Déri Attila

Informatikai eszközeink sebezhetősége, támadása, védelme

1. Bevezetés

A számítógépes eszközeink ellen irányuló támadások napjaink része. Ezek a támadások érinthetnek állami és magáncégeket, bankokat és otthoni felhasználókat egyaránt. A támadásokat és azok hatásait meg lehet közelíteni jogi, információ-technológiai, szociológiai stb. irányból. Én az információ-technológiai irányt választottam. A támadások módjai közül mutatok be néhányat a teljesség igénye nélkül.

Rövid történeti áttekintés után betekintést nyújtok néhány érdekes támadásba. Részletesen kifejtem azokat a támadási formákat, melyek az átlagos felhasználót érintheti. A támadások több formáját is bemutatom, de a támadási lehetőségek nagy száma miatt nem törekedhettem a teljességre. Röviden szólok az okos eszközök sérülékenységéről. A támadások elleni lehetséges védekezésekről is írok, majd legvégül a szakemberképzést mutatom be. A pályázati anyagomat több, személyes példával is színesítem.

Mielőtt rátérnék a részletes leírásra, néhány fogalmat szeretnék tisztázni. A legtöbb helyen kártékony, károkozó programnak hívom a károkozásra, az adatok megszerzésére, számítógépbe történő behatolásra írt programokat, vírusokat, trójaiakat, spam-eket, exploitokat[1], stb. Azokat az embereket hackereknek hívom, akik ezeket a programokat írják, károkozásra, adatok megszerzésére, bűnös célból történő behatolásra használják. Ez a fogalom kicsit bővebb a hétköznapi szóhasználatnál, mert ott általában csak a számítógépekbe

[1] 1.Vírus: önmagát másolni tudó károkozó program, trójai: olyan károkozó program, mely „jóindulatú programnak álcázza magát, a fogadók által nem kért elektronikus levél, exploit: olyan program, mely alkalmas egy szoftver vagy egy hardver biztonsági résének kihasználására.

behatoló embereket nevezik hackereknek. A hackerek céljaik érdekében gyakran több módszert is ötvöznek. Az internet alatt a számítógépek közötti tcp/ip protokollt használó összeköttetéseket és az összekötött informatikai eszközöket (szerver, router, stb.) értem. A word wide web (www, világháló) alatt az interneten hyperlinkekkel összekötött dokumentumok összeségét értem.

Több olyan dologról írok, amit az informatikabiztonsági szakemberek úgy gondolnak, hogy a többi informatikus is ismer. Sajnos a tapasztalatok azt mutatják, hogy az informatikusok között a biztonsági ismeretek szintje messze nem egyenletes. Vannak, akik kiválóan képzettek, míg mások egyáltalán nem. A BSC képzés első évfolyamán oktatott informatikai és matematikai ismereteket tudottnak feltételezem, azok magyarázatára, bizonyítására külön nem térek ki. Szintén ismertnek gondolom az alapvető titkosítási eljárások ismeretét is.

2. Rövid történeti áttekintés

Az elmúlt 15-20 évben az informatikai eszközök mindennapjaink részévé váltak. Ma már szinte minden háztartásban megtalálható a számítógép és az internet. Egyre több eszközünk csatlakozik az internetre, válik „okos” eszközzé. Az informatika fejlődésével megjelentek azok a programok, melyeket károkozásra, számítógépek működésének megakadályozására fejlesztettek ki. Ezek a programok kezdetben nem önálló programként léteztek, hanem más programokhoz kapcsolódtak, illetve a rendszerlemezek boot szektoraiba másolódtak be. A hordozó program indítása, illetve rendszerindítás után a számítógép memóriájában maradtak és képesek voltak önmagukat másolni másik programokhoz, illetve másik rendszerlemezt megfertőzni. Ezeknek a programoknak az írása kezdetben ártatlan játéknak tűnt. Azonban az idő múlásával, a technika fejlődésével a bűnözők is felismerték ezekben a programokban rejlő lehetőségeket.

A 90-es évek elején Magyarországon is megjelentek azok a hardvereszközök, melyekkel csalást követtek el. Itt említeném meg a végtelenített telefonkártyákkal elkövetett csalásokat, valamint a 450 MHz-en működő mobiltelefonok sérülékenységét. A mobiltelefonokban lévő epromot át lehetett programozni oly módon, hogy a hívásokat ne a mobiltelefon használójának, hanem másnak számlázza a szolgáltató.

Az internet fejlődésének, elterjedésének nagy lökést adott a word wide web (www, web) megalkotása. A web tette lehetővé, hogy a hétköznapi ember is könnyen hozzáférjen a szervereken tárolt adatokhoz. Kijelenthetjük, hogy a web-technológia vitte be a háztartásokba az internetet. Az internet kapcsolat kiépítéséhez először telefonhálózatra kapcsolt modemet használtak. Később a kapcsolt vonalat használó modemet felváltotta az állandó on-line kapcsolat, adsl illetve optikai összeköttetés. Az internetes kapcsolat új sérülékenységet is jelentett, amit a vírusírók ki is használtak. Az állandóan on-line kapcsolatban lévő számítógépek folyamatosan a fertőzések kereszttüzében állnak. Ezt a vírusírtó programokat készítő cégek is felismerték és állandóan futó víruskereső programokat készítenek. A víruskereső programok a vírusokkal egyidejűleg jelentek meg. A működésük során a kártékony programok kódjainak mintáit keresik a számítógép adathordozóin lévő állományokban. A víruskereső programok megtévesztésére a hackerek a vírusok több változatát hozták létre oly módon, hogy kis mértékben megváltoztatták a vírus kódját. A kód átírása a vírus működésében nem okozott jelentős változást, de a víruskeresők dolgát megnehezítette. A vírusok kódjainak megváltoztatásával kialakultak a polimorfikus víruscsaládok.

Az internet elterjedésével megjelentek azok az informatikai eszközök is, melyeket az internetre kapcsolva az életünket tovább könnyítik (pl.: programozható, távvezérelhető termosztát stb.). Sajnos ezzel megteremtettük ezeknek az eszközöknek a támadhatóságát is.

Az utóbbi években a támadások jelentőségét a kormányok is felismerték. Megjelentek azok a támadások, melyek mögött kormányokat, vagy kormányzati megrendeléseket lehet sejteni. A védekezésre történő felkészülés fontossága is megnőtt, ezért is tartanak évente NATO kibervédelmi gyakorlatot. A legutóbbi tavaly Észtországban volt (http://www.honvedelem.hu/cikk/54201_nato_kibervedelmi_gyakorlat_esztorszagban).

3. Néhány támadás bemutatása

A mai napig bekövetkezett támadások széles spektrumot fognak át. A pályázati anyagomban csak néhánnyal foglalkozok részletesen, de a támadások más dimenzióit is szeretném érzékeltetni a teljesség igénye nélkül:

Elsőként a túlterheléses támadásokról, más néven Dos/Ddos támadásokról írok. Ezek a támadások több lépcsőben zajlanak. A hackerek első lépésben általában vírussal vagy trójai programmal fertőznek meg számítógépeket. A vírus rejtett támadóprogramot telepít, ezeket a fertőzött számítógépeket hívják zombiknak. A fertőzött számítógépek a víruskészítő utasítására egyidejűleg az interneten küldött adatcsomagokkal bombázzák az utasításban meghatározott számítógépet, szervert. A támadás során a támadó gépek egyenként kis mennyiségű adattal dolgoznak, viszont mivel egy ilyen támadás során sok támadó gép lehet, ezért a megtámadott gép próbálja feldolgozni az interneten kapott nagy mennyiségű adatot, ezért működése akadozhat, vagy le is állhat.

A túlterheléses támadás jellegéből adódik, hogy sok, akár a háztartásokban lévő számítógépeket fertőznek meg és alakítanak zombi gépekké. Az ilyen gépekből alakított hálózatot nevezzük botnet hálózatnak. A támadás célpontja egy kiemelt jelentőségű gép, sok esetben szerver.

