Sérülékenységek hatásának vizsgálata a biztonsági követelmények aspektusából

Dr. Horváth Attila

Vezető 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

Absztrakt

Az elektronikus tartalmak kezelésének fogalomrendszere a digitális világ bővülésével került előtérbe és habár számos különböző módon valósították meg azokat, közös jellemzőjük a digitális rendszereknek, hogy különböző szoftveres eszközök együttesét alkalmazzák funkcióik megvalósítására. A hacktivizmus elterjedésével megnövekedtek a szoftverek sérülékenységeit kihasználó támadások száma, melyek sikeres megvalósítása a rendszerek biztonságát negatívan befolyásolja. Felmerül az a kérdés, hogy a sérülékenységek hogyan fenyegetik a biztonságot, van-e szignifikáns korreláció a bizalmasság, a sértetlenség és a rendelkezésre állás fenyegetettségében az ismertté vált sérülékenységek exploitálását követően. Ebben a cikkben az elektronikus információs rendszerek biztonsági kitettségét járjuk körbe. A sérülékenységek vizsgálatához saját adatbázist építettünk, mely az eseménykezelő központok által összegyűjtött információk és a sérülékenység-leíró vektorok alapján készült. Elsődleges vizsgálatunkban arra a kérdésre kerestük a választ, hogy a sérülékenységeknek a biztonságra gyakorolt hatásában milyen korrelációk fedezhetők fel és mivel lehetséges a kapott eredményeket megmagyarázni. A sérülékenységek hatásai közötti korrelációk vizsgálatára vonatkozó eredményeinket részletes statisztikai elemzéssel támasztjuk alá.

Kulcsszavak: *sérülékenységi vektor, kiberbiztonság, kiberfenyegetés, kockázat, bizalmasság, sértetlenség, rendelkezésre állás, korreláció*

Bevezetés

A szoftveres sérülékenységek a rendszerekben benne rejlő olyan hibák, hiányosságok, tulajdonságok, melyeket alkalmas módon kihasználva a rendszer biztonsági mechanizmusait esetenként megkerülve a támadó olyan tevékenységeket lesz képes

elvégezni az adott rendszerben, mely a rendszer tulajdonosa, fenntartója, üzemeltetője és felhasználója számára egyaránt nem kívánatosnak minősíthető. Az internetes sérülékenységek feltárásával és jelzésével már a nyolcvanas évek végétől elkezdtek foglalkozni [3] és ennek hatására a védelem eszközéül létrehozták az eseménykezelő központok (CERT[1]) hierarchikus láncolatát szerte az egész világon. Kezdetben az incidenseket tartották nyilván [1] ezek a központok – például a CERT/CC 1989 és 1995 között 4.299 incidensről kapott értesítést [3: iii], melyeket kategorizáltak és 1997-ben létrehozták ezekből az internetes incidensek taxonómiáját, amit kisebb változtatások mellett mind a mai napig használnak az eseménykezelő központok.

Az internetes sérülékenységek legfontosabb jellemzője, hogy távolról kihasználható, általában hálózatba kötött gépeken, de minden olyan szeparált számítástechnikai eszköz is veszélyeztetett, amely adatot fogad be valamely külső adathordozóról, amit megfertőznek [6]. A támadókat feltételezésünk szerint a kibertér rejti. A támadó kilététől és az általa realizált támadásoktól függően osztályozni lehet a támadásokat is. A kibertéren keresztül realizálható támadásoknak négy formáját különböztethetjük meg Krasznay Csaba munkája alapján [4]:

„Ezek a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés. A kiberbűnözés célja az informatikai eszközökön keresztüli haszonszerzés, elsősorban a hagyományos szervezett bűnözői csoportokhoz köthető. A hacktivizmus és a kiberterrorizmus ugyan fogalmilag különálló cselekmény, de közös bennük, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat az informatikai bűncselekményeket, melyek célja az, hogy minél szélesebb tömegek lássák a csoport által képviselt ideológiai véleményt. Hatásuk elenyésző, ugyanis azt a fajta szervezettséget nem tudják felmutatni, mely egy hatékony kibertámadáshoz szükséges lenne. A médiahatásuk azonban igen komoly. A kiberkémkedés az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést jelenti. A kiberhadviselés az államok közötti konfliktusokban jelenik meg, melynek során a felek informatikai eszközöket vetnek be egymás elektronikus információs rendszereinek befolyásolásának céljából.”

A szórványos támadások világából mára átléptünk a folyamatos fenyegetések világába, ma az interneten minden időpillanatban realizálódhat egy támadás földrajzi elhelyezkedéstől függetlenül. A támadások kifinomultsága az automatizálás révén magas is lehet, melyet új névvel is illettek, Folyamatosan Fennálló Fejlett Fenyegetés [2]. A támadók azonban

[1] CERT: Computer Emergency Response Team, számítógépes vészhelyzet elhárító csoport.

továbbra is a megtámadott rendszer sérülékenységein keresztül próbálják meg saját céljaikra felhasználni az áldozatok információs rendszereit.

