DÉRI ATTILA

NAPJAINK INFORMATIKAI KIHÍVÁSAI - GONDOLATOK A KRITIKUS INFRASTRUKTÚRÁK INFORMATIKAI SÉRÜLÉKENYSÉGÉRŐL ÉS VÉDELMÉRŐL

1. Bevezetés

A XXI. században a technikai fejlődésével az informatika az élet újabb területeit hódította meg. Ez a változás megjelenik a mindennapjainkban is. Könnyítheti, kényelmesebbé teheti az életünket, de nehézségeket, biztonsági kihívásokat is hozhat.

Napjainkban előtérbe került az interneten keresztüli ügyintézés. Az elektronikus ügyintézésnek jelentős előnyei vannak, ilyen lehet például a kényelmes, otthonról történő ügyintézés. Azonban a hátrányairól sem szabad megfeledkezni. Ezek lehetnek az ügyintézéshez szükséges programok nem megfelelő minősége, digitális kompetenciák hiánya, stb. A dolgozatom első részében ezzel foglalkozom, a felhasználói oldalra helyezve a hangsúlyt.

A dolgozatom második részében az informatikai biztonság kérdéskörét járom körül, részletezve két idei, az informatikai rendszerek elleni támadást.

Az informatika elterjedésével új biztonsági kihívások jelentkeztek, mivel megjelentek a számítógépes adatlopások, vírusok, stb. A bűnözők felismerték az ebben rejlő lehetőségeket. Dr. Bencsik Balázs, a Nemzeti Kibervédelmi intézet vezetőjének becslése szerint, jelenleg a kiberbűnözéssel okozott kár a világgazdaság 1%-val mérhető össze, és megelőzi a kábítószer-kereskedelemből származó bevételt is (https://www.vasarnapihirek.hu/fokusz/ a_drognal_is_nagyobb_uzlet).

Az elektronikus ügyintézés megjelenése is új biztonsági intézkedéseket igényel. Ma már az interneten keresztül el lehet érni azokat a hatóságokat, állami-, illetve a versenyszférában működő cégeket, melyek biztonságkritikus rendszereket üzemeltetnek. Ezeknek a rendszereknek a működtetése fokozott biztonságot tesz szükségessé.

Nem csak napjaink jelensége a terrorizmus. Az idősebb nemzedék emlékezhet a Vörös brigádok, ETA, stb. terrorszervezetekre, melyek Európa különböző országaiban hajtottak végre merényleteket. A terrorizmus az utóbbi években újra felütötte fejét.

A terrortámadások célpontjai lehetnek a kritikus infrastruktúrák informatikai rendszerei. Eddig nem jutott tudomásomra sikeres terrortámadás a kibertérben a kritikus informatikai rendszerekkel szemben.

A biztonság növelése érdekében új, megelőző lépéseken is el kell gondolkozni. Az eddig tudomásomra jutott esetekből kitűnik a fokozott sértetti közrehatás. A lehetséges sértettek felvilágosításával, oktatásával az informatikai biztonság nagymértékben növelhető lenne.

A technológia fejlődésével létrejött egy új hadviselési forma a kiberhadviselés. A szakértők a hadviselés új, ötödik hadszínteréről beszélnek a föld, a víz, a levegő és a világűr után. Ez az új hadszíntér a kibertér. Itt említeném meg, mint tipikus példát, az iráni atomprogram elleni kibertámadást. A kritikus infrastruktúrák is lehetnek a kiberhadviselés célpontjai, hiszen így megbénítható egy ország közüzemi (víz, gáz, villany) hálózata, lakosságának ellátása, vasúti hálózata, légiközlekedése, egészségügyi rendszere, stb. A pályamunkámban a jelentőségétől függetlenül a kiberhadviselést nem részletezem.

Sajnos az informatikai támadások kapcsán megjelent a politika is. Példaként említeném a BKV bérlet- és menetjegyvásárlási rendszere elleni támadást, és az azt követő politikai csatározást. A dolgozatomban a politikai oldallal nem foglalkozom, csak az informatika oldaláról mutatom be a sérülékenységeket, a támadásokat.

2. Elektronikus ügyintézés előnyei és hátrányai

Az informatikai rendszerek fejlődésével, elterjedésével az állami és a magánszférában is felismerték, hogy az ügyintézést érdemes átterelni informatikai útra. Az ügyfelek az interneten keresztül, a weboldalakon lévő információk alapján tájékozódhatnak, elektronikus úton adhatják be irataikat (pl.: kérvények, panaszok, stb.), e-mailben kaphatják meg számláikat. Az elektronikus ügyintézés előnyei mellett megjelentek hátrányai is. Meglátásom szerint az elektronikus ügyintézést a lehető legegyszerűbbé kell tenni, hogy vonzó legyen az emberek számára. Ebben a fejezetben erről lesz szó.

2.1. Informatikai háttér megteremtése

Az elektronikus ügyintézés alapfeltétele a megfelelő informatikai háttér megteremtése. Gondolok az internet felől elérhető, interaktív weboldalak megírásától, beüzemelésétől, az elektronikus ügyintézés miatt várhatóan megnövekvő e-mail forgalom kiszolgálását végző munkaállomások beállításáig. Gondoskodni kell a weboldalak, számítógépek frissítéséről. Az informatika fejlődésével naponta jelennek meg új technológiák. Ezek bevezetése is jelentős plusz feladatot, költséget eredményezhet. Példaként említeném meg, hogy a régebben fejlesztett Java nyelven írt programok között van olyan, ami nem kompatibilis az újabb Java futtató környezettel.

Az informatikai háttérnél meg kell külön említeni, hogy az ügyintézésre szolgáló webszervereken futó programoknak hozzá kell férni az adott szervezet belső szerverein lévő adatbázisokhoz, a bejövő leveleket továbbítani kell a belső rendszeren lévő munkatársakhoz. Ez biztonsági kockázatot hordozhat magában.

Az informatikai hátteret – ha a fogalmat bővebben értelmezzük – a felhasználóknak is meg kell teremteni. Környezetemben az idősebb korosztály nem rendelkezik számítógéppel, okostelefonnal, internethozzáféréssel, valamint informatikai tudással.

Azt tapasztalom, hogy az elektronikus ügyintézés lehetősége nem elég motiváló számítógép vásárlására, bővítésére, informatikai tudás elsajátítására.

2.2. Azonnali rendelkezésre állás

A XXI. században sok helyen rendelkezésünkre áll az internet, és sok embernek van internet használatra alkalmas számítástechnikai eszköze (számítógép, mobiltelefon, stb.). A mobiltelefonhálózatok fejlődésével egyre több helyen érhető el telefonról is az internetet. Azonban vannak még olyan helyek, ahol nem tudjuk használni a mobiltelefonunkat. Ilyenek lehetnek például a magas hegyeken lévő lefedetlen helyek, repülőgépek fedélzete, stb. Külföldi kiránduláskor nehézséget okozhat a mobilinternet használatának jelentős költsége. Az előző részben már esett szó arról, hogy az idősebb korosztály nem rendelkezik

internetelőfizetéssel és számítógéppel. Ezek a tényezők nehezítik az elektronikus ügyintézés elérését.

Az informatikai rendszeren végzett ügyintézésnek nagy előnye, hogy bármikor tudjuk az ügyintézést kezdeményezni. Nem kell várnunk a hivatal kinyitására, nem kell sorba állni, nem kell szabadságot kivenni, nem kell utazni.

Az ügyek feldolgozását sok esetben lehet algoritmizálni, gépesíteni, ezért ezekben az esetekben nem szükséges az emberi beavatkozás. Példaként említeném a tantárgyak felvételét az egyetemeken működő Neptun programban, vagy a banki átutalást. Abban az esetben, ha az ügyintézéshez emberi beavatkozás szükséges, az rendszerint munkaidőben történik. Ritka az elektronikusan beküldött anyagok azonnali feldolgozása 7/24 órás rendszerben.

