XX. Fiatal Műszakiak Tudományos Ülésszaka, 2015. Kolozsvár, 155–158. *DOI: 10.33895/mtk-2015.03.31*
http://hdl.handle.net/10598/28656

VÁLLALATI INFORMATIKAI BIZTONSÁG SZEREPE NAPJAINKBAN

THE ROLE OF CORPORATE SECURITY TODAY

Göcs László[1], Johanyák Zsolt Csaba[2]

[1]*Kecskeméti Főiskola, GAMF Kar, Informatika Tanszék, 6000 Kecskemét, Izsáki út 10. Telefon / Fax: +36-76-516-417/+36-76-516-399, gocs.laszlo@gamf.kefo.hu*

[2]*Kecskeméti Főiskola, GAMF Kar, Informatika Tanszék, 6000 Kecskemét, Izsáki út 10. Telefon / Fax: +36-76-516-303/+36-76-516-399, johanyak.csaba@gamf.kefo.hu*

Abstract

In January 2015 a virus called CryptoLocker popped up in the IT systems of several Hungarian companies. This virus spreads mostly through e-mail attachments and encrypts documents on the infected machines making them inaccessible for their right owners. Thus it represents a serious security risk for enterprise information systems with inadequate protection. Many companies have suffered serious damage owing to the inaccessible or corrupted data as a result of a CryptoLocker attack. Establishing a proper defense strategy plays a key role in preventing such attacks.

In this paper, we are going to show how an attack of this kind can be fended off and prevented. Defense procedures being able to ensure the integrity and availability of data are also going to be discussed. HIDS (Host -based Intrusion Detection System) plays an important role in the proposed solution. Besides, a key security policy should also be the prohibition of the use of external or public mail servers by the help of proper firewall configuration.

***Keywords**: data security, enterprise security, e-mail, encrypted document, virus attack.*

Összefoglalás

2015. januárjában Magyarországon, több helyen is felbukkant egy többnyire elektronikus levelezéssel terjedő CryptoLocker nevű vírus, amely komoly vállalatbiztonsági kockázatot jelenthet a nem megfelelő védelemmel ellátott informatikai rendszerek számára. A támadás megtörténte után a vírus által titkosított dokumentumok hozzáférhetetlenné válnak. A támadás eredményeképpen több cégnél is sérült az információk hozzáférhetősége. Az ilyen jellegű támadások megelőzésében fontos szerepe van megfelelő védelmi stratégia kialakításának.

Cikkünkben bemutatjuk, hogy egy ilyen támadást hogyan lehet kivédeni, meggátolni, valamint milyen védelmi megoldásokat kell kialakítani az informatikai rendszerben ahhoz, hogy az adatok sértetlenek maradjanak, és a rendelkezésre állásuk biztosítva legyen. Az ajánlott megoldásban fontos szerepet játszik a hoszt alapú illetéktelen hálózati behatolást jelző rendszer, a HIDS (Host-based Intrusion Detection System) alkalmazása. Emellett egy másik fontos biztonsági eszköz lehet egy vállalat életében a külső elektronikus levelező kiszolgálók elérésének tiltása a tűzfal segítségével.

***Kulcsszavak:** adatbiztonság, vállalat biztonság, elektronikus levelezés, titkosított dokumentum, vírus támadás.*

1. Bevezetés

Napjainkban a vállalati életben fontos szerepet játszik az adatbiztonság és az adatvédelem. Az információk, a személyes és céges adatok jelentős része az informatikai infrastruktúrában van jelen. Ezen adatok védelme érdekében meg kell határoznunk a kockázat mértékét, a védelmi stratégiát, és annak megvalósítási lehetőségeit. Mivel erőforrásaink általában korlátosak, ezért a védelemre fordított erőfeszítés arányos kell legyen a kockázattal. Az informatikai biztonságot úgy határozhatjuk meg, hogy az az állapot, amikor az informatikai rendszer védelme - a rendszer által kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása, és funkcionalitása szempontjából zárt, teljes körű, folyamatos és a kockázatokkal arányos [1].

2. Vállalati informatikai biztonság

A biztonság megteremtésének fontos lépése a vállalat biztonsági osztályba sorolása. Ennek során figyelembe veszik a vállalat felépítését, tevékenységét, és működését.
Minden biztonsági osztálynál külön követelményrendszernek (hardver, szoftver, adattárolás, stb.) kell megfeleljen a cég.
A vállalatoknál a támadások és védelem érdekében kockázatelemzést is kell készíteni.
A hatékony kockázatkezelési folyamatok alkalmazásától függ egy szervezet azon képessége, hogy meg tudja oldani a kritikus infrastruktúrájával, költség-hatékony biztonságával és az üzemelés folyamatosságával kapcsolatban felmerülő aktuális problémáit [2].