Az internet topológiájából adódik, hogy a routerek kapacitásának eloszlása hatványfüggvényhez[2] hasonló (Dr. Barabási Albert László Behálózva c. előadása, Szeged Ifjúsági Ház 2016. 10. 04.). Abban az esetben, ha valamilyen – esetleg túlterheléses – támadással sikerül a legnagyobb forgalmú routerek működését gátolni, akkor az internet megbénulhat. Az internet routereinek kapacitását nem ismerem, ezért nem tudom, hogy a legnagyobb kapacitású routerek közül hányat kell működésképtelenné tenni, hogy a többi router kapacitása elégtelen legyen az adatforgalom lebonyolítására. Elméletben lehetséges egy olyan nagyméretű támadás, amely az internet fizikai széteséséhez is vezethet.

[2] Hatványfüggvény: $f(x) = x^a$ alakú függvény, ahol a konstans

Nem a túlterheléses támadás témakörébe tartozik, de itt említem meg az internet topológiájának egy másik sérülékenységét. A routerek közötti összeköttetések kapacitásának eloszlása is hatványfüggvényhez hasonló. A legnagyobb kapacitású összeköttetések megbénításával jelentős csapást lehet mérni az internetre. A többi összeköttetés túlterhelődhet és ez az internet lassulásához vezethet.

Egy másik figyelemre méltó támadás volt az iráni atomcentrifugák elleni támadás. Ez nemcsak a technikai, hanem politikai vetülete miatt is érdekes, előre vetíti a kiberháborúk lehetőségét is. Közismert, hogy a nagyhatalmakon kívül több ország is rendelkezik atomfegyverrel, illetve törekszik előállításukra. Ezek közé tartozott az Iráni Iszlám Köztársaság. Az atomfegyverben az egyik legyakrabban használt hasadó anyag az urán 235 tömegszámú izotópja. Az urán – mint minden más kémiai elem – izotópjainak kémiai tulajdonságai azonosak, ezért az izotópok eltérő tömegét használják fel azok szétválasztására. Az elkülönítés egyik módszere az atomok centrifugában történő szétválasztása. Az iráni atomprogramban használt centrifugák működésének megakadályozására készült a Stuxnet nevű vírus. Ez a vírus a Siemens SCADA nevű ipari szoftverének sebezhetőségét használta ki. A vírus a szoftver által vezérelt frekvenciaváltókat kereste. Ezekkel a frekvenciaváltókkal[3] vezérelték a centrifugák motorjait. A vírus a frekvenciaváltóknak adott utasítással a motorok forgási sebességét változtatta meg, ezzel akadályozva a dúsított urán gyártását. A vírusnak sikerült több éven keresztül észrevétlen maradnia, így hosszú időn keresztül akadályozta az urándúsítást. (http://www.origo.hu/techbazis/20101116-az-urandusitok-ellen-irtak-a-stuxnet-virust-a-symantec-szerint.html)

Szintén figyelemre méltó volt az RSA Security informatikabiztonsági cég elleni támadás. A támadás azért nagy jelentőségű, mert világszerte több millió felhasználó, számos vállalat és kormány használja az RSA SecurID tokenjét. A SecurID token egy kisméretű hardver eszköz. Az eszköz 60 másodpercenként generál egy 6 jegyű számot. Ezt a számot, mint jelszót tudjuk használni programokba történő belépéshez. Az RSA cég elleni sikeres támadás során megszerzett kódok más cégek biztonságát is veszélyeztetik. Nem tudni pontosan, hogy a támadók milyen adatot loptak az RSA-tól, de a cég lecserélte az összes SecurID tokent. A nyilvánosságra hozott adatok szerint a támadók közösségi oldalon választották ki az áldozataikat, akiknek e-maileket küldtek. Az e-mailekhez csatoltak egy Excel állományt. A

[3] Frekvenciaváltó: az iparban használatos készülék, a hálózati áramból állít elő tetszőleges frekvenciájú áramot

csatolt Excel állomány megnyitáskor az Adobe Flash program akkor még meglévő sebezhetőségét kihasználva hátsó ajtót, un. backdoort telepített a gépre. A hackerek lépésről lépésre jutottak közelebb a céljukig, végül sikerült az adatokat eltulajdonítaniuk (http://www.hwsw.hu/hirek/46444/rsa-securid-biztonsag-adobe-flash.html, http://www.hwsw.hu/hirek/46832/rsa-securid-token-lockheed-martin-biztonsag.html). A így megszerzett adatokkal a támadók több haditechnikai céghez próbáltak betörni.

4. Sérülékenységek, támadási lehetőségek

A számítógépes károkozók sokszor a számítógépre telepített programok sérülékenységeit használják ki. Ezek a sérülékenységek adódhatnak csak a kártékony program írója által ismert programhibákból, a gyártó cég által is ismert, de ki nem javított program hibából, régebbi programverziók használatából, a felhasználó gondatlanságából. Több esetben a hackerek kihasználják képzetlenségünket, jó indulatunkat. Az alábbiakban ezeket a sérülékenységeket, valamint a különböző támadásokat, támadási technikákat és az ellenük történő védekezést részletezem.

4.1 Frissítések szükségessége

A programok készítésekor előfordulnak kisebb-nagyobb hibák, amiket a tesztelés folyamán nem vesznek észre. A kártékony programok írói is igyekeznek felderíteni ezeket a hibákat, hogy ezeket kihasználva juttassák be a kódjukat az adott gépre, illetve a programjaik minél nagyobb kárt tudjanak okozni. A felderített és még nem publikált hibákat nulladik napi hibáknak, illetve ezeket a hibákat kihasználó támadást nulladik napi támadásnak is hívjuk. Sok nulladik hibát jó indulatú hackerek (etikus hackerek) fedeznek fel és közlik a program írójával.

A programok írói igyekeznek a felderített hibákat javítani, és a javított kódot eljuttatni a felhasználókhoz. A javított kódot idegen szóval pach-nek hívjuk. A pach-eket nem mindegyik felhasználó futtatja le, így nem frissül a szoftvere. Sok hacker ezt ki is használja, mert a patch-ek visszafejtéséből igyekszik megismerni azokat a sérülékenységeket, melyeket éppen az adott patch-el javítanak. Ezekre a sérülékenységekre írt támadó kóddal próbálnak kárt okozni azokon a gépeken, melyeken nem futtaták le az adott pach-t. A programok frissítése maga után vonhatja más programok frissítését, illetve újabb verziók megvásárlását is. Példaként

említeném a java futtató környezet frissítését. A java népszerű nyelv a programozók körében. Sok programot írnak ezen a nyelven. A nyelv népszerűségéből is ered, hogy a java futtató környezet sérülékenységére sokan figyelnek. A java frissítésével jelentősen csökkenteni tudjuk számítógépünk sérülékenységét. Sajnos előfordulhat, hogy a régebbi verziójú java nyelven írt program már nem fut a frissített futtató környezetben. Ilyenkor csak a program frissítése, vagy az újabb verziója a segítség. Előfordulhat, hogy át kell térni másik gyártó programjára, ami sok kellemetlenséggel (pl.: adatvesztéssel) járhat.

Az információs technika gyors fejlődése nem kíméli az operációs rendszereket sem. Az operációs rendszerek írói is újabb verziókkal igyekeznek követni a technika fejlődését, új hardvereszközök megjelenését. Megfigyelhetjük, hogy a felhasználók jelentős része nehezen cseréli le megszokott operációs rendszerét. Ennek oka lehet a megszokás, az operációs rendszer ára, valamint az, hogy sokszor az új operációs rendszer csak erősebb hardveren fut, ezért a számítógép cseréje, bővítése is szükséges. Példaként említeném meg, hogy a Windows-XP a mai napig népszerű operációs rendszer annak ellenére, hogy támogatása véget ért. Az XP-t jelenleg is sok gépen használják. Az XP felváltására is több operációs rendszert készített a Microsoft, ezek között voltak sikeresek és kevésbé sikeresek. A Microsoft az XP támogatásának, azaz a javítások kiadásának végső határidejét több alkalommal is kitolta, végül 2014. április 8-a lett a végleges határidő. A Windows-XP operációs rendszerre ezután nem lettek kiadva javítások, annak használata már nem biztonságos. Fennáll a lehetősége, hogy az újabb Windows operációs rendszerek javításait visszafejtve az XP sérülékenységére is fény derül, és erre a sérülékenységre készül támadó program. Mivel az XP-re már nem készül javítás, ezért ezek a sérülékenységek javítás nélkül maradnak. Érdekessége miatt említeném meg, hogy az XP javításokat minden hónap első keddjén az un. patch kedden jelentette meg a Microsoft.