Az elektronikus ügyintézésben a kommunikáció kiterjeszthető oly módon, hogy az okostelefon, vagy a megfelelő szenzorokkal felszerelt számítástechnikai eszköz, bizonyos események bekövetkezésekor automatikusan küldjön sms-t, e-mailt. Lehetséges más jellegű internetes kommunikáció is. Erre jó példa a vészhívások helyének lokalizálására szolgáló, az Android operációs rendszerű mobiltelefonokra telepíthető Advanced Mobile Location (AML) alkalmazás. Az alkalmazás a segélyhívó központ hívásakor automatikusan, sms-ben elküldi a telefon földrajzi koordinátáit. Az alkalmazás a GNSS (global navigation satelit system), köztudatban lévő nevén GPS alapján határozza meg a telefon helyzetét. Az ügyintézés ilyen irányú kiterjesztése esetén a fogadó központnak, illetve a mögötte álló kiszolgáló rendszernek is fel kell készülni az üzenetek fogadására. Az AML alkalmazás esetén a segélyhívó központnak és az általa irányított egységeket is fel kell szerelni megfelelő technikával, informatikai alkalmazásokkal, ki kell alakítani az új munkamódszereket. Ebben az esetben olyan alkalmazásra gondolok, amely térképen mutatná a hívás helyét, illetve a helyszínre kivonuló járművekben is lenne egy térképes megjelenítő eszköz. Az ilyen alkalmazásokkal lehetne csökkenteni az operátorok leterheltségét, illetve a helyszínre vonuláshoz szükséges időt.

2.3. Az AVDH szolgáltatás egyszerűsítése

Az elektronikus ügyintézés térhódítása, valamint a jogszabályi környezet változása miatt úgy gondolom, hogy egyre többen fogják használni az elektronikus aláírást. Sajnos az informatikai szakemberek egy része sincs tisztában az elektronikus aláírás fogalmával, annak részeivel, funkciójával. Itt gondolok az aláírt irat megváltoztathatatlanságát biztosító hash adatra, időbélyegzőre, az aláíró azonosítására szolgáló adatokra.

Az Ügyfélkapurendszerben felhasználói fiókkal rendelkezők az irataikat elektronikusan aláírhatják az Ügyfélkapuhoz kapcsolódó Azonosításra Visszavezetett Dokumentum Hitelesítés (AVDH) szolgáltatással. Személyes tapasztalatom alapján fontosnak tartom a szolgáltatás megújítását, hogy az informatikában járatlan személyek is könnyebben írhassák alá irataikat. Az AVDH szolgáltatás elérése sokkal könnyebb lenne, ha az Ügyfélkapu felületére is ki lenne rakva. Az aláírható dokumentumok formátumának bővítését is fontosnak érzem. A pdf formátum mellett jó lenne, ha a program fogadni tudná a word, szövegszerkesztő program doc, docx formátumát, valamint az open office ODF formátumát is. Előre mutató lenne az AVDH honlapján történő szövegszerkesztési lehetőség megteremtése is.

Jelentős akadálynak gondolom, hogy az Ügyfélkapu a legtöbb ügyintézési formánál egyirányú. Nagy könnyebbség lenne, ha az Ügyfélkapun keresztül be tudnánk nyújtani elektronikusan aláírt iratokat. Jelenleg az ABEV Java program segítségével tudunk küldeni iratokat, viszont – tapasztalataim alapján – annak telepítése, az űrlapok letöltése sokszor nehézségbe ütközik az átlagos felhasználónak. Ez utóbbi miatt lenne könnyebbség az iratok Ügyfélkapun keresztüli benyújtása.

Az AVDH használata biztonsági problémákat is felvet. Az Ügyfélkapus bejelentkező nevünkkel és jelszavunkkal tudjuk használni az AVDH szolgáltatást. Az Ügyfélkapus azonosító adatainkra nagyon kell vigyáznunk, mert ha azok illetéktelen kezekbe kerülnek, akkor a nevünkben bármilyen elektronikus iratot alá tudnak írni. Javaslom az AVDH szolgáltatáshoz a dupla autentikáció bevezetését a biztonság növelése érdekében.

3. Kritikus infrastruktúra

A pályamunkám további részében az informatikai támadásokkal foglalkozok. Az informatikai sérülékenység és a támadások bemutatásakor sokszor lesz szó a kritikus infrastruktúráról, ezért először azt definiálom.

Általánosságban infrastruktúrán azon eszközök, intézmények összességét értjük, amelyek bár nem részei a közvetlen termelési folyamatnak, viszont annak nélkülözhetetlen feltételei. (Belügyi Szemle 2011/2 szám 27. old.)

Az infrastruktúrát többféleképpen csoportosíthatjuk. Beszélhetünk energia-, közlekedési-, telekommunikációs infrastruktúráról. Tágabb értelemben oktatási, egészségügyi, honvédelmi, rendvédelmi, stb. intézmények hálózatát is infrastruktúrának nevezhetjük.

Hagyományosan biztonságkritikusnak nevezzük azokat az egyedülálló (stand-alone) mérnöki rendszereket vagy alkalmazásokat, amelyek működése emberéleteket veszélyeztető baleseti kockázatokat rejt, és/vagy a hibás működésük nagyon jelentős gazdasági, környezeti vagy akár szociális károkat okozhat (Biztonsági kihívások a 21. században 345. old.).

A kritikus infrastruktúra: a nemzeti és uniós infrastruktúra azon létfontosságú elemei, melyek jelentős károsodása, üzemzavara vagy megsemmisülése esetén, súlyos következményekkel járna a nemzet vagy a nemzetek biztonságára, a gazdaságra, a környezetre és közegészségre, illetve az egyes kormányok, az állam hatékony működésére (Belügyi Szemle 2011/2 szám 27. old.).

Teljesség igénye nélkül a kritikus infrastruktúrák:

- energiatermelő és elosztó infrastruktúrák
- banki és pénzügyi infrastruktúrák
- vízellátó és közmű infrastruktúrák
- távközlési és kommunikációs infrastruktúrák

- szállító infrastruktúrák
- katasztrófavédelmi infrastruktúrák (rendőrség, tűzoltóság, egészségügy, stb.)
- honvédelmi, katonai infrastruktúrák
- élelmiszer-ellátási infrastruktúrák

A kritikus infrastruktúra működését számítógépes rendszerek segítik. Ezek lehetnek teljesen automatizáltak is, természetesen emberi felügyelet mellett. Ilyenek működnek például az energiaelosztó infrastruktúrában. A kritikus infrastruktúrában működő rendszerekről sokszor elmondható, hogy biztonságkritikusak is.

A mai világban gyakran lehet hallani informatikai támadásokról. Sajnos ezek a kritikus infrastruktúrát sem kímélik. A kritikus infrastruktúra elleni informatikai támadás irányulhat a szerverek, a számítógépes hálózat ellen, de irányulhat az adatok felhasználási helyén lévő munkaállomások ellen is. Azt gondolhatjuk, hogy a munkaállomások elleni támadás nem okoz jelentős kárt, mert a fontos adatok a szerveren tárolódnak. Azonban a munkaállomásokon is lehetnek olyan adatok, melyek törlése nagy veszteséget jelent. A munkaállomások tömeges kiesése is károkat okoz, azok újratelepítése jelentős időt igényel, és a költsége sem elhanyagolható. A munkaállomások kiesését egy példával szemléltetném. Képzeljük el azt az esetet, hogy bemegyünk az orvoshoz és nem működik a számítógépe, nem látja a leleteinket, nem tud receptet felírni, röntgenfelvételt készíteni, stb.