3. CryptoLocker támadás

2015. januárjában Magyarországon, több helyen is felbukkant egy többnyire elektronikus levelezéssel terjedő CryptoLocker nevű vírus, amely komoly vállalatbiztonsági kockázatot jelenthet a nem megfelelő védelemmel ellátott informatikai rendszerek számára.
A vírus támadási módszere, hogy elsősorban ingyenes email rendszereken lévő postafiókokra küld levelet, melynek mellékletet tartalmaznak. A melléklet megnyitása után a vírus támadásba lendül, és az adott gépen lévő dokumentumok (szöveges állományok, táblázatok, képfájlok) titkosításra kerülnek, majd egy képfájlban közli a felhasználóval, hogy ellenszolgáltatás fejében a visszafejtéshez szükséges kulcsot megkaphatja.

4. Védelem kialakítása

A hatékony védelem kialakításához a következő alfejezetekben ismertetésre kerülő négy tényezőre kell összpontosítanunk.

4.1 Emberi tényező

Az informatikai jellegű meghibásodások, károk oka majdnem 60%-ban valamilyen emberi mulasztás következménye. Gyakori veszélyforrás az emberi hanyagság, a munkatársak figyelmetlensége.
Az informatikai biztonságpolitika alapján ki kell dolgozni az egységes szerkezetbe foglalt, az egész intézményre érvényes és a többi szabályzattal összhangban álló Informatikai Biztonsági Szabályzatot (IBSZ).
Az IBSz egy olyan belső szervezeti intézkedés-együttes, amely a szervezeten belül működtetett informatikai rendszerekre vonatkozóan szabályozza a biztonsági intézkedéseket, szervesen illeszkedve a hatályos jogszabályokhoz és a szervezet egyéb működési és ügyrendi előírásaihoz [3].

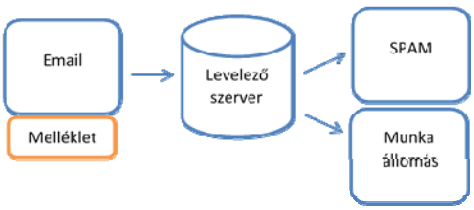
4.2. Tűzfal

A vállalatoknál a hálózati eszközök segítségével súlyos támadásokat tudunk korlátozni, meggátolni. Példaként említhetjük a nyilvános levelező szerverekhez való hozzáférés szabályzását egy proxy szerver segítségével. Ilyen megoldás lehet egy Linux alapú Squid Proxy, ahol tartalomszűréssel megadhatjuk egy ACL (Access Control List) listában a tiltandó domain neveket,

esetünkben a nyilvános levelező rendszerek címét, vagy akár reguláris kifejezések alapján is szűrhetünk. Így a felhasználók számára elérhetetlenné válik az érintett nyilvános levelezőrendszer.

4.3 Email védelem

Egy olyan vállalat életében, ahol számos felhasználói elektronikus postafiók van használatban, elengedhetetlen a saját levelező rendszer működtetése. Itt kapcsolódhat be akár az IBSZ-be foglalt szabályozás is, miszerint semmilyen külső postafiók nem engedélyezett a vállalaton belül, csakis kizárólag a saját levelező rendszer használata lehetséges. Az ilyen rendszerekben lehetőség nyílik komoly szűrési feltételek meghatározására is. Ezek szerint vizsgálhatjuk a bejövő és kimenő levelek tartalmát, mellékleteit. Például a CryptoLocker támadást ki lehet szűrni, ha a rendszerünk vizsgálja a mellékletek kiterjesztését és tartalmát.



1. ábra *Elektronikus levelezés vizsgálata*

4.4 Adatmentés

A CryptoLocker által végrehajtott titkosítás visszafejtése gyakorlatilag lehetetlen, így a már megtámadott fájlok használhatatlanná válnak. Amennyiben a támadás már megtörtént, kizárólag a biztonsági mentés megléte segíthet az adatok helyreállításában. A biztonsági mentésnek több változata létezik, így időszakos (napi, heti, havi), teljes, különbségi, növekményes.

A biztonsági mentés hasznossága függ az adatok használatának a gyakoriságától is. A támadás bekövetkezése után az adatmentésből egy korábbi állapotra tudjuk visszahozni a konkrét fájlokat. Abban az esetben, ha napi mentés történik, akkor a támadást megelőző napi állapot állítható helyre.

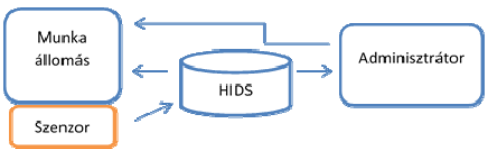
4.5 IDS rendszer alkalmazása

A behatolás-érzékelő rendszerek a hálózat illetve a számítógépes erőforrásokon olyan speciális események, nyomok után kutatnak, amelyek rosszindulatú tevékenységek, támadások jelei lehetnek. Ezeket más néven behatolás-észlelésnek is nevezzük, angol nevén Intrusion Detection System (IDS).

