váratott magára. A törvény megjelenését követően kiadták a részletszabályokat, végrehajtási rendeleteket is, mely közül a védelmi intézkedések megtervezésében és végrehajtásában a legfontosabb rendeletnek már két éven belül a módosítása meg is történt, a kezdeti időszak tapasztalatai és a jogalkotó további szándékai alapján. A végrehajtásra való hajlandóság – tekintettel a szankcionálás nehézségeire (az állam büntesse meg saját magát), az értelmezési problémákra és a forráshiányra (szakember-hiány) alacsonynak volt mondható a kezdeti időszakban. Az ellenőrzés szintjének növekedésével a végrehajtási hajlandóság növekedése várható.

A szervezetek számára előírt legfontosabb védelmi tevékenységek a megelőzés, detektálás, reagálás és incidenskezelés voltak, amit a saját biztonsági szintjének és a rendszerei biztonsági osztályainak megfelelő módon kell végrehajtania, egy besorolási procedúrát

követően. A szervezetenkénti minimális besorolásokra az alábbi javaslat jelent meg adja az Ibtv. 9. § (2)-re való hivatkozással [4]:

1. táblázat: Állam- és közigazgatási szervezetek minimális biztonsági szintje (készült: [4] alapján)

1. szint	Köztársasági Elnöki Hivatal, Országgyűlés Hivatala, Alkotmánybíróság Hivatala, Alapvető Jogok Biztosának Hivatala, helyi és nemzetiségi önkormányzatok hivatalai, hatósági igazgatási társulások
2. szint	központi államigazgatási szervek, bíróságok, ügyészségek, Állami Számvevőszék, Magyar Nemzeti Bank, fővárosi és megyei kormányhivatalok
3. szint	Magyar Honvédség
4. szint	állami nyilvántartások adatfeldolgozói, az európai és a nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemekhez tartozó szervezetek

Az Ibtv. 9. § (2) kimondja, hogy ha egy szervezeten belül külön szervezeti egység foglalkozik a fejlesztéssel, az üzemeltetéssel, felelős az üzemeltetésért vagy az információbiztonságért, akkor ezeket a szervezeti egységeket is ugyanúgy be kell sorolni a biztonsági szintekbe, mint a szervezetet. Összesen tehát 5 különböző besorolással rendelkezhet egy szervezet, amelyek mindegyike 5 értéket vehet fel teoretikusan, belátható tehát, hogy a lehetséges besorolások száma $5^4 = 3.125$ lenne, persze pusztán matematikai értelemben. Ez a bonyolultság azonban nem könnyítette meg az alkalmazók dolgát.

A biztonsági szintek összehasonlítása

Ebben a fejezetben a különböző biztonsági szintek közötti különbségek felvázolására teszünk egy kísérletet. Már itt meg kell jegyeznünk, hogy az Ibtv. két különböző, de sokszor összetévesztett fogalmat használ a biztonság rétegzésére. A bizonytalanságot fokozza, hogy az értékkészlete mindkét fogalomnak azonos ([9] [11] közötti zárt intervallum által tartalmazott pozitív egész szám). Az egyik fogalom a biztonsági szint, mely a szervezetekre vonatkozik, és a szervezet számára fogalmaz meg különböző megteendő intézkedéseket, míg a másik fogalom a biztonsági osztály, mely az elektronikus információs rendszerek (amelyek nem csak szoftverek és nem csak hardverek) számára ír elő védelmi adminisztratív, fizikai és logikai védelmi intézkedéseket. A kettő fogalom besorolási követelményei különbözők és nem feltétlenül kell, hogy létezzen szoros kapcsolat a két érték között sem, mivel azok több tényező és elvárás figyelembe vételével állnak elő. A törvény definícióját beidézve a következő meghatározások adhatók erre a két fogalomra:

1. biztonsági szint: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére,
2. biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.

A helyzetet bonyolíthatja esetenként a törvénynek az a rendelkezése, hogy a teljes szervezet mellett be kell sorolni az elektronikus információs rendszer fejlesztését, és üzemeltetését végző, valamint az üzemeltetéséért vagy az információbiztonságáért felelős szervezeti egységeket is a meghatározott biztonsági szintekbe, melyek lehetnek mások, mint a szervezet biztonsági szintje. Vajon igaz-e itt is, hogy az alacsonyabb biztonsági szintre besorolt szervezeti egység lesz a szervezet leggyengébb láncszeme információbiztonsági szempontból?