4. Kiberfizikai rendszerek

Az infrastruktúrák kérdéskörét tárgyalva nem mehetünk el a kiberfizikai rendszerek mellett. A hétköznapi eszközeinkben is használunk beágyazott számítógépeket. Ezek a számítógépek az eszközeink működését szabályozzák. A szabályozások lehetnek nagyon egyszerűek, de nagyon bonyolultak is. Ezeknek a számítógépeknek az összekapcsolását hívjuk kiberfizikai rendszereknek. Ilyen értelemben például egy okos ház is kiberfizikai rendszer.

Tudományos definíció: kiberfizikai rendszer alatt (angolul „cyber-physical system“ - CPS) az informatikai, szoftvertechnológiai, valamint mechanikai- és elektronikai elemek egységbe kapcsolását értjük, ahol az elemek egy olyan „adat-infrastruktúrán” keresztül kommunikálnak egymással, mint pl. az internet. A kiberfizikai rendszer egyik legfőbb jellemzője az igen magas fokú összetettség (komplexitás). A kiberfizikai rendszerek kialakítása beágyazott rendszerek hálózatba kapcsolása révén jön létre vezetékes illetve egyre inkább vezeték nélküli kommunikációs hálózatok segítségével.

Az életünk számos területét átszövik a kiberfizikai rendszerek. A kiberfizikai rendszerek biztosítják több kritikus infrastruktúrának a működését, pl.: a villamosenergia hálózat működését. A kiberfizikai rendszerek jelentős része biztonságkritikus, ezért ezeknek a hibás, sérült vagy rosszindulatúan módosított működése emberéletet követelő baleseteket, ellátási zavarokat, környezeti katasztrófákat eredményezhet. Ezért elvárás, hogy ezek a rendszerek megbízhatóan működjenek. Ez a megbízhatóság messze felülmúlja a hétköznapi életben használt programoktól megszokott megbízhatóságot. Ha a Windows operációs rendszer alatt futó program lefagy, vagy munka közben újra kell indítani a Windowst, az általában nem okoz gondot. A biztonságkritikus kiberfizikai rendszereknél az ilyen újraindítás elképzelhetetlen.

Az informatika és a mérnöki tudományok fejlődésével új kiberfizikai rendszerek fognak megjelenni, amik új biztonsági kihívásokat is tartogatnak. A jövőben ezeknek a biztonsági kihívásoknak is meg kell felelnünk.

5. Informatikai kockázatok és azok csökkentése

Az informatikai támadások igyekeznek kihasználni az informatikai rendszerek, programok sérülékenységeit, gyenge pontjait. Ezek a gyenge pontok eredhetnek a programok, valamint a felhasználók hibáiból is. A következő részben ezekről a hibákról, mint kockázati tényezőkről és azok csökkentésének lehetséges módjairól lesz szó.

5.1. Sértetti közrehatás

Az informatikai bűncselekmények közül az eddig tudomásomra jutott esetek jelentős részében meghatározó volt a sértetti közrehatás. A sértettek informatikai biztonsági ismereteinek alacsony szintje, és ebből eredően a programok kezelésének és karbantartásának hiányosságai jelentősen növelik az elkövetők esélyeit. A teljesség igénye nélkül néhány főbb hiányosságot vázolok fel. Ezek a hiányosságok nemcsak a munkahelyeken, hanem otthoni környezetben is növelik az esetleges támadások sikerét.

A sikeres támadások első okaként kell megemlíteni a programok elavultságát. Legfontosabb lenne az operációs rendszer frissítése. Az operációs rendszerekhez a kibocsájtásuk után több évig készítenek frissítő állományokat. A támogatási időszak operációs rendszerenként változik. A felhasználói szoftvereket gyártó cégek – egy idő után – a már nem támogatott operációs rendszereken futó programjaikat sem frissítik. Lehetőleg ne használjunk olyan operációs rendszert, melyre már nem készítenek frissítéseket.

Sok cégnek inhomogén gépparkja van. Számítógépeiket eltérő időpontokban, és más-más cégektől vásárolták, ezért különböző időpontokban avulnak el. Sok helyen az a gyakorlat, hogy a számítógépeken az operációs rendszert ritkán cserélik le, gyakorlatilag egy számítógépen a rendszerbe állítástól a kivonásig ugyanaz az operációs rendszer fut. Ez abból is adódhat, hogy az új operációs rendszereknek gyakran magasabb a hardver igénye, mint a régieknek. Elmondható, hogy sok helyen a régi, elavult operációs rendszerek száma az adott cég hardver beruházásainak függvénye. Ezért fordulhatnak elő jelentős számban a régi, már nem támogatott operációs rendszerekkel működő számítógépek.

Fontos, hogy az operációs rendszerre kiadott minden frissítést lehetőleg minél hamarabb futtassuk le. A frissítések futtatását sokszor a felhasználók is elvégezhetik. Viszont nem egy felhasználónál látom, hogy a frissítések futtatását rendszeresen kihagyja. Halottam olyan vélekedést, hogy minek azt futtatni, értékes időt vesz el a munkától. Ők valószínűleg nem tudják, hogy a frissítések elhanyagolása is hozzájárulhat több vírus terjedéséhez, ez történhetett például a WannaCry vírus esetében is. Itt említeném meg, hogy a Windows alapú hálózatokat be lehet úgy állítani, hogy a

munkaállomásokon a frissítéseket csak rendszergazdai jogosultsággal rendelkező felhasználó tudja lefuttatni. Ez a beállítás nagy hálózatok esetében nagyon leterheli az informatikusokat, az összes számítógépen a frissítések futtatása nagyon sok időt vesz igénybe, extrém esetben – a gépek nagy száma miatt – lehetetlen a frissítés elvégzése.

A Windows operációs rendszer verziójáról a parancssorba begépelt winver utasítással győződhetünk meg. Ez a parancs nemcsak a fő verziót (pl.: Windows 7, Windows 8, Windows 10), hanem az alverziót (pl.: 1703) is kiírja. A Windows 10-nél az alverzió az adott módosítás kiadásának dátumára utal. A Windows XP operációs rendszer SP2 verziójában jelent meg az új parancssor, a powershell. Ezt a régi, DOS-ból örökölt parancssor utódjának szánta a MicroSoft. A powershell-ben a get-hotfix paranccsal tudjuk kiíratni, hogy milyen frissítések futottak le az adott operációs rendszeren.

Az operációs rendszeren kívül a többi programot is fontos frissíteni. Az internet felöl jövő támadások kivédése szempontjából fontos a webböngésző és ahhoz kapcsolódó megjelenítő programok (pl.: Adobe Flash) frissítése. Ide sorolnám a Java futtató környezetet is. Sajnos ezeknek a programoknak a frissítését nem, vagy csak késve követik a felhasználói programok. Példaként említem, hogy az idei év szeptember 21- én kiadott Java SE 9 alatt – e sorok írásakor – nem fut a NAV nyomtatványkitöltő programjának aktuális verziója (v2.77) (http://www.uzletresz.hu/penzugy/20170927- nem-kompatibilis-a-java-a-nav-nyomtatvanykitoltojevel.html). A programok frissítése, újabb verziókra történő áttérés azért is fontos, mert több szoftvercég a régi verziójú programjaiban kevésbé törődött a biztonsággal. A felhasználói programoknál is előfordulhat az, hogy a frissítések futtatásához rendszergazdai jogosultság kell, ami szintén megnehezítheti a programok frissítését.

Azt is el kell ismerni, hogy a napi munkához egy szervezet számtalan programot használhat, amikhez rendszeresen érkeznek frissítések. A frissítések telepítése előtt szükséges azok tesztelése, hogy használatuk nem akadályozza-e a napi munkát. A frissítő állományok tesztelése, telepítése jelentős humánerőforrást igényelhet, ami nem biztos, hogy rendelkezésre áll.

Szintén biztonsági kockázatot hordoz magában a nem megfelelő felhasználói szoftverek választása. A szoftverek jelentős része tartalmaz biztonsági réseket. Figyeljünk

oda, hogy megfelelő biztonságú programokat használjunk. A víruskereső megválasztása is fontos, hiszen az biztosítja a számítógép megfelelő védelmét.