4.2 Középre állás

Középre állás technikának nevezik azt a technikát, amikor a támadók a számítógépünk internetes adatforgalmát eltérítik a saját gépükre, és azt rögzítik. A titkosított kapcsolatok (SSL/TLS adatátviteli protokoll) sem lehetnek akadályai az ilyen támadásoknak. Több weboldal (pl.: banki oldalak) csak titkosított kapcsolatokon keresztül érhető el. A titkosított kapcsolatot több böngésző külön is jelzi, de abból is láthatjuk, hogy a weboldal címében nem http, hanem https jelölés van. Az ilyen kapcsolathoz használt titkosítási kulcs hitelesített tanúsítvánnyal van ellátva. A tanúsítvány azt jelenti, hogy az adott titkosítási kulcs biztonságos. Sajnos nem minden webszolgáltató használ hitelesített tanúsítvánnyal rendelkező

titkosítási kulcsot. Az ilyen kulccsal titkosított kapcsolat esetén a böngésző hibaüzenettel jelzi, hogy a webszerverrel a kapcsolat annak ellenére nem biztonságos, hogy az adatátvitel titkosított csatornán történik. Ennek az esetek többségében nincs is biztonsági kockázata.
Középre állás technikával lehetőség van a titkosított csatornán folyó adatforgalmat rögzíteni. Abban az esetben, ha az adatforgalom titkosított, akkor azt a középre állás technikát alkalmazó rögzítő program felismeri, a szerver oldali titkosítást feloldja, a felhasználó felé az adatokat újra titkosítja, de ez a titkosítás már nincs hitelesített tanúsítvánnyal ellátva. A felhasználó számítógépén a böngésző jelzi, hogy a titkosítás nincs ellátva hitelesített tanúsítvánnyal. Abban az esetben, ha olyan weboldalt nézünk, ami eddig hitelesített tanúsítvánnyal ellátott kulccsal volt titkosítva, és most kiírja a böngésző program, hogy a titkosítási kódnak nem hiteles a tanúsítványa, akkor érdemes ezt az oldalt megnézni másik számítógépen is, ami a szomszédban, munkahelyünkön, stb. van. Ha akkor is jelez a böngésző, hogy a tanúsítvány nem hiteles, akkor megnyugodhatunk, mert nem valószínű, hogy heckerek vannak a háttérben.

4.3 Jelszavaink megválasztása

A számítógépek sérülékenységéhez szervesen nem kapcsolódó, viszont a biztonságunk miatt fontos téma a különféle jelszavak helyes megválasztása. A szakfolyóiratok is több alkalommal foglalkoznak a számítógép operációs rendszerébe, valamint a különféle alkalmazásokba, programokba történő belépésre jogosító jelszavak helyes megválasztásával. A jelszóval védett programjainkat, alkalmazásainkat a leggyakoribb jelszavakat tartalmazó szótárral próbálják feltörni a hackerek. A leggyakoribb jelszavakról sok szótár van a világhálón. A legnagyobb szótárak több millió jelszót is tartalmaznak. A 25 leggyakoribb jelszóról az F-Secure informatikai biztonsági cég honlapján is olvashatunk (http://www.antivirushaz.hu/a-25-leggyakoribb-jelszo-es-pin-kod-az-one-kozte-van).
A téma fontosságát mutatja, hogy jelentős informatikabiztonsági cégek is belefoglalják előadásaikba a jelszavak helyes megválasztását. A HWSW informatikai portál által szervezett 2016. június 23-i rendezvényen Peter Košinár az ESET informatikabiztonsági cég képviseletében beszélt jelszavaink fontosságáról. Megemlítette, hogy sokan csak kis mértékben térnek el a leggyakoribb jelszavaktól pl.: 12345 helyett 12346-ot választanak. Természetesen ez a jelszóválasztás nem növeli meg a védelmet megbízható mértékben. Célszerű minél hosszabb jelszót kitalálni. A szakemberek jelenleg a minimum 8 karakter hosszúságú jelszót tartják biztonságosnak. Fontos, hogy legyen benne nagy és kis betű, valamint szám is, és ne kapcsolódjon hozzánk semmilyen formában. Gondolok itt

keresztnevekre, születési dátumokra stb. A jelszavak rendszeres cseréje növeli a biztonságot, mert ha a jelszavunk kitudódik, akkor is csak rövid ideig tudják illetéktelenül használni. Ha cseréljük a jelszóinkat, akkor mindig olyan jelszót találjunk ki, amire az előző jelszavakból nem jöhetnek rá. Rossz lehet például a jelszo01, jelszo02, jelszo03, … jelszavak választása. Természetesen a hosszú, bonyolult, önmagukban értelmetlen jelszavak megjegyzése nehezebb, de ezek jelentik a nagyobb biztonságot. A jelszavak megjegyzését nehezíti, hogy egyre több dolgot intézünk on-line és mindegyik rendszerhez külön jelszó ajánlott.

Itt írnék egy személyes történetről. Az említett HWSW előadás után néhány nappal az egyik mobiltelefon-szolgáltatónál kötöttem új szerződést. Az új szerződéshez 5 számból álló jelszót (pin kódot) kellett választanom. Néhány jelszót (pl.: 12345) nem lehetett választani. Az eladót megkérdeztem az 12346 jelszó választásáról. Azt mondta, hogy ezt a jelszót a rendszer már elfogadja. Az előadáson hallottak alapján arra gondoltam, hogy könnyen lehetséges nem biztonságos jelszót választani.

Az interneten lévő alkalmazások közül sokat csak úgy lehet használni, ha regisztráljuk magunkat az adott programban. Lehetnek olyan alkalmazások, melyekhez a regisztrációkor nem kell megadni jelszót. A regisztrációt követően egy alap jelszóval tudunk belépni és magában az alkalmazásban kell jelszót változtatni. Ilyen helyzet a jelszó elfelejtésekor kért új jelszó is. Abban az esetben, ha ilyen alkalmazásba regisztráltunk, illetve valami miatt új jelszót kaptunk, javaslom, hogy a lehető legrövidebb időn belül cseréljünk jelszót. A cserét akkor is végezzük el, ha az adott időszakban nem akarjuk használni az alkalmazást.

A routerek esetében a gyártás során beállítanak az admin felhasználónak egy alap jelszót, amivel be tudunk lépni, és konfigurálni tudjuk a routert. Javaslom, hogy ezt a jelszót a konfigurálás első belépésekor cseréljük le egyedi jelszóra.

A témához szervesen nem kapcsolódik, de itt említeném meg, hogy az F-Secure fenti honlapján megtalálható a leggyakoribb 25 PIN kód listája is. A honlap szerint az első 10 adja az összes PIN kód 15 %-át. Ez azt jelenti, hogy valaki 10 próbálkozással minden 7. PIN kóddal védett alkalmazást, ajtózárat, stb. fel tudja törni. A bankjegykiadó automatákat a PIN kódokkal történő próbálkozások ellen úgy védik, hogy három elrontott kód után az automata bevonja a kártyát.

4.4 Illegális behatolás a számítógépekbe

A számítógépen futó programok sérülékenységei lehetőségeket adnak arra, hogy a számítógépbe az internetkapcsolat segítségével kívülről hackerek lépjenek be. A programok

feltárt sérülékenységeiről adatbázisokat állítottak össze a világhálón. Ezek az adatbázisok az adott sérülékenységre írt támadó programot is tartalmazzák.