A sérülékenységek és az információs rendszerek összerendelése

A sérülékenységek az információs rendszerek elemeihez, azaz IT alkalmazásokhoz, adatbázis-kezelőkhöz, operációs-rendszerekhez kapcsolódnak, ezért el kell még végeznünk az információs rendszer elemeinek és az informatikai sérülékenységeknek az egymáshoz rendelését. Ezt az adott elektronikus információrendszer IT környezetének (IT_ENV) a meghatározásával kezdhetjük, amikor is az információs rendszerhez tartozó, szoftveres vezérléssel rendelkező informatikai rendszerelemeket (IT_ENV_i) soroljuk fel és rendezzük be az $IT\_ENV = \Sigma\, IT\_ENV_i$ halmazba. Mivel egy rendszerelemhez több sérülékenység is tartozhat, az IT_ENV halmaz kétszintű lesz, lesz egy szoftveres szintje és egy sérülékenységi szintje. Most már elvégezhető az egyes IT_ENV_i környezetek és sérülékenységek összerendelése és az érintettség meghatározása. Figyelembe kell venni azonban azt is, hogy a rendszerek – és egyben alrendszereik is – folyamatos mozgásban lehetnek [7: 101], így érintettségük is folyamatosan változhat.

1. táblázat: IT környezet szintjei (Forrás: saját táblázat)

4. szint:	Alkalmazás
3. szint:	Köztesréteg, adatbázis-kezelő
2. szint:	Operációs rendszer (driverek) Virtualizációs rendszer
1. szint:	Hardver

Az adatbázis deskripciója

A vizsgálatunk tárgyát képező adatbázis 2011. október 1. - 2015. április 30. között megjelent (riportolt) sérülékenységeket tartalmaz. Az adatbázis a jelzett időszakra vonatkozóan 1.101 darab sérülékenységet foglalt magában. 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[2]
2. Secunia advisories adatbázis[3]
3. CVE adatbázis[4]

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, denéhány 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). Tekintettel arra, hogy a sérülékenységek forrása bővebb, mint a felsoroltak, ebből adódóan további kutatási feladat lehet a fenti forrásokból származó még teljesebb adatbázisok biztonsági célú vizsgálata.

Az adatbázis struktúrája az alábbiakat követi:

1. A sérülékenység azonosító száma
2. A sérülékenység megjelenésének dátuma
3. A sérülékenység magyar nyelvű megnevezése
4. A sérülékenység angol nyelvű megnevezése
5. A sérülékenység működésének összefoglalása magyarul
6. A sérülékenység által érintett szoftverek verziói
7. A sérülékenység kihasználásának részletes leírása

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

8. Megoldás a sérülékenység javítására (megoldásnak tekintjük a frisssítés és a javítócsomag telepítése mellett a beállítások megváltoztatását vagy bizonyos funkciók elhagyását is)
9. Referenciák, melyek a sérülékenységre vonatkoznak és a gyártónál vagy biztonságtechnikai portálokon, cégeknél megjelennek
10. Támadás típusa, mely a taxonómia alapján meghatározza, milyen módon fejti ki a hatását a sérülékenységre alapozott támadás, ami a következők egyike vagy csoportja lehet:

    a. Authentication / Hitelesítés
    b. Crypthographical / Titkosítás
    c. Deny of service / Szolgáltatás-megtagadás
    d. Hijacking / Visszaélés
    e. Information disclosure / Információ- vagy adatszivárgás
    f. Infrastructure / Infrastruktúra
    g. Input manipulation / Bemenet-módosítás
    h. Misconfiguration / Konfiguráció
    i. Other / Egyéb
    j. Race condition / Versenyhelyzet
    k. Security bypass / Biztonsági szabályok megkerülése
    l. System access / Rendszer-hozzáférés
    m. Unspecified (Nem részletezett)

11. Hatás, ami

    a. a bizalmasság,
    b. a sértetlenség és
    c. a rendelkezésre állás elvesztése lehet bármilyen variációban

12. Szükséges hozzáférés, ami lehet

    a. távoli,
    b. helyi hálózati vagy
    c. konzolról történő beavatkozás

13. Súlyosság: a CVSSv2 összesített értékén alapuló kvalitatív érték, illetve ennek kvantitatív besorolása a kritikus, magas, közepes, alacsony osztályokba
14. Érintett rendszerek, azokat a gyártókat és termékeik megnevezését soroltuk itt fel, akik a sérülékenységben érintettséggel rendelkeztek

Az egyes információrendszerek érintettségének meghatározásához a sérülékenység-vektor azon elemének ismerete szükséges, mely az érintett verziókat sorolja fel. Leszűrve az adatbázist az adott IT_ENV_i elemekre megkapjuk az adott elemre vonatkozó összes

nyilvántartott sérülékenységet. Elvégezve ezt az összes rendszerelemre, megkapjuk az adott elektronikus információs rendszer kitettségét az adatbázisban található sérülékenységekre és a súlyosság révén priorizálási segédlet is kialakítható.