A felhasználók gondatlansága is biztonsági kockázatot hordozhat. Nagyon sok felhasználó gondolkodás nélkül nyitja meg az e-mailekhez kapott csatolmányokat. Ezek a csatolmányok lehetnek rosszindulatú kódot tartalmazó programok is. A rosszindulatú programok lehetnek különböző vírusok, akár zsarolóvírusok, de nyithatnak úgynevezett hátsó kaput (back door) az operációs rendszeren, melyen keresztül a bűnözők kívülről, az internet felől be tudnak jelentkezni az operációs rendszerbe, és rendszergazdai jogokkal tudnak kárt okozni.

Azoknál a cégeknél, hivataloknál, ahol ügyfélforgalom is van különösen fontos az informatikai eszközök elhelyezése, fizikai védelme is. Ez különösen igaz a kritikus infrastruktúrához tartozó cégeknél, hivataloknál. Sajnos azt tapasztalom, hogy ez a szemlélet még nem ment át a köztudatba. Az egyik kórházban láttam, hogy a lokális hálózat switcheit tartalmazó üvegfalú rack szekrényt a betegek, illetve a vizsgálatokra érkezők által elérhető helyen, kb. 1 méter magasságban helyezték el. Szintén kórházban láttam, hogy a szerverhelyiség a betegfelvételi pulttal szemben található, amire az ajtón olvasható felirat hívta fel a figyelmet.

Végül, de nem utolsó sorban a mentések fontosságára hívnám fel a figyelmet. A számítógépünkben található adathordozók (merevlemez, SSD) tartalmát rendszeresen mentsük külső eszközre. Az informatikai eszközök fejlődésével a vírusok is fejlődtek. Már nem jelent biztonságot a NAS-ra illetve a felhőbe végzett mentés. Vírusfertőzés esetén a NAS-on illetve a felhőben lévő adataink is károsodhatnak. Sok munkahelyen csak a szerver merevlemezeiről készül biztonsági mentés. A munkaállomások adathordozóit nem mentik. Sajnos sok munkáltató a szerverein nem biztosít elegendő tárhelyet a munkavállalóknak, ezért a munkavállalók a saját munkaállomásukon lévő merevlemezt, SSD-t használják adataik tárolására. Ezek az adatok megsemmisülhetnek egy meghibásodás illetve egy vírusfertőzés következtében.

5.2. Oktatás fontossága

Az informatika gyors fejlődése megkívánja, hogy az informatikai szakemberek is és a felhasználók is tovább képezzék magukat. A folyamatos tanulást az is indokolja, hogy az iskolarendszerű oktatásból kikerült fiatal munkavállalók a legújabb technológiát ismerik és velük kell felvenni a versenyt az idősebb korosztálynak. Sajnos elmondható, hogy sokan önerőből nem akarnak tanulni és azt várják, hogy a munkáltatója iskolázza be őket.

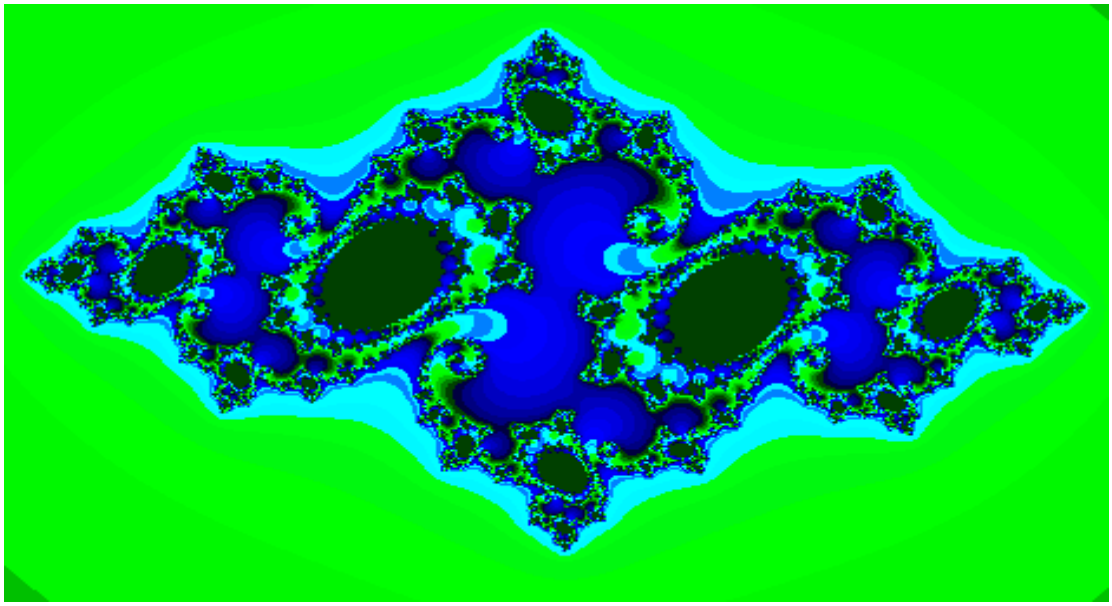
A számítógépes biztonság is olyan terület, ahol szintén szükséges a rendszeres tanulás. Az ismeretek nagyrészét újságcikkekből, internetről lehet elsajátítani. Sajnos kevés a tanfolyam és azok is viszonylag drágák. Néhány éve még a legmagasabb szintű nemzetbiztonsági átvilágításnak kellett átesniük a számítógép biztonsági tanfolyamra jelentkezőknek (Forbers NEXT magazin 2017. nyár 35. old.).

Az informatikai szakembereknek az informatikai biztonság széleskörű oktatása különösen fontos lenne, hiszen sokaknak hiányos ismerete van ezen a területen. Erre az eddig tudomásomra jutott esetek is utalnak. Több esetben, a sértettek által alkalmazott informatikusok, a biztonságra nem gondolva, gondatlanul alakították ki az informatikai rendszereket és ez segítette a kiberbűnözőket a bűncselekmény elkövetésében. Az oktatás során figyelembe kell venni a szakmai sajátosságokat, hiszen egy rendszergazdának más ismeretre van szüksége, mint egy programozónak.

A felhasználók informatikai ismeretei is sok esetben hiányosak. A 45 évesnél idősebb korosztály esetében a legfőbb okot abban látom, hogy nem nőttek bele az informatikába, gyerekkorukban nem volt lehetőségük elérni a számítógépeket. Az informatika elérhetővé válásával a 80-as, főleg a 90-es években sokan vásároltak számítógépet gyerekeiknek, de a szülők annak használatát ritkán tanulták meg. Később az élet kényszerítette ki, hogy elsajátítsák a munkához, életükhöz szükséges informatikai ismereteket. Általánosságban – életkortól függetlenül – elmondható, hogy a hiányos ismeretekhez az érdeklődés hiánya is vezethet. Sokan nem természettudományos, vagy műszaki érdeklődésűek, idegen tőlük az informatika, a számítógép világa. A gondolkodásuk is távol áll a matematikai vagy a mérnöki gondolkodástól. Ezekhez az emberekhez közelebb kell vinni az informatikát. A programok minősége is szülhet

nehézségeket, ami elfordítja az embereket az informatikától. Sokszor hallok olyan vélekedést, hogy ez a probléma sem lenne, ha a „… programot” nem kellene használni.

A következő képpel egy olyan oldalról szeretném megmutatni a matematikát, ami sokkal izgalmasabb és nem olyan „száraz”, mint a számok világa. Természetesen itt is komoly „számtan” van, de remélem, hogy ezt feledteti a látvány.