Rendelkezésre állnak programok, melyek fel tudják térképezni az internetre kapcsolódó számítógépeket. Akár a gépeken futó operációs rendszer gyártójáról és verziójáról is tudnak információt adni. A sérülékenységi adatbázisból keresni lehet megfelelő támadó programot az adott operációs rendszerre. Abban az esetben, ha létezik támadó program, a heckerek megpróbálhatják a belépést a számítógépre. A behatoláskor használhatják a világhálón lévő szótárakból letölthető jelszavakat is.

A hackerek rendszergazdai jog megszerzésére törekszenek, hogy átvegyék a teljes felügyeletet a megtámadott számítógép felett. Lehet, hogy ezt a jogot nem sikerül sikeres elsőre megszerezni. Ekkor további sérülékenyéget keresnek céljaik eléréséhez.

4.5 Levelekkel terjedő kártékony programok

A vírusok voltak a legrégebbi támadó programok. Sajnos napjainkban naponta születnek újabb és újabb vírusok. A víruskereső programokat készítő vállalkozások versenyt futnak a víruskészítőkkel. A vírusok gyakran az e-mailekhez kapcsolt állományokkal terjednek, illetve kihasználják az operációs rendszer még ki nem javított sérülékenységét.

A levelekkel terjedő kártékony programok sok esetben a felhasználók hiszékenységét, képzetlenségét használják ki. A levelek csatolmányaként elküldött Word dokumentumok, Excel táblák, képek, PDF állományok tartalmazhatnak kártékony kódot. Ezek a kódok önállóan is kárt okozhatnak, de sok esetben csak arra szolgálnak, hogy az interneten keresztül letöltsenek más kártékony kódokat. A kártékony kódok lehetnek zsaroló vírusok, billentyűzetnaplózó programok (keylog), hátsó ajtót (backdoor) nyitó programok, kiolvashatnak különböző adatokat (pl.: e-mail címeket) a gépről stb.

A másik gyakorta alkalmazott módszer, hogy a levélben linket küldenek és igyekeznek rávenni a levél olvasóját, hogy a linkre kattintson. A letöltődő weboldal tartalmazhat kártékony kódot. Egy példán mutatom be az ilyen károkozást. A napokban két munkatársam is megkapta az alábbi angol nyelvű levelet:

Tárgy: MICROSOFT FINAL WARNING

Levél tartalma:

MICROSOFT OUTLOOK NOTIFICATION

Your email box account needs to be verify immediately due to irregularities found in your mail box account. Failure to do this your email box account will be suspended now.

Microsoft Outlook © 2016

Copyright Inc. All rights reserved.

Első ránézésre a levél eredeti Microsoft által írt levélnek tűnik. Még megnyitás előtt érdemes megnézni a feladót, és rögtön gyanússá válik a levél, ugyanis a feladónak vietnami e-mail címe van. Az is gyanús lehet, hogy angol nyelvű a tárgya, mert a Microsoftnak van magyarországi képviselete. A levelet kinyitva azt olvashatjuk, hogy ellenőrizzük le az e-mail fiókunkat, mert szabálytalanságot találtak. Abban az esetben, ha nem ellenőrizzük le, az e-mail fiókunk felfüggesztésre kerül. A levél írója az ellenőrzéshez segítséget is nyújt, mert a levélben a verify szó egy hyperlink. Az egérmutatót rámozgatva a verify szóra, elolvastam, melyik weboldal jelenne meg a böngészőben, ha rákattintok a szóra. Azt találtam, hogy nem a Microsoft weboldalára mutat a hyperlink. További vizsgálatokat ezzel az e-maillel nem végeztem.

A feladó címéből és a levél tartalmából elképzelhetőnek tartom, hogy a levél károkozó kódot tölt le a számítógépre. Abból, hogy egyidejűleg két munkatársam is megkapta a levelet, feltételezem, hogy a károkozó kód a fertőzött számítógép levelező programjából kiolvassa a partnerek e-mail címeit, és interneten elküldi a szerverre. A szerver az így megszerzett új címekre is kiküldi a levelet.

A levél mellékleteként terjedő kártékony programok elterjedésének megfékezésére nem csak technikai lehetőségeink vannak. A járványmatematika és a hálózatkutatás eredményeit is felhasználhatjuk. Például a munkahelyeken a külső partnerekkel kapcsolatot tartó emberek jelenthetnek nagyobb veszélyt. A legtöbb e-mail kapcsolattal rendelkező emberek is veszélyt jelenthetnek, gócpontjai lehetnek egy lehetséges fertőzésnek.

4.6 Zsaroló vírus

A károkozó programok egy újabb formája a zsaroló vírus. A vírusok veszélyességét, illetve az általuk okozott károkozás súlyosságát jelzi, hogy napjaink konferenciáin több előadás is ezzel a témával foglalkozik. A Kapsersky Lab informatikabiztonsági cég jelentése alapján 2015 áprilisa és 2016 májusa között közel egymillió felhasználó vált a zsaroló vírusok áldozatává (http://www.origo.hu/techbazis/20160726-itt-keressen-megoldast-ha-zsarolovirus-aldozata-lett.html). A fertőzések számának gyarapodása mellett, a víruscsaládok száma is ugrásszerűen növekszik.

A vírusok a fertőzött számítógépeken található állományokat erős aszimmetrikus kriptográfiával titkosítják, és a program írói, illetve terjesztői pénzt kérnek az állományok visszakódolásáért. A vírus terjedési formája sokféle. A megfigyelések szerint leginkább netezéssel, e-mailek csatolmányaként (pl.: Word dokumentumban, Excel táblázatban lévő macro program tartalmazza a vírus kódját) terjed. Abban az esetben, ha fertőzött csatolmányt nyitunk meg, a vírus a merevlemezen található állományokat titkosítja erős, az esetek többségében 4096 bites RSA titkosítással. A felhasználó ekkor csak azt veszi észre, hogy a program folyamatosan írja, olvassa a gép merevlemezét. A titkosítás kiterjedhet a dokumentumokra, Excel táblákra, kép-, filmállományokra. A vírus a felhasználónak jelzi, hogy az állományai titkosítva lettek, és egy meghatározott időn belül fizessen bitcointal[4] egy jelentős összeget. A vírus szerzői lehetőséget biztosítanak néhány állomány visszakódolására, ezzel jelezve, hogy birtokukban van a titkosítás magánkulcsa. A vírus elküldi a kiválasztott állományokat a szervernek, majd onnan letölti visszakódolva. A vírus készítői vigyáznak arra, hogy az aszimmetrikus titkosítás magánkulcsa ne kerüljön ki a szerverről a pénz megfizetése előtt. Mindegyik támadáshoz más titkosítási kulcspárt használnak.

A zsaroló vírusok ellen a merevlemezen található állományok mentése biztosít megfelelő védelmet. A mentésre többféle eszközt is lehet vásárolni. A legegyszerűbb megoldás a külső merevlemez, amit USB csatlakozóval tudunk a számítógépünkhöz kapcsolni. Ennél a mentési módnál csak a mentés idejére van a gépünk összekapcsolva a külső merevlemezzel, ezért ez a legbiztonságosabb. A fontosabb állományokról ajánlott több mentést is végezni.

[4] Bitcoin: nyilt forráskódú digitális fizetőeszköz. Tranzakcióknál a felek csak a bitcoincímükkel jelennek meg, amik a tulajdonoshoz nyilvános adattal nem köthetők.

A másik mentési lehetőség a NAS (Network Attached Storage, hálózati adattároló eszköz). A NAS egy speciális hardver eszköz, melyet eredetileg hálózati adattároló eszköznek fejlesztettek ki. Napjainkban a NAS-t az adattároláson kívül használhatjuk adatbázis szervernek, média szervernek, FTP szervernek, nyomtató szervernek stb.

