Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2010. II. negyedéves jelentés

Tartalomjegyzék

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2010. évi II. negyedéves jelentését, amely ezúttal rendhagyónak mondható, hiszen az aktuális IT- és hálózatbiztonsági trendek és sérülékenységi információk mellett egy lényeges bejelentéssel kíván élni, miszerint:

> *a PTA - Nemzeti Hálózatbiztonsági Központ 2010. július 5-ével új külsővel és funkciókkal látja el a szakmai közönség számára pozicionált tech.cert-hungary.hu oldalát, amely a cert-hungary.hu oldalt kiegészítő, aktuális és naponta frissített technikai információkat nyújt a felhasználók számára.*
> *Az új technikai-szakmai oldal rendszeres böngészése – remélhetőleg – hatékonyan kiegészíti majd a Központ által negyedévente kiadott jelentésekben olvasottakat.*
>
> *A minél hatékonyabb és kényelmesebb felhasználói lehetőségek érdekében a Központ a közeljövőben még több hasznos funkciót élesít majd a szakmai-technikai oldalon.*

A jelentésben olvashatnak még a napjainkra fokozott figyelmet érdemlő kritikus infrastruktúravédelemről, ill. annak hazai és nemzetközi gyakorlatairól, továbbá a korszerű behatolás érzékelési rendszerekről és azok felépítéséről, valamint a jelentés külön fejezetben taglalja a napjainkra egyre elterjedtebb háló nélküli internetkapcsolat biztonságos és hatékony kiépítését.

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 felkészülésükben.

Budapest, 2010. június

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

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

Dr. Suba Ferenc
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
testületi elnök

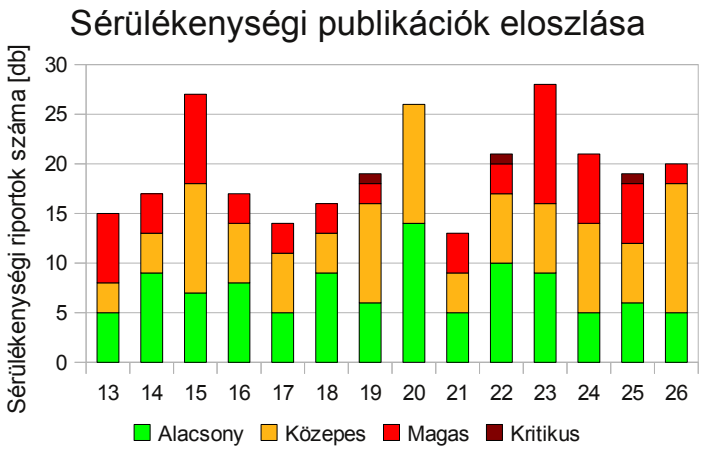
Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

Szoftver sérülékenységek

Szoftver sérülékenység minden olyan szoftver gyengeség vagy hiba, amelyet kihasználva egy rosszindulatú támadó megsértheti az informatikai rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását.

A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ** a 2010. 2. negyedéve során 273 **db szoftver-sérülékenységi információ**t publikált, amelyekből 103 db alacsony, 102 db közepes, 65 db magas és 3 db kritikus kockázati besorolású.



A sérülékenységi információk eloszlása, a 15., 20. és 23. heteken kimagasló értékeket mutat. Ennek oka a 15. és 23. heteken a Microsoft patch Tuesday, illetve a 20. héten Drupal modulok kapcsán kiadott sérülékenységi publikációk magas száma.

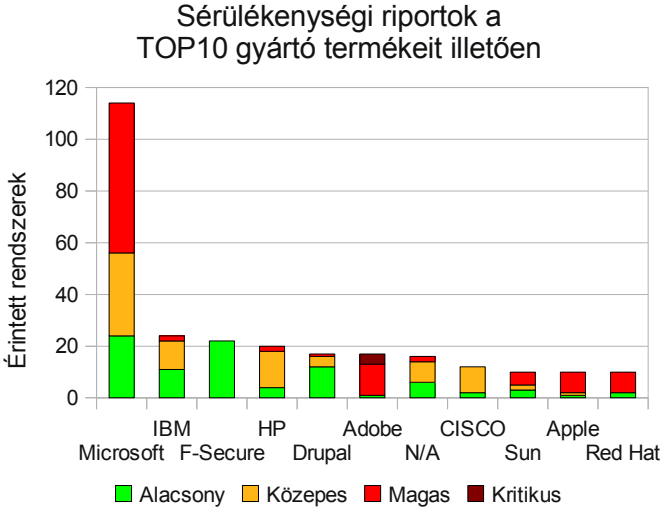
A negyedév során kiadott sérülékenységi publikációk közel egynegyede magas és/vagy kritikus kockázati besorolású. A legnagyobb veszélyt ezek jelentik, mivel ezek mind széles körben elterjedt és használt alkalmazásokat érintenek, továbbá távoli hozzáféréssel kihasználhatóak.

Ezen belül is a legnagyobb károk okozására a kritikus sérülékenységek alkalmasak, melyek kapcsán Központunk ebben a negyedévben összesen 2 ízben adott ki sérülékenységi tájékoztatót támogatott szervezetei részére, továbbá tett közzé publikációt weboldalán:

- Mozilla SeaMonkey sérülékenységek – 2010. június 23.
- Adobe termékek AVM2 "newfunction" utasítás kezelés sérülékenysége – 2010. június 05.
- Adobe Shockwave Player távoli kód futtatási és egyéb sérülékenységei – 2010. május 12.

Az előző negyedévekhez hasonlóan az egyes gyártók termékei kapcsán készült kimutatást még mindig a Microsoft (MS) vezeti.

Figyelembe véve a magyarországi IT-eszköz használat sajátosságait, miszerint a számítógéppel ellátott háztartások 87%-ban használják valamelyik Windows operációs rendszert. Az irodai alkalmazások terén is hasonló a helyzet, hiszen az azokat használó háztartások mintegy 83%-a használ Office-t.



A vállalati szektort tekintve a Microsoft, mint szoftver szállító jelenléte még erőteljesebb, hiszen a vállalatok több mint 98%-ánál alkalmazzák valamely Windows verziót (itt is kiemelten elterjedt az XP és a 2000), a Szerver oldali arány valamivel alacsonyabb, de itt is kétharmad körüli a termékeket alkalmazó vállalatok aránya. Az irodai programcsomagok között az Office verziók részesedése nagyjából 90%-os.

Gyártótól függetlenül, fontos, hogy az esetleges sérülékenységek kihasználásával bekövetkező incidensek száma és az általuk okozott károk mértéke jelentősen csökkenthető, ha a használt szoftvereket rendszeresen a kiadott aktuális frissítésekkel telepítve használjuk.

Az adatbáziskezelési területen a magyarországi, legalább 10 főt foglalkoztató vállalatok mintegy 45%-a használ valamiféle adatbáziskezelő megoldást, a nagyvállalati szektorban azonban ez az érték 90% körüli. Adatbáziskezelő rendszerek szintjén a Microsoft SQL 2005 és 2000 vannak túlsúlyban, ám nemzetgazdasági szempontból legkritikusabb nagyvállalati szférában az Oracle is – ~40%-os részesedésével – igen jelentős szereplő.

Bár a vállalati szférában, a biztonságtudatosság és a biztonsági eszközök használata jóval elterjedtebb, mint a lakossági felhasználók körében, de a sérülékenységek még mindezek ellenére is komoly kockázatok jelentek, hiszen itt is széles körben alkalmazzák a legkritikusabb sérülékenységeket hordozó szoftvereket, operációs rendszerként, a napi irodai munkához és akár a vállalat egyik legfontosabb vagyonát jelentő adatbázisok kezeléséhez is.

A vállalati biztonsági politikák nem egyenszilárdságú alkalmazása, a védelmi eszközök alkalmazásának túlsúlya az integrált, és sokszor egyszerűbb, szervezési intézkedéssel szemben, nemzetgazdasági szintű kitettséget jelent, veszélyezteti a vállalati szektor működését és adatainak bizalmasságát, integritását.

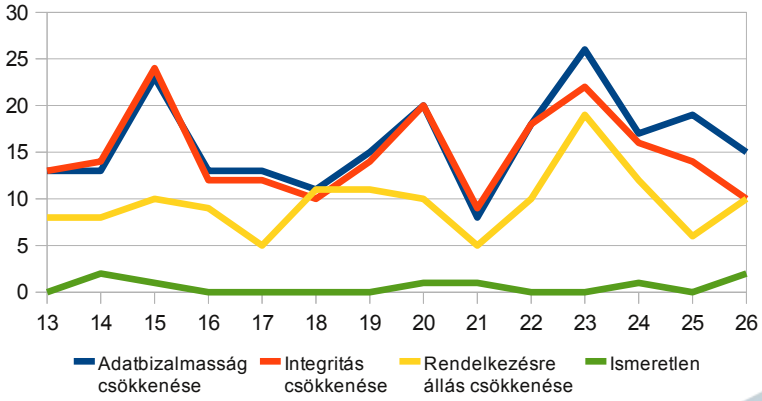
A védelmi mechanizmusok hiányában vagy azok nem megfelelő használatával, a sérülékenységeket kihasználva támadást intézni adott rendszer ellen legkönnyebben távoli kapcsolat használatával lehet, és a grafikonon is jól látszik, hogy a távoli kapcsolaton keresztül kihasználható sérülékenységek vannak jelen a legnagyobb számban.

Mindemellett aggasztó, hogy a potenciális veszélyek ellenére a lakossági felhasználók csak háromnegyede alkalmaz az informatikai biztonság alapszintjének tekinthető vírusvédelmi megoldásokat, sok esetben ezek sem megfelelően frissítettek, amely lényegesen rontja hatékonyságukat. Tűzfal a felhasználók felét védi, kémprogramok elleni (anti spyware) szoftver pedig mindössze a PC-vel rendelkező háztartások tizedében található meg.

Egy sikeresen lefolytatható támadás esélyét tovább növelik a kihasználáshoz szükséges - az interneten publikusan elérhető - előre elkészített kódok, kód-részletek.

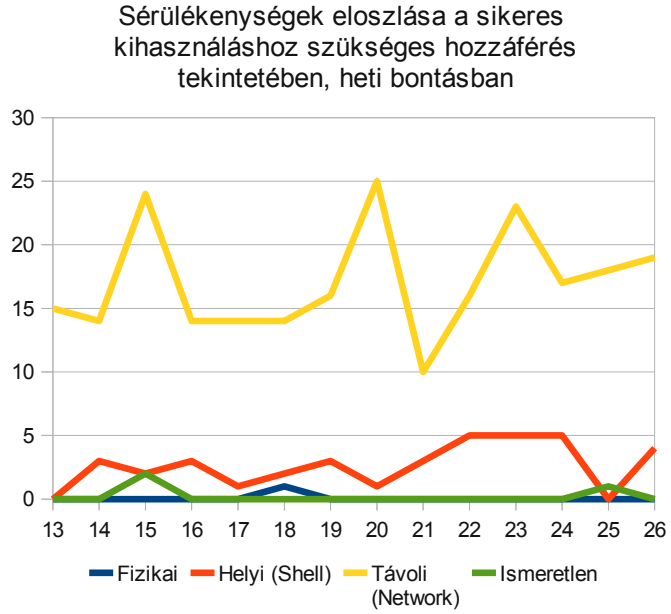
Az így beszerezhető kódok használatával, egyre kevesebb szakmai tudással rendelkező "ifjú titánok", egyre több és nagyobb volumenű támadások kivitelezésére lehetnek képesek.