1. A matematika „színes” világa – Julia halmaz ábrázolása a szerző programjával

A leírtak miatt a felhasználókat is szükséges az ő szintükhöz igazodó oktatásban részesíteni. Ez nemcsak az új programok kezelésének elsajátítása, illetve a régi programok használatának elmélyítése, begyakorlása miatt fontos, hanem azért is, mert az így elsajátított biztonsági ismeretek alapján megvédhetik a számítógépeiket, adataikat a különféle támadásoktól. A szervezett oktatás mellett fontosnak tartom az önképzést is. A felhasználók kellő ismeret hiányában nem akarnak, nem képesek, vagy nem mernek önállóan a munkájuk, otthoni számítógépük használata során felmerült informatikai problémákra – az interneten – megoldást keresni, és a kapott megoldásokat kipróbálni.

Az oktatásra meg kell találni a megfelelő csatornát. A munkahelyi programok használatának oktatását munkahelyi keretek között kell megoldani, viszont szélesebb kört megcélzó oktatásnak más csatornákat kell keresni.

A hétköznapi élet különböző területeiről jövő szakembereknek az informatikusokkal történő együttműködés is nehézségekbe ütközhet az eltérő szakmai nyelvezet, illetve gondolkodásmód miatt. Példaként említeném, azoknál a munkahelyeken, ahol az informatika kiszolgáló szerepet tölt be, az informatikusnak a szakkifejezések helyett hétköznapi kifejezéseket kell alkalmaznia, hogy szót értsen kollegáival.

5.3. A matematika szerepe a védelemben: hatványfüggvények jelentősége az informatikai támadások kivédésében

A számítógépek hálózatba kapcsolása napjaink technológiája. Itt nemcsak az internetre gondolok, hanem vállalati hálózatokra (intranetre) is. Barabási-Albert László erdélyi származású fizikus munkássága nyomán ismerjük, hogy a számítógépes hálózatok aktív eszközeinek (router, switch) eloszlása hatványfüggvényhez hasonló. Ez az eloszlás a véletlen meghibásodásokkal szemben biztonságot ad, de nem ad biztonságot a szándékos károkozás ellen.

Barabási Albert László 1999-ben végzett kísérletét ismertetném a hálózatok sebezhetőségével kapcsolatban. A kísérletben 40000 elemből álló hálózatot hoztak létre. A hálózati elemek kapcsolatait leíró függvény hatványfüggvényhez hasonló. P(k) jelentette annak valószínűségét, hogy egy véletlenül kiválasztott elemnek k kapcsolata van. A kísérletben $P(k) \sim k^{-3}$. A kísérlet során megvizsgálták a véletlenszerű meghibásodásokat. A meghibásodások nem okoztak jelentős hibát a hálózat működésében. A rendszer elleni célzott támadásokat is tanulmányozták. Ennek során kivették a hálózatból azt a 10 db elemet, melyek a legtöbb kapcsolattal rendelkeztek. Ekkor a hálózat 500 részre (komponensre) esett szét. (Barabási-Albert László: A hálózatok tudománya 31. oldal) A kísérlet eredményéből látható, hogy a hálózat mennyire sebezhető a támadásokkal szemben.

Barabási Albert László mérései alapján az internet működését biztosító aktív eszközök eloszlása hasonló a 3,42 kitevőjű hatványfüggvényhez. Ez a kritikus infrastruktúrába tartozó vállalatoknak, szolgáltatóknak, hatóságoknak rossz hír, mert ha a nyílt internetet használják például a telephelyei közötti kapcsolattartásra, akkor egy célzott támadással megbénítható az informatikai hálózatuk. Magánhálózat esetében viszont a hálózat kialakítása az adott cég

kezében van. Célszerű a hálózat nagy forgalmú, sok kapcsolódással rendelkező, fontos elemeit földrajzilag messze telepíteni egymástól, hogy egy természeti katasztrófa esetén ne essen szét a hálózat. A kibertámadás ellen a megfelelő informatikai védelmet, például víruskereső programok használatát, valamint a redundancia növelését látom megoldásnak.

A jelentős számú munkavállalót foglalkoztató cégeknél előfordulhat, hogy nem mindenkit tudnak megfelelő informatikai oktatásban részesíteni. Ilyen esetben kockázatelemzést érdemes alkalmazni. Első körben javaslom azok oktatását, akiknél jelentős a külső partnerekkel történő levelezés. Ilyen lehet például a sajtós és a személyzetis munkatárs.

Az e-mailekkel terjedő vírusok visszaszorítása érdekében is igénybe vehetjük a hálózatkutatás legújabb eredményeit. Az e-mailek forgalma is hatványfüggvényhez hasonló eloszlást követ. A bejövő e-mailek címzettek szerinti eloszlása hasonló a 3,43 kitevőjű hatványfüggvényhez. (Barabási-Albert László: A hálózatok tudománya 144. oldal) Másrészről a közösségi média elemzéséből ismert, hogy az emberek kapcsolatai számának eloszlása is hatványfüggvényhez hasonló. Az e-mailekkel terjedő vírusok visszaszorítását a célzott oktatás is segítheti. Az oktatás célcsoportja a legtöbb külső kapcsolattal rendelkező munkatársak, felhasználók csoportja. Az oktatás középpontjába javaslom helyezni az e-mailek biztonságos kezelésével kapcsolatos ismereteket.

6. Informatikai támadások

Az informatikai támadások többfélék lehetnek. A támadók kárt okozhatnak különféle programokkal. Kihasználhatják az operációs rendszer illetve a felhasználói programok hibás kódjait a számítógépbe történő behatolásra. Ellophatják adatainkat. Ezek az adatok lehetnek saját számítógépeinken vagy különböző hivatalok, szolgáltatók, cégek szerverein. Én a károkozó programok közül a vírusokat emelném ki.

Az első számítógépes vírusokat az 1980-as években alkották meg. Azóta a kárt okozó programok széles köre fejlődött ki. Cégek alakultak a számítástechnikai eszközeink biztonságának növelésére. Ezektől a cégektől ingyen vagy anyagi ellenszolgáltatás

fejében tölthetjük le a víruskereső programokat. Más cégek a programok biztonsági bevizsgálására szakosodtak.

Az elmúlt években megjelentek a zsarolóvírusok. Ezek a vírusok a sértett merevlemezén található állományokat titkosítják, és pénzt kérnek a dekódolásért. Idén júliusban az sg.hu honlapon megjelent cikk szerint a San-Diego-i és a New York-i egyetem, valamint a Chainalysis és a Google szakemberei szerint az elmúlt két esztendőben összesen 25 millió dollárt fizettek ki a bűnözőknek a zsarolóvírusok áldozatai. (https://sg.hu/cikkek/it-tech/126459/zsarolovirusok-25-millio-dollar- bevetel-ket-ev-alatt).

A Cisco hálózati eszközök fejlesztésével, gyártásával foglalkozó cég weboldalán megjelent cikk szerint 2016-ban a zsarolóvírusokból származó bevétel elérhette az 1 milliárd dollárt (https://www.cisco.com/c/dam/global/hu_hu/solutions/ security/ransomware/pdf/ransomware-infographic_hun.pdf). A becslések nagy szórást mutattak, de látható, hogy a zsarolóvírusok jelentős bevételt hozhattak a bűnözőknek.

A Magyarországi tapasztalatok is azt mutatják, hogy a zsarolóvírusok jelentősen elterjedtek. A Nemzeti Kibervédelmi Intézet által felügyelt rendszerekben 2016. I. negyedévében több száz zsarolóvírus-fertőzést regisztráltak (https://www.vasarnapihirek.hu/fokusz/a_drognal_is_nagyobb_uzlet).

A zsarolóvírusok általában e-mail csatolmányaként vagy különféle programokkal jutnak el a számítógépekbe. 2016 tavaszán a népszerű uTorrent kliens program tartalmazott zsarolóvírust. A vírus képes különféle folyamatok leállítására a Windows operációs rendszerben (https://pcworld.hu/szoftver/virusos-a-%C2%B5torrent- 176272.html).