4.7 Billentyűleütéseket naplózó programok

A károkozó programok másik fajtája a billentyűleütéseket rögzíti és továbbítja az interneten keresztül. A vírus írói így próbálnak jelszavakat, és más fontos adatokat megszerezni. A banki rendszerek esetében a szerződés megkötésekor lehetőség van biztonsági belépésikód-szolgáltatást kérni. Ebben az esetben minden alkalommal, mikor belépünk a banki oldalra, SMS-ben kapunk egy plusz, egyszerhasználatos belépési kódot. A biztonsági kód megnehezíti az illegális belépést. Az okos mobiltelefonok terjedésével a mobilon is tudjuk a banki weboldalakat nézni, banki ügyeinket on-line intézni. A hackerek is felfigyeltek erre a fejlődésre és olyan kártékony programokat készítenek mobilokra, melyek a billentyűleütések mellett az SMS üzenetek tartalmát is elküldik az interneten. Így lehetővé válik az illegális belépés a biztonsági kóddal védett oldalakra is. A banki ügyek intézéséhez javaslom, hogy mindig másik eszközről jelentkezzünk be, mint amire a biztonsági SMS kódot kapjuk.

A károkozó programok elleni védelmet a programok frissítésein kívül víruskereső program telepítésével növelhetjük. Sokat segíthet, ha nem rendszergazdai jogokkal rendelkező felhasználóként használjuk a gépet, csak a legszükségesebb esetben jelentkezünk be rendszergazdaként.

Kritikus alkalmazások (pl.: banki oldalak, pornó oldalak stb.) felkeresésekor nagyobb figyelmet kell fordítani a biztonságra. Javaslom, hogy ilyenkor Linux operációs rendszert használjunk. A Linuxra lényegesen kevesebb támadó program készül, mint a Windowsra. A Linux operációs rendszert rá lehet másolni CD-re vagy pendrive-ra oly módon, hogy erről lehessen indítani a számítógépet (live Linux). A live Linux használata közben nem fut semmilyen vírusvédelmi program és így támadhatóvá válik a merevlemez. A live Linux használata előtt javasolt a merevlemez eltávolítása a számítógépből. Természetesen időnként a Linux lemezt is frissíteni kell.

A kritikus alkalmazások és más oldalak olvasásakor használhatunk virtuális gépet. Abban az esetben, ha virtuális gépre telepített operációs rendszert és böngészőt használunk, megvédjük

a gépünket az esetleges támadástól. Ha böngészés során mégis elszenvedünk egy támadást, akkor nem sérül a virtuális gépen kívüli környezet.

4.8 Mobiltelefonok sérülékenysége és támadásuk

A mobiltelefonok elterjedéséről, sérülékenységéről a banki adatok megszerzésekor már írtam. Most megpróbálok néhány összefüggésre, további sérülékenységre rávilágítani.

Sajnos a mobiltelefonok többségén és a táblagépeken futó Android operációs rendszer is népszerű a vírusírók között. Sok vírus készül Androidra. A vírusok a hagyományos károkozás mellett képesek kiolvasni és az interneten továbbítani a telefonunk telefonkönyvét, az SMS-eket, a tartózkodási adatainkat a cellainformációk alapján vagy a beépített GPS vevő bekapcsolásával.

Az Android operációs rendszer sérülékenységeit is kihasználják a hackerek. A Nemzeti Kibervédelmi Intézet honlapján (http://neih.gov.hu/stagefright) olvasható az Android egyik sérülékenységére írt támadás. A támadóknak elég egy speciálisan összeállított videót elküldeni MMS-ben. A támadás sikeres végrehajtásához felhasználói interakció sem szükséges. A támadással a kiválasztott telefonon távoli kódfuttatás válik lehetővé, amin keresztül képesek lehetnek átvenni az irányítást a fertőzött eszköz felett.

Manapság rendelkezésre állnak víruskereső alkalmazások, melyeket a mobiltelefonokon tudunk használni. Ezekkel az alkalmazásokkal tudjuk megvédeni mobilunkat a nem kívánatos támadástól.

Itt térek ki a 2014. évi Ethical Hacking konferencián elhangzott Kovács Zsombor „Egy kínai androidos mobil vizsgálata” című előadására (https://www.youtube.com/watch?v=UGL6Huo4ay0). Az előadás Kínában belső piacra szánt mobiltelefon teszteléséről szólt. Elhangzott, hogy a telefont nem boltban vásárolták. Bemutatták az Androidos alkalmazások elemzésének módjait, magát a telefonnak a vizsgálatát. A vizsgálat alatt a telefon adatforgalmát routeren keresztül bonyolították le, így lehetőség nyílt az adatforgalom naplózására és elemzésére. Az adatok elemzése során megállapítást nyert, hogy a telefonon lévő kártékony alkalmazások az interneten keresztül

elküldték az összes telepített alkalmazás adatait, GPS adatokat, IMSI, IMEI[5], MAC számokat, híváslistákat, SMS-eket. A leírtakból látszik, hogy az ismeretlen forrásból vásárolt mobil telefonon keresztül mennyire sebezhetőek vagyunk.

4.9 WiFi törése, lehallgatása

Napjainkban is megfigyelhető, hogy a WiFi hálózatok jelentős része kódolatlan, annak ellenére, hogy egyre több hálózaton állítanak be titkosítást. A kódolatlan WiFi hálózatra kívülről rá lehet csatlakozni és ingyen lehet használni, ami a hálózat sebességét csökkenti. Valószínűleg az ilyen jellegű, illegális belépések fordulnak elő a legtöbb esetben, hiszen a külső használónak nem kell díjat fizetni az internet használatáért. Sokan úgy gondolják, hogy az ingyenes használat megelőzése miatt kell beállítani a titkosítást a WiFi routeren. Azonban az ingyenes WiFi hálózat használata másoknak lehetőséget biztosít az adatforgalmunk lehallgatására, továbbá arra, hogy a hackerek a WiFi hálózatot használják fel bűncselekmények végrehajtására. Véleményem szerint az internet illegális használatából a tulajdonos számára jelentkező kényelmetlenség (sávszélesség csökkenése) eltörpülhet, a lehallgatásból eredő veszteség mellett.

A WiFi routeren az adatforgalom titkosítására több féle mód is beállítható. A WEP és a WPA titkosítás nem biztonságos, rövid idő alatt feltörhető. Javasolt a WPA2 titkosítás beállítása.

Évekkel ezelőtt a titkosítatlan WiFi hálózatok számának nagymértékű növekedését eredményezte, hogy a laptopok elterjedésével sok, nem informatikával foglalkozó felhasználó vásárolt otthonába WiFi routert. Ők azok beállításával nem voltak tisztában. Az informatikai boltok nagy hányada rendelkezik szerviz háttérrel és kérésre konfigurálják is a routereket. A konfigurálás ára a router árához képest azonban jelentős. Ezért megfigyelhető, hogy sok felhasználó családtagját, ismerősét kéri meg routerének beállításához, ez is oka lehet a sok titkosítatlan hálózatnak. Szerencsére az utóbbi években előtérbe került a biztonság, így a konfigurálásnál egyre jobban ügyelnek a titkosított kapcsolat beállítására is.

A WiFi eszközzel ellátott számítógép, általában laptop segítségével fel tudjuk deríteni a fogható WiFi hálózatokat. Erre több program is lehetőséget biztosít. A programok kiírják a

[5] A mobiltelefon nemzetközi szabvány szerinti azonosító számai

hálózatok adatait, köztük a titkosítás típusát. Rendelkezésre állnak olyan USB csatlakozású WiFi eszközök un. WiFi stick-ek, melyek külső antennával, vagy antenna csatlakozóval rendelkeznek. Ezekkel az eszközökkel a vételi hatótávolságot tudjuk növelni.

A felderített WiFi hálózat forgalmát több programmal is ki tudjuk fürkészni. Gyakorlatilag a nem titkosított adatforgalmazást teljes egészében fel lehet deríteni. Itt nemcsak a web használatára gondolok, hanem FTP, telnet, e-mail stb. programok (protokollok) forgalmára is. Az így szerzett adatokat, jelszavakat, e-mailek tartalmát fel lehet használni bűnös szándékkal is. Az ingyenes (free) WiFi szolgáltatással rendelkező vendéglők, szállodák, közlekedési eszközök is sok esetben kódolatlan WiFi hálózatot kínálnak. Ilyenkor az adatainkat csak úgy tudjuk védeni, ha titkosított kapcsolatot használó weboldalhoz csatlakozunk (SSL/TLS protokollt használó weboldal).