A kitettségek nagyságát a sérülékenységek számossága tehát nyilvánvaló módon befolyásolja. Az adatbázisban rögzített sérülékenységek hatása további fontos tényező a biztonságszervezésben, vagyis fontosnak gondoljuk azt is ismerni, hogy a sérülékenység mely biztonsági követelmény (bizalmasság, sértetlenség, rendelkezésre állás) teljesülését veszélyezteti. Ha egy sérülékenység több biztonsági követelményt is veszélyeztetett, akkor mindegyikhez felsoroltuk. Az érintettség meghatározásához a CVSSv2 (Common Vulnerability Scoring System Version 2[5]) vektor bizalmasságra, sértetlenségre és rendelkezésre állásra mutató elemeit vettük figyelembe. Megjegyezzük, hogy az érintettséget fennállónak tekintettük a részleges (P) és a teljes (C) érintettségek esetében is. Tekintettel arra, hogy a támadások java része távolról végrehajtható, felmerül a kérdés, hogy az internetes sérülékenységek biztonsági követelményekre gyakorolt hatásai között létezik-e bármilyen összefüggés?

Statisztikai elemzés

Az elemzés elvégzése előtt fogalmazzuk meg a hipotéziseket. Nullhipotézisnek ebben a vizsgálatban azt tekintjük, hogy az egyes sérülékenységek fenyegetése a biztonsági követelmények tekintetében korrelál, vagyis erős lineáris függés mutatható ki közöttük. El kell vetnünk a nullhipotézisünket és további megfontolásokat kell tenni, ha az erős függés a változók között nem igazolható. A vizsgált változók tehát a bizalmasság, a sértetlenség és a rendelkezésre állás elvesztése volt, a változók gyakorlatilag bináris változóként értelmezhetők, az esetek számosságát a sérülékenységes száma adta meg (1.101). A változókat statisztikailag az alábbi leírások jellemzik:

Frequency Table

Bizalmassag

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	72	6,5	6,5	6,5
	1	1029	93,5	93,5	100,0
	Total	1101	100,0	100,0	

1. ábra: A bizalmasság frekventáltsága

[5] Lásd: https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

Láthatóan az 1.101 értékből túlnyomó többségben vannak a bizalmasságot támadó sérülékenységek (93,5%), más szóval a támadók információt szerezhetnek a sérülékenységek túlnyomó többségének kihasználásával.

Frequency Table

Sertetlenseg

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	118	10,7	10,7	10,7
	1	983	89,3	89,3	100,0
	Total	1101	100,0	100,0	

2. ábra: A sértetlenség frekventáltsága

A sértetlenséget támadó sérülékenységek száma kevesebb, mint a bizalmasságot támadóké, de még így is a sérülékenységek 89,3%-a okozhatja a sértetlenség megszűnését.

Frequency Table

Rendelkezesre_allas

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	278	25,2	25,2	25,2
	1	823	74,8	74,8	100,0
	Total	1101	100,0	100,0	

3. ábra: A rendelkezésre állás frekventáltsága

Habár a rendelkezésre állást még kevesebb sérülékenység támadja, mint a sértetlenséget, de a sérülékenységek közel háromnegyede (74,8%) okozhatja a funkcionális működőképesség elvesztését.

A változók közötti összefüggés fennállásának a megállapításához a Pearson-féle korrelációs együttható kiszámítását alkalmaztuk, és a megfelelő szignifikancia-szint után megerősítésként a Cramer-féle V értékkel próbáltuk meg a dependencia erősségét alátámasztani.

A statisztikai elemzés lefuttatásával az alábbi eredményre jutottunk:

Correlations

Correlations

		Bizalmassag	Sertetlenseg	Rendelkezesre_allas
Bizalmassag	Pearson Correlation	1	,360**	,100**
	Sig. (2-tailed)		,000	,001
	N	1101	1101	1101
Sertetlenseg	Pearson Correlation	,360**	1	,326**
	Sig. (2-tailed)	,000		,000
	N	1101	1101	1101
Rendelkezesre_allas	Pearson Correlation	,100**	,326**	1
	Sig. (2-tailed)	,001	,000	
	N	1101	1101	1101

**. Correlation is significant at the 0.01 level (2-tailed).

A Pearson-féle korrelációs együttható létező szignifikáns függőséget jelez mind a bizalmasság és a sértetlenség, a sértetlenség és a rendelkezésre állás, valamint a bizalmasság és a rendelkezésre állás támadása között, azonban erős lineáris függést nem sikerült kimutatni, így a nullhipotézisünket el kellett vetni. A szignifikancia-szint erőssége azonban a függés létezésre utalt, így indokolt volt a függőség alátámasztásául szolgáló további vizsgálatot is elvégezni. A magas mintaszám miatt (N = 1.101) a Pearson-féle együttható és a Cramer-féle V érték mindhárom változónál megegyezett nulla (Approx.Sig=0,000), illetve a bizalmasság-rendelkezésre állás viszonylatában 0,001 szignifikancia szint mellett.