Sérülékenyégek eloszlása, azok sikeres kihasználásával előidézhető, a sérülékeny rendszerre gyakorolt hatásuk tekintetében, heti bontásban



A Sagesecure kutatásai szerint a különböző biztonsági incidensekből fakadó problémák naponta átlagosan 240 percnyi hasznos munkaidő kihasználhatóságát korlátozzák, vagy teszik teljesen lehetetlenné a vállalati szférában. Ez az idő látszólagosan rövid, 10-15 perces kiesésekből áll össze és a különböző kártékony programokkal (vírus spyware, keylogger, féreg, stb.), konkrét támadásokkal kapcsolatos események mellett leginkább az ezek ellen való szakszerűtlen és átgondolatlan védekezési megoldások okoznak kiesést. Gyakoriak az üzemidőben futtatott teljes biztonsági ellenőrzések, melyek kapacitás kieséseket okozhatnak. A rosszul menedzselt sávszélesség és hálózati topológiák, a frissítések és biztonsági patchek munkaidőben való telepítése, valamint az ezekből fakadó kompatibilitási problémák megoldása is további hasznos munkaidő kieséssel járhat. Látható, hogy a hatékony és jól végrehajtott biztonsági politika mennyire fontos, hiszen **a nem kellően szervezett védekezés legalább akkora kieséseket tud okozni, mint a valódi támadások**. (A fenti 240-ből 100 percnyi kiesés teljes egészében az IT-biztonsági politika végrehajtásának tudható be.) Ide sorolhatók egyébként a túlbonyolított, túl szigorú biztonsági ellenőrzési, jogosultsági és beléptetési rutinok is, amelyek rendszerhasználati nehézségekhez vezetnek az alkalmazottak körében.

Természetesen ezen adatok alapján nem jelenthető ki, hogy 8 órás aktív munkaidővel számolva, a munkaidő fele kiesik informatikai biztonsági problémák miatt, de **a hatékonyság mindenképpen romlik, és akár a megtermelhető napi GDP 10-15 %-os csökkenésével lehet számolni** egy informatikailag nem kellőképpen felkészült szervezetnél. Nem feledkezhetünk meg az **áttételes hatásokról** sem**, főként a közhivatalok és az államigazgatási rendszerek esetében,** hiszen ez esetben **nem csak a munkavégzés elmaradása vagy lassulása a probléma, hanem az ügyfélkiszolgálás lassulása/kimaradása miatt, a nemzetgazdaság többi részéből is elvonja a munkára fordítható időt.**



A támadók helyének és a támadások fizikai vagy logikai típusának megoszlását vizsgálva jól szembetűnik **a távoli, interneten keresztül végrehajtható támadások lényeges súlyponteltolódása**, fizikai, illetve helyi támadások kockázata mindössze az esetek ~13%-ában merült fel, míg a többi kockázatot a távolról végrehajtható támadások jelentették. Ez azt jelzi, hogy továbbra sem lehet a védelmi megoldásoktól, mint pl. a tűzfalaktól eltekinteni, működésük és szabályrendszereik ellenőrzése ajánlatos minden szervezet számára, a fizikai biztonságot megvalósító intézkedések további fenntartása mellett.

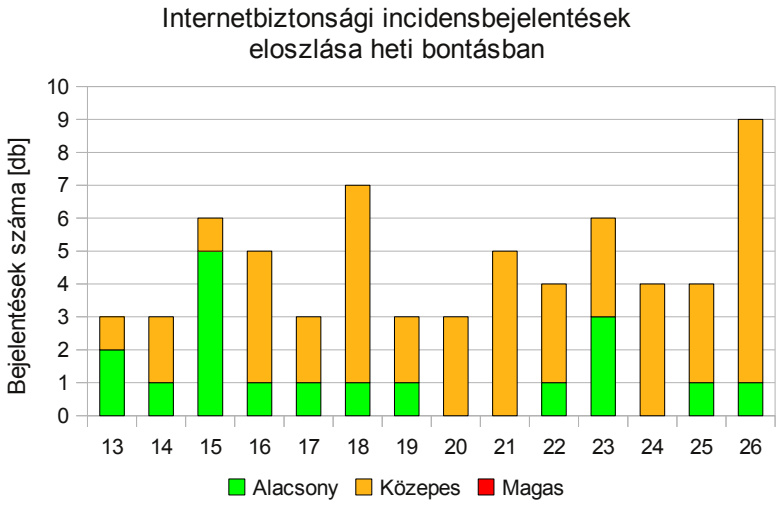
A szoftver elterjedtségi sztatisztikai adatok forrása: Információs Társadalomért Alapítvány

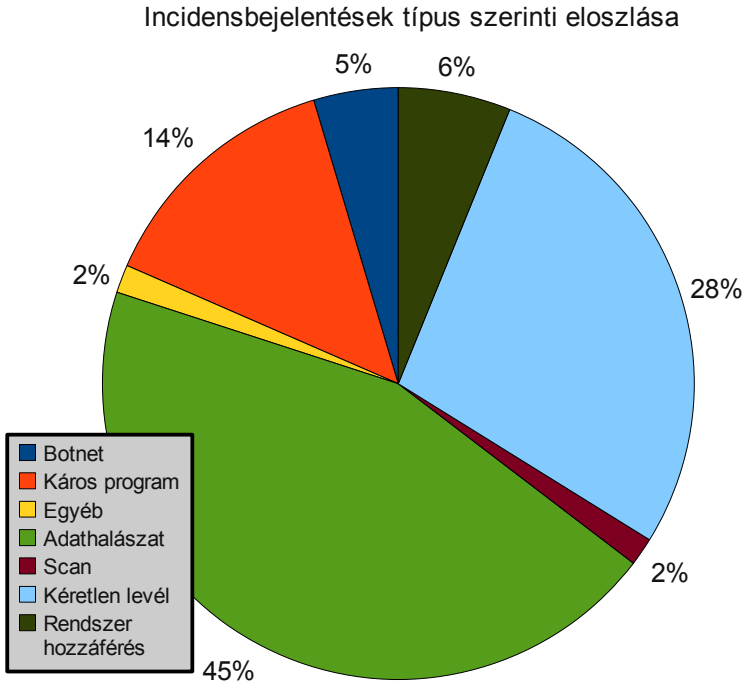
Internetbiztonsági incidensek

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. év második negyedéve során összesen **65 db incidens bejelentést** regisztrált és kezelt, ebből 18 db alacsony és 47 db közepes kockázati besorolású.

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





2010 második negyedévében legnagyobb számban adathalász tevékenység (44%), spam tevékenység (28%) és káros szoftverek terjesztése (14%) kapcsán érkeztek bejelentések, leszámítva a Shadowserver Foundation-től beérkező botnet hálózatokról szóló bejelentéseket.

A bejelentések több mint 90%-a hazai forrású káros tevékenységgel vagy tartalommal állt össze-függésben, és túlnyomó részt külföldi partnerszervezetektől érkezett. Az egyes incidensek elhárítása kapcsán összesen 20 hazai és 5 külföldi szolgáltató került bevonásra.

Hazai és nemzetközi gyakorlatok a kritikus infrastruktúrák védelme érdekében

Az NHBK, mint Nemzeti Kapcsolati Pont, ellátja a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé az internetet támadási csatornaként felhasználó beavatkozások kezelését és elhárításának koordinálását. A hatékony koordináció érdekében elengedhetetlen a jó kapcsolat a kialakított támogatott szervezeti körrel. **A rendkívüli helyzetekre való felkészülés egy módja a gyakorlatok szervezése a kritikus IKT infrastruktúrák védelmében.**

> *A nemzetközi trendnek megfelelően az NHBK is időben bekapcsolódott a gyakorlatok szervezésébe. A **223/2009. (X. 14.) számú Kormányrendelet értelmében, az NHBK** együttműködik a magyar informatikai és hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmében érintett bűnüldöző szervekkel, akadémiai és iparági szereplőkkel, ennek keretében **gyakorlatokat tart** és munkacsoportokat működtet, illetve **azokban részt vesz**.*

Több éves hagyománya van már a **bankszektor szereplőivel közösen szervezett incidenskezelési gyakorlatok**nak, melyek kettős célt szolgálnak. Egyrészről, a résztvevők közös erőfeszítéssel oldanak meg egy szimulált incidenst, másrészről az értékelést követően a résztvevők pontosítani tudják belső munkafolyamataikat, illetve együttműködéseiket.

Az **NHBK nyitott az energia ellátó szektor felé** is. A korábbi Nemzeti Fejlesztési és Gazdasági Minisztérium (NFGM) megbízásából került megszervezésre a Kritikus Infrastruktúra Védelmi (KIV) munkacsoport, amely egy alapos előkészítő munka után 2009-ben tartotta meg első kommunikációs gyakorlatát, amely egy jelentősebb üzemi kiesés hatásait vizsgálta a többi energia ellátó szolgáltatóra, illetve a korlátozott energia ellátás interdependenciáit a távközlési szolgáltatásokkal.

Az együttműködés a KIV munkacsoportban **2010-ben** is folytatódott. Ezáltal, a Kritikus Infrastruktúra Védelem (KIV) Nemzeti Programjáról elfogadott 2080/2008. (VI. 30.) kormányhatározatban foglaltak végrehajtása érdekében, **az NFGM megbízásából** a Puskás Tivadar Közalapítványon belül működő **NHBK a Nemzeti Hírközlési Hatóság együttműködésével** és támogatásával **kétnapos KIV gyakorlatot** szervezett, amelynek célja a magyarországi **távközlési és energiaszektor** kölcsönös **függőségi viszonyainak feltárása** volt egy szimulált természeti katasztrófa (földrengés) kapcsán.

A gyakorlaton **öt hírközlési szolgáltató**, az **energia szektorból** pedig **négy vállalat** biztonsági szakértői vettek részt. Megfigyelőként jelen voltak az Energia Hivatal, az NFGM és az NHH delegált képviselői is. A gyakorlatot megelőzően a résztvevők több ízben is munkacsoporti **egyeztető megbeszéléseket** folytattak, hogy rögzítsék a gyakorlat célját, kiváltó okát és annak lefolyását. A **gyakorlaton résztvevők** felkészülése (a végleges forgatókönyv megismerése után) arra irányult, hogy **a forgatókönyv lépéseinek megfelelően**, illetve azon belül, **kidolgozzák saját szimulált eljárásaikat**, **amelynek keretét** a résztvevőknél működő, hatályos szabályozások, **vészhelyzeti eljárási szabályok** képezték.

A gyakorlat infrastrukturális feltételeit és informatikai hátterét az NHBK biztosította. A gyakorlat, az elkészített forgatókönyv alapján került lebonyolításra. A gyakorlók kommunikációja kizárólag a közös (zárt) hálózaton történő elektronikus levelezés (e-mail üzenetek) útján valósult meg.

Az NHBK, Nemzeti Kapcsolati Pontként, nemzetközi kezdeményezésekben is részt vesz. Európai szinten, jelenleg szerveződik az a **pán-európai kritikus információs infrastruktúra védelmi gyakorlat**, mely az Európai Bizottság kritikus informatikai infrastruktúrák védelméről szóló 2009-es közleményének (COM(2009) 149) fejleménye. A közlemény témája Európa védelme a **nagyszabású számítógépes támadások és hálózati zavarok ellen**: a felkészültség, a védelem és az ellenálló képesség fokozása. A cselekvési terv szerint, egy egész Európára kiterjedő gyakorlatok a hálózatbiztonságot veszélyeztető nagyszabású események kezelésére A Bizottság támogatást nyújt az internet biztonságát veszélyeztető események kezelésére irányuló, egész Európára kiterjedő gyakorlatokhoz, amely egyben Európa olyan nemzetközi hálózatbiztonsági gyakorlatokban történő részvételének operatív platformjául is szolgálhat, mint például az USA „Cyber Storm" elnevezésű gyakorlata.