4.10 RFID sérülékenysége

Jelenleg még a nagyközönség által kevésbé ismert sérülékenység a rádiójelekkel automatikus azonosítást, adatközlést végző eszközök az un. RFID tag-ek illegális olvasása, és az így szerzett adatok felhasználása. Az RFID áramkörök megtalálhatóak hétköznapi eszközeinkben, pl. az érintéses fizetésre alkalmas bankkártyákban, az e-személyiben, útlevelekben, bolti lopásgátlókban, Londonban a közlekedési bérletekben is.

Az RFID eszközök rádiós frekvenciás adatátvitellel olvashatóak, írhatóak. Mindegyik tartalmaz speciális egy chipre integrált számítógépet. Több, különböző RFID tag-et készítenek. Az áramellátás szempontjából megkülönböztetünk aktív és passzív tag-et. A passzív tag nem tartalmaz saját áramforrást, a működéshez szükséges áramot indukcióval nyeri a külső elektromágneses mezőből. Röviden leírnám a működését: A tag-et elektromágneses mezőbe helyezve, a tag-ben lévő tekercsben áram indukálódik, a tag ekkor feléled, idegen szóval bebootol és a chip programjában lévő műveleteket elvégzi. A passzív tag-ek is lehetnek többfélék, az egyszerűbbek csak egy számsor tárolására és rádiófrekvenciás továbbítására alkalmasak, a bonyolultabbak kétirányú kommunikációra, programok futtatására is képesek.

A témához látszólag nem kapcsolódik, hogy a bűnözők a bolti lopásoknál felismerték a rendszer egyik hiányosságát. A boltokban a kijáratnál elhelyezett olvasók a termékeken lévő tag-eket olvassák. Abban az esetben, ha a tag-et a pénztárban nem olvasták le, akkor a

kijáratnál lévő olvasó riasztja a bolt személyzetét. A bűnözők ezért belülről árnyékolt táskákkal tulajdonítják el a termékeket.

Az utóbbi időben elterjedőben vannak az RFID chipet tartalmazó bankkártyák (paypass kártyák). A pár éve megjelent mini számítógépekre (pl.: Raspberry pi számítógép) épülő eszközökkel is lehetséges az ilyen bankkártyák olvasása. A mini számítógép méretéből adódóan elrejthető a felső ruházat alatt. Az elkövetők pl. zsúfolt közlekedési eszközön rejtett módon tudják a bankkártya adatokat kiolvasni. Az adatok kiolvasása után könnyen készíthető klón kártya. Ennek elkerülése érdekében lehetőségünk van a bankkártyánk árnyékolására, és így az adatok leolvasásának megakadályozására. Árnyékoló bankkártyatok a világhálón több cégtől is rendelhető. Az ilyen tok ugyanazt a technikát alkalmazza, amivel a bolti riasztók működését is kijátsszák.

Az útlevelekben is RFID chipen tárolják a személyes adatainkat elektronikusan. Ezek az adatok is kiolvashatók, és visszafejthetők (Tomcsányi Domonkos „E-útlevelek biztonsága" Ethical Hacking konferencia 2011.). Az igazolványokban, útiokmányokban tárolt adatok védelmét megnehezíti az okmányok – az információs technológia fejlődési üteméhez képest – hosszú, akár 10 éves érvényességi ideje.

4.11 Dolgok internete, azaz okos eszközeink

Az otthonainkban egyre több eszköz kapcsolódik az internethez, ezeket az eszközöket hívják okos eszközöknek is. Ezek az eszközök önállóan is kommunikálhatnak egymással, illetve másik számítógéppel, szerverrel. Az okos eszközök lehetnek tv, hűtő, kazán stb. Az okos eszközök az internetre kapcsolódása szórakoztatásunk, életünk megkönnyítésére szolgál. A tv esetében el tudjuk érni a különféle közösségi médiákat, hálózati adattároló eszközeinket (NAS), felhőben tárolt fotóinkat stb. A kazán, illetve okos otthon esetében hálózaton keresztül tudjuk a hőmérsékletet, világítást stb. szabályozni.

A hálózatra kapcsolt eszközeink informatikai kapacitása (pl.: processzor sebessége, RAM nagysága, stb.) nem bővíthető. Az eszközökre nem készül, illetve csak korlátozott ideig készül frissítés. Előfordulhat, hogy a weboldalak fejlődése is lehetetlenné teszi egyes funkciók használatát.

Szeretném a következőkben saját tapasztalatomat megosztani. 6 évvel ezelőtt cseréltem le a televíziómat egy akkor modern típusra. Az új tv-t bekötöttük az internetre és tudtuk nézni a közösségi média oldalakat. Az idő múlásával a közösségi média weboldalát fejlesztették. A tv beépített szoftverét próbáltuk frissíteni a gyártó által közzétett programokkal, de a közösségi média weboldalát továbbra sem tudjuk nézni. A tv alap funkciója továbbra is működik, így modernebb készülék vásárlásában nem gondolkozunk. A személyes példából is látszik, hogy az internet gyors fejlődését az eszközök frissítésével nem mindig tudjuk követni.

Kártevő programoknak, illetve hacker támadásoknak is ki lehetnek téve okos eszközeink. Az okos eszközök nagy része speciális hardverrel rendelkezik. Ezekre a hardverekre nem készül víruskereső program. A hardver kapacitása sem elég a védelem biztosításához szükséges programok futtatására. Megfelelő védelmet biztosítana, ha a helyi hálózatban lenne egy biztonsági szűrő. Gondolok olyan routerre, ami alkalmas víruskereső program futtatására.

Abban az esetben, ha eszközeink jelszóval védettek, akkor a jelszavakat is tartsuk karban. Az admin felhasználónak a jelszavát minden esetben cseréljük le. Ha az okos eszköz jellegéből fakadóan lehetséges, akkor hozzunk létre új felhasználót, aminek nincs admin joga. Az admin felhasználót csak a legszükségesebb esetben használjuk.

4.12 Adathalászat

Nem technikai jellegű támadások közé tartozik az adathalászat. Ennek egy tipikus esetét mutatom be:

A bűnözők e-mailt küldenek a bank nevében, különféle okra hivatkozva kérik, hogy adjuk meg az adatainkat. A levélben található link segítségével rögtön a bűnözők által elkészített, a bank oldalára megtévesztésig hasonló weboldalra mehetünk. A linkben található URL nagyon hasonló, illetve látszólag teljes mértékben megegyezik a bank weboldalának címével. Az ilyen URL-ben sok esetben található olyan karakter is, amit a böngésző, illetve a levelező program nem jelenít meg.

A bűnözők a bank weboldalával összetévesztésig hasonló oldalon bekérik banki adatainkat, számlaszámunkat, bankkártyánk számát stb. Ezek az adatok a bűnözők adatbázisába kerülnek. Az adatok felhasználásával lehetőségük van a bankszámlánk megcsapolására. Előfordul, hogy

az adatokat bekérő oldal nem használ titkosított kapcsolatot (SSL/TLS protokoll). Ilyenkor mások is láthatják adatainkat.

Sajnos az adathalász levelek sok embert tévesztettek meg. Azokat a leveleket mindig fogadjuk fenntartással, melyekben banki, vagy más védendő adatot kérnek tőlünk. A bankok soha nem kérnek e-mail-ben, interneten adatokat. Ha ilyen levelet kapunk, érdeklődjünk személyesen vagy telefonon bankunknál.

5. Védekezés

A leírtakból látszik, hogy a támadások elleni védekezés a felhasználó, rendszergazdák feladata. Az informatikabiztonság témakörében kevésbé jártas felhasználók jelentős része nincs tudatában annak, hogy támadás célpontja lehet. Nem ismerik sem a támadás, sem a védekezés módjait. Eddig sajnos nem találkoztam a lakosság informatikabiztonsági ismereteit bővítő széleskörű programmal.