A zsarolóvírusok kódolás alapján három félék lehetnek: aszimmetrikus kódolást használók, szimmetrikus kódolást használók, vagy mindkét kódolást használók. Azok a vírusok, amik mind a két kódolást használják, a szimmetrikus kódolást használják az állományok titkosítására, és csak a szimmetrikus kódolás kulcsát rejtjelezik aszimmetrikus kódolással, ezáltal optimalizálják a kódolásra fordított erőforrásokat (processzor idő, memória).

Az idei évben a zsarolóvírusok új nemzedéke jelent meg. A WannaCry és a NotPetya névű vírusok ehhez az új nemzedékhez tartoznak és óriási pusztításokat hajtottak végre a

kritikus infrastruktúrákban is. A következőkben támadás részletes leírásával rámutatok arra, hogy a károkozás nagy mértékéhez a rendszerek üzemeltetői és felhasználói egyaránt hozzájárultak.

6.1. WannaCry vírus

A WannaCry vírus 2017. május 12-én bukkant fel. A vírus óriási károkat okozott világszerte. A szakirodalom által ismertté vált támadások közül említek néhányat. Nagy Britanniában a National Health Service egészségügyi szolgáltató számítógépes rendszerét érte támadás. A vírustámadás a számítógépeken kívül orvosi műszereket (MRI scannert, robotsebészeti rendszereket, stb.) is érintett. A károkozás nagyságát mutatja, hogy néhány kórházban teljes szárnyakat kellett bezárni, orvosi beavatkozásokat elnapolni, mentőket átirányítani. Spanyolországban a Telfónica telekommunikációs szolgáltatót, valamint több nagyobb méretű vállalatot bénított meg a vírus. Németországban a Deutsche Bahnt (Német Vasúttársaság) érte támadás. Franciaországban a Renault egyik gyárában állt le a termelés szintén a WannaCry vírus miatt. A támadásra jellemző, hogy a vírus egy hétvége alatt több mint 10000 cég, szervezet több mint 200000 számítógépét fertőzte meg, összesen 150 országban (https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware- attack-spread-150-countries). Magyarországon a Telenort érintette a kibertámadás.

A megtámadott intézmények között több volt a kritikus infrastruktúrához tartozó szolgáltató, egészségügyi intézmény, vállalat. A vírus két fertőzési módot ötvözött, amire eddig nem volt példa, ezért a szakirodalomban az ilyen jellegű vírusra megjelent a ramsomworm név.

A WannaCry titkosította a gép merevlemezén lévő állományokat, melyek feloldásáért először 300 USA dollárnak megfelelő bitcoint kért. Ha ezt nem fizették ki, akkor a fizetendő összeg 600 USA dollárnak megfelelő bitcoinra emelkedett. Ha pedig egy hét után sem fizettek a zsarolóknak, akkor – a technika mai állása szerint – örökre elveszett a remény az állományok dekódolásra.

A vírus által használt sérülékenységet az elérhető szakirodalom alapján feltehetően az NSA (az Amerikai Egyesült Államok elektronikai hírszerzéssel foglalkozó szervezete) fedezte fel. A szakirodalomban EthernalBlue néven vált ismertté. Az EthernalBlue a puffertúlcsorduláson (buffer overflow) alapuló biztonsági rések közé tartozik. A sérülékenység abból eredt, hogy a Windows operációs rendszerben rosszul implementálták az SMB (Server Message Block) protokollt. Az SMB protokollt a számítógépes hálózatokban az erőforrások, file-ok, nyomtatók, soros portok, stb. megosztására használják. A Windows operációs rendszerben úgy implementálták az SMB protokollt, hogy az érkező adatcsomagok hosszát nem vizsgálta az operációs rendszer. Abban az esetben, ha az adatcsomag meghaladta a puffer hosszát, akkor az adatcsomag átírhatta az operációs rendszer kódjának egy részét. A WannaCry vírus ennek a sérülékenységnek a segítségével volt képes terjedni a lokális hálózaton kapcsolódó számítógépek között.

A sérülékenységre 2017. április 14-én hívta fel a figyelmet a The Shadows Brokers hackercsoport. A MicroSoft 1 hónappal korábban 2017. március 17-én adta ki az MS17-010 jelű biztonsági frissítést (security update) a Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows RT 8.1,

Windows Server 2012, Windows Server 2012 R2, Windows 10, Windows Server 2016 operációs rendszerekre. A frissítés az SMB protokoll implementációját javította. A WannaCry fertőzés bekövetkezése után – a fertőzés súlyosságára való tekintettel – a MicroSoft a már nem támogatott operációs rendszerekre (Windows XP, Windows 8, Windows Server 2003) is elkészítette a javítást, amit a támadás után 1 nappal ki is adott. Ebből világosan kitűnik, hogy a WannaCry nem Zero Day sérülékenységet használt ki, a felhasználók többségének lett volna idejük felkészülni a támadás elhárítására.

Az előző bekezdésben szereplő operációs rendszerek listájából látható, hogy a sérülékenység a szervereket is érintette, ezért a szervereken tárolt adatok is veszélybe kerültek. A cégek, illetve a szolgáltatók a szervereken tárolt adatokat általában rendszeresen mentik, ezért a sikeres támadás csak az utolsó mentés és a támadás időpontja között keletkezett adatokat érintette. Viszont a céges környezet munkaállomásain lévő adatokról sokkal ritkábban készül mentés, így az ott tárolt adatok sokkal kiszolgáltatottabbak, ugyanez elmondható az otthoni környezetről is.

A továbbiakban a WannaCry vírus működését és a kódjában talált hibákat mutatom be.

A vírus általában egy e-mailben érkező állománnyal kerül a számítógépre (https://pcworld.hu/pcwpro/wannacry-ransomware-228438.html). A vírus a sikeres fertőzés után az SMB protokoll sérülékenységét kihasználva szabadon szétterjed a számítógépes hálózat többi gépére is. A vírus működése során generál egy RSA kulcspárt. A vírus 176 féle állományt keres a merevlemezen, és azokat az állományokat titkosítja AES-128 kulccsal. Minden állományhoz új AES kulcsot generál. Az AES kulcsot is titkosítja az RSA kulcspár nyilvános kulcsával. Az így kapott titkosított kulcsot hozzámásolja a titkosított állomány elejéhez.

2. WannaCry vírussal fertőzött számítógép képernyője (Forrás: wikipedia.com)

Szerencsére a WannaCry vírus is tartalmazott bug-ot. A vírus az RSA titkosítási kulcs kiszámításának első lépéseként prímszámokat generált. Ezekből a prímszámokból számolta ki a kulcspárt. A kulcspár kiszámolása után a prímeket nem törölte ki a számítógép memóriájából, így lehetséges volt később azokat egy másik programmal

megkeresni és elmenteni. Az elmentett prímszámokból és a nyilvános kulcsból a titkos kulcsot az

$$\text{??} + l(\text{?} - 1)(\text{?} - 1) = 1$$

lineáris diofantoszi egyenlet megoldása adja, ahol ? a nyilvános kulcs, ? a titkos kulcs, ? és ? prímszámok. A kódolás műveletigényének csökkentése érdekében gyakran Fermat prímeket használnak nyilvános kulcsnak, ezért a nyilvános kulcs ismerete nélkül is van esélyünk a titkos kulcsot kiszámolni.

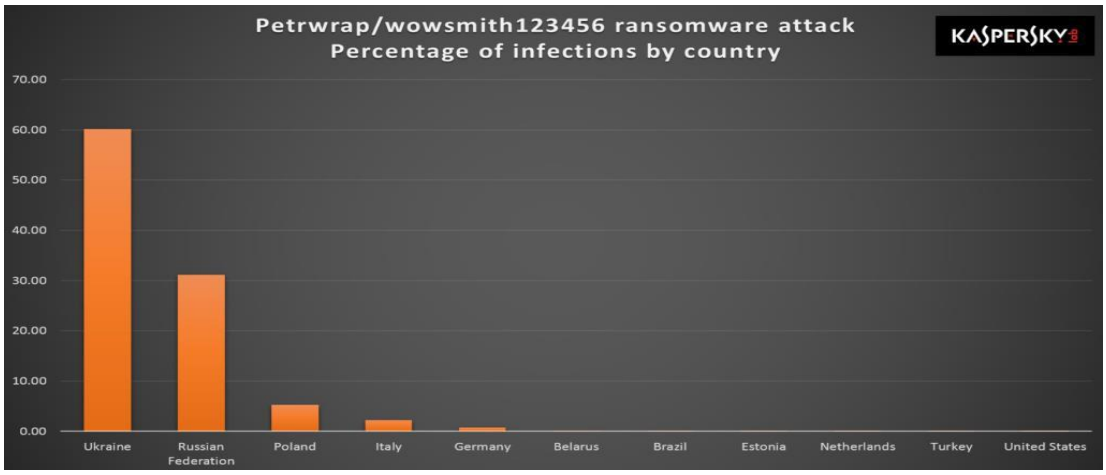
A vírus hibáját kódjának elemzésekor fedezték fel. Adrien Guinet francia biztonsági kutató készítette a Wannakey nevű programot (letölthető: https://github.com/aguinet/wannakey weboldalról), mely a prímszámokat megkeresi a számítógép memóriájában. A prímszámokból és a nyilvános kulcsból a program kiszámolja az RSA kódpár másik tagját és kikódolja a gépen lévő titkosított állományokat (https://sg.hu/cikkek/it-tech/125410/wanna-cry-mar-valtsagdij-fizetes- nelkul-is-kikodolhatok-a-fajlok). A programot csak akkor lehet eredményesen futtatni, ha a gépet nem kapcsolták ki, illetve nem resetelték. Sajnos megeshet, hogy a jövőben minket is ér zsarolóvírus-fertőzés. Ebben az esetben célszerű a számítógépet tovább működtetni, hátha annak a vírusnak a kódjában is előfordul az előbb említett hiba, és dekódolni tudjuk a titkosított állományainkat. Ilyen fertőzés esetén feltörő programot kell rögtön keresni az interneten.

A WannaCry vírus kódjában találtak egy másik hibát is. A kód elemzésével a szakértők észrevették, hogy a vírus minden fertőzéskor megpróbál csatlakozni a www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com címre. Abban az esetben, ha a csatlakozás sikeres, akkor a vírus leállítja magát (http://24.hu/tech/2017/05/13/egy-hetunk-maradt-visszaszerezni-az-adatainkat/). A biztonsági szakértők regisztrálták a domain nevet, és így megállították a vírus terjedését. Később több domain nevet is azonosítottak, aminek regisztrálásával szintén le tudták állítani a vírus terjedését (http://www.cert-hungary.hu/node/370). A siker ideiglenesnek bizonyult a regisztrációk után pár nappal a vírust új, módosított kóddal regisztrálták a biztonsági cégek.

6.2. NotPetya vírus

A másik vírus, ami szintén az EthernalBlue sérülékenységet használja ki, NotPetya néven vált ismertté. A vírus támadását 2017. június 27-én észlelték. A járvány Ukrajnában tört ki. Az első fertőzéseket egy elterjedt számlázó-, illetve könyvelő program, az M.E.Doc egy manipulált, trójai programmá alakított frissítése okozta. A frissítés telepítésekor a vírus megfertőzte a gépet. Ez a terjedési mód megmagyarázza, hogy a vírusnak miért sikerült számos, köztük védett környezetben lévő számítógépet megfertőzni. A fertőzött gépek között volt az ukrán miniszterelnök-helyettes, számos bank, köztük az Ukrán Nemzeti Bank és az OTP ukrán leányvállalatának számítógépei is. A felsoroltakon túl a fertőzés fennakadásokat okozott a közlekedési hálózatban, a kijevi metróban, a kijevi repülőtéren, továbbá a csernobili atomerőmű állapotát monitorozó rendszerben (manuális mérésre álltak át), az orosz Rosznyeft kőolajipari nagyvállalat kitermelési és fimonítási rendszerében (tartalék rendszerre kapcsoltak), a TNT szállítmányozási cég rendszerében. A sort még hosszasan lehetne folytani.

A támadások 60%-át Ukrajnában észlelték, de jelentős arányban észlelték Oroszországban (több mint 30%), Lengyelországban (kb. 5%), Olaszországban, Németországban. Igen kis arányban még az Amerikai Egyedült Államok és Magyarország is érintett volt (https://www.hwsw.hu/hirek/57452/microsoft-windows-ransomware-kriptovirus-petya.html). A támadások országok közötti megoszlását mutatja a következő grafikon.



3. A vírus támadásának országok közötti megoszlását mutató grafikon (Forrás: securelist.com)

A vírus a terjedéshez az EthernalBlue sérülékenységen kívül más módot is használ. Megpróbálja visszafejteni a Windows operációs rendszer jelszavait. A jelszavak visszafejtéséhez a Mimikatz jelszófeltörő programot vagy annak kódbázisát használja. A kiberbűnözők a vírust arra az esetre is felkészítették, ha szerverhez vagy tartományvezérlőhöz nyer hozzáférést. Ebben az esetben a vírus igyekszik megkeresni a tartományban lévő összes számítógépet és megpróbálja ezeket a gépeket megfertőzni. Ehhez a távoli indítási mechanizmust (RPC) használja fel. Az RPC a Windows része, ez szolgál arra, hogy az adott gép erőforrásait más gépekről is használni lehessen.

A vírus által végrehajtott titkosítás módja attól függ, hogy a vírus milyen jogosultságot tud szerezni az adott gépen, és milyen környezetben találja magát. A támadás során összehasonlítja egy előre meghatározott listával a megtámadott számítógépen futó folyamatokat, valamint ellenőrzi saját jogosultságait és ennek alapján dönt a további működéséről. Az első támadási mód, hogy átírja a fő meghajtó master boot recordját, és a gépet újraindítja. Ekkor rögtön a vírus indul el és az NTFS filerendszer Master File Tábláját kódolja le. Ezt a folyamatot azzal álcázza, hogy a képernyőn a chkdsk program futása látható. Abban az esetben, ha a vírus nem fut megfelelő jogosultságokkal, és nincs hozzáférése a Master File Táblához, akkor a merevlemezen lévő állományokat titkosítja. A titkosítás során meghagyja az állományok eredeti nevét és kiterjesztését. A vírus törli a Windows naplóállományait, ezzel álcázza a tevékenységét.

A vírus írói 300 dollárnak megfelelő bitcoint kértek az állományok kikódolásáért. Ezt a sértettek már nem tudják befizetni, mert az ESET informatikai biztonsági cég értesítése szerint a támadók által megadott e-mail címet a szolgáltató törölte. Egyes szakértők a könnyen kikapcsolható e-mail fiókból és más jelekből feltételezik, hogy a vírus készítőinek nem a pénzszerzés, hanem inkább a káosz keltése és az ukrán gazdaságban történő károkozás volt a célja.

A NotPetya vírus elleni védekezés is több lépést követel meg. A legfontosabb a Windows operációs rendszer rendszeres frissítése. A vírus működését blokkolni lehet, ha a Windows mappában létrehozzuk a perfc, perfc.dat és perfc.dll állományokat és ezeknek az írás és végrehajtási jogát blokkoljuk. Amennyiben nem használjuk a WMIC szolgáltatást, akkor tiltsuk le a „net stop winmgmt” paranccsal. A vírus e- mailek

segítségével is terjed. Az e-mailek csatolmányában lévő káros kód a vírust az internetről tölti le, ezért az alábbi címek elérését érdemes letiltani a tűzfalon: french- cooking.com, benkow.cc, 185.165.29.78, upd.me-doc.com.ua, 95.141.115.108, 111.90.139.247, 84.200.16.242, 185.165.29.78, yadi.sk (http://www.cert-hungary.hu/node/381, http://www.cert-hungary.hu/node/382).

7. Összefoglalás

A pályázati anyagból látható, hogy mindannyian válhatunk informatikai támadás áldozataivá. Az is látható, hogy odafigyeléssel, a rendszerek beállításával, frissítésével a támadások nagyrésze kivédhető, károkozásuk csökkenthető. A rendszerek tervezésekor, üzemeltetésekor azt kell eldöntenünk, hogy mennyi időt, pénzt és energiát áldozunk a védelemre. Ez igaz otthoni, és vállalati környezetben is. Fő szabály, hogy minden informatikai fejlesztésre szánt összegnek 5-8, esetenként 10 százalékát kell a biztonságra fordítani. Minden fejlesztésnél fel kell tenni a kérdést: mekkora kárt okozhat, ha az adott informatikai rendszer a felhasználók számára elérhetetlenné válik, és így nem tudnak hozzáférni számos fontos adathoz? Mennyit érhetnek a számítógépes rendszerben tárolt információk? Otthoni rendszerre vetítve, hétköznapi nyelvre lefordítva, mennyit érnek a számítógépemen tárolt családi fotók? Ha ezt mérlegeljük, nagyjából kiszámítható, mennyit kell költeni az adatok védelmére. A védelem megteremtése a víruskereső program beszerzésétől, az operációs rendszer frissítésén keresztül, az új operációs rendszer és az ehhez szükséges hardverbővítés megvásárlásig terjedhet.

A két informatikai támadás (WannaCry és a NotPetya) leírásából látszik, hogy a támadás időpontjában már ismert sérülékenységet használtak ki a vírus írói. Az is látszik, hogy a támadás a kritikus infrastruktúrát sem kímélte. Többek között bankok, egészségügyi intézmények, a szállító infrastruktúra szereplői (pl.: Német Vasúttársaság, kijevi metró és repülőtér, TNT) is áldozatául estek a támadásnak. A kritikus infrastruktúra esetében különösen fontos a folyamatos működés fenntartása, ezt a megfelelő redundancia, és támadás esetén a gyors reagálás biztosíthatja. A kritikus infrastruktúrákat működtető hivatalok, cégek alkalmazottjai közül is sokan dolgoznak számítógéppel. Abban az esetben, ha nem mindenki tartja be a biztonsági intézkedéseket, akkor sokkal könnyebb

dolguk van a kibertámadóknak. A pályázati anyagomban megpróbáltam összegyűjteni azokat a biztonsági javaslatokat, melyek a sikeres támadás esélyét csökkenthetik.

Pályamunkámban nem tértem ki az adatlopásokra és az adatlopásokkal összefüggő visszaélésekre, csalásokra. Gyakran fordul elő, hogy a felhasználókat hamis e- mailekkel ráveszik személyes adataik, jelszavaik megadására. Az ilyen e-maileket mindig fenntartással kell fogadni.

Az Európai Unióban a személyes adatok biztonsága kiemelt helyen szerepel. A különböző hatóságok, szolgáltatók, magáncégek szerverein tárolt személyes adatok biztonságát szigorítja az EU Általános Adatvédelmi Rendelete (GDPR), amely az Európai Parlament és a Tanács 2016/679 rendelete. A tagállomoknak 2018. május 25- ig kell eleget tenni a rendeletben foglaltaknak.

Az első részben néhány gondolatban írtam az elektronikus ügyintézés előnyeiről és hátrányairól. Részben felhasználói szemmel nézve, részben a felhasználóktól kapott információk alapján azt látom, hogy az elektronikus ügyintézés egyszerűsítésre szorul. Az AVDH szolgáltatást emeltem ki az elektronikus ügyintézések közül. Javasoltam az AVDH szolgáltatást jobban összekapcsolni az elektronikus ügyintézés többi elemével.

Remélem, hogy pályázati anyagommal sikerült rávilágítanom az informatikai biztonság kiemelt fontosságára.

Irodalomjegyzék

Önálló mű

Barabási-Albert László: A hálózatok tudománya, Libri Kiadó, Budapest, 2016

Tanulmánykötet

Biztonsági kihívások a 21. században, szerk.: Finszter Géza, Sabjanics István, Dialóg Campus Kiadó, Budapest, 2017

Folyóiratban megjelent tanulmány

Laza Bálint: Minden szombaton dolgozik, Forbes NEXT magazin, 2017. nyár, 32. old.
Mezey Nándor Lajos: Kiberterrorizmus: Valós veszély, Belügyi Szemle, 2011/2 szám, 21. old.

Internetes forrás

Bercze András: Brutális zsarolóvírus söpört végig a neten, pár óra alatt több tízezer gépet fertőzte meg, PC World, 2017. Forrás: https://pcworld.hu/pcwpro/wannacry-ransomware-228438.html

(2017. 10. 01.)

Berta Sándor: Több millió dollárt lehet keresni egy zsarolóvírussal, 2017. Forrás: https://sg.hu/cikkek/it-tech/126459/zsarolovirusok-25-millio-dollar-bevetel-ket- ev-alatt (2017. 10. 01.)

Berta Sándor: Wanna Cry – már váltságdíj nélkül kikódolhatók a fájlok, 2017. Forrás: https://sg.hu/cikkek/it-tech/125410/wanna-cry-mar-valtsagdij-fizetes-nelkul-is- kikodolhatok-a-fajlok (2017. 10. 01.)

Cisco: Zsarolóvírusok: Valóság nem mese Köztünk vannak, kifinomultak – és rafináltak Forrás: https://www.cisco.com/c/dam/global/hu_hu/solutions/security/ ransomware/pdf/ransomware-infographic_hun.pdf (2017. 10. 01.)

Gállfy Csaba: Petya: Minden, amit tudunk a támadásról, 2017. Forrás: https://www.hwsw.hu/hirek/57452/microsoft-windows-ransomware-kriptovirus-petya.html (2017. 10. 01.)

Kormányzati Eseménykezelő Központ: Az SMB sérülékenységet kihasználó PetrWarp Ramsomware kampány, 2017. Forrás: http://www.cert-hungary.hu/node/381 (2017. 10. 01.)

Kormányzati Eseménykezelő Központ: Az SMB sérülékenységet kihasználó WannaCry Ramsomware kampány, 2017. Forrás: http://www.cert-hungary.hu/node/370 (2017. 10. 01.)

Kormányzati Eseménykezelő Központ: Közlemény a PetrWarp zsarolóvírusról, 2017. Forrás: http://www.cert-hungary.hu/node/382 (2017. 10. 01.)

Kövesdi Péter: A drognál is nagyobb üzlet - A Nemzeti Kibervédelmi Intézetben beszélgettünk a kibertámadásokról, 2016. Forrás: https://www.vasarnapihirek.hu/fokusz/ a_drognal_is_nagyobb_uzlet (2017. 09.01)

Andrew Liptak: The WannaCry ransomware attack has spread to 150 countries,

2017. Forrás: https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries (2017. 10. 01) PC World: Vírusos az uTorrent, PC World 2016. Forrás: https://pcworld.hu/szoftver/virusos-a-%C2%B5torrent-176272.html (2017. 10. 01)

Pintér Mónika: Egy hetünk maradt visszaszerezni az adatainkat, 2017. Forrás: http://24.hu/tech/2017/05/13/egy-hetunk-maradt-visszaszerezni-az-adatainkat/ (2017. 10. 01.)

Origo: Frissítette a Javát? Hiba volt, 2017. Forrás: http://www.uzletresz.hu/penzugy/20170927-nem-kompatibilis-a-java-a-nav-nyomtatvanykitoltojevel.html (2017. 10. 01)

Wikipedia: WannaCry Forrás: https://hu.wikipedia.org/wiki/WannaCry (2017.10.01.)
Wikipedia: WannaCry ransomware attack Forrás: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (2017.10.01.)