A cél megvalósítása érdekében az Európai Információs és Hálózatbiztonsági Ügynökség (ENISA) egy szakértői csoportot hozott létre a gyakorlat céljait, feltételeit és szerepkörök meghatározására. A szakértői – tervezői – csoportban Magyarország is részt vesz az NHBK-n keresztül. Az első gyakorlat időzítése 2010 novemberére esik.

A pán-európai gyakorlat célja a tagállamok nagyszabású számítógépes támadások és zavarok esetére vonatkozó közös felkészültségének mérése. Számos tagállam rendelkezik nemzeti szintű eljárásrenddel, illetve nemzeti gyakorlatokból eredő tapasztalattal, de EU szinten még nem került sor az eltérő eljárásrendek és szervezeti struktúrák közötti kommunikáció tesztelésére. Ezért az első gyakorlatot várhatóan több is követi majd. Első körben a tagállamok ügynökségei/hatóságai közti kommunikációs csatornák tesztelése és a bizalmon alapuló kapcsolatok kialakítása lesz a cél, illetve az országonként lefolytatandó eljárásrend megismertetése a többi tagállam résztvevőivel.

Behatolásérzékelő rendszerek evolúciója

> *„A természet arcát derűsen ragyogónak látjuk, és néha a táplálék túlzott bőségével találkozunk; de nem látjuk vagy elfelejtjük, hogy a körülöttünk gondtalanul csicsergő madarak főként rovarokon és magokon élnek, és így folyamatosan pusztítják az életet; vagy elfeledjük azt, hogy ezeket az énekeseket, meg az ő tojásaikat és fiókáikat milyen nagy mértékben pusztítják más madarak és ragadozók."*
>
> *Charles Darwin: A fajok eredete*

Számos információvédelmi technika létezik, melyek lehetőséget adnak az információs rendszerek védelmére az illetéktelen behatolás és egyéb kártékony tevékenységek ellen. Az IDS[1] egy olyan alkalmazás, mely eseményeket analizál és azok alapján próbál következtetni az információs eszközök helytelen használatára. A dokumentum a behatolás érzékelő rendszerekkel kapcsolatos alapfogalmakat, az érzékelésnél használatos módszereket, valamint a technológia fejlődését igyekszik olvasmányosan bemutatni.

1 Behatolás érzékelő rendszer (Intrusion Detection System)

Alapfogalmak

Napjainkban a számítógépes infrastruktúrák elleni támadások egyre komolyabb problémákat okoznak. A számítógépes biztonság a számítógépes rendszerek védelmét jelenti a bizalmasság, a sértetlenség és a rendelkezésre állás területein. A bizalmasság, azt takarja, hogy az információk felfedése a stratégiai elveknek megfelelően történik. A sértetlenség azt a jelentést hordozza, hogy az információ nem semmisül meg, illetve a tartalma nem módosul a rendeltetésszerű használat mellett. A rendelkezésre állás kifejezést pedig úgy értelmezzük, hogy a rendszer szolgáltatásai elérhetőek, amikor szükségesek. A számítógépes rendszerek alatt számítógépeket, számítógépes hálózatokat és az általuk kezelt információkat értjük.

A biztonsági fenyegetések számos forrását ismerjük, úgy mint természeti erők (pl.: áradás), balesetek (pl.: tűz), szolgáltatás kimaradás (pl.: áram), valamint a behatolóknak nevezett személyek.

Mit jelent a behatolás? A behatolás egy olyan biztonsági esemény, amikor valaki egy bizonyos rendszert, esetleg információt próbál elérni, mely normális esetben számára nem megengedett. Gyakorlatilag egy személy belépési próbálkozása kívülről a hálózatba, esetleg egy helyi felhasználó visszaélése a hozzáférési privilégiumával ugyanabba a kategóriába esik és behatolási kísérletként hivatkozhatunk rájuk. Gyakran a behatolás kategóriájába sorolják a DoS[2] támadásokat, melyek során egy rendszert vagy egy szolgáltatást kísérelnek meg elérhetetlenné tenni.

A behatolók információs rendszerekhez szereznek hozzáférést különböző módokon. Az egyik legelterjedtebb behatolási formát a szoftverekben lévő hibák teszik lehetővé. Tetszőleges kódok futtatásra adnak lehetőséget a véletlenül elhelyezett belépési pontok, illetve a gyenge kódolási gyakorlat, mely puffer túlcsorduláshoz vezethet. A szoftver hibák felfedezése töretlen, még a legbölcsebben használt rendszerek esetén is. Jó példa erre a Code Red féreg, mely a Microsoft IIS web szerverén lévő puffer túlcsordulási sérülékenységet használta ki.

További problémát okoz az információs rendszerek helytelen konfigurációja. Az alapértelmezett fiókok és jelszavak használata, esetleg a könnyen kitalálható jelszavak számos rendszert tesznek elérhetővé a támadók számára. A „brute force”[3] és a „password guessing”[4] a támadások eltérő formái. Míg a „brute force” támadásoknál az összes lehetséges jelszó kipróbálásával igyekeznek a helyes jelszót kitalálni, addig a „password guessing” során valamilyen megfontolás alapján csak a valószínűnek tartott jelszavak próbálgatása történik. A jelszavak kitalálását nagy mértékben elősegítheti az alapértelmezett fiókok használata.

Behatolásérzékelő rendszerek felépítése

Látszólagosan az összes behatolásérzékelő rendszer azonos struktúrával rendelkezik. Létezik egy szenzor, mely egy vagy több adatforrást monitoroz és bizonyos érzékelő algoritmus(oka)t használ, illetve nulla vagy több reakciót hajt végre meghatározott események észlelésekor. Továbbá létezik egy vezérlő rendszer, mely lehetőséget nyújt a biztonsági adminisztrátoroknak, hogy megfigyeljék, analizálják és konfigurálják a behatolási adatokat. Ezek a komponensek nem feltétlenül azonos számítógépen futnak és a rendszerek nem szükségszerűen tartalmazzák az összes fenti összetevőt.

2 Szolgáltatás megtagadás (Denial of Service)
3 Nyers erő
4 Jelszó találgatás

Mindamellett a legtöbb jelenlegi IDS ezt a modellt alkalmazza.

Ősi behatolásérzékelési technika – Egyszerű mintaillesztés

A legelső behatolás érzékelő rendszerek az operációs rendszerek naplófájljait használták adatforrásként és a kritikus szervereken futottak, esetleg azokon a rendszereken, ahol ezeket a naplófájlokat tárolták. Ezek a rendszerek egyszerű mintaillesztést hajtottak végre a beérkező naplófájlokon. A minták általában ASCII[5] karakterláncok voltak és ezen minták táblázata reprezentálta azokat a jellemvonásokat, melyek a behatolók ismert módszereire voltak jellemzőek. A naplófájlokat gyakran archiválták és az analízis csak egy későbbi időpontban történt meg. Természetesen ez korlátozta az IDS reagálási képességeit, ugyanakkor egy alaposabb logelemzést tett lehetővé.

Az alapmegközelítést gyorsan átültették a hálózati oldalra. Az első hálózat alapú behatolásérzékelő rendszerek (NIDS[6]) a hálózaton áthaladó csomagokat hasonlították össze az ismert támadásokra jellemző karakterláncok listájával. A minták ASCII karakterláncokat jelentettek és minden egyes láncot bájtról-bájtra vetettek össze mindazon forgalommal, mely a szenzor által látható volt.

Ezen metódusok implementálása viszonylag egyszerű volt és a hálózati adminisztrátorok által végzett manuális feladatok gyors automatizálását jelentette. Sajnálatos módon a minták számának emelése vagy az adatok mennyiségének növekedése exponenciális teljesítménybővítést igényelt a feldolgozás során. További hátrányt jelentett, hogy az algoritmusok még kevésbé voltak csiszoltak és gyakran generáltak riasztást olyan esetekben is, amikor valójában nem merült fel probléma. Az ilyen riasztások „false positive”-ként kerültek a köztudatba.

Az első multi-cellás organizmus – Protokoll tudatosság

A fejlődés következő szakaszában alkalmazták a protokollokkal és a csomagokkal kapcsolatos ismereteket a hálózati forgalom elemzésénél. A csomagok ismerete lehetővé tette az IDS technológia számára, hogy észlelje az ismert és rosszindulatú viselkedések bizonyos típusait. A protokollkövetés ellenőrzésével lehetőség nyílt a gyanús aktivitás jelzésére. A módszer alkalmazására jó példa a „Ping of Death”[7] észlelése. Egy 65535 bájt méretű ICMP csomag már bizonyos esetekben rendszer-összeomláshoz vezethet és mindez észlelhető a forgalom típusának vizsgálatával.

A protokoll fejlécek dekódolásával a mintaillesztés is fejlődött. Már nem csak a csomagok egyes részeinek (pl.: fejléc, adat) összehasonlítására korlátozódott a mintaillesztés. Megfigyelhető lett, hogy milyen forgalomhoz hasonlított az adatfolyam.

5 Az ASCII (angol betűszó: **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange) egy karakterkészlet és karakterkódolási szabvány, amely a latin ábécén alapul és az angol nyelvben és sok nyugat-európai nyelvben használatos betűket tartalmazza.

6 Hálózati behatolás érzékelő rendszerek (Network-based Intrusion Detection System)

7 A Ping egy számítógépes hálózati eszköz – egy szoftver – , melynek segítségével ellenőrizhető, hogy egy távoli hálózati eszköz elérhető-e az adott IP hálózaton keresztül. Továbbá mérhető vele a válaszidő. A „Ping of Death” a Pinggel való visszaélés egy formája, melynél azt használják ki, hogy a 65536 bájtnál nagyobb adatcsomagokkal pingelt számítógép összeomolhat. Igaz, IP-n keresztül küldött csomagok nem lehetnek nagyobbak 65536 bájtnál, de ha a csomagokat feldarabolják, majd a célgépen összerakják, a csomag valódi mérete puffertúlcsordulást okozhat.

Az email szolgáltatásokat célzó támadások osztályozásával, lehetővé vált a forgalom analízise és azonosítása, melynek célja a 25-ös port volt. Mivel a 25-ös port az SMTP[8] szolgáltatás jól ismert portja, lehetséges, hogy ezen port vizsgálatával az email alapú támadásokat analizáljuk. Hasonlóan a 80-as vagy a 8080-as portok segítségével ellenőrizhetők a HTTP[9] alapú támadások. Mindezen optimalizációk a teljesség kisebb áldozata mellett, jelentős fejlődéshez vezettek a teljesítményben. Ugyanis a webforgalom mindössze egy bizonyos porton történő figyelése során, elmulasztjuk a más portokon történő HTTP forgalom vizsgálatát.

Megjelent a cselekményeket számláló technika. Az alkalmankénti ping nem jelent komoly eseményt. Ugyanakkor egy másodperc alatt érkező ping csomagok ezrei már jelentőséggel bírnak. Egy aktív szolgáltatás portjának próbálgatása nem különösen érdekes. Mindamellett egy számítógépről érkező és egy másik gépet érintő nagy számú próbálgatások, több port esetében, már információgyűjtési támadás feltételezésére ad okot.

Összességében a fenti mechanizmusok szolgáltatták behatolók tevékenységének első átfogó áttekintését. Az idők során azonban a támadások egyre csiszoltabbá váltak. Példaként szolgál a fragmentálásnak elnevezett folyamat. Ebben az esetben a támadó a csomagokat kisebb darabokra tördeli. Mivel a teljes minta soha nem szerepel egyetlen csomagban, ezért az IDS a támadást nem észleli. Az áldozat rendszere ugyanakkor a csomagokat újra egyesíti és a támadás sikeresen végbemehet.

Az ilyen jellegű támadások észlelésének céljából, a fragmentálás és a csomagok újra összerakásának funkcióival bővítették a behatolásérzékelő rendszereket. Így az IDS-ek ugyanazt a forgalmat tapasztalhatták meg, mint a lehetséges áldozatok.

Felmerészkedés a szárazföldre – A hálózati munkamenetek értelmezése

Az egyszerű csomag-analízisen túl, az IDS technológiát felvértezték a munkamenet-alapú támadások kezelésével, amelyek két rendszer párbeszéde alatt észlelhetők és jellemzően nem egyetlen csomag tartalmazza a támadás jellemvonásait. Ahhoz hogy az ilyen típusú támadások hatékonyan láthatóak legyenek, szükségessé vált a „stream reassembly”, azaz a rendszerek közti adatfolyamok „újra összerakása”. A „stream reassembly” a kommunikációs kapcsolatok feldolgozásának egy újabb állapota. Ez az állapot lehetővé teszi a teljes információcserét a forrás és a cél között. Nem korlátozódva a dialógus kisebb darabjaira. A „stream reassembly”-re képes IDS-ek látják a teljes párbeszédet és képesek kiszűrni a kártékony aktivitást.

Szárnyra kapás – Teljes protokoll analízis

A korszerű hálózati behatolásérzékelő rendszerek hasznosítják az összes fent említett érzékelő és reagáló eljárásokat. A protokollok különleges ismeretének alkalmazása lehetővé teszi az ismerten rosszindulatú aktivitás észlelése mellett a rendellenes, vagy gyanús viselkedés megjelölését. Így megállíthatók az újabb, még nem publikált támadási technikák is.

A szignatúra alapú mintaillesztés örökletes hibája, hogy a támadó képes megváltoztatni a támadását

8 Az SMTP a Simple Mail Transfer Protocol rövidítése. Ez egy de facto kommunikációs protokoll az emailek Interneten történő továbbítására.

9 A HTTP (*HyperText Transfer Protocol*) egy információátviteli protokoll a világhálón. Az eredeti célja HTML lapok publikálása és fogadása volt.

olyan mértékben, hogy az ne illeszkedjen ahhoz a mintához, melyet az adott IDS elvár a támadás során. Az IDS-ek adminisztrátorai a probléma leküzdése érdekében több és több szignatúrát adtak a rendszerhez egyazon típus variációjaként. Mindezek ellenére a támadók újabb és érdekesebb módokat találnak az érzékelés elkerülésére. Mivel a teljes protokoll-analízis azonosítja az egyes elemek értelmezési módját a célponton, a támadás összes variációjának azonosítása lehetséges egyetlen mechanizmus használatával. Mindez nagyságrendekkel egyszerűsíti az érzékelést és a reakciót.

Konkrét példaként szolgálhat egy HTTP támadás, mely során bizonyos cgi-bin szkript formának megfelelő parancsok kerülnek elküldésre. A szignatúra alapú IDS-ek esetén szükség van számos mintára, melyek segítségével azonosítható a támadás. Unicode[10] útvonal, vagy fájlnév használata a karakterlánc különböző variációit vonhatja maga után a minta készítésekor. Teljes protokoll analízis nélkül különösen bonyolult lenne az ilyen támadások során elküldött kérések normalizálása a feldolgozás előtt. Valamint további nehézségeket okozna a támadás mindig azonos esetként történő azonosítása függetlenül a támadó variációitól.

A protokoll-analízis további előnye az, hogy használható a támadási metódusok megelőzésére. Az információcsere során, amikor egy bizonyos elem hosszúsága nem haladhat meg egy adott méretet, minden protokoll elleni próbálkozás anomáliaként érzékelhető. A puffer túlcsordulás egy támadási metódus, melynek lényege, hogy az adott szoftver nem megfelelően ellenőrzi a változók méreteit. Számos változó mérete általában bizonyos határokon belül mozog. Bármely mező, amely eléri ezt a határt, puffer túlcsordulási kísérlet eredményeként jelölhető meg a teljes protokoll analízis segítségével. Nincs szükség különleges szignatúrákra minden egyes puffer túlcsordulást célzó támadáshoz. A rendellenesség érzékelés ezen típusa lehetővé teszi a támadások nagy számú variációinak érzékelését platformtól függetlenül és az előzetes ismeretük nélkül.

A modern IDS-ek képesek felismerni az adott munkamenet által használt protokollokat az alkalmazott port számoktól függetlenül. Mivel a HTTP szerver működése beállítható bármely port használatára, az IDS-ek korlátozása egy bizonyos porton történő HTTP forgalom figyelése számos támadást figyelmen kívül hagyhat. Az aktívan ellenőrzött munkamenetek által használatos portok láthatóvá teszik az összes támadást.

A repülőgép – Specializált hálózati eszközök

A legtöbb üzleti IDS alkalmazás jelentős problémája volt az alap hálózati eszköztől való függőség. A munkaállomásokon található hálózati eszközöket nem hatékonyságra és nem is nagy terhelésre tervezték. A standard hálózati csatoló elégséges a mindennapi felhasználónak. Ugyanakkor egy rendszerhez, melynek feladata egy komolyan terhelt hálózat forgalmának elemzése, speciálisan erre a feladatra optimalizált eszközre van szüksége. Ráadásul az üzleti eszközök vezérlő programjai, gyakran váltak támadások célpontjaivá.

Egy nagy kapacitású IDS alkalmazás számára 100 MB-os hálózaton ajánlott egy optimalizált csatoló használata. Gigabites hálózat monitorozásához viszont már elengedhetetlen egy ilyen eszköz alkalmazása. Számos Gigabites hálózati csatoló gyártója megjegyzi, hogy a csatoló maximum 500-600 MB/s sebességű hálózati érzékelést támogat. Ugyanakkor a nem szükséges forgalom feldolgozásának kiszűrésével és a behatolás érzékelés optimalizációjával elérhető a gigabites hálózatok analízise.

10 A Unicode a különböző írásrendszerek egységes kódolását és használatát leíró nemzetközi szabvány.

IDS értékelés

A technológia fejlődésével az IDS-ek értékelése is nagyot változott. A korai IDS-ek elsődleges megkülönböztető jellemzőjük szerint, az ismert támadások száma alapján differenciálták. Amennyiben egy forgalmazó több ellenőrzést tüntetett fel a termék leírásában, feltételezhető volt, hogy alaposabb védelmet szolgáltat.

Ez a perspektíva azonban mára már nem használatos. A fejlett protokoll-analízis technikákkal, az ellenőrzések száma gyakorlatilag csökkent. A forgalom értékelésének hatékonyabb módszereivel az exploit[11]-ok kategorizálhatók kártékony viselkedésük szerint. A jelenleg használt jellemvonások az értelmezett protokollok száma, esetleg a protokollonként ismert paraméterek, elemek mennyisége.

A rugalmasság és a konfiguráció könnyedsége ugyancsak fontos szempontok. Egy IDS az alapértelmezett beállításaival nem alkalmazható minden környezetben. A hálózatok rugalmasan alakíthatók, és nagy mértékben eltérhetnek szervezetenként. Ezért szükséges a beállítások finomhangolása.

További fontos szempont a menedzsment és a riasztások rugalmas beállításának lehetősége. Egy IDS szenzor komoly értéket szolgáltat a káros tevékenységek riasztásával. Azon felhasználóknak, akik preferálják az aktív válaszokat, lehetőséget kell biztosítani a kártékony műveletek automatikus megállítására. A képzett felhasználóknak ugyancsak fontos lehet, hogy az alkalmazás támogassa a saját kódok, szkriptek és programok illesztését a rendszerhez.

A biztonsági ismeretek szolgáltatása elengedhetetlen. Még abban az esetben is, amikor az alkalmazás operátorai jól képzett biztonsági szakemberek, szükség van részletes információkra a veszélyek felméréséhez. Nem csak az adott eseményhez köthető részletek prezentálására van szükség, hanem a kapcsolódó, más források linkjeire, melyek további információkat szolgáltatnak. Mindezek mellett fontos az aktív kutatás a problémák naprakész ismeretéhez, így minden IDS fejlesztő számára lényeges egy erre a feladatra dedikált csapat fenntartása.

A teljesítmény az értékelés egy másik faktora. A kiválasztott behatolás érzékelési rendszernek képesnek kell lennie az adott hálózati szegmens monitorozására. A teljesítmény tesztelésekor különleges figyelemmel szükséges megkülönböztetni az almát az almától. A rendszert élő szegmensen igazi adatokkal kell értékelni. Továbbá az összehasonlítás során figyelembe kell venni, hogy az egyes rendszereken mekkora terheléssel jár az azonos számú események azonos körülmények közti észlelése, ellenőrzése.

Összefoglalás

A behatolásérzékelő rendszerek mögött rejlő technológia jelentősen fejlődött az idők során. Kezdetben a fárasztó és bonyolult naplófájl feldolgozási folyamatokra tervezték. Napjainkra csiszolt, valós-idejű alkalmazássá fejlődött, mely már képes a különösen összetett forgalomból is kiszűrni a káros és gyanús aktivitást. Nagy sebességű és összetett forgalom kezelésére képes és részletes bepillantást szolgáltat az aktív veszélyekkel kapcsolatos információkba.

11 Az exploit olyan forráskódban terjesztett vagy bináris program, adathalmaz vagy parancssorozat, amely alkalmas egy szoftver vagy hardver biztonsági résének, illetve hibájának kihasználására, így érve el a rendszer tervezője által nem várt viselkedést.

Referenciák

- Ajith Abraham, Crina Grosan, Yuehui Chen – Cyber Security and the *Evolution of Intrusion Detection Systems [http://cilab.ujn.edu.cn/paper/kerala.pdf]*
- Internet Security Systems – The Evolution of Intrusion Detection Technology [http://documents.iss.net/whitepapers/TheEvolutionofIntrusionDetectionTechnology.pdf]
- Guy Bruneau – The History and Evolution of Intrusion Detection [http://www.sans.org/reading_room/papers/?id=344]

A „zsebiroda” biztonsága

A távmunkában dolgozók álma, hogy bármikor, bárhol hozzáférjenek fájljaikhoz és alkalmazásaikhoz. Ennek az álomnak vége szakad, ha a biztonság kérdése rémálommá válik. Az alábbiakban áttekintjük a virtuális munkahelyek biztonságának fejlődését.

Az elmúlt tíz évben a vállalatok a munkaerő mobilitás markáns emelkedését tapasztalták. Bevett gyakorlat, hogy az alkalmazottak az otthoni személyi számítógépükről csatlakoznak VPN kapcsolaton keresztül az irodáikhoz, ezenkívül használják a reptéri hotspot-okat vagy hivatali email-eket kapnak 'okos' telefonjaikra. Sőt mi több, a szervezetek hozzáférési lehetőséget biztosítanak partnereiknek és szállítóiknak is.

Amilyen előnyös a termelékenységre és a hatékonyságra nézve az alkalmazásokhoz és erőforrásokhoz a „bármikor és bárhol” lehetővé tett hozzáférés, ugyanolyan jelentős ennek a biztonsági kockázata a vállalkozásokra nézve. A különböző távoli hozzáférési eljárásokat legelőször az üzleti életben használták. Néhány dolgozó céges laptopot vagy otthoni személyi számítógépet használ az irodához való csatlakozáshoz VPN-en keresztül; míg mások hivatali email-jeiket 'okos-telefonon' vagy egyéb kézi eszközökön kapják meg. Más csoportok vezeték nélküli hotspot-okat vagy nyilvános internet kávézókat használnak, esetleg partnereik, ügyfeleik személyi számítógépeiről jelentkeznek be.

Ezek közül a távoli végpontok közül néhány valamilyen IT csoport kezelése és felügyelete alatt áll, míg a többi teljesen megbízhatatlan és semmilyen felügyelet alá sem tartozik. Mindegyik szervezetnek komoly fejfájást okoz, hogyan terjesszék ki a biztonságos hozzáférést ezen lehetőségek és eszközök széles skálájára. Másodsorban, maguknak a vállalkozásoknak kell megvédeniük saját céges és az ügyfeleik adatait a rendszerfeltörés kockázataitól. A céges laptopok és 'okos-telefonok' túl könnyen elvesznek vagy ellopják őket, gyakran nincsenek titkosítva sem - így a tolvajok könnyű prédájává válhatnak.

Egy távoli hozzáférési munkafolyamat során olyan érzékeny információk maradhatnak a megbízhatatlan eszközökön, mint például jelszavak, bejelentkezési tanúsítványok, titkos fájlok. Ezzel lehetővé válik, hogy a következő felhasználó is elérje ezeket. Természetesen állandóan fennáll a káros szoftverek, kémprogramok és bármilyen támadás veszélye, mind az internetről, mind a nem biztonságos személyi számítógépekről.

Végül, de nem utolsó sorban, a mobil munkavégzéshez szükség van saját tulajdonú vagy gyors céges laptopokra esetleg más hordozható eszközökre. Ezek teljes költsége tartalmazza a vételárat, a szoftver licencet, a biztonsági alkalmazásokat, a frissítések- és javító csomagok kezelését, a javításokat és cserealkatrészeket, stb.

Mire van szükség a távmunkához?

A cégeknek, olyan megoldás kell, ami:

- Rugalmas és biztonságos hozzáférést biztosít az információforrásokhoz és alkalmazásokhoz, csaknem bárhonnan és bármilyen típusú számítógépről.
- Mindig megőrzi az érzékeny adatok biztonságát, az eszköz elvesztése, eltulajdonítása és az eszközbe történő jogosulatlan behatolás esetén is.
- Legyen olcsóbb a telepítése és kezelése a hagyományos laptop számítógépnél, így elősegítve a tulajdonjogok teljes költségének csökkentését (total cost of ownership - TCO).

Ideális esetben a megoldás a távmunkások számára észrevétlenül és átláthatóan működik, így az idejüket hatékonyan használhatják ki. A felhasználónak nem kell az idejét felesleges újra bejelentkezésekkel, esetleg VPN-ek használatakor újra csatlakozásokkal elvesztegetnie. Ezzel szemben, nem szabadna megfeledkeznie másoláskor vagy mentéskor a saját fájljai vagy dokumentumai titkosításáról sem. A megoldás ne legyen zavaró, a működése során ne gátolja a felhasználói tevékenységeket, miközben védelmet nyújt a külső fenyegetettségek ellen, a felhasználó saját hibái és figyelmetlensége ellen.

A követelmények felsorolásával szembesülve ijesztően bonyolultnak tűnhet a megoldás a hagyományosan használt biztonsági termékekhez képest – mint például a független VPN, vírusirtók, titkosítás, személyi tűzfal és behatolás megelőzés.

Habár, az utóbbi években bevezetett virtualizációs technológia olyan új eszközök kifejlesztéséhez vezetett, amelyek nagymértékben csökkentik a távoli hozzáférés biztonsági problémáit, egyszerűsítik a központi vezérlést és felhasználóbarát is. Ez a biztonságos munkahely fogalma.

A végpontok biztonsági követelményei

Ez az elgondolás négy éve került először ismertetésre, a továbbfejlesztett távoli hozzáférési átjárók (gateway) jellemzőjeként. Ezek az átjárók képesek voltak a felhasználók távoli számítógépei felé közvetíteni 'a végponti biztonsági követelményeket', a végpontoknak való megfelelés és a biztonságos munkahely folyamatok egyesítésével.

A végpontoknak való megfeleltetés folyamata:

- A szabályok kikényszerítése – az átjáró megvizsgálja a távoli számítógépet, mielőtt engedélyezné a hozzáférést, majd a vizsgálat eredményei alapján érvényesíti a hozzáférési szabályokat. Ez teszi lehetővé a hozzáférési jogosultságok összeegyeztetését a távoli számítógép megbízhatóságával, olyan tényezők alapján, hogy van-e rajta telepítve és futtatva biztonsági szoftver, mint például vírusellenőrző vagy valamilyen tűzfal alkalmazás, vagy a legutóbbi Windows javító csomagok telepítésre kerültek-e.

- A vendég számítógép biztonsági vizsgálata – ha a szabályok végrehajtatása befejeződött, akkor egy távoli káros szoftver ellenőrzés kerül lebonyolításra, annak érdekében, hogy felismerje a keylogger programokat (billentyűleütés naplózása), a trójai programokat és bűncselekményekre alkalmas szoftvereket.

Amennyiben a távoli számítógép megfelel a végponti követelményeknek, akkor létrejön a 'biztonságos munkahely', és a felhasználó részére a munkafolyamat egy megbízható VPN csatornán keresztül valósul meg, amelynek tartalma:

- Egy titkosított SSL VPN munkafolyamat a távoli számítógéppel, védettek a bemeneti adatok és ezek feldolgozása a csatlakozás időtartama alatt. Ez garantálja, hogy nem marad használható információ a számítógépen a munkafolyamat befejezése után.
- A távoli számítógép gyorsító tára (cache) törlődik a munkafolyamat végén és törlésre kerülnek a böngészőben az előzmények, a letöltött fájlok, a vágólap elemek stb. A titkosítással együtt ez segít megszüntetni a munkafolyamat nyomon követhetőségét.

Habár, ez a követelményeken alapuló eszköz igen hasznos, mind a biztonság érvényesítése, mind a viszonylag rugalmas távoli hozzáférés engedélyezés szempontjából, mégsem ez a legtökéletesebb megoldás. Mi történik akkor, ha a távoli számítógép nem felel meg a végponti követelmény vizsgálatnak, és a csatlakozás nem engedélyezett a vállalati hálózathoz? Ebben az esetben a felhasználó nem fér hozzá a szükséges adatokhoz vagy alkalmazásokhoz, ami megakadályozza őt a munkavégzésben – hacsak, nem sikerül egy másik számítógépet találnia, ami megfelel a követelményeknek.

A másik probléma az, ha a távoli munkafolyamat során csak VPN hozzáférésen keresztül lehet egyes engedélyezett alkalmazásokhoz hozzáférni. Ez ugyanis nem teszi lehetővé, hogy a felhasználó hozzáférjen ezeknek a számítógépeknek a desktop-jához, úgy mintha az irodai számítógépe előtt ülne.

Online és offline biztonság

Mire van szükség ahhoz, hogy a követelményeken alapuló eszközt kibővítsék úgy, hogy a felhasználó biztonságos hozzáférését engedélyezze a desktop-okhoz és a vállalati hálózatokhoz bármilyen számítógépről, attól függetlenül, hogy az mennyire biztonságos, milyen káros szoftvert vagy más fertőzést hordoz.

Továbbá, ha a felhasználó nem tud létrehozni egy VPN munkafolyamatot az általa használt távoli számítógépről, mert a csatlakozási követelményeknek nem felel meg, akkor miért ne lehetne engedélyezni a biztonságos offline hozzáférést a desktop-okhoz vagy az adatokhoz? Amennyiben ez a biztonságos munkahely könnyen hordozhatóvá tehető, valamint teljes mértékben felügyelt, állandóan be van kapcsolva, és bizonyítottan titkosított, akkor ez a megoldás sokkal jobb lenne.

Egy biztonságos számítógép a zsebben

Még több évbe telik, míg a felhasználóknak egy 'flash drive számítógépük' lehet. A fő ok az, hogy egy multi-gigabit USB mini meghajtóhoz könnyen hozzá lehet jutni. Például az IT magazinok rendszeresen leírják, hogyan hozzunk létre boot-olható flash meghajtókat, melyek tartalmazzák

kedvenc alkalmazásainkat és adatainkat, így akár zsebben is magunkkal vihetjük az egész számítógépünket.

A hagyományos flash meghajtók nem támogatják a távoli hozzáférést és a biztonsági alkalmazásokat, mint a vírusvédelmi megoldások vagy mint a titkosítási módszerek, valamint a központi felügyeletet sem. Habár, már ma is elérhetőek a biztonságos flash meghajtók, automatizált hardver titkosítással. Minden meghajtóra írt fájlra elrendelik a hozzáférés ellenőrzést, amit egy erős titkosítással és jelszóval védett elkülönített területen tárolnak. A meghajtó automatikusan zárolásra kerül, ha előre meghatározott számú helytelen jelszó-megadási kísérlet történik, így biztosítva a tárolt adatokat elvesztés vagy lopás esetén.

Ezeknek a biztonságos meghajtóknak a központi felügyeletét IT vállalkozói csoportok támogatják. Ez azt jelenti, hogy a meghajtó használatot folyamatosan felügyelik, a felírt fájlok rekordjaitól az egész meghajtóig, így elvesztés vagy lopás esetén a felhasználókat könnyebb ellátni egy új meghajtóval. Néhány meghajtó támogatja a távoli megszüntetést, ami használhatatlanná teszi ezeket a meghajtókat, amennyiben azok rossz helyre kerülnek vagy ellopják őket.

Az informatika és a számítástechnikai eszközök fejlődésével újabb és újabb módszerek jelennek meg, amelyekkel növelhető egy vállalat informatikai biztonsága, illetve, amelyeknek segítségével a vállalat alkalmazottjai a munkahelyükről és távolról (például otthonról) is biztonságos csatornán keresztül férjenek hozzá adataikhoz és alkalmazásaikhoz. Összességében az IT és a vállalati vezetőkön múlnak azok a döntések, amelyek eredményeképpen valamelyik fentebb említett megoldás bevezethetővé válik. Nyilván ez a vállalat 'beállítottságától' nagymértékben függ, sőt ezeknek a döntéseknek az anyagi vonzata is mérvadó.

Forrás: http://www.net-security.org/dl/insecure/INSECURE-Mag-26.pdf

A VirusBuster Kft. összefoglalója 2010 második negyedévének IT biztonsági trendjeiről

Mi történt a második negyedévben az informatikai biztonság területén? Beszámolónkban trend értékű híreket, adatokat igyekszünk sorra venni, majd a VirusBuster Kft. víruslaboratóriumának észlelései alapján áttekintést nyújtunk a 2010. április-június időszak leggyakoribb számítógépes károkozóiról, illetve azok legjelentősebb webes forrásairól.

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

Biztonságon nem spórolunk

Vannak országok, térségek, amelyeket erősebben sújtott a világgazdasági válság, vannak, amelyeket kevésbé. Úgy tűnik, egy dologban azonban mindenhol egyetértenek a cégek, szervezetek vezetői: a biztonságot minden körülmények között fenn kell tartani - nehéz időkben pedig különösen.

Legalábbis erre következtethetünk a piackutatók jelentéseiből. A Canalys a vállalati biztonsági világpiacot felmérve, a Deloitte a pénzintézetek IT-biztonsági költségvetését tanulmányozva jutott pozitív eredményre.

Van keret, a cégek frissítik rendszereiket, így a Canalys a vállalati biztonsági piacon idén nemzetközi viszonylatban 13,8 százalékos növekedésre számít. Jól jelzi a visszatérő optimizmust, hogy a szektor 2010 első negyedévi forgalma 15,2 százalékkal haladta meg a tavalyi év hasonló időszakáét. A Canalys úgy becsüli: az esztendő végére a piac eléri a 15 milliárd dolláros volument.

Ennek 33,6 százaléka - mintegy 5 milliárd dollár - realizálódik várhatóan Európában. Az oroszlánrész - 46,4 százalék, azaz közel 7 milliárd dollár - Észak-Amerikának jut. A Canalys elemzői szerint a 2010-es növekedés jó része az infrastruktúra biztonsági eszközök értékesítéséből származik majd - ezek teszik ki a szektor végfelhasználói vásárlásainak 48,7 százalékát.

Folytatódik a szegmens növekedése 2011-ben is. Jövőre a Canalys 9,2 százalékos bővülést, 16,3 milliárd dolláros forgalmat jósol.

Hasonló képet fest a Deloitte tanulmánya is, amely megállapítja: a pénzintézetek IT-biztonsági költségvetése általában legalább a korábbi szinten maradt, sőt sok esetben pedig nőtt.

A neves tanácsadó társaság évről-évre felméri: hogyan alakul a világ pénzintézeteinek biztonsági költségvetése, melyek a terület fő prioritásai. Az idei, sorrendben hetedik tanulmány szerint a megkérdezettek 56 százaléka költ többet 2010-ben IT-biztonságra, mint tavaly. 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 tervezi, hogy a következő 12 hónapban 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. Ez az első esztendő, amikor a törvényeknek és hatósági szabályozásnak való megfelelés felkerült a prioritások ötös toplistájára.

Adatainkért mindent megtesznek?

Miközben a cégek úgy érzik: kellően védik ügyfeleik adatait, kívülről nézve más a kép. Az Accenture és a Ponemon Intézet közös kutatásában a megkérdezett szervezetek háromnegyede nyilatkozott úgy, hogy megfelelően óvják az érzékeny, illetve személyi információt. Mégis, több mint felük beismerte: az elmúlt két év folyamán vesztett el érzékeny adatokat. A felmérés, mely 19 országra terjedt ki, 5.500 cégvezető és 15.500 felnőtt fogyasztó véleményét összegzi.

Mint kiderült: a szervezetek adatvédelmi szándékai és a valóság között jókora szakadék tátong. Valójában az érzékeny személyi adatok - név, cím, születési idő, faji hovatartozás, személyi azonosító számok, orvosi leletek - egyáltalán nincsenek akkora biztonságban, mint azt maguk az őket kezelő cégek gondolják.

Néhány érdekes szám a tanulmányból:

- A cégek 58 százalékánál számoltak be legalább egy adatbiztonsági incidensről az elmúlt két évben, mégis 73 százalékuk szerint szervezetük megfelelő intézkedésekkel és szabályozással védi az általa kezelt személyes adatokat.
- A céges válaszadók közel fele nyilatkozott úgy, hogy fontos vagy nagyon fontos:
  - az érzékeny személyi információk gyűjtésének és kiadásának korlátozása (47, illetve 46 százalék);
  - a fogyasztói személyiségi jogok védelme (47 százalék);
  - annak megakadályozása, hogy személyi adatokat adjanak át olyan országnak, ahol nem kielégítő az adatvédelem jogi szabályozása (47 százalék);
  - a fogyasztók ellen irányuló számítógépes bűnözés megakadályozása (48 százalék);
  - az adatlopás és adatvesztés megakadályozása (47 százalék).
- Az adatbiztonsági incidenseket leggyakrabban üzleti vagy rendszerhiba, továbbá emberi mulasztás vagy tévedés okozta (57, illetve 48 százalék); csak az incidensek 18 százalékában történt hackertámadás.
- A fogyasztók 70 százaléka tartotta fontosnak vagy nagyon fontosnak személyiségi jogait és személyi adatait, ugyanakkor 42 százalékuk úgy vélte: a szervezetek nem védik eléggé a rendelkezésükre bocsátott ilyen jellegű információt.
- Minden második fogyasztó (53 százalék) úgy vélte: joga van ellenőrizni, hogyan használják fel a vele kapcsolatos személyes információt. Ugyanilyen arányban voltak azok, akik arra is jogot formáltak, hogy hozzáférhessenek a szervezetek által gyűjtött és felhasznált adatokhoz, s szükség esetén felülvizsgálhassák azokat.

- Arra a kérdésre: kinek az elsődleges felelőssége a megfelelő információvédelem biztosítása, a válaszadók 4 százaléka a kormányt, 21 százaléka a cégeket, 19 százaléka az érintett személyeket jelölte meg, 20 százalék pedig úgy vélte: közös erőfeszítésre van szükség.

Bizony, az elővigyázatosság mind a szolgáltatók, mind az ügyfelek oldalán nagyon fontos - intette a cégeket a Verisign, miután kutatói megállapították: egyre könnyebb és olcsóbb egy-egy online támadásra botnetet szerezni.

Már óránként 7 euró körüli összegért is lehet botnetet bérelni, s az átlagos napidíj valamivel 53 euró alatt van - derítették ki a Verisign iDefense részlegének szakemberei. Márpedig ha a hackertámadásra alkalmas infrastruktúra ilyen könnyen és olcsón, szolgáltatásként hozzáférhető, akkor arra is mind nagyobb az esély, hogy egy cég site-ja ilyen támadás célkeresztjébe kerüljön - figyelmeztetnek a kutatók.

A Verisign három fórumon 25 botnet-üzemeltető "kampányát" követte. A bűnözők nem egy esetben hagyományos marketing eszközökkel, például bannerrel hirdették szolgáltatásukat. Mindez jól mutatja, mennyire kifinomult, iparszerű tevékenységről van szó. Az egyik fórumon még arra is külön árat ajánlottak, ha a megrendelő támadások ellen jól felkészített, védett site-ot szeretne megbénítani.

Napjaink legelterjedtebb, pénzügyekre szakosodott rosszindulatú programja egyébként a Zeus, amely áldozata online banki belépőire vadászik. A kártevő legújabb kiadása HTML-befecskendezéssel (HTML injection) és tranzakció-hamisítással (transaction tampering) támad, s így az erős autentikáción és a tranzakció-aláíráson is át tud törni - állítja a Trusteer IT-biztonsági cég.

A fegyverkezési verseny szakadatlanul folyik - mind a bűnözők, mind az ellenük védelmet kínáló cégek újabb és újabb technikákat dolgoznak ki.

Nemrég a Mozilla Firefox vezető tervezője, *Aza Raskin* mutatott be - saját blogján demonstrálva - egy új támadási elvet, amely egyelőre nemcsak a Firefox, hanem az Internet Explorer és más böngészők ellen is bevethető.

Magyarul talán "lapító lapos" technikának nevezhetnénk az eljárást, melyet Raskin angolul "tabnapping"-nek keresztelt. A támadás akkor érheti a felhasználót, ha egyszerre több böngészőlapot (tab-et) tart nyitva. Ha az áldozat ekkor az éppen aktív lapon rosszindulatú vagy feltört site-ot nyit meg, akkor az új technika segítségével a hacker észrevétlenül megváltoztathatja valamelyik másik, nem aktív lap (tab) tartalmát és fejét. Így, amikor a felhasználó kiválasztja (aktiválja) az időközben meghamisított lapot, akkor ott akár egy csali beléptető oldallal - például egy Gmail beléptető-utánzattal - találkozhat. Raskin jelezte: a Firefox következő kiadásához készülő fiókkezelő (Account Manager) megvéd majd az ilyen támadásoktól

A hírre reagálva *Jerry Bryant,* a Microsoft biztonsági kommunikációs vezetője hangsúlyozta: csak akkor adjuk meg egy site-on a belépési azonosítóinkat, ha a böngésző [az Internet Explorer] címsorában megjelenik a lakat szimbólum, s ha meggyőződtünk a cím helyességéről. Az Internet Explorer legfrissebb, 8-as változatának SmartScreen szűrője is segíthet egy esetleges támadás kivédésében, miután kiszűri azokat a webhelyeket, amelyek bizonyítottan vagy feltételezhetően adathalászattal foglalkoznak - tette hozzá.

Jóllehet hazánk nincs igazán a világgazdaság középpontjában, s magyarul jóval kevesebben tudnak, mint angolul, a világhálón tekergő adathalász hálók bennünket sem kerülnek el.

Április elején, majd alig egy hónappal később ismét közlemény kiadására kényszerült az OTP Bank: csalók próbáltak visszaélni a pénzintézet nevével. "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 - mondja *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."

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.

Felvenni a kesztyűt!

Globális fenyegetés ellen csak globális fellépéssel lehet igazán hatékonyan tenni valamit. Össze kell fogniuk a kormányzati, piaci, non-profit szereplőknek és polgároknak egyaránt ahhoz, hogy érzékelhető eredmény szülessen. A társadalom minden szintjén tudatosítani kell a veszélyt. Ennek szellemében brit, amerikai, kanadai, ausztrál és holland szervezetek 2010. június 1-jét a tömeges piaci csalás elleni harc világnapjává nyilvánították. A kezdeményezés útnak indítója a brit bűnüldöző hatóság, a SOCA (Serious Organised Crime Agency) volt, melyhez más szigetországbeli, valamint külföldi partnerek is csatlakoztak.

Miért volt erre szükség? Egyedül Nagy-Britanniában évi 3,5 milliárd fontra becsülik a tömeges piaci csalás által okozott kárt. A szerelmi történetekkel, hamis lottóval, örökséggel, részvényekkel és még ezernyi más trükkel operáló csalók egyre kifinomultabb eszközöket alkalmaznak, s a korszerű technológiát nemzetközi szinten szervezetten bevetve igyekeznek túljárni az emberek eszén és kijátszani a törvényt.

Az adathalászat mind komolyabban veszélyezteti a felhasználók személyi adatainak, belépési azonosítóinak biztonságát. Tavaly az Adathalászat-ellenes Munkacsoporthoz (Anti-Phishing Working Group, APWG) 410 ezer különböző adathalász üzenetről érkezett bejelentés, s a szakmai szervezet adatai szerint az adathalászok minden korábbinál több márkát, céget támadnak.

A csalás elleni világnap szervezőinek célja természetesen az, hogy felhívják a figyelmet a növekvő veszélyre, s mozgósítsanak a bűnözőkkel szembeni fellépés érdekében. Álljon alább néhány jó tanács a SOCA-tól és partnereitől:

- Aki már áldozatul esett a csalók trükkjeinek, ne hallgasson, hanem beszéljen róla!
- Aki azt hiszi, őt nem érheti ilyen baj, gondolja át még egyszer!
- Ne feledjük: ha nem neveztünk be egy játékba, nem is nyerhettünk rajta!
- Nyugodtan kérdezzünk! Akinek nincs vaj a füle mögött, nem fog sem erőszakoskodni, sem lelépni.
- Sose nyúljunk rögtön - különösen előre - a zsebünkbe!
- Jól fontoljuk meg, kinek adunk ki magunkról személyes jellegű információt!
- Ha egy levélben helyesírási és nyelvtani hibákat látunk, legyünk különösen óvatosak, mert az ilyesmi gyakran csalásra utal.
- Website-ot is lehet hamisítani, azt pedig bárki mondhatja, hogy egy közismert cégnél dolgozik. Mindig ellenőrizzük a cégadatok valódiságát! Ha a legkisebb kétségünk van, hívjuk fel a céget!

Szükség van a szabályozás és a törvények újragondolására is.

Talán példát statuál a brit igazságügyi minisztérium április óta hatályos rendelete, amelynek értelmében a szigetország adatvédelmi biztosi hivatala (Information Commissioner's Office, ICO) a korábbi 5 ezer helyett 500 ezer fontig terjedő bírsággal sújthatja azokat a cégeket és önkormányzatokat, amelyektől személyi adatok jutnak illetéktelen kezekbe.

Az ICO-nál kijelentették: az új, százszorosra növelt felső határt az olyan esetekre tartják fenn, mint a tavaly novemberi T-Mobile-történet. Akkor a mobilszolgáltató brit leányvállalata azért értesítette a hivatalt, mert egyes alkalmazottai az ügyfelek szerződésében szereplő adatokat adtak el ügynököknek, akik azután az információt a konkurenciánál értékesítették. Kiadták például a szerződések lejárati dátumát. Így a versenytárs szolgáltatók jó időben fel tudták hívni az érintetteket, hogy vonzó ajánlattal megpróbálják átcsábítani őket.

Nagyobb súlyt fektetnek a digitális információ védelmére a megújuló európai biztonsági, igazság-, vámügyi, jogi és bűnüldözési szabályozásban.

Idéntől ötéves programot indított az Európai Bizottság az unión belüli biztonsági, jogi, bűnüldözési, menekültügyi, bevándorlási, igazság- és vámügyi együttműködés, illetve szabályozás korszerűsítésére. A svéd elnökség idején felvázolt, Stockholmi Program néven ismert akcióterv mintegy 170 elképzelést tartalmaz. A dokumentumot nemrég részletesebben ismertették Strasbourgban.

Mi a várható menetrend? Idén terjesztik elő az EU átfogó biztonsági stratégiájának tervezetét, amely számos témával foglalkozik a katasztrófavédelemtől a terrorizmus-elhárításig. Szerepel a tervek között egy európai légiutas-adatbázis felállítása is, amelyet a tagországok esetleg nemcsak egymással, hanem más országokkal is megosztanának. Az EU már ma is átadja az utaslistákat az Egyesült Államoknak, a tagállamok azonban nem osztják meg automatikusan egymással az adatokat.

Ugyancsak 2010-re várható a számítógépes bűnözés elleni, valamint az unión kívülről érkező idénymunkások foglalkoztatásáról szóló jogszabály tervezete. Az elképzelések szerint szigorítanák

az adatvédelmet és súlyosabb büntetéssel sújtanák azokat, akik visszaélnek mások személyi adataival. Még idén értékelő tanulmány készül az adatmegőrzésről, s felvázolják, hogyan lehetne korszerűsíteni az 1995-ös adatvédelmi kezdeményezést, amely a kormányzati és üzleti célra használt személyi adatok védelmét célozta.

Jövőre azután következik az EU-ba beutazókat és onnan kilépőket nyilvántartó számítógépes rendszerre vonatkozó javaslat, majd 2012-ben az előterjesztés, amely bűncselekménnyé nyilvánítaná a személyi adatok eltulajdonítását. A Stockholmi Program utolsó évében, 2014-ben kerülne terítékre az egységes uniós menekültügyi rendszer felállítását szorgalmazó javaslat.

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.

Becslések szerint a nagy webes cégek által begyűjtött személyes jellegű információ hasznosításának piaca elérheti a 3 milliárd eurót - a 2007-es adat nyolcszorosát.

Ide kapcsolódik a hír, miszerint egy uniós adatvédelmi testület felszólította a Google-t, a Microsoft-ot és a Yahoo-t: tegyenek eleget az EU adatvédelmi irányelvében lefektetett előírásoknak.

Nyílt levélben fordult a vezető keresőket üzemeltető három céghez az EU független adatvédelmi és személyiségi jogi tanácsadó testülete, az úgynevezett "29-es törvénycikk adatvédelmi munkabizottság" (Article 29 Data Protection Working Party, W29). Ebben leszögezik: jóllehet üdvözlik, hogy a trió tagjai igyekeztek összhangba hozni adatmegőrzési gyakorlatukat a törvénnyel, még van mit tenniük az ügyben.

A W29-et az EU adatvédelmi irányelve (95/46/EC) 29-es törvénycikke alapján hozták létre, s munkájában az EU tagállamok adatvédelmi hatóságainak képviselői mellett az európai adatvédelmi felügyelő, valamint az Európai Bizottság vesz részt. Az ismert keresőgépekhez intézett levelében a testület kimondja: a cégek még mindig nem tesznek maradéktalanul eleget az adatvédelmi irányelvnek, amely szerint a felhasználók keresési adatait hat hónap elteltével beazonosíthatatlanná (anonimmé) kell tenni.

Már 2007 óta sürgeti az EU, hogy a keresők üzemeltetői rövidítsék le a felhasználóhoz köthető adatok megőrzési idejét. Mindhárom cég tett lépéseket ebbe az irányba, de a törvény betűjének még mindíg nem tesznek eleget.

"Az adatmegőrzési idő lerövidítésén kívül csökkenteni kell annak lehetőségét, hogy a keresési naplókban azonosíthassák a felhasználókat. Emellett külső ellenőrző (auditálási) folyamatot kell

kialakítani. Ez utóbbi biztosíték a felhasználók számára, hogy [a keresőgépek] betartják adatvédelmi és személyiségi jogi ígéreteiket, s erre a célra független, külső auditáló szervezetet kell bevonni" - áll a W29 levelében. A testület úgy nyilatkozott: az Egyesült Államok fogyasztóvédelmi hatóságát, az FTC-t is felkéri, hogy vizsgálja ki, nem sértette-e meg a három cég az amerikai adatmegőrzési jogszabályokat.

Eközben persze az ipar sem marad adós kezdeményezésekkel. Internet Fraud Alert (Internetes Csalásriasztás) néven a Microsoft és a hozzá csatlakozó amerikai bűnüldözést támogató, 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.

Közösségi veszélyek

Nemcsak a pénzintézeti site-ok állnak a számítógépes bűnözők érdeklődésének homlokterében. Kedvelt vadászterepeik közé tartoznak a közösségi portálok is. Minél látogatottabb egy ilyen webhely, annál inkább keresik rajta a réseket a hackerek.

Nem csoda hát, hogy a negyedév a Facebook biztonsági és adatvédelmi problémáitól volt hangos. Egymást követték a portál réseit kiaknázó támadások. Az egyik, nemrégiben indult hullám "a világ 101 legjobb nőjével" ("the 101 hottest women in the world") kecsegtetett.

Úgy tűnik, a Facebook körül az utóbbi időben felmerült biztonsági és adatvédelmi aggályok legalábbis elgondolkodtatták a felhasználókat. Amikor pár hónapja a portál 1500 felhasználójának feltették a kérdést: otthagynák-e a hálókikötőt az említett problémák miatt, a megkeresettek 60 százaléka azt mondta, hogy fontolóra vennének egy ilyen lépést. Ugyanakkor 16 százalék kijelentette, hogy már nem is látogatja a Facebookot, mivel úgy érzi: nem tudja megfelelően kézben tartani a személyes adatait a site-on. Mindössze 12 százalék maradt feltétlenül hű a népszerű közösségi hálózathoz. A fennmaradó 12 százalék úgy nyilatkozott: nem valószínű, hogy kilép.

Tegyük hozzá az objektivitás kedvéért: azért szó nincs a Facebook hanyatlásáról - ellenkezőleg, tábora rohamosan gyarapszik a világ minden táján. Ám, ha hosszú távon meg akarja őrizni a cég piaci pozícióit, a vezetésnek még nagyobb figyelmet kell fordítania a biztonságra és az adatvédelemre.

Trend értékű híre volt a negyedévnek, hogy egy másik rendkívül népszerű közösségi szolgáltató, a Twitter - igaz, hatósági nyomásra - vállalta, hogy keményebb biztonsági rendszabályokat érvényesít.

A mikroblog portál ellen az amerikai fogyasztóvédelmi felügyelet, az FTC indított vizsgálatot két tavalyi incidens kapcsán, amikor is Twitter-fiókokat törtek fel, s céges adatok kerültek illetéktelen kezekbe. A vállalat végül megegyezett a hatósággal. A megállapodásban a Twitter vállalta, hogy a jelszóválasztásban és -ellenőrzésben az ágazatban bevált legjobb gyakorlatot érvényesíti, s rendszeres biztonsági felülvizsgálatnak veti alá magát.

Mit jelent mindez? Többek között azt, hogy a cégnek egyedi - más fiókhoz nem használt -, nem szótárból vett jelszót kell alkalmaznia, s az nem állhat nyílt (titkosítatlan) e-mailben. A jelszavakat rendszeresen le kell cserélni. Előírás továbbá, hogy az adminisztrációs felülethez csak egyedi bejelentkező lapon lehessen hozzáférni, s annak bizonyos számú sikertelen belépési kísérlet után le kell zárnia. A Twitternek változtatnia kell a felhasználóknak küldött értesítésein is, hogy ne lehessen félreértés a cég adatvédelmét illetően. A vállalat közölte: több intézkedést már foganatosítottak is.

"Ha egy cég azt ígéri a fogyasztóknak, hogy megvédi a személyes adataikat, akkor meg is kell tartania a szavát - jelentette ki *David Vladeck,* az FTC illetékes vezetője. - Ugyanígy: ha egy cég lehetővé teszi, hogy a fogyasztók bizonyos információkat magánjellegűnek minősítsenek, akkor kellő biztonságot kell teremtenie ahhoz, hogy más csakugyan ne férhessen hozzá ezekhez az adatokhoz."

Fertőzés a zsebben

Jó, ha tudjuk: nemcsak számítógépek fertőződhetnek és fertőzhetnek, hanem bármely intelligens digitális készülék. Okostelefon és számítógép egyaránt lehet kártevő-célpont és -hordozó.

A Windows Mobile operációs rendszerű okostelefon-tulajdonosok például jobb, ha nem töltik le készülékükre ingyenes file-megosztó site-okról a "3D Anti-terrorist action" elnevezésű játékot - pontosabban annak az ilyen helyeken fellelhető kalózváltozatát. A kínai Beijing Huike Technology termékének ugyanis jelentések szerint orosz hackerek vírusos változatát dobták a (fekete)piacra. Ha egy Windows Mobile alapú készülék megfertőződik, automatikusan - a tulajdonos tudta nélkül - drága nemzetközi hívásokba fog. Az alattomban hívott külföldi fizetős szolgáltatások aztán igencsak drága mulatsággá teszik az "ingyenes" játékot.

Júniusban gyors egymásutánban két cég digitális készülékein is gyárilag szállított rosszindulatú programot találtak. Mindkét esetben microSD kártyán érkezett a kártevő.

Előbb a Samsung Wave (S8500-as) okostelefonjairól derült ki: egy sorozat microSD kártyáján trójai rejtőzik. A készülékeket a német piacra gyártották. Röviddel ezután féreggel fertőzött microSD kártyával került a japán boltokba az Olympus több mint 1700 Stylus Tough 6010-es digitális fényképezőgépe. Az Olympus elnézést kért a hibáért, s külön weblapot állított fel, amelyen a vásárlók megnézhetik: fényképezőjük gyári száma rajta van-e a fertőzött készülékek listáján.

Miután több hasonló eset történt az utóbbi időben, elemzők figyelmeztetnek: a cégek egyre súlyosabb jogi következményekkel nézhetnek szembe, ha nem javítják a gyártási folyamat biztonságát. Szakértők azt tanácsolják a felhasználóknak: tiltsák le PC-jükön az autorunt, s mielőtt egy készüléket megnyitnának számítógépükön, feltétlenül futtassanak le rajta egy vírusellenőrzést.

Folt hátán folt

Bőséggel kaptak biztonsági frissítéseket a legelterjedtebb szoftverek az elmúlt hónapokban is. A következőkben röviden, időrendben a legfontosabb foltokat tekintjük át.

Előrebocsátjuk: trend értékű volt az Adobe-nak az a negyedév folyamán elhangzott bejelentése, miszerint elképzelhető, hogy a mostani 90-ről 30 napra rövidítik a Reader és az Acrobat biztonsági frissítési ciklusát.

Alig egy éve tért át az Adobe a népszerű PDF-programok rendszeres, negyedéves foltozására. Azóta háromhavonta, mindig a hónap második keddjén - a Microsoft aktuális foltozó keddjéhez igazítva - bocsátja ki biztonsági frissítéseit. Az utóbbi hónapokban azonban annyi sérülékenységre derült fény, hogy a jelek szerint a nagy ügyfelek növekvő nyomást gyakorolnak az Adobe-ra: pörgesse fel foltozóciklusát.

Brad Arkin, a cég termékbiztonsági és adatvédelmi vezetője úgy nyilatkozott: egyik lehetőségként fontolóra vették a havi frissítési ciklus bevezetését. Hozzátette: ha a helyzet megköveteli, ma már az Adobe akár 15 nap alatt is ki tud rukkolni - soron kívüli - folttal.

Szerepel a tervekben az is, hogy az Adobe Reader és Acrobat mellett más termékekre - így a Flashre és a Shockwave-re - is kiterjesszék a rendszeres frissítést. Azt nem tudni: ezekre a programokra is bevezetnék-e a PDF-es szoftvereknél már alkalmazott automatikus frissítési mechanizmust.

Április

Tizenegy biztonsági frissítést bocsátott ki április 13-ai foltozó keddjén a Microsoft. A foltok a Windows, az Office és az Exchange összesen 25 sérülékenységét orvosolták. A 11 javítócsomagból öt "kritikus", öt "fontos", egy pedig "mérsékelten fontos" minősítést kapott. Utóbb az egyik, csak Windows 2000 Server felhasználókat érintő foltot (az MS10-025-öst) visszavonta a szoftveróriás.

Nemcsak a Microsoft bocsátott ki biztonsági frissítéseket április 13-án. Így tett az Oracle és az Adobe is.

Ami az Oracle-t illeti, a cég áprilisban másodszor rukkolt ki foltsorozattal, s összesen 47 rést tömött be. A foltozás persze kiterjedt a nemrég felvásárolt Sun portfolióra is. Így a 47-ből 16 hibát a most Oracle Solaris névre hallgató termékegyüttesben javítottak. Ezek közül nyolc felhasználó-azonosítás nélkül, távolból kiaknázható sérülékenység volt. Nyolc folt került az Oracle e-business szoftverére, egy az Oracle Collaboration csomagra, öt pedig az Oracle Fusion Middleware-re. Emellett a cég az Oracle PeopleSoft/JD Edwards EnterpriseOne csomag négy, valamint az Oracle Industry Applications együttes hat hibáját is kijavította. (Ugyancsak áprilisban menetrenden kívül biztonsági frissítést is kibocsátott az Oracle, hogy orvosolja a Java virtuális gép egy kritikus sérülékenységét.)

A hónap foltozó keddjén jelentkezett javításaival az Adobe is, amely a Reader és az Acrobat 15 sérülékenységét orvosolta. A cég egyszersmind bevezette október óta tesztelt automatikus frissítési funkcióját. Ennek köszönhetően a windowsos gépek felhasználói beállíthatják, hogy Readerjük, illetve Acrobatjuk automatikusan, beavatkozásuk nélkül fogadja a frissítéseket.

Az Apple áprilisban a MacOS X és a MacOS X Server 10.5-ös, illetve 10.6-os változatának sérülékenységét orvosolta. A Type Services komponens résén át támadó hacker a távolból a saját kódját hajthatta végre a megcélzott gépen.

Május

Májusi foltozó keddjén - 11-én - a Microsoft mindössze két biztonsági frissítést bocsátott ki. A foltok a Windows, illetve az Office egy-egy sérülékenységét orvosolták. Mindkét folt "kritikus" minősítést kapott.

A szoftveróriás egyszersmind - nem először - felhívta a figyelmet arra: július 13-ával megszűnik a Windows 2000 és a Windows XP SP2 platform támogatása. A felhasználók csak akkor kaphatják tovább a biztonsági frissítéseket, ha támogatott operációs rendszerre vagy a legfrissebb szervizcsomagra (SP-re) térnek át.

Június

A negyedév utolsó foltozó keddjére - június 8-ára - tíz Microsoft biztonsági frissítés jutott. A foltok összesen 34 rést tömtek be. A tíz javítócsomagból három "kritikus", hét "fontos" minősítést kapott. A Windowshoz hét, az Office-hoz három, az Internet Explorerhez, a Microsoft szerver szoftveréhez és .NET keretrendszeréhez egy-egy biztonsági frissítés szolgál.

Június végén soron kívül legalább 17 rést tömött be népszerű PDF-szoftverein az Adobe. Windows, Mac és Linux platformon egyaránt kijavította a cég az olvasószoftvernek egy sérülékenységét, amelyet kiaknázva egy esetleges támadó rosszindulatú programot telepíthetett a célba vett gépre - feltéve, hogy az áldozat előzőleg megnyitott egy csalidokumentumot. Ugyanezt a hibát körülbelül három héttel korábban a Flash Playerben már orvosolta az Adobe. Akkor a megkezdődött támadások miatt szintén soron kívüli frissítést bocsátott ki a cég. Ugyancsak orvosolták azt a sérülékenységet, amelynek révén a hackerek - visszaélve a PDF specifikáció egy pontjával - rosszindulatú kódot ágyazhattak egy dokumentumba, majd az Adobe Readerrel, Acrobattal vagy a konkurens FoxIT Readerrel végrehajtathatták azt. A szoftvert emiatt úgy módosították, hogy alapértelmezésben ne futtathasson le programkódot. Megváltoztatták a felhasználókat figyelmeztető párbeszédpanelt is, hogy elejét vegyék bizonyos, már ismert hacker-trükköknek.

"Kiemelkedő" kártevők

Melyek voltak egyébként az elmúlt negyedév leggyakoribb kártevői a magyar neten? Nos, 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 freemailes 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).

Kártevő	Részesedés
Backdoor.Nepoe.IF	22.63%
Trojan.Wigon.AE	11.78%
Trojan.DR.Agent.WQBB	7.91%
Trojan.Kryptik.QGV	5.24%
Backdoor.Nepoe.DL	4.23%
Trojan.Meredrop.ZXX	3.81%
Worm.Rbot.MCG	3.12%
Trojan.DR.Inject.WFA	2.86%
Trojan.FakeAlert.CHH	2.62%
TrojanSpy.Bredolab.CCA	2.40%
Egyéb:	33.40%

A második negyedévnek informatikai biztonsági szempontból (is) a júniusi labdarúgó világbajnokság adott egyedi hangulatot - kommentálta az elmúlt hónapok fogását *Szappanos Gábor,* a VirusBuster 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, hogy nyissa meg a levél csatolmányát. Persze a mellékelt küldeményben szinte mindig valamilyen kártevő lapult."

Erőteljesen jelen voltak az e-mailben küldözgetett Javascript letöltő kártevők, amelyek spamet és trójaiakat egyaránt terjesztettek - tette hozzá a szakember.

Emellett - mint világszerte - szakadatlanul ostromolták a magyar felhasználókat is a botnetekhez és a hamis antivírus alkalmazáshoz köthető kártevők. Az utóbbiak a gép megtisztításával kecsegtetnek, ám valójában vagy semmit nem végeznek - ez a jobbik eset -, vagy valamilyen kártékony tevékenységbe fognak. Akárhogy is, készítőik pénzt kérnek értük - vagyis (csalárd) üzleti vállalkozásról van szó.

Mégpedig nem is akármilyenről. Hogy mennyi pénzt hozhat ez az üzletág a bűnözők konyhájára, jól jelzi, hogy - egy nemrég kezdődött amerikai bírósági tárgyalás vádirata szerint - egy nemzetközi trió több mint 100 millió dollárt zsebelt be ilyen szoftver árusításából.

Már nagyjából minden hetedik rosszindulatú program, amivel a Google találkozik a világhálón, a hamis vírusirtók családjába tartozik - közölte nemrég a keresőóriás egy konferencián. Tavaly január és idén február között összesen 240 millió weblapot elemzett a Google, s közülük nem kevesebb, mint 11 ezerről derült ki, hogy hamis antivírus programot terjeszt. A Google kutatói a vizsgált időszakban hétről hétre több hamis vírusirtót terjesztő domainnel találkoztak. Míg tavaly január első hetében 93 különböző csalárd antivírus domaint észleltek, idén január utolsó hetében már 587 volt a számuk.

Napjaink elterjedtebb kártevőit alkotóik weboldalakon keresztül (is) folyamatos frissítik. A kártevők felismerésének biztosítása érdekében más víruslaborokhoz hasonlóan a VirusBuster is folyamatosan nyomon követi ezeket a webhelyeket. A gyakori frissítések miatt természetesen csak generikus felismerési módszerekkel kezeljük őket, az utánkövető feldolgozás nem szolgálná a felhasználók érdekeit.

Íme április-június legaktívabb kártevő-terjesztő domainjei:

Domain	Földrajzi hely	Fájlok száma	Kártevő-család
host127-0-0-1.com	Shalimar, USA	821	Swizzor
screenblaze.com	Trinity, USA	597	Trojan.DL.Delphi.BSO
cfteam.net	Szöul, Dél-Korea	513	Virut, Adware.Cashplus
host192-168-1-2.com	Shalimar, USA	512	Swizzor
rapidshare.com		366	Alureon, TDSS, OnlineGames
fileave.com		355	Worm.DR.Rebhip.Gen, Banker
8i9i.com	Jinan, Kína	300	Adware.Cinmus
hpg.com	Raleigh, USA	278	Banker
3322.org	Peking, Kína	206	Trojan.Servstart, OnlineGames
uol.com	Sao Paolo, Brazília	186	Banker

Mint a táblázatból kitűnik, a hagyományosan terjesztett, régi ismerős reklámterjesztő kártevők (adware-ek) - mint a Swizzor és a Cinmus - mellett nagyobb tömegben jelentek meg a banki jelszólopó trójaiak is. Szokás szerint a domainoknak otthont adó országok tekintetében ebben a negyedévben is az Egyesült Államok és Kína vezet.

A VirusBuster Kft.-ről

A több mint 15 éves szakmai tapasztalattal rendelkező, kizárólag magyar tulajdonú VirusBuster Kft. (www.virusbuster.hu) 1997 óta nyújt teljes körű vírusvédelmi és biztonságtechnikai megoldásokat szinte minden platformon a magyar és a külföldi piac számára. A Kft. termékei számos magyar és nemzetközi független teszten kaptak kitűnő minősítést. A cég fő terméke, a VirusBuster Professional több alkalommal szerezte meg a "Virus Bulletin 100%" díjat, a "Checkmark Anti-Virus Level One" és "CheckVir" elismerést, valamint az ICSA Labs nagy nemzetközi presztízsű "Desktop/Server Anti-Virus Detection" minősítését, majd 2007-ben és 2008-ban elnyerte az ICSA Labs "Desktop/Server Anti-Virus Cleaning" tanúsítványát. 2008-ban a cég megszerezte az OESISOK tanúsítványt, mely azt igazolja, hogy egy alkalmazás tökéletesen együttműködik a vezető piaci fejlesztők –- a Cisco, a Juniper, a NORTEL, a 3Com, az F5 –- hálózati eszközeivel, illetve a hálózatok védelmét szolgáló, a csatlakozó végpontok "egészségét" ellenőrző NAP, NAC és TNC rendszerekkel.

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 VirusBuster webáruháza 2009-ben kiérdemelte a "Fair Business" minősítést, s ugyanebben az évben a cég 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