A támadás lehetőségének csökkentése érdekében az alábbi lépéseket javaslom:

- Operációs rendszer és a programok megfelelő frissítése. A már nem támogatott programokról áttérés a támogatott verzióra.
- Jelszavak beállítása, a felhasználói fiókok, jogosultságok karbantartása, a nem használt felhasználói fiókok törlése. Ez nemcsak az operációs rendszer felhasználói fiókjainkra, hanem a programjainkra és az internetes accountjainkra (levelezőprogram, közösségi megosztó programok stb.) is vonatkozik. A jelszavak beállítását hajtsuk végre a routerünkön és az okos eszközeinken is.
- Megfelelő vírusvédelmi program kiválasztása. A programok között akad ingyenes és megvásárolható. A hazai szaklapok rendszeresen összehasonlítják a különböző programokat. A vírusvédelmi programok nevükkel ellentétben nemcsak a vírusokat szűrik ki internetezés, külső adathordozó (pl.: pendrive) használata során, hanem védenek az internetes támadásoktól is. Az állandó védelem mellett a programok különféle vizsgálati lehetőséget (gyors vizsgálat, teljes vizsgálat,stb.) is biztosítanak. A vizsgálatok során a merevlemezek és egyéb adathordozók teljes, illetve részleges

átvizsgálásával keresnek támadó programokat. A vizsgálatokat rendszeres időközönként le kell futtatni.

- Figyeljünk oda bejövő elektronikus leveleinkre. A levelek feladói, tárgyai támpontot adhatnak. Ismeretlentől kapott levelet fenntartással fogadjuk. A levelek mellékletét csak akkor nyissuk meg, ha biztosak vagyunk benne, hogy megbízható személy küldte. Ha a melléklet neve gyanús, megnyitás előtt inkább érdeklődjünk a feladónál.

A védelem megteremtésén túl meg kell oldani a rendszeres adatmentés technikai lehetőségét is. A mentéseket megfelelő időközönként javasolt elvégezni. A számítógép használata közben oda kell figyelni a gyanús eseményekre. Abban az esetben, ha gyanús dolgot tapasztalunk, kapcsoljuk ki a számítógépet, és forduljunk szakemberhez. Ilyen gyanús dolog lehet például a képernyő rendszeres elsötétedése.

A web használatának is vannak fontos biztonsági szabályai. A SSL/TLS protokoll használatáról már írtam. A különböző bankoknál, szolgáltatóknál, közösségi oldalakon, levelező rendszerekben lehetnek felhasználói fiókjaink, amiket a weben tudunk elérni. Abban az esetben, ha valamelyik felhasználói fiókunkban a munkánkat befejeztük, akkor mindig szabályosan lépjünk ki a felhasználói fiókunkból és utána zárjuk be a böngészőt. Egy másik számítógépről ugyanis lehetőség van a nyitott fiókot elérni, és az ott tárolt leveleinket, adatainkat elolvasni, nevünkben műveleteket végezni. Abban az esetben, ha web böngészés alatt a böngésző újra kéri a jelszavunkat, mindig nézzünk meg, hogy az adott weboldalhoz tartozik-e időkorlát és az lejárt-e. Ha nincs időkorlát, vagy nem járt le, okkal gyanakodhatunk támadásra.

6. Képzések

A tapasztalatok azt mutatják, hogy sok informatikai szakember sincs tisztában az informatikabiztonsággal, a rendszerek sérülékenységével. Azt is tapasztaljuk, hogy a támadás, károkozás bekövetkezése után sem térnek el a régi, hibás gyakorlattól.

A megfelelő védelem kulcsa a szakemberek képzettsége. A felsőoktatásban az informatikai szakokon van informatikabiztonsági tantárgy. Sajnos azonban tudok olyan egyetemről, ahol

az informatikabiztonsági kurzust csak a közelmúltban vezették be. Az egyetemek lehetőséget biztosítanak a téma iránt érdeklődő hallgatóknak a mélyebb ismeretek elsajátítására is. Itt emelném ki a Budapesti Műszaki és Gazdaságtudományi Egyetem CrySys „!SpamAndHex" nevű hacker csapatát. Elmondható, hogy ők Magyarország legeredményesebb csapata. A csapat az idén másodszorra jutott a DefCon elnevezésű konferencia hackerverseny döntőjébe, amit az amerikai Las Vegasban tartottak meg (https://www.bme.hu/hirek/20160826/Muegyetemi_hackerek_sikere_a_Capture_the_Flag_viadalon). A nemzetközi versenyek mellett a különböző hazai egyetemek is szerveznek versenyeket, ahol a hallgatók mérhetik fel tudásukat.

Érdekesség képpen a BME által szervezett tavalyi Security Challenge versenyről bemutatok egy feladatot.

A feladatban szereplő python programozási nyelven írt program generál egy 1024 bites RSA kulcspárt, ahol e=17. A program a titkos kulccsal dekódolást végez egy 1000 bites véletlenszámon. A generált véletlenszámot jelöljük a-val, az a szám dekódolásának eredményét jelöljük b-vel. Az eredeti véletlenszámot megjeleníti a program. A program ezek után ciklusban bekér egy számot a billentyűzetről. A bekért számnak különböznie kell az a számtól. Ha azonos, akkor leáll a program futása. Ha a szám eredmény megegyezik a b-vel, akkor a program gratulál és futása leáll. Egyéb esetben a program titkos kulccsal titkosítja a beírt számot és kiírja a titkosítás eredményét, majd visszatér a ciklus elejére. A ciklus tízszer fut le. A feladat az, hogy a program segítségével a számból meghatározzuk a b számot.

A feladatnak két megoldását ismertetem. Mind a két megoldás során első lépésként az n-t kell meghatározni. Indítsuk el a programot. A program kiírja a véletlenszám titkosítását, jelöljük ezt b-vel. A program a ciklusba belépve kéri az inputot. Egy tetszőleges természetes számot adjunk meg inputként. A beírt szám kettes alapú logaritmusa legyen kisebb 1024-nél. Jelöljük ezt a számot c-vel. A beírt számot a program titkos kulccsal titkosítja, és az eredményt kiírja. A titkosított számnak vegyük a 17. hatványát. A kapott szám és c szám azonos maradékosztályban vannak modulo n, azaz két szám különbsége az n többszöröse. Jelöljük a különbséget n_1-gyel. Ezután válasszunk 3 egymástól és a c számtól is különböző természetes számot, melyeknek a kettes alapú logaritmusa kisebb 1024-nél. A számokat rendre írjuk be a programba, majd az outputként kapott számokon végezzük el a leírt számolást. Az eredményt jelöljük n_2, n_3, n_4 betűkkel. Az n számot megkapjuk, ha az n_1 n_2, n_3, n_4 számoknak vesszük a legnagyobb közös osztóját.

A két megoldás ettől a lépéstől elkülönül egymástól. Az első megoldás: számoljuk ki a b számnak a multiplikatív inverzét. Az így kapott számot már beírhatjuk a programba és titkosíthatjuk. A titkosítás eredménye a feladatban keresett szám multiplikatív inverze. A másik megoldás: a b számot szorozzuk 131072-vel (2 17. hatványával). A kapott számot titkosítsuk a programmal. Abban az esetben, ha a titkosítás eredménye páros szám, akkor a kapott számnak fele a keresett szám. Abban az esetben, ha páratlan szám a titkosítás eredménye, akkor adjunk hozzá n-t és az összege osztva 2-vel megkapjuk a keresett számot.

A versenyek nagy lehetőséget adnak az informatikabiztonsági cégeknek szakemberek toborzására. A versenyek mellett az egyetemi tananyagtól elkülönülő képzések köre is egyre szélesebb. Az Óbudai Egyetem a hallgatóknak meghirdetett kurzusoktól teljesen elkülönülő, szélesebb kör által látogatható informatikabiztonsági képzést is szervez. A képzés fizetős és más egyetem hallgatói is elvégezhetik. A képzés ára messze nem olyan magas, mint az üzleti alapon szerveződőknek. Az egyetemi képzések mellett megjelentek az üzleti alapon szerveződő képzések is. Ezeket a képzéseket vállalkozások (Kürt KFT, NetAcademia Oktatóközpont stb.) szervezték és szervezik a mai napig. A képzések alatt az informatikabiztonság alapjai mellett olyan információkat is átadnak, amik a sérülékenységek felderítéséhez, etikus hacker munkakörök betöltéséhez is elegendőek. Itt emelném ki a témában rendszeresen tartott konferenciákat (pl. Budapesten évente megtartott Hacktivity konferencia), ahol az aktuális ismeretetekre is szert lehet tenni.