Ennek a kérdésnek a megválaszolásához hasonlítsuk össze az egyes biztonsági szintekhez előírt védelmi intézkedéseket, védelmi tevékenységeket. Az egyes szintek egymásra épülését a következő felsorolás mutatja be az Ibtv. alapján:

1. **biztonsági szint:** ha a szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és erre más szervezetet, vagy szolgáltatót sem bízott meg, továbbá az adatfeldolgozás módját nem maga határozza meg, az adatkezelés tekintetében technikai, vagy információtechnológiai döntést nem hoz, a használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre nincs. A szervezet egyedi adatokat és információkat kezel, vagy dolgoz fel, és kritikus adatot nem kezel. Az információbiztonsági tevékenység gyakorlatilag az érintettek kötelezettségeinek szabályozására és számonkérésére terjed ki.
2. **biztonsági szint:** ha az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe .
3. **biztonsági szint:** ha a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus, nem minősített de nem közérdekű vagy közérdekből nyilvános adatot kezel, központi vagy zárt célú elektronikus információs rendszerek felhasználója, illetve feladatai támogatására külső szolgáltatót vesz igénybe.
4. **biztonsági szint:** ha a 3. szinten túl elektronikus vagy zárt célú információs rendszert üzemeltet vagy fejleszt.
5. **biztonsági szint:** ha a 4. szinthez rendelt jellemzőkön túl európai és nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve ellenőre vagy tesztelője.

Tekintettel arra, hogy a törvény további részleteket korlátozottan tartalmaz (ahogyan erre [4] is rámutatott), érdekes lehet összevetni a különböző biztonsági szintek számára megfogalmazott követelmények preventív, feltáró vagy javító jellegét. Előrebocsátjuk,

hogy a szabályozás létezése minden esetben preventív kontrollt jelentett abból a megfontolásból, hogy a szabályozás megakadályozza az ad-hoc feladatvégzést vagy annak megindoklását a szabályozás hiányával.

2. táblázat: 1-es biztonsági szinthez tartozó követelmények értékelése (készült: a 41/2015. BM rendelet alapján)

Szint / előírás	Megelőző (preventive)	Feltáró (detective)	Javító (corrective)
1.1.1.	információbiztonságot érintő munkautasítás, belső rendelkezés, szabályozás (közös szabályozás) létezik		
1.1.2.		folyamatos kockázatelemzési eljárás definiált	
1.1.3.	az informatikai biztonsági szabályzat lehet teljes vagy részelemre vonatkozó		
1.1.4.	Az IBSZ-t az erre jogosult vezető jóváhagyja		
1.1.5.	az információbiztonsággal kapcsolatos kötelezettségek és felelősségek rögzítettek	információbiztonság felügyeleti rendszere meghatározott	
1.1.6.	szankcionálás jogkövetkezménnyel		

3. táblázat: 2-es biztonsági szinthez tartozó követelmények értékelése (készült: a 41/2015. BM rendelet alapján)

Szint / előírás	Megelőző (preventive)	Feltáró (detective)	Javító (corrective)
2.1.1.	biztonsági kontrollfolyamatok részletesen szabályozottak		
2.1.2.	az eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét		
2.1.3.	egyértelműen meghatározott információbiztonsági felelősségek és biztonságtudatos viselkedés		
2.1.4.	az egyes folyamatok a közvetlenül érintettek felügyelete alá tartoznak		
2.1.5.		olyan dokumentálás, melyből az elvégzett kontroll tevékenység megállapítható	

4. táblázat: 3-as biztonsági szinthez tartozó követelmények értékelése (készült: a 41/2015. BM rendelet alapján)

Szint / előírás	Megelőző (preventive)	Feltáró (detective)	Javító (corrective)
3.1.1.	a biztonsági kontroll folyamatokba a személyek be vannak vonva és az elvárásokról tájékoztatást kapnak		
3.1.2.	a biztonsági kontroll folyamatok szabályozottan és ellenőrizhető módon vannak bevezetve és oktatás tárgyai		
3.1.3.	a biztonsági kontroll folyamatok nem alkalmazottak egyéni, vagy eseti eljárásokra		
3.1.4.	a biztonsági kontroll folyamatokat jogosult vezető hagyja jóvá		
3.1.5.		a folyamatok előzetes tesztelése biztosítja a folyamatok adott követelmények szerinti működését	
3.1.6.	van információbiztonsági költség- és haszonelemzési módszertan		

5. táblázat: 4-es biztonsági szinthez tartozó követelmények értékelése (készült: a 41/2015. BM rendelet alapján)

Szint / előírás	Megelőző (preventive)	Feltáró (detective)	Javító (corrective)
4.1.1.		az üzemeltetési, vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztek biztosítják a vonatkozó információbiztonsági intézkedések hatékonyságát és megfelelőségét	
4.1.2.	minden szabályozási folyamat és kontroll működése biztosított		
4.1.3.			azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt, vagy bekövetkezett biztonsági események kezelésére
4.1.4.		az egyes információ, rendszer, vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelősége és hatékonysága folyamatba épített rendszeres belső értékelés tárgya	
4.1.5.	a szervezet folyamatba épített belső értékelései nem helyettesíthetőek		

4.1.6.		a biztonsági információk, vagy riasztások alapján tesztelési eljárást, vagy biztonsági ellenőrzést végeznek	
4.1.7.		a tesztelés értékelése alapján megállapított követelményeket dokumentálják	a követelményeket az arra jogosult jóváhagyja és be is vezetik
4.1.8.		az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése	

6. táblázat: 5-ös biztonsági szinthez tartozó követelmények értékelése (készült: a 41/2015. BM rendelet alapján)

Szint / előírás	Megelőző (preventive)	Feltáró (detective)	Javító (corrective)
5.1.1.	biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését	biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését	biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését
5.1.2.		biztosítani kell a szabályzatok, tesztelési eljárások, biztonsági folyamatok folyamatos felülvizsgálatát	biztosítani kell a szabályzatok, tesztelési eljárások, biztonsági folyamatok folyamatos továbbfejlesztését
5.1.3.	átfogó információbiztonsági program biztosítja a személyi állomány biztonságtudatosságának növelését		
5.1.4.	a szervezet személyi állományának rendelkeznie kell információbiztonsági operatív képességgel és a feladat elvégzéséhez szükséges szaktudással;		
5.1.5.		a biztonsági sérülékenységek felismerésének a képességét a szervezet egésze tekintetében meg kell valósítani	a biztonsági sérülékenységek kezelésének a képességét a szervezet egésze tekintetében meg kell valósítani
5.1.6.		a fenyegetettségek folyamatos újraértékelésével, a kontrollfolyamatok	

		felülvizsgálatával nyomon kell követni információbiztonsági környezet változását	
5.1.7.			az információbiztonságot érintő külső, vagy belső környezeti változásokra figyelemmel további információbiztonsági alternatívákat kell meghatározni;
5.1.8.	a szervezetnek kialakította az információbiztonsági képesség- és állapotmérési és értékelési módszertanát, meghatározta annak mutatóit		és változáskor aktualizálni kell azt.

Látható a táblázatokból, hogy az egyes intézkedések a jelenlegi besorolásban a következő megoszlásban tartalmaznak megelőző, feltáró és javító jellegű intézkedéseket. Ha egy intézkedés kétfajta tulajdonsággal is rendelkezett, akkor meg lett duplikálva, ha pedig két eltérő tulajdonságú részt tartalmazott, akkor meg lett bontva – ez az oka annak, hogy a követelmények számai nem egyeznek meg a táblázatban szereplő elemek számosságával:

7. táblázat: Az egyes biztonsági szinthez tartozó követelmények típusai (készült: a 41/2015. BM rendelet alapján)

Szint / előírás	Megelőző (preventive)	Feltáró (detective)	Javító (corrective)
1. szint	5	2	0
2. szint	4	1	0
3. szint	5	1	0
4. szint	2	5	2
5. szint	4	5	5

Szembetűnő, hogy csak a 4. szinttől jelennek meg olyan követelmények melyeket javító kontrollokkal kell teljesíteni, az alsóbb szintek erőteljesen fókuszálnak a prevencióra (benne lényegében a szabályozottságra) és kisebb mértékben a feltárásra. A javító intézkedések ebben az esetben ad-hoc módon történhetnek csak meg. Felmerül tehát a kérdés, hogy mit tud tenni egy szervezet különböző biztonsági szinteken a folyamatosan fennálló fejlett fenyegetések [2] ellen, különösen, ha azok a szervezet által használt szoftverek sérülékenységeit használják ki és hogyan tud ebben segíteni az érintett állami szervezet [9]?

Érintett rendszerek vizsgálata sérülékenységi riportok alapján

A vizsgálatunk tárgyát képező adatbázis 2011. október 1. – 2015. április 30. között megjelent (jelentett) sérülékenységeket tartalmaz, szám szerint. Az adatbázis a jelzett időszakra vonatkozóan 935 darab sérülékenységet foglalt magában (egy sérülékenység több termékre is vonatkozhatott). Az adatbázist a (2013-ban megszűnt) Puskás Tivadar Közalapítvány Nemzeti Hálózatbiztonsági Központ (PTA-CERT) és az Információs Társadalomért Alapítvány (INFOTA) együttműködése hozta létre.

Az adatbázis alapját a PTA-CERT munkatársainak gyűjtőmunkájával létrehozott sérülékenység-vektorok jelentették, melyhez – az adatbázis specifikációra vonatkozó interjúk alapján – három forrást vettek igénybe:

1. US-CERT adatbázis[1]
2. Secunia advisories adatbázis[2]
3. CVE adatbázis[3]

A fenti adatbázisokban megtalálható sérülékenységek között a PTA-CERT előszűrést végzett, így az adatbázisba csak azok a sérülékenységek kerültek bele, amelyek a PTA-CERT munkatársainak megítélése szerint a kormányzati szektort érintették vagy érinthették, továbbá valódi (proof of concept, exploitálható) sérülékenységek voltak, nem pedig feltételezettek. Túlreprezentáltak voltak a távolról kihasználható sérülékenységek, de néhány esetben lokális jelenlétet igénylő formák is előfordultak. A PTE-CERT adatbázis az US-CERT által riportolt sérülékenységekkel ki lett egészítve a 2013. január 1. és 2015. április 30. közötti adatokkal, de csak a valódi fenyegetést jelentő sérülékenységekkel (a téves riportokat kiszűrtük).

[1] US-CERT elérhető: http://www.us-cert.gov/
[2] SECUNIA Advisories elérhető: http://secunia.com/community/advisories/
[3] CVE adatbázis elérhető: http://cve.mitre.org/

A vizsgálatot elvégezve az érintett rendszerekre, azt az eredményt kaptuk, hogy az első kvartilisben benne foglaltatik minden ismertebb és frekventáltan használt termék, nehezen lehet elképzelni olyan munkaállomást vagy szervert, amelyik legalább az egyik elemet ebből a listából nem tartalmazza, ennélfogva jogosnak tűnik az a megállapítás, hogy a sérülékenységi adatbázist összevetve a leggyakrabban alkalmazott szoftver-kombinációkkal, nagyon magas valószínűséggel lehet találni egyezést a kettő között, más szóval a jelenleg használt rendszerelemek sérülékenységét vásárlással, termékválasztással nem lehetséges eliminálni.

8. táblázat: Az egyes termékek fenyegetettsége a sérülékenységek szempontjából (készült: saját elemzés alapján)

Termék	Gyakoriság	Százalék	Kumulatív százalék
WordPress	47	2.71	2.71
Chrome	33	1.91	4.62
Oracle	33	1.91	6.52
Windows7	31	1.79	8.31
Windows XP	30	1.73	10.05
Windows Vista	29	1.67	11.72
Windows Server 2003	28	1.62	13.34
Windows Server 2008	27	1.56	14.9
Windows Server 2008 R2	25	1.44	16.34
Internet Explorer	18	1.04	17.38
Office 2007	16	0.92	18.3
Solaris	16	0.92	19.23
Thunderbird	16	0.92	20.15
Firefox	15	0.87	21.02
Flash Player	12	0.69	21.71
Office 2010	12	0.69	22.4
SeaMonkey	12	0.69	23.09
Office 2003	11	0.64	23.73

Termék	Gyakoriság	Százalék	Kumulatív százalék
VMware	11	0.64	24.36
.NET Framework	8	0.46	24.83
Acrobat	8	0.46	25.29

Összefoglalás

A sérülékenységek számosságának a trendje nem látszott csökkenni a vizsgált időszakban, minden negyedévben egy alulról-felülről korlátos, jól behatárolható sávban mozgott. A sérülékenységek átfogták a gyakrabban és a ritkábban használt szoftvereket is, de nem szabad elfeledkezni az eleve fertőzött firmware programmal kereskedelmi forgalomba kerülő számítástechnikai eszközökről, ami új frontot nyitott az információbiztonságért folytatott küzdelemben. Hogyan lehetséges védekezni egy olyan sérülékenység ellen, amit maga a felhasználó emel be a rendszerébe csupán azzal, hogy számítástechnikai eszközöket kell használnia az informatika-függő világban? Az elektronikus információs rendszerek biztonságának menedzselése [8] szintfüggő, ahogyan ezt fentebb kimutattuk. Minden szinten nem feltétlenül lesz lehetséges szofisztikált teszteléseket elvégezni, elvégeztetni vagy megkövetelni az egyes szereplők által, bármennyire is célszerűnek látszik elméletben [7]. A szoftverértékelés során természetes módon magasabb garanciális szinten van megkövetelve erősebb sérülékenységvizsgálat, de mit tudunk tenni akkor, ha a szoftvereink többsége nem rendelkezik biztonságtechnikai értékeléssel, vagy annak a szintje alacsony? [1] A sérülékenységek létezése és elterjedtsége komoly társadalmi hatásokkal is járhat. Ennek a helyzetnek a fennmaradása valószínűsíthető, erre utal az is, hogy ma már egy kiberkonfliktusban is védeni szükséges a polgárokat [6].

A prevenció alacsony hatásfokának egyik magyarázó tényezője lehet az, hogy ha olyan támadási képességekkel rendelkező entitások ellen implementálunk védelmi intézkedéseket, akik nagy valószínűséggel nem is akarnak megtámadni, akkor a preventív eredmények változása ettől nem várható, mivel az eltérő támadási képességű támadók ellen ez a fajta védelem valóban nem lesz hatásos. Az információbiztonsági képzés 2014-ben indult el a Nemzeti Közszolgálati Egyetemen, kimondottan a köztisztviselők, közigazgatási szervezetek információbiztonsági felelősei számára kidolgozott módszertannal [5]. Ennek szükségességét szervezetek belső erőforrásból történő problémamegoldási igénye támasztotta alá, aminek megoldása egyrészről segíti a megfelelő információbiztonsági tudatossággal rendelkező köztisztviselők megjelenését a rendszerben, másrészről – mivel az oktatásban megtett lépések társadalmi hatása általánosságban évtizedekben, de az információbiztonsági egyetemi képzésben is legalább 5 évben mérhető – ennek fenntartása

és az információbiztonsági felelősi számosság növelése véleményem szerint továbbra is szükséges. A tudás többszörözésének az útjában két tényező áll, egy 2001-ben 26 országra kiterjedő kutatás szerint, mégpedig az eszköz hiánya és a képzett tudás-átadó hiánya [10]. Ameddig a sérülékenységek és a kihasználási lehetőségük fennáll, addig a védelemnek folyamatosnak kell lennie az időben távoli eredmények realizálhatóságához is és a fókuszpontot véleményem szerint meg kell tartani a szervezetek biztonsági incidensek elleni reagálóképességének kialakításán és fenntartásán, a rendszerek védettségének minden határon túl való növelési igényével szemben.

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] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003, (https://www.commoncriteriaportal.org/files/ccfiles/ccpart3v3.1r4.pdf, 2016. szeptember 28.)

[2] Gyebrovszky, Tamás. 2014. Folyamatos fenyegetések a kibertérben. *Hadmérnök* (IX) 3: 137-153.

[3] Horváth, Attila. 2011. *IT és hálózati sérülékenységek tovagyűrűző hatásai a gazdaságban. In: Networkshop 2011: Kaposvár., 2011. április .27-2011. április 29.* (https://nws.niif.hu/ncd2011/docs/ehu/013.pdf, 2016. szeptember 20.)

[4] Krasznay, Csaba - Szádeczky Tamás. 2014. *Az információbiztonság és állami szabályozása In: Nemeslaki András (szerk.) E-közszolgálat fejlesztés: Elméleti alapok és tudományos kutatási módszerek.* Budapest: Nemzeti Közszolgálati Egyetem. 249-264.

[5] Krasznay, Csaba - Törley, Gábor. 2015. *e-Safety, Privacy and Information Security: Requirements in Public Administration. In: Alexander Balthasar, Blaž Golob, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Alexander Prosser (eds), Central and Eastern European e|Dem and e|Gov Days 2015. Time for a European Internet? Conference Proceedings.* Wien: Austrian Computer Society. 431-441

[6] Krasznay, Csaba. 2012. A polgárok védelme egy kiberkonfliktusban. Hadmérnök (VII) 4: 142-151

[7] Krasznay, Csaba. 2014. E-közigazgatási rendszerek és alkalmazások sebezhetőségi vizsgálata. *Hadmérnök*, (V) 3: 125-137

[8] Muha, Lajos - Krasznay Csaba. 2014. Az elektronikus információs rendszerek biztonságának menedzselése. Budapest: Nemzeti Közszolgálati Egyetem, Vezető- és Továbbképzési Intézet

[9] Orbók, Ákos. 2015. Rövid áttekintés a Nemzeti Kibervédelmi Intézet megalakulásáról, működéséről és előzményeiről. *Hadmérnök* (X) 4: 247-251

[10] Pelgrum, W.J.. 2001. Obstacles to the integration of ICT in education: results from a worldwide educational assessment. *Computers & Education* (2001) 37: 163–178

[11] The White House, Washington. 2003. The National Strategy to Secure Cyberspace. (https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, 2016. szeptember 20.)

[12] Vasvári, György. 2011. Válogatott tanulmányok a vállalati biztonság témaköréből. Budapest: Információs Társadalomért Alapítvány