Ennek alapján megállapítható volt, hogy egyrészről a bizalmasság és a rendelkezésre állás között ugyan gyenge lineáris függés tételezhető fel (r=0,1), de ez nagyon gyengén alátámasztott (V=0,1) – más szóval a változók közötti lineáris függés magyarázatához várhatóan további vizsgálatok lesznek szükségesek. Másrészről a bizalmasság és sértetlenség közötti gyenge lineáris függés (r=0,36) nagyon erősen fennáll (V=0,36), ennek több oka is lehetséges, attól függően, hogy az értékelő vagy a rendszer oldaláról közelítjük meg az eredményt. Harmadrészt a sértetlenség és a rendelkezésre állás közötti szintén gyenge lineáris dependencia (r=0,326) erős fennállására utal a V=0,326 érték.

Összefoglalás

Az eseménykezelő központok által nyilvántartott sérülékenységi vektorok megmutatják a sérülékenység karakterisztikáját számos aspektusból. Az egyes információrendszerek teljes érintettségének meghatározásához szükséges ismernünk az egyes rendszerelemek kitettségét is. A biztonság megteremtésekor a bizalmasság, sértetlenség és rendelkezésre állás biztonsági követelményeknek kell teljesülniük az adott információs rendszerre és elemeire is. A sérülékenységek a biztonsági követelményeket különböző módon támadjak. Statisztikai vizsgálattal igazoltuk az egyes biztonsági követelmények támadása közötti dependenciák létezését. A bizalmasság és a sértetlenség támadása között fennálló gyenge korreláció adódhat egyrészről az értékelő gondolkodásmódjából (ha egy rendszerhez olvasásra hozzá lehet férni, akkor sok esetben a módosítás is lehetséges), másrészről a nem teljes mértékben differenciált jogosultsági rendszerek implementációiból is, hiszen elméletben az egyes informatikai műveletek jogosultságai nagyon differenciáltan is kioszthatók, a gyakorlatban azonban a rendszeradminisztrátori és felhasználói jogosultságok mellett további differenciálás csak jelentős adminisztrációs erőforrások bevonásával oldható meg. Ennek elmaradása azt okozza, hogy ha egy entitás hozzáfér olvasásra egy adathoz, akkor annak módosítására is sok esetben képes. A sértetlenség és a rendelkezésre állás közötti gyenge lineáris függés magyarázata lehet az, hogy ha a sértetlenség megszűnik, akkor az eredeti információ rendelkezésre állása nyilvánvaló

módon sérül, de ez nem áll fenn, ha az eredetiség megváltozása a forrásra korlátozódik és a tartalmat nem érinti.

További érdekes vizsgálati irány lehet nem lineáris függések keresése és kimutathatóságának megállapítása, a feltárt dependenciák magyarázatának finomítása és verifikálása mellett. A jelen cikkben feltárt függés természetének mélyebb megismerése az informatikai biztonság mérésben is szerepet játszhat, mivel a mérési módszereknek szükséges garantálniuk a megvalósítás hatékonyságának a mérhetőségét és le is kell tudni írnia a biztonság méréshez felhasznált adatok gyűjtésének és elemzésének a módszereit is [5: 5].

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] CERT Annual Reports 1994-2003. http://www.cert.org/historical/annual_rpts/ (2016. július 14.)

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

[3] Howard, John D. 1997. *An Analysis of Security Incidents on The Internet 1989 – 1995*. A dissertation submitted to the graduate school in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering and Public Policy. http://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_52455.pdf. (2016. július 14.)

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

[5] Muha, Lajos. 2010. *Az informatikai biztonság mérése*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem. http://real.mtak.hu/12938/1/1278547.pdf. (2016. július 14.)

[6] SYMANTEC. 2011. Nicolas Falliere, Liam O Murchu, Eric Chien: W32. Stuxnet Dossier, Version 1.4 (February 2011). http://i69.fr/autoblog/autoblogs/korben.info/media/0ae4f7a1.w32_stuxnet_dossier.pdf. (2016. július 14.)

[7] Vasvári, György. 2003. *Bankbiztonság*. Budapest, BME GTK Információ- és Tudásmenedzsment Tanszék.