A tűzfallal összevetve elmondható, hogy míg a tűzfal feltétel nélkül blokkolja a szükségtelen és engedélyezi a biztonságosnak vélt forgalomtípusokat, de nem (feltétlen) riaszt, addig az IDS feladata a támadásnyomok észlelése, a riasztás és az esetleg ellenlépések megtétele [4].

4.5.1. HIDS

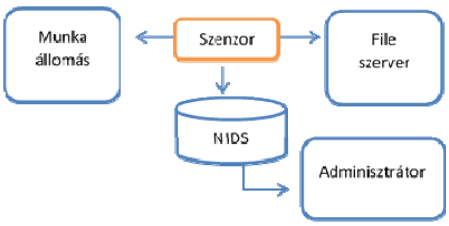
A hoszt alapú (Host Intrusion Detection System – HIDS) behatolás érzékelő rendszerek egy önálló rendszer tevékenységének a figyelésére szolgálnak. Ilyen lehet egy levelezőszerver, vagy munkaállomás. A HIDS lényege, hogy csak azzal a hoszt-tal foglakozik, amire feltelepítették, tehát nincs kapcsolata a környezettel. A HIDS szenzorjai összegyűjtik az analizálandó adatokat, majd továbbítják azokat az elemző motorhoz, ami eldönti, hogy a tevékenység engedélyezett-e vagy tiltott. Képesek megfigyelni a támadás eredményét, a futó processzek és tevékenységek elemzésével. Ha a rendszert egy támadás, veszély fenyegeti, akkor a HIDS értesítést küld, valamint az adatok sértetlenségének a megtartása érdekében megteszi az előre definiált ellenintézkedéseket [5].



2. ábra *HIDS alkalmazása*

4.5.2. NIDS

A hálózat alapú IDS (Network Intrusion Detection System – NIDS), mely a hálózati kommunikációt felügyeli, fontos szerepet játszik a vállalat kommunikációs vizsgálatában. Az ilyen behatolás érzékelő rendszerekkel detektálható a hálózati meghajtók elleni támadás, ugyanis a fájlok titkosításához komoly algoritmus párosul, ami nagyban terhelheti a hálózati kommunikációt, így megfelelő szenzor konfigurálásával kiszűrhető és leállítható a támadási folyamat, ugyanis egy központi fájlszerver mindig nagyobb védelmet kell kapjon, mivel azon több felhasználói adat, információ, védendő érték van.



3. ábra *NIDS alkalmazása*

5. Következtetések

Egy vállalat életében az adatok sértetlenségének biztosítása érdekében több tényezőt kell figyelembe venni. Egyik ilyen a kommunikáció, és azon belül is az elektronikus levelezés, amin keresztül történő támadás komoly károkat okozhat. Hiszen az elektronikus levelezéssel tart kapcsolatot egy vállalat a külvilággal, és egy informatikai rendszert elsősorban a külvilágtól kell megvédenünk. A cikkben szereplő lehetőségek figyelembevételével és alkalmazásával biztosítani tudjuk a védelmet egy esetleges e-mailen terjedő vírustámadással szemben, vagy megvalósíthatjuk a helyreállítást a már bekövetkezett káresemény után. Ezek a felsorolt védekezési módszerek nem csak kifejezetten erre a támadásra adnak védelmet, hanem más jellegű károkozó programok kiszűrésére is alkalmasak, ugyanis egy károkozó működését a helyi gépen vagy akár a hálózaton is tudjuk érzékelni, erre vannak az IDS rendszerek. Az adatok védelme érdekében a központi fájltárolás elengedhetetlen, hiszen egy helyi gépen mindig nagyobb a kockázat. A fájlszerveren is történhet károkozás, de ha megfelelő mechanizmussal automatizált adatmentés zajlik, az adatok megőrzése biztosított. Bármenynyire is sikerül biztonságossá tenni technikai szempontból informatikai rendszerünket, gyakran az emberi tényező jelenti a legnagyobb kockázatot. Ezt a kockázatot jól megfogalmazott szabályzattal (IBSZ) és a dolgozók képzésével tudjuk leghatékonyabban csökkenteni és kiküszöbölni.

Szakirodalmi hivatkozások

[1] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése*, Nemzeti Közszolgálati Egyetem, Budapest, 2014, 6.

[2] *Útmutató az IT biztonsági szintek meghatározásához*, HunGuard Kft., MEH, 2008. 11.

[3] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, Informatikai Tárcaközi Bizottság ajánlásai - *Informatikai rendszerek biztonsági követelményei 12.sz ajánlás*, Budapest 1996, 96.

[4] MTA SZTAKI – *Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai,* Budapest 2004, 215-216. oldal.

[5] Symantec Corporation – *Symantec Host Intrusion Detection System,* 2002, 2.