Az elmúlt években az informatikabiztonság egyre fontosabbá vált. Ez a törvényeinkben is megjelent. A régi bűntető törvénykönyvbe (1978. évi IV. törvény) a 1994. évi IX. törvénnyel emelték be a számítógépes csalás tényállását. Természetesen az új büntető törvénykönyvben (2012. évi C. törvény) is szerepelnek a számítógépben tárolt, feldolgozott adatok védelmét szolgáló tényállások. A cselekmények büntethetőségének törvénybe emelésével egyidőben nem született törvény a megfelelő védelem megteremtéséről. Az Országgyűlés az állami és önkormányzati szervek elektronikus információbiztonságáról csak 2013-ban hozott törvényt (2013. évi L. törvény (Ibtv.)). A szakemberek képzését a törvény 23. § szabályozza, a Nemzeti Közszolgálati Egyetemet (NKE) jelöli ki a képzés kidolgozására, valamint a képzés megszervezésére, tartására. A törvényben szereplő felhatalmazások alapján megalkotott alacsonyabb szintű jogszabályok közül kiemelném a 26/2013. (X. 21.) Közigazgatási és Igazságügyi Miniszteri rendeletet. A rendelet az Ibtv. által meghatározott vezetők képzését és az elektronikus információs rendszer biztonságáért felelős személyek képzését szabályozza. A

rendelet háromféle oktatást ír elő: képzés, továbbképzés, éves továbbképzés, melyeket az NKE tart. A képzés a legmagasabb szintű, 2 féléves. A képzésre felsőfokú végzettséggel és alapfokú angol nyelvvizsgával lehet jelentkezni. Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában résztvevő személyek és az elektronikus információs rendszer védelméért felelős vezetők részére továbbképzést szervez az NKE. Ez alacsonyabb szintű a képzésnél, időtartama 50 óra. Az NKE kötelező jelleggel éves továbbképzést tart a jogszabály által meghatározott személyek részére.

Az Ibtv. gondoskodik az állami és önkormányzati szervek információ biztonságáról. Ugyanakkor elmondható, hogy a versenyszférára nem vonatkozik törvény. Itt csak a szakemberek felkészültsége adhat megfelelő védelmet. Mindenképpen örvendetes a felsőoktatási képzés kiszélesedése ebben az irányban, valamint a versenyek és a konferenciák szervezése.

7. Összefoglalás

Az eltelt évtizedekben az informatikai eszközöket ért támadások a gyermeki csínytevésből, laboratóriumi kísérletezésből, komoly, minden felhasználó számára veszélyt jelentő cselekményekké nőték ki magukat. A kormányok is felfigyeltek a támadásokban rejlő lehetőségekre és a védekezés fontosságára. Kijelenthetjük, hogy napjainkra az internet is hadszíntéré vált.

A támadások jelentős száma és súlyossága miatt napjaink egyik fontos feladata lett az informatikai eszközeink védelme. Látható, hogy az informatikai eszközeink állandó támadásnak vannak kitéve. A támadások nagyon sokfélék lehetnek, ezekbe próbáltam bevezetni az olvasót. Számba vettem a támadások elleni védekezési lehetőségeket is.

A leírtakból kitűnik, hogy a teljes biztonság nehezen vagy egyáltalán nem érhető el. A biztonságunk megteremtése, illetve fenntartása kellemetlenségbe, időráfordításba és nem utolsó sorban pénzbe kerül. Sokunknak kényelmetlenség lehet a biztonsági szabályok betartása, amivel csökkenteni tudjuk támadhatóságunkat. Meg kell fizetni a mentésekre használt eszközeinket, víruskereső programokat, a verziófrissítésből eredő kényszerű

hardverbővítéseket. Sajnos ezek a költségek sok esetben nem megkerülhetők, viszont körültekintéssel csökkenthetők. A költségek mérlegelésekor megállapíthatjuk, hogy a hackerek az adatok ellopásával, jelszavaink megszerzésével, zsaroló vírusokkal, sokkal nagyobb kárt okozhatnak, mint amibe a biztonságunk kerül.

Megállapítható, hogy a felsőoktatásban megjelentek az informatikabiztonsági kurzusok. Az órarendben beépített képzés mellett, az érdeklődő hallgatóknak lehetőségük van az ismeretek mélyebb elsajátítására. A versenyek is jó próbatételt biztosítanak a hallgatóknak. A posztgraduális képzések is megjelentek, amivel a korábban megszerzett ismereteinket frissíteni tudjuk. Itt említeném meg a különféle konferenciákat is. Ellenben az is látható, hogy régebben a szakemberképzésben ez a terület elmaradt a szükségestől. Sok esetben a régebben végzet szakemberek az informatika más területeiben mélyedtek el, illetve nem érdeklődtek az informatikabiztonság iránt. Ez jelentős veszélyt rejthet, hiszen az általuk felügyelt rendszerek sebezhetősége így nagyobb.

A közszférát érintő törvényi szabályozás nagymértékben növeli a biztonságot azáltal, hogy többek között kötelező képzést ír elő.

Sajnos a mindennapi életben azt tapasztalom, hogy az átlagos felhasználók nincsenek tudatában a rájuk leselkedő veszélyekkel, nem ismerik a védekezés lehetőségeit. A széleskörű felvilágosítás, a könnyen elérhető képzések jelentősen csökkentenék a sebezhetőségüket.

Irodalomjegyzék:

1. A Flash sebezhetőségét használták ki az RSA támadói, Forrás: http://www.hwsw.hu/hirek/46444/rsa-securid-biztonsag-adobe-flash.html
2. A leggyakoribb jelszavak és PIN kódok, Forrás:http://www.antivirushaz.hu/a-25-leggyakoribb-jelszo-es-pin-kod-az-one-kozte-van
3. Az urándúsítók ellen írták a Stuxnet vírust a Symantec szerint, Forrás: http://www.origo.hu/techbazis/20101116-az-urandusitok-ellen-irtak-a-stuxnet-virust-a-symantec-szerint.html

4. Barabási Albert László: Behálózva, Helikon Kiadó, Budapest, 2013

5. Itt kaphat segítséget, ha zsarolóvírus áldozata lett Forrás: http://www.origo.hu/techbazis/20160726-itt-keressen-megoldast-ha-zsarolovirus-aldozata-lett.html

6. Kovács Zsombor: Egy kínai androidos mobil vizsgálata Ethical Hacking konferencia 2014., Forrás: https://www.youtube.com/watch?v=UGL6Huo4ay0

7. NATO kibervédelmi gyakorlatot Észtországban, Forrás:http://www.honvedelem.hu/cikk/54201_nato_kibervedelmi_gyakorlat_esztorszagban

8. Műegyetemi hackerek sikere a Capture the Flag viadalon, Forrás: https://www.bme.hu/hirek/20160826/Muegyetemi_hackerek_sikere_a_Capture_the_Flag_viadalon

9. Tomcsányi Domonkos: E-útlevelek biztonsága Ethical Hacking konferencia 2011 Forrás: https://www.youtube.com/watch?v=vTmY0mN3WF8

10. RSA kicseréli az összes SecuriID tokent, Forrás: http://www.hwsw.hu/hirek/46832/rsa-securid-token-lockheed-martin-biztonsag.html

11. Stagefright sérülékenység (Android), Forrás: http://neih.gov.hu/stagefright

Jogszabályok:

1. 1978 évi IV törvény a Büntető Törvénykönyvről

2. 1994. évi IX. törvény a büntető jogszabályok módosításáról

3. 2012 évi C törvény a Büntető Törvénykönyvről

4. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

5. 26/2013. (X. 21.) Közigazgatási és Igazságügyi Miniszteri rendeletet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról