WWW.IT-SECURITY.HU

IV. ÉVFOLYAM 4. SZÁM 2007. ÁPRILIS 17.

IT-SECURITY

AZ INFORMATIKAI BIZTONSÁG LAPJA

AZ IT-BUSINESS MELLÉKLETE

6. OLDAL

Elszivárgó biztonság

Tolvajkulcs a zsebben

7. OLDAL

Arccal a gép felé

Megnéz és felismer

20. OLDAL

Képviselők noteszgéppel

Nem érzik veszélyben

28. OLDAL

Mobil-védőőrizet

Illetéktelen fülek

Szigorúan bizalmas!

Számítógépes titkosítás 14. oldal

IT-SECURITY TODAY

INFORMATIKAI BIZTONSÁGI HÍRLAP NAPI ONLINE TÁJÉKOZTATÓJA

- informatikai döntéshozóknak, technológiai szakembereknek
- az elmúlt 24 óra legfontosabb hazai és külföldi informatikai biztonság és információbiztonság hírei
- ingyenes napi online hírlevél

Regisztráljon!

www.it-business.hu/hirlevel

TITKOK

Politikai berkekben megszokott, hogy egy amúgy kisebb-nagyobb port felvert ügy iratait vagy 80 évre titkosítják.

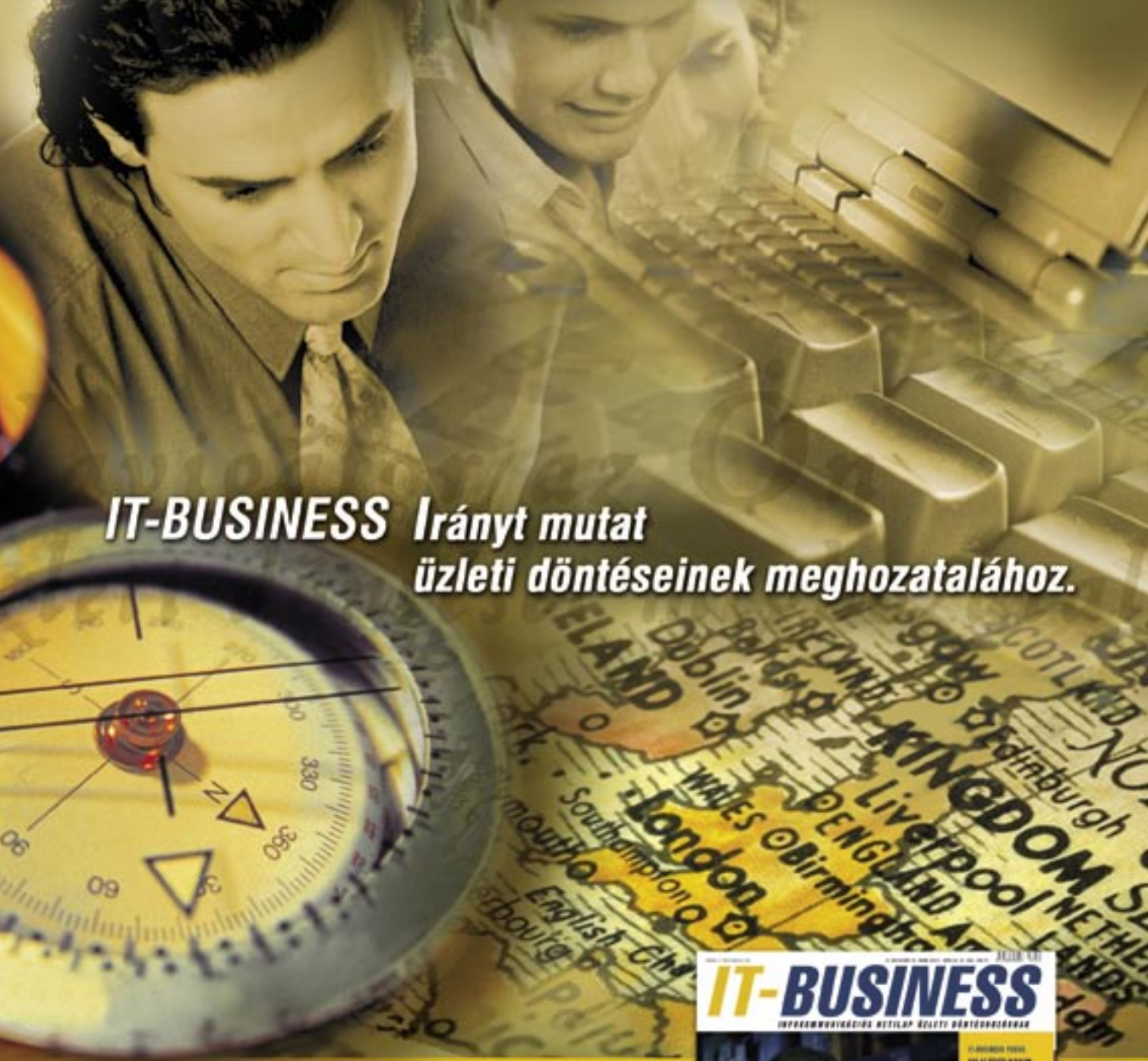
Vélhetően akadnak a politikai színezetű ügyeknél sokkal izgalmasabb dolgok is, amelyeknek a titkosítására nem ártana odafigyelni. Értve ezen az információkhoz való hozzáférést és magának az információnak a titkosítását. Léteznek ugyanis kitűnő titkosítási algoritmusok, amelyek az infrastruktúra részévé váltak – építkezni lehetne, mi több, kellene rájuk. A gyakorlatban azonban nem igazán használják ezt a technológiát, holott üzleti haszna is lenne.

Gondoljunk csak arra, micsoda kincsek tárolódnak a különféle adatbázisokban, adathordozó eszközökön. És mennyinek kél lába! Számtalan mobiltelefont, PDA-t felejtünk taxik hátsó ülésén, és a rendszeres szinkronizálásoknak köszönhetően azokon szép számmal találhatók üzleti infók is. Előfordul az is, hogy valamilyen rejtélyes okból elhagyjuk noteszgépünket. Vagy valaki meglovasítja… Ha ez az autónkkal történik, akár milliókat is hajlandók fizetni egyesek a „becsületes” megtalálónak. Vajon a notebookon tárolt információknak mekkora értékük lehet? Bizonyára más az árfolyama egy vezérigazgatói noteszgépnek, más egy pénzügyi igazgatóénak, s egészen más egy alkalmazotténak. Persze ha az ott tárolt információk titkosítva lennének, akkor nem biztos, hogy akkora lenne a baj.

Az országgyűlési képviselők noteszgépeinél ez a probléma már megoldott: ott inkább az a kérdés, hányan használják napi rendszerességgel ezt a munkaeszközt. Talán sem ők, sem mi nem gondolunk bele abba, hogy a leveleink jókora hányada bizony titkosítatlanul közlekedik a neten.

Sziebig Andrea

Sziebig Andrea
főszerkesztő



IT-BUSINESS Irányt mutat üzleti döntéseinek meghozatalához.

Ön vezetői döntések egész sorát kénytelen meghozni naponta. Lépjen-e üzleti kapcsolatba leendő partnerével? Kit válasszon egy adott feladatra? Vagy éppen melyik gombot nyomja meg, hogy egy projekt beinduljon?

A körültekintő döntések előtt a kép azonban csak akkor lehet teljes, ha a szükséges információk ott vannak, ahol a legnagyobb szükség van rájuk. Az Ön íróasztalán.

www.it-business.hu
Telefon: (06 1) 888 3461

IT-BUSINESS *Infokommunikációs hetilap üzleti döntéshozóknak*

TERMÉKHÍREK

MEGKÉRDEZTÜK

CÍMLAPON

Szigorúan bizalmas!

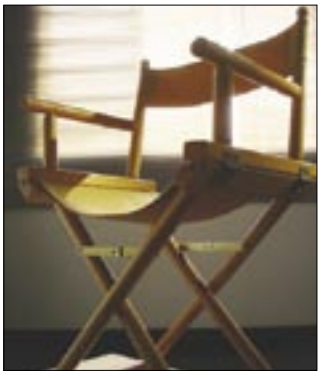
A titkosítás tudománya – a kriptológia – bizonyos vonatkozásaiban az emberiség egyik legnagyszerűbb kulturális vívmánya. Szinte az írásbeliség megjelenése óta próbálnak üzeneteket kódolni azzal a céllal, hogy azokat csak a címzett tudja elolvasni, másoknak meg ahhoz fűződik érdekük, hogy feltörjék ezeket az üzeneteket. Bonyolult titkosítási módszerek jöttek létre, közben pedig a kriptológia a mindennapok része lett.

14. oldal

ESZKÖZTÁR

KOMMUNIKÁCIÓ

MENEDZSMENT



Elszivárgó biztonság

Az adatvédelem ajtaját nyitó tolvajkulcs szinte mindenkinek ott lapul a zsebében.

Az a rossz, aki rosszra gondol – tartja a mondás. Az viszont biztosan nem jó gazdája a vállalati adatoknak, aki nem gondol rosszra, tudván, hányféle eszközön lehet kivinni az értékes információkat az ajtón. Szinte mindenkinek a zsebében van legalább egy, nagy memóriakapacitású eszköz – mobiltelefon, pendrive, mp3-lejátszó vagy digitális fényképezőgép –, amelyen könnyedén elfér majd' minden fontos adat: ügyfél- és partnerlista, üzleti terv, könyvvizsgálói jelentés. Ezeket elég a nagy sávszélességű portokra csatlakoztatni, és máris megvan, amire új céget lehet alapozni, vagy amivel a jelenlegi munkaadót lehet kínos helyzetbe hozni.

Információt – vagy akár szoftvert – nemcsak kivinni, hanem behozni is lehet, és ez sem feltétlenül örömteli: az otthon letöltött zene, videó, fénykép, jópofa program a szoftverleltárnál okozhat meglepetést, a káros kódok pedig annál is hamarabb.

Persze a legegyszerűbb megoldás volna letiltani a portok használatát, ez azonban a többi, nélkülözhetetlen periféria (USB-s nyomtató, egér stb.) miatt nem oldható meg, ráadásul ott van a többi kiskapu: a wifi, a firewire, az „egyenlőbb" felhasználók pedig a tiltás dacára is kivívhatják maguknak a kivételes bánásmódot, hogy azután náluk kuncsorogjanak kivételért a többiek.

Nem egy olyan szoftver található a piacon, amellyel menedzselhető az USB-, infravörös, bluetooth- vagy wifi-csatornák forgalma. A Pointsec Device Detector azzal emelkedik ki ezek közül, hogy a portok menedzsmentjét tartalomszűréssel és titkosítással

Megosztható titkosítás

kombinálja. Meghatározható, mely eszközök csatlakoztathatók, és melyek nem, az adattárolásra alkalmasak titkosítva legyenek-e, és azokon milyen adatok kerülhetnek ki a cégtől, illetve milyenek juthatnak be róluk. A szoftver még a Windows betöltődése előtt működésbe lép, így még az előtt elindítja a vírusellenőrzést, hogy az operációs rendszer felismerné az eszközt. Kiszűri az átnevezett végrehajtható állományokat, és a számítógépre átmásolt fájlok futtatását is képes blokkolni. Lehet vele a pendrive egy részét titkosíttatni, a titkosítást kikényszeríteni, illetve a területet többszörösen felülírva végleg törölni adatokat, és meghatározható, mely programokból lehet pendrive-ra menteni, melyekből nem; csoport-, gép- és felhasználói szintű szabályok állíthatók be. Egyénileg ellenőrzi az eszközöket típus, márka vagy modell szerint, és a rend-

www.emib.hu
www.filtermax.hu

szergazda is konkrét eszközök engedélyezéséről/tiltásáról dönthet.

Az első lépés annak felmérése, mekkora veszélynek van kitéve a cég. Az ingyenesen letölthető Device Discovery segít feltérképezni, milyen eszközöket használtak és használnak a munkatársak, s így a védelem tervezésénél konkrét tapasztalatokra lehet építeni.

Kelenhegyi Péter

Vészes könnyelműség

A cégek többsége még mindig nem veszi komolyan a leselkedő veszélyeket.

Hatszáz globális vállalatot kérdeztek meg a Webroot kutatói arról, hogy milyen hatással vannak üzletmenetükre az internetes fenyegetések. 43 százalékuk nyilatkozott úgy, hogy leállásokat kell elszenvednie a rosszindulatú kódok garázdálkodása miatt. 40 százalékuknak okoztak üzleti károkat a kémprogramok, és ami még ennél is megdöbbentőbb, 26

www.webroot.com

százalékuknál bizalmas adatok kerültek veszélybe az alattomos kórokozók miatt. 39 százalékukat érte már trójai támadás, 24 százalékuk számolt be az informatikai rendszerének megfigyeléséről, és 20 százalékuk esett áldozatául webhely-átirányításnak, illetve billentyűleütés-rögzítő programoknak.

Nincs mit csodálkozni azon, hogy a nagyvállalatokat ilyen komolyan érintik a támadások: a felmérés szerint több mint 60 százalékuk nem rendelkezik információbiztonsági politikával.

A Webroot becslése szerint a világszerte üzemelő mintegy 250 milliónyi webhely 1,7 százaléka ad otthont rosszindulatú programoknak.

Tóth István

APRÓCSKA TÉVEDÉS

Márciusi tesztjében a Virus Bulletin a Suse Enterprise Linux alatt mérkőztette meg egymással a vírusellenes programokat. A VB100% minősítést az elmúlt 5 évben minden egyes részvételekor megkapó NOD32 ezúttal tévesen jelzett fertőzöttnek egy vírusmentes állományt, így a minősítést annak ellenére nem érdemelte ki, hogy a többi fertőzött minta mindegyikét felismerte.

A tesztet végző mérnökök tájékoztatása szerint a téves riasztás egy régi, 1991-es eredetű DOS-állomány kapcsán generálódott, amit a vírusirtó program heurisztikája „valószínűleg fertőzést tartalmaz" címkével jelölt meg. Amikor az állományt a Virus Bulletin szakemberei úgy is megvizsgáltatták a programmal, hogy a fertőzött állományok automatikus törlését bekapcsolták, a NOD32 törölte azt.

Arccal a gép felé

Folyamatosan fejlődik a testi jellemzők alapján történő felismerés.

Sokszor elhangzott már, hogy a biometrikus azonosítás a jövő, amelynek egyik módszere, az arcfelismerés most egy ígéretes eszközzel gyarapodott. A Bioscrypt-féle VisionAccess 3D DeskCam segítségével számítógépre és helyi hálózatba jelentkezhetünk be, vagy programok használatára szerezhetünk jogosultságot.

www.bioscrypt.com

Konfigurálásakor a VisionAccess egy 40 ezer pontból álló háromdimenziós maszkot feszít rá az adatbázisába felvenni kívánt személy arcára, és rögzíti annak térbeli alakját. Mivel infravörös fénnyel térképezi fel az arcot, mind sötétben, mind gyenge fényviszonyok közepette működőképes. A 300 dollár körüli áron megvásárolható berendezést elsősorban asztali PC-khez szánták fejlesztői, de hordozható számítógépek perifériájaként ugyancsak használható. A gyártó tervei között szerepel a VisionAccess beépítése noteszgépekbe. Az arcfelismerési technológiához az A4Vision márciusi felvásárlásával jutott a Bioscrypt.

Figyel a részletekre

Tóth István

TRÓJAI TAVASZ

Ahogy azt a biztonsági cégek megjósolták, egyre nagyobb méreteket ölt az idén a kártékony falovak garázdálkodása. A NOD32 vírusellenes program használóinak adatszolgáltatásán alapuló ThreatSense statisztikái szerint márciusban a vírusfertőzések többségéért trójai kórokozók voltak a felelősek.

Az előfordulás gyakorisága alapján összeállított Top 10-es listát a jelszavak ellopására szakosodott Win32/PSW.Agent.NCC nevű trójai vezette, amely az összes incidens két százalékáért volt okolható. Az 1,77 százalékos „piaci részesedést" elérő Win32/Netsky.Q (másnéven Netsky.P) féreg elektronikus levelek mellékleteként és állománymegosztó hálózatokon keresztül terjed. A harmadik helyet a weboldalakról vírusokat begyűjtő, bothálózat-építő Win32/TrojanDownloader.Agent.AWF szerezte meg 1,69 százalékkal.

Kockázatos kattintások

Aki sokat internetezik, előbb-utóbb rosszindulatú weboldalra téved.

Közzétette a McAfee a világháló legkockázatosabb és a legbiztonságosabb weboldalait feltérképezni hivatott globális kutatásának eredményeit. A biztonsági cég szakértői 265 legfelső szintű doménbe – ország (.jp, .nl stb.) és általános (például .com) – tartozó weboldalakat elemeztek, majd osztályoztak a kémprogramokra, spamekre, rosszindulatú kódokra és scamekre kiterjedő biztonsági tesztek alapján.

A „Rosszindulatú web feltérképezése” című jelentés meglepően nagy eltéréseket mutat ki az egyes domének biztonságában. A globális felmérés becslése alapján az internethasználók havonta több mint 550 millió alkalommal látogatnak meg veszélyes weboldalakat, és még az olyan viszonylag biztonságos tartományok is, mint Németország (.de) vagy az Egyesült Királyság (.uk) is több millió kockázatos kattintásért tehetők felelőssé.

Mit kell elkerülni?

Bizonyos webes tevékenységek – ide sorolható a regisztrálás és az állománylétöltés – egyes doménekben kifejezetten kockázatosak lehetnek. Így például az e-mail-cím megadása egy véletlenszerűen kiválasztott .info tartományban elképesztően magas, 73,2 százalékos valószínűséggel eredményezi spamek érkezését.

A legkockázatosabb országtartománynak Románia (.ro) és Oroszország (.ru) bizonyult, ezeknél a veszélyes oldalak aránya 5,6, illetve 4,5 százalék volt. Ezekben az országtartományokban tévedhetünk a leggyakrabban rosszindulatú kódokat tartalmazó és megkérdezés nélküli letöltést végrehajtó webhelyekre. A legnagyobb veszélyeket rejtő általános domén az .info, az ide tartozó oldalak 7,5 százaléka esik a kockázatos besorolásba. A .com a második legkockázatosabb, itt az oldalak 5,5 százaléka jelent fenyegetést. A .gov az egyetlen olyan vizsgált domén, amelynél a McAfee nem bukkant kockázatos oldalakra. Ebben a tartományban kizárólag az Egyesült Államok kormányzati ügynökségei létesíthetnek webhelyeket.

Tóth István

E-mailek nagyító alatt

Komoly veszélyt jelentenek a biztonságra az ellenőrizetlenül terjedő levelek.

Megjelent a Microsoft Exchange-hez kifejlesztett, levélszűrési célú rendszer, a Sunbelt Ninja legfrissebb, 2.1-es verziója, amely a kéretlen levelek és a mellékletekben megbúvó programkártevők ellen egyaránt védelmet nyújt. A két levélszűrő motorral – köztük a Cloudmarkkal – dolgozó program új szolgáltatása a levél végi üzenetkezelő modul, amelynek segítségével jogi nyilatkozatok helyezhetők el a levelezőkiszolgálót elhagyó e-mailek végére. A Ninja további újdonsága, hogy a rendszergazda az Exchange levélkiszolgáló terheltségét a szűrésre fordított rendszererőforrások pontos meghatározásával tudja szabályozni.

http://mpp.hu
www.sunbelt.hu

Vadonatúj funkciókkal bővült a magyar fejlesztésű és nyelvű MPP Desktop spamszűrő program legújabb, 3.4-es változata, amely hatféle módszert vet be a kéretlen levelek kiszűrésére. Grafikonokkal szemlélteti az utolsó 24 órában, héten és hónapban beérkezett spamek arányát, amelynek révén nyomon követhető a fekete- és fehérlisták hatékonysága. Az MPP Desktop bármelyik Windows-verzió alatt futtatható, és egyszerre több Outlook-postafiókot képes kezelni.

Sasszemek az irodában

Fizikai védelem nélkül nem létezik informatikai biztonság.

Kényelmesen, webböngészőn keresztül lehet figyelemmel kísérni a Vivotek döntheto, forgatható és zoomolható, hangfelvételre is képes biztonsági IP-kamerájának a képét. A PZ6112 változat vezetékkel, a PZ6114-es jelű modell pedig 802.11g szabványú vezetéknélküli összeköttetéssel csatlakoztatható az Ethernet-hálózathoz. Vezérlésük az interneten keresztül, távolról történhet; a forgatás 270 fokban, a döntés pedig 135 fokban végezhető. Az intelligens mozgásérzékelővel felszerelt berendezéssel nyomon követhetők a gyanús események. A mellékelt szoftver segítségével a kamera képe és hangja a számítógép merevlemezére menthető.

www.vivotek.com

Barátságos biztonság

Alapos technológiai ismeretek nélkül eddig szinte lehetetlen volt jól konfigurálni a védelmi programokat.

Manapság az internetes veszélyek ellen átfogó védelmet nyújtó szoftver nélkül nem lehet biztonságosan üzemeltetni a világhálóra kapcsolódó számítógépeket. Mivel azonban a biztonsági csomagok megfelelő beállítása komoly szakértelmet igényel, az otthoni felhasználók többsége képtelen megbirkózni a feladattal. Most a Symantec a számítástechnika rejtelmeiben kevésbé jártas PC-használók segítségére sietett. Új termékük, a Norton 360 nem csupán egyesíti a cég vírus- és kémprogramellenes, tűzfalas, betörésvédelmi, adathalászat elleni, archiválási, valamint beállítási technológiáit, hanem nagyfokú automatizáltsága révén egyszerű használatot biztosít. A gyártó szerint a műveletek a szokásos számítógépes tevékenységek megzavarása nélkül, a háttérben futnak.

www.symantec.hu

A Norton 360 megóvja a felhasználók személyes adatait az online tranzakciók során, felderíti és kijavítja a fellépő problémákat, valamint optimalizálja a számítógép teljesítményét. Alkalmazza mindazokat a fejlett védelmi eljárásokat, amelyek a Symantec többi termékeiben megtalálhatók. Ezek közül megemlítendő a viselkedés alapú felderítést megvalósító Symantec Network for Advanced Response (SONAR) technológia; a kernel módú rootkitek heurisztikus eltávolítása; és az adathalász webhelyekre figyelmeztető Norton Toolbar böngészőeszköztár.

Automatizált védelem

Ami az archiválási lehetőségeket illeti, a Norton 360 két gigabájtos ingyenes online tárhelyet biztosít (további tárhely vásárolható 5–25 gigabájtos méretben), automatikusan felismeri az új vagy módosított állományokat, és a számítógép holtidejében haladéktalanul menti a változtatásokat. A spamellenes és a szülői felügyelet funkciót egy, az internetről ingyenesen letölthető csomaggal lehet integrálni a Norton 360-ba.

Tóth István

Ajaxra lőnek

Nem kedvez a biztonságnak a gyors fejlesztés.

Ahogy valamilyen újdonság megjelenik az informatika világában, a hackerek máris azon kezdik el törni a fejüket, hogyan lehetne annak gyengeségeit kihasználni. Úgy tűnik, most a web 2.0-s technológiákat felvonultató, korszerű szolgáltatásokat kínáló webhelyek kerültek az elméleti támadások célkeresztjébe. A Fortify Software nevű biztonsági cég kutatói olyan új incidensek lehetőségére hívták fel a figyelmet, amelyek a web 2.0-s webhelyek és az azokat dinamikussá tevő Ajax-alkalmazások ellen irányulhatnak.

A JavaScript Hackingnek nevezett módszerrel a számítógépes bűnözők felkutathatják az Ajax-eszközkészletek esetleges sebezhetőségeit, amelyek kihasználásával aztán kritikus információkat szerezhetnek meg áldozataiktól. Szakértők szerint, ha a sérülékenységeket nem javítják ki, hasonló problémával szembesülünk majd, mint a puffertúlcsordulás esetében, amelyről évtizedek óta tudunk, még sem tudjuk kezelni.

Súlyosbítja a helyzetet, hogy a gomba módra szaporodó web 2.0-s webhelyek készítőinek sokszor kell dönteniük, hogy a biztonságot vagy a funkcionalitást választják-e, s nem mindig a józan megfontolás győzedelmeskedik.

www.fortifysoftware.com

Jelentés a frontról

A bizalmas adatok megszerzése a számítógépes bűnözők legfőbb célja.

Közzétette a Symantec az internetes veszélyekről szóló legújabb jelentését, amely a 2006 második félévében tapasztalt eseményeket foglalja össze. A tanulmány legfontosabb megállapítása, hogy a számítógépes bűnözők az egész világot behálózó, együttműködő közösségeket szerveznek a titkos információk ellopására és az erre szolgáló rosszindulatú kódok létrehozására. A bizalmas adatokat az 50 leggyakrabban előforduló programkártevő 66 százaléka veszélyeztette, szemben az előző időszak 48 százalékával. 2006 második félévében a Symantec szakemberei több mint 160 ezer olyan spamüzenetet találtak, amelyet adatgyűjtési célokra készítettek.

A vizsgált időszakban a cég kutatói több mint 6 millió bottal fertőzött számítógépet észleltek, 29 százalékkal többet, mint 2006 első felében. A botokhoz a parancsokat eljuttató vezérlőszerverek száma azonban 25 százalékkal csökkent, ami azt jelzi, hogy folyik a bothálózatok egyesítése és méretének növelése.

A trójaiak az 50 leggyakoribb kódminta 45 százalékát alkották, ez 23 százalékos emelkedés 2006 első félévéhez képest. Ez alátámasztja a Symantec korábbi előrejelzését, mely szerint a hackerek a levélözönt küldő férgekről a trójaiakra térnek át. A bűnszervezetek saját kiszolgálóikon tárolják a lopott hitelkártyaszámokat, PIN-kódokat, e-mailes címlistákat és hasonló bizalmas információkat, melyeket szabott áron próbálnak meg értékesíteni. Az Egyesült Államokban kiadott hitelkártyák adataihoz 1–6 dollárért, míg az online banki rendszerekbe való belépéshez szükséges azonosítókhoz és jelszavakhoz 14–18 dollárért lehet hozzájutni.

Most először mérte fel a Symantec, hogy mely országokból indult ki a legtöbb rosszindulatú tevékenység. E kétes dicsőségű listát 31 százalékkal az Egyesült Államok vezette, a második Kína lett 10 százalékkal, a harmadik helyen pedig Németország végzett 7 százalékkal.

Tóth István

A pénzünkre hajtanak

WINDOWSOS GONDOK

Biztonsági figyelmeztetést adott ki a Microsoft, amelyben a Web Proxy Automatic Discovery (WPAD) protokollt érintő új típusú támadásra hívja fel a vállalati felhasználók figyelmét. Az amerikai kormány internetes fenyegetésekkel foglalkozó központja, a US-CERT arról számolt be, hogy egy DNS (Domain Name System) vagy egy WINS (Windows Internet Naming Service) kiszolgálóba egy WPAD-bejegyzést regisztrálni tudó támadó képes lehet egy WPAD-konfigurált ügyfelet egy tetszés szerinti gazdagéppel való kapcsolatra kényszeríteni, hogy onnan áttöltse a rosszindulatú WPAD.dat állományt.

Ennek révén a támadó hozzáférhet az ügyfél forgalmához oly módon, hogy azt egy rosszindulatú proxykiszolgálóra irányítja. A US-CERT azt tanácsolja a hálózati adminisztrátoroknak, hogy tartózkodjanak a statikus WPAD DNS gazdanevek és a WPAD WINS névrekordok használatától. A sebezhetőség húsz Microsoft-terméket érint: a Windows Server 2003 16 változatát, a Windows 2000 több verzióját és a Microsoft Small Business Server 2000 Standard Editiont.

www.us-cert.gov
www.microsoft.com

VESZÉLYES IKONOK

A sebezhetőség rendkívüli súlyosságára való tekintettel nem várta meg a Microsoft az animált kurzorokkal kapcsolatos Windows-hiba kijavításával az április közepén esedékes szokásos frissítést, és még a hónap elején közzétette a javítást az interneten. Az .ani kiterjesztésű állományok hibás kezeléséből eredő sérülékenység kihasználásával átvehető az irányítás a megtámadott számítógép felett, és kártékony programok futtathatók rajta.

A felhasználók akkor válhatnak áldozattá, ha az Internet Explorer 6-os és 7-es változatával vagy a Firefoxszal a hackerek által készített, rosszindulatú weboldalra látogatnak, vagy megnyitnak egy speciális kialakítású, html-formátumú elektronikus levelet. A hiba a Windows 2000 Prót, valamint a Windows 2000 Server, 2003 Server, XP és – igencsak meglepő módon – a Vista különféle változatait érinti.

KOMBINÁLT FENYEGETÉS

Az Internet Explorer automatikus kitöltés funkcióját használja ki a Therat.B nevű trójai, amely a böngésző által tárolt jelszavakat és felhasználói azonosítókat lopja el. Akinek a gépén ez a kényelmi funkció be van kapcsolva, eleve veszélynek teszi ki magát. De azok sincsenek biztonságban, akik nem veszik igénybe a szolgáltatást, mert a trójai képes rögzíteni a billentyűleütéseket. Mi több, módosítja a Windows rendszerleíró adatbázisát annak érdekében, hogy az operációs rendszer minden újraindításakor automatikusan a memóriába töltődjön.

A megszerzett információkat előbb a merevlemezen tárolja, majd egy előre megadott e-mail-címre küldi. Elektronikus levélben, fertőzött állományok letöltésével és fájlcserélőkön keresztül terjed. Szakértők szerint a Therat.B igazi többfunkciós programkártevő, az ilyeneket a sérülékenységek minél hatékonyabb kihasználására hozzák létre a számítógépes bűnözők.

Hordozható védelem

A mobileszközök komoly veszélybe sodorhatják a vállalati hálózatokat.

Ugyanolyan biztonsági és adatvédelmi szolgáltatásokat kínál a Windows Mobile rendszerű okostelefonokhoz és PDA-készülékekhez a Symantec-féle Mobile Security 5.0, mint amilyeneket az asztali és noteszgépeknél megszokhattunk. A vírusellenes modul felismeri a fertőzött állományok megnyitását. A vizsgálat és a frissítések letöltése a Symantec LiveUpdate szolgáltatáson keresztül történik. A tűzfal mind a bejövő, mind a kimenő forgalmat szűri, míg az smsspam elleni funkció automatikusan törli vagy külön mappába helyezi a kéretlen szöveges üzeneteket.

www.symantec.hu

Az adatvesztést ellopás esetén megakadályozó szolgáltatások között megtalálható a belső tárban és a memóriakártyán lévő információk kódolása, valamint többszöri sikertelen belépési kísérlet észlelése esetén az összes adat törlése.

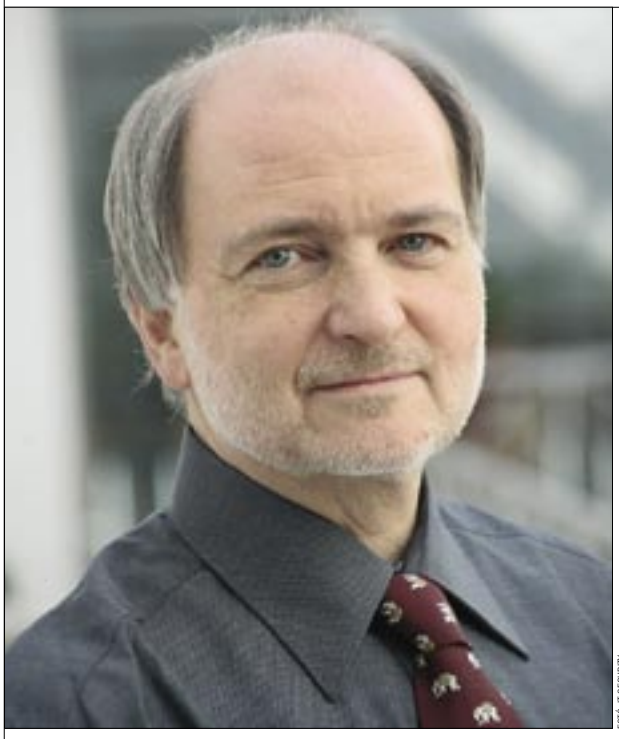
A fokozott biztonságot szolgálja a Bluetooth- és wifi-kapcsolat, valamint az adatszinkronizáció kikapcsolhatósága. A Mobile VPN funkció révén biztonságos IPSec-csatornákon keresztül lehet elérni a céges hálózatot.

Ehhez a szolgáltatáshoz kapcsolódik a hálózati belépést ellenőrző funkció, amely biztosítja, hogy csak az előírásoknak megfelelő, biztonságos eszközök csatlakozhassanak a vállalati erőforrásokhoz, valamint a hamisítás elleni védelem, amely a hálózathoz való csatlakozás előtt megvizsgálja, hogy módosították-e az eszköz biztonsági alkalmazásait.

Tóth István

TÁMADHATÓ AZ IPOD

Felfedezték a Kaspersky Lab szakértői az első, kifejezetten az iPod megfertőzésére készített vírust, amely azonban kísérleti (proof of concept) volta miatt nem jelent valódi veszélyt a népszerű médialejátszóra. A Podloso nevű programkártevő egy olyan állomány, amely nem fut automatikusan, aktivizálódásához felhasználói beavatkozás szükséges. Kizárólag olyan iPodon hozható működésbe, amelyre telepítették a Linuxot. Miután elindították, a vírus átvizsgálja a médialejátszó merevlemezét, és megfertőzi az azon található összes, .elf formátumú végrehajtható állományt. Ezek elindításakor aztán megjelenít egy üzenetet: „Megfertőződtél az Oslóval, az első iPodLinux vírussal”.



FOTÓ: IT-SECURITY

Székely Iván
társadalmi informatikus

Közérdek és magántitok

A vállalatok szeretnek titkolózni, amikor saját adataikról van szó, de sokkal kevésbé érzékenyek mások adatainak sérthetetlenségére. Pedig a jogszabályok mindkét esetben elég világosan megfogalmazzák a cégek és vezetőik lehetőségeit és kötelességeit.

– Mi jellemzi a magyar vállalatok adatkezelési gyakorlatát?

– Tudni kell, hogy minden vállalatnál számos, különféle adat gyűlik fel. Vannak nyilvános forrásból beszerzett, mindenki számára hozzáférhető adataik; vannak, amelyeket bizalmas kezelésre kaptak meg a partnereiktől; vannak az ügyfelekre és munkatársakra vonatkozó személyes adatok; és vannak a cég működése során keletkezett üzleti adatok.

Létezik a gyakorlat, de attól még nem lesz törvényes

Magyarországon nagyon sokszor előfordul, hogy egy cég vezetője azt hiszi: ő döntheti el, mi számít üzleti titoknak, ki férhet hozzá az adatokhoz, és ő választja ki az adatok bizalmasságát szolgáló biztonsági eszközöket is. Nem véletlen, hogy néhány kivételtől eltekintve nem is tartják megfelelőnek a magyar adatbiztonsági színvonalat. Pedig ezekre az adatokra is számos jogszabály vonatkozik, amelyek meghatározzák kezelésük miként jét is.

– Kezelési szempontból melyek az adatok legfontosabb csoportjai?

– Az egyik nagy csoport a személyes adatoké. Ez az egyik legjobban védett adatfajta, és legfontosabb jellemzője, hogy sohasem az adatkezelést végző cég rendelkezik felette, hanem mindig az, akire vonatkozik: ő jogosult eldönteni, hogy mi legyen a róla szóló adatok sorsa, mire lehet azokat felhasználni (persze van számos kivétel is). Bizonyos fokig le lehet mondani a személyes adatok feletti önrendelkezésről, de korlátlanul nem.

A másik nagy csoport a közérdekű adatok köre: ezek a közfeladatokat ellátó szervezeteknél (amelyek lehetnek akár gazdasági társaságok is) keletkeznek. Közfeladatnak számít viszont az is, amikor egy magáncég valamilyen terméket vagy szolgáltatást elad az államnak, pályázik valamilyen állami tulajdonra.

Vannak aztán bizonyos adatok, amelyek a vállalatok működése közben keletkeznek, illetve magára a vállalatra vonatkoznak. Ezek egy részének nyilvánosságát megint csak jogszabályok írják elő, például, hogy mit kell közzétenni a cégnyilvántartásban.

– Hol férnek bele ebbe a felosztásba az üzleti titkok?

– Nos, azok ezen kívül állnak. Az üzleti titkok olyan adatok, információk, amelyek titokban tartásához a cégnek méltányolható érdeke fűződik, és amelynek titokban tartásáért tett is valamit az adott szervezet. (Tehát ha valamit a cég közzétesz az interneten, akkor utána nem lehet arra hivatkozni, hogy ez voltaképpen üzleti titok volt.) Egy cégvezetőnek igazából az ilyen adatok védelmének esetében van döntési jogköre: ő határozhatja meg a védendő adatok körét és a védelem mikéntjét is.

– Mennyire élesek a határvonalak az egyes kategóriák között?

– Mindig ott van a legtöbb kétség és a legélesebb vita, ahol az üzleti élet és a közérdek találkozik, vagyis ahol közjavak mennek át magántulajdonba: egy cég terméket vagy szolgáltatást ad el az államnak, vissza nem térítendő támogatást kap, részt vesz a privatizációban, vagy koncessziót vásárol. Mivel itt közpénz, illetve állami tulajdon cserél gazdát, mindenképpen közérdekű adatokról beszélhetünk, amelyeket minden érdeklődő jogosult megismerni. A vállalatok viszont nagyon gyakran igyekeznek eltitkolni ezeket az információkat, mondván, az üzleti érdekeiket sértené nyilvánosságra kerülésük. Szerencsétlenségükre azonban a törvények erről másképp rendelkeznek.

Vegyük például az állami tendereket. Ezek három, egymást követő szakaszra oszthatók: a pályázat kiírása, az ajánlatok beérkezése és a tenderezés, végül a győztes kiválasztása és a szerződés megkötése. Az első szakasz értelemszerűen nyilvános: nem lehet titokban meghirdetni egy pályázatot. A második fázis – megint csak értelemszerűen – nem lehet

nyilvános: nem tenne jót a versenynek, ha a pályázók ismernék egymás ajánlatát, másrészt abban benne van a későbbi vesztesek anyaga is. Méltányolható érdek ugyanakkor, hogy titokban maradjon az, amivel nem nyert egy pályázó.

A nyertes ajánlat viszont már közérdekű adat, ezért a harmadik fázisnak már megint csak a legteljesebb nyilvánosság előtt kell zajlania. És ez a nyilvánosság nemcsak az árra vonatkozik, hanem a teljes szerződésre: milyen feltételekkel kötötték meg, milyen kedvezményeket kapott és milyen kötelezettségeket vállalt a cég, és így tovább; a törvény szerint a szerződésben nem létezhetnek „titkos záradékok" sem. Ám a fentiek olyan adatok, amelyeket a cégek igyekeznek minden eszközzel titokban tartani, noha jogilag nem számítanak üzleti titoknak.

– Hol vannak még hasonló ütközések a nyilvános és a titkolható adatok között?

– Létezik egy átmeneti kategória: a közérdekből nyilvános adat. Alapesetben a személyes adatok közé tartozik a fizetés, javadalmazás is: a dolgozón és munkáltatóján kívül senkinek semmi köze sincs ahhoz, hogy ki mennyit keres. Ugyanakkor egyes állami hivatalnokok javadalmazása – mivel az is közpénzből megy – már nyilvánosságra hozható. Erről már bírósági ítélet is született: a Társaság a Szabadságjogokért pert indított és nyert a Magyar Hivatalos Közlönykiadó ellen, mert az nem volt hajlandó elárulni, milyen juttatásban részesülnek szerkesztőbizottságának tagjai. De említhetnénk a Miniszterelnöki Hivatal kommunikációs stábjának példáját is, ahol szintén nyilvánosságra kellett hozni a kifizetett pénzek nagyságát.

FOTÓ: IT-SECURITY

Van még egy érdekes eset: amikor valamilyen jogellenes tevékenységet igyekeznek az üzleti titok védőernyője mögé rejteni. Volt olyan cég, amely a környezetet erősen szennyezve veszélyes vegyi hulladékot ásott el a Hortobágyi Nemzeti Parkban. Amikor felvilágosítást kértek a cégtől, hogy mégis, hova miből mennyit ásott, arra hivatkozva akarta megtagadni a választ, hogy ez az üzleti titka, mert ebből következtetni lehetne például a termelési volumenére. Jogilag ez természetesen nonszensz: könnyen belátható, hogy egy jogellenes cselekmény nem képezheti üzleti titok tárgyát.

– Arra van-e valamilyen kötelező érvényű jogi szabályozás, hogy miként alakítja ki belső információvédelmi és hozzáférésjogosultsági rendszerét egy vállalat?

– Abba nem szólhat bele külső fél, hogy a cég működése során keletkezett belső vállalati adatok esetében hogyan szabályozzák a hozzáférési jogosultságokat a szervezetek. Ez alól csak az ügyfelekről gyűjtött személyes adatok jelentenek kivételt. Azok esetében van egy fontos előírás, a célhoz kötöttség: előre meg kell mondani, hogy mire gyűjtik be az adatokat, és csak arra szabad azokat felhasználni. Ez a kötelezettség persze csak a cég egészére vonatkozik, így a szervezetnek magának kell arról gondoskodnia, hogy a szervezeten belül is csak az férjen hozzá ezekhez az adatokhoz, akinek a munkájához szüksége van rájuk.

Egy jogellenes cselekmény nem képezheti üzleti titok tárgyát

Érdekes módon ez egy olyan terület, ahol többnyire egybevágnak az adatkezelésre vonatkozó előírások és az üzleti élet farkastörvényei. Amikor az IT-biztonsági támadások többségét vállalaton belülről követik el, akkor a cégeknek is elemi üzleti érdekük, hogy a belső jogosultsági rendszer szegmentált legyen, mindenki csak a szükséges és elégséges mértékben férjen hozzá az adatokhoz. Így kerül a lehető legkevesebb, potenciálisan „veszélyes" (kiszivárogtatható, ellopható) adat a felhasználók, dolgozók birtokába.

– Mi a helyzet a kereszt-értékesítéssel? A vállalatok óriási pénzeket fektetnek be olyan informatikai megoldásokba, amelyek lehetővé teszik az ügyfelek adatainak „összefésülését", hogy az eddigi tapasztalatok birtokában új termékeket tudjanak neki eladni; ez viszont ellentmondani látszik a célhoz kötöttség elvének.

– Addig ezzel rendszerint nincs is probléma, amíg az adatok vállalaton belül maradnak. Az viszont már problémásabb, ha ugyanahhoz a tulajdonosi körhöz tartozó bank, biztosító vagy brókercég osztja meg egymással az ügyfelek személyes adatait. Hiába tartoznak ugyanahhoz a tulajdonos körhöz, jogilag külön vállalatnak számítanak, és úgy vonatkoznak rájuk az adatkezelőkre előírt jogszabályok, vagyis nem adhatják át egymásnak az adatokat. Persze nem vagyok naiv, tudom, hogy létezik a gyakorlat, de ez ettől még nem lesz törvényes.

– A technológia fejlődésével semmi akadálya nincs annak, hogy egy Magyarországon működő vállalat központi rendszereit például Indiában üzemeltessék. Nem kizárt, hogy ezek a rendszerek személyes adatokat is kezelnek; ilyenkor milyen előírások vonatkoznak rájuk?

– Minden attól függ, hogy hol van az adatközpont. Ha az Európai Gazdasági Térségen belül van (ami az EU-n kívül felöleli Svájcot és Norvégiát is), akkor olyan, mintha Magyarországon lenne, és ugyanazok a szabályok vonatkoznak rá, ugyanazok az adatkezelő kötelességei és az alanyok jogai.

Van aztán néhány ország, amely megkapta az úgynevezett adekvát védelmi státuszt az EU-tól: Kanada, Argentína, a Csatorna-szigetek és néhány kisebb állam. Itt is gyakorlatilag ugyanezek az elvek érvényesülnek.

A harmadik csoportba tartozik az összes többi ország, élükön természetesen az Egyesült Államokkal, amellyel kapcsolatban ez a kérdés a legtöbbször felmerülhet. Ezek a személyes adatok kezelése terén nem felelnek meg az EU normáinak, és ezért van is korlátozás velük szemben. Így aztán műszakilag-informatikailag bármennyire is könnyen megoldható, hogy egy személyes adatokat kezelő szervert az Egyesült Államokban vagy a világon bárhol üzemeltessenek, a magyar és az EU-jog alapján ezt nem lehet minden további nélkül megcsinálni.

Ilyenkor az a megoldás, hogy az adatkezelésben érintett felek – például a hazai leányvállalat és az anyacég – adatvédelmi szerződést kötnek, amely tisztázza a felelősségi viszonyokat.

Ha viszont egy külföldi cég, szervezet Magyarországon kezeltet adatokat, akkor az itteni törvények vonatkoznak rá, bárhol is legyen a vállalat központja.

Schopp Attila

Szigorúan bizalmas!

Az információk titkosításának igénye gyakorlatilag egyidős az írással. Nagyjából időszámításunk előtt 1900-ra datálható az első olyan emlék, amelyet egy egyiptomi sírkamrában találtak, és amely arra utal, hogy szándékosan megváltoztattak egy üzenetet – azzal a céllal, hogy csak a címzett értse meg.

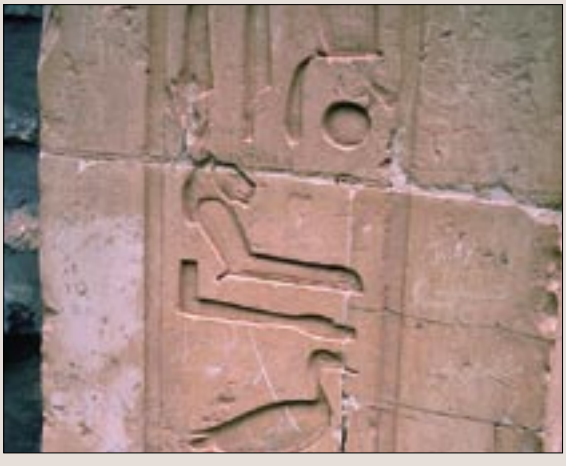
A magyar nyelvben a „titkosítás” szónak több jelentése van. Az egyik alapvető fogalomkör, a „klasszifikáció” szerint valamilyen szempontból bizalmasnak tartott adatok titkossá nyilvánítását és a hozzáférések fizikai és/vagy szabályokkal – akár törvényekkel – előírt korlátozását jelenti. Más – ebben az írásban tárgyalt – vonatkozásában azoknak a „kriptográfiai” (kriptosz – görög: rejtett) eljárásoknak az összessége, amelyek az információk technológiai értelemben vett kódolására vonatkoznak.

Alapok

A kriptográfiai módszerek tudománya – a kriptológia – bizonyos vonatkozásaiban az emberiség egyik legbriliánsabb intellektuális vívmánya. A cél kezdettől olyan rendszerek kifejlesztése volt, amelyekkel el lehetett érni, hogy a feladó úgy készíthesse el – kódolhassa – az üzeneteit, hogy azokat csak a címzett tudja elolvasni. Ugyancsak a kezdetektől sokaknak fűződött hozzá érdekük, hogy ezekben a rendszerekben megtalálják azokat a réseket, amelyeket kihasználva fel tudják törni az elfogott titkosított üzenetek kódját. A két törekvés közti ellentét és az egyre „magasabb” matematikától kölcsönzött módszerek az idők során oda vezetettek, hogy a kriptológia már a múlt század elejére is jócskán meghaladta az egyszerű halandók képességeit, a fejlett számítógépes technológiák pedig eszközként betöltött és motivációs szerepük miatt elképesztően bonyolult – és elegáns – titkosítási és kódfejtési módszerek kialakulásához vezettek.

Története során a kriptológia számos szociális, politikai, katonai, üzleti, személyes és más aspektusból is fontos fogalomkör lett.

Elnökválasztási, pénzügyi és harctéri sikerek múlhatnak rajta, vagy éppen az átlagpolgár bankszámlája bánja, ha valakinek sikerül hozzáférnie a – titkos – személyes és banki információihoz. Márpedig az internet megjelenése óta számos bizalmas adat utazik olyan publikus csatornákon, amelyekhez bárki hozzáférhet, és ebben a közegben különösen fontos, hogy az érzékeny adatok rejtve maradjanak az avatatlanok elől.



Egyidős az írásbeliséggel

A kriptológián belül a kriptográfia maga az a titkosító eljárás, amellyel egy információt kódolnak. A kriptológia „ellentudománya” a kriptanalízis; ennek törekvése az ismeretlen módszerrel kódolt, ismeretlen tartalmú információ feltörése. A titkosított üzenet információs egysége a kód vagy sifre. A kódban a betűk, számok, jelek vagy szavak más betűket, számokat stb. jelentenek. A legegyszerűbb kódolásnál egy szám vagy egy betűsorozat helyettesít egy szót vagy kifejezést – például a 47635 kódszám helyettesítheti a „Lánchíd” szót vagy a oierutz kódszó jelentése lehet „Megjött a tavasz”.

A legtöbbször azért kódolnak valamit, hogy titkosítsák, de néha csak azért, hogy lerövidítsenek gyakran használt kifejezéseket – példa: veár = „vásárolj ezer álomrészvényt”.

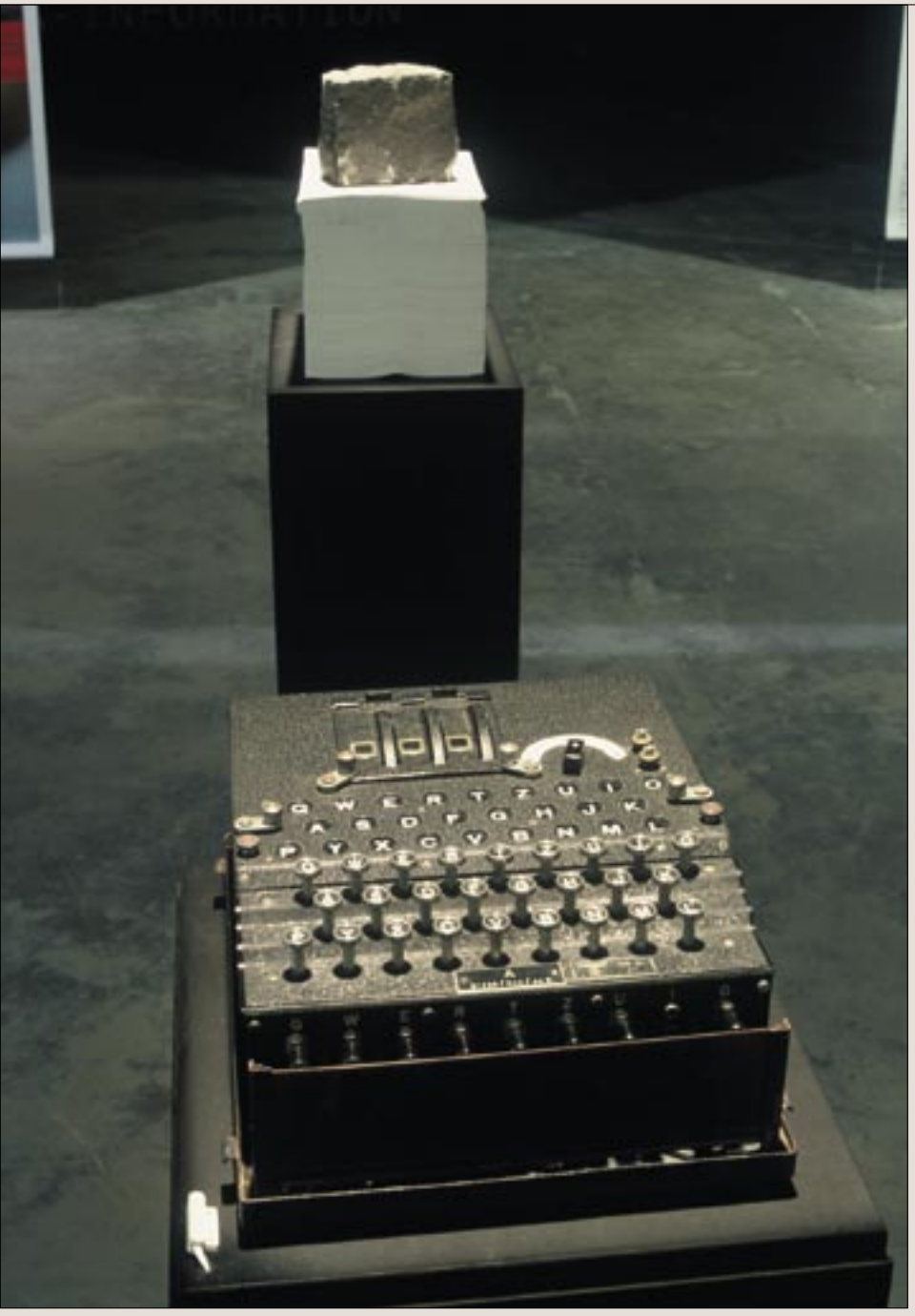
A valamilyen nyelven megírt eredeti, titkosítatlan üzenet a sima szöveg (plaintext), a titkosított változata a rejtjelezett szöveg (ciphertext).

Egy szöveges információt alapvetően kétféleképpen lehet titkosítani:

Transzpozíciós módszer. Ebben az esetben egy előzetes megegyezésen alapuló szisztéma szerint átcsoportosítjuk az adatokat hordozó szavakat vagy betűket. Ha két személy megegyezik abban, hogy egymásnak írt leveleikben minden szót visszafelé írnak le, akkor az eredetileg „menj el dolgozni” kifejezésből „jnem le inzoglod” rejtjelezett szöveg lesz.

A teljesség igénye és magyarázat nélkül íme néhány transzpozíciós módszer: oszlopos, geometriai, sorompó- és irányított transzpozíció.

Szubsztitúció. Ilyenkor az eredeti üzenet betűit, számai más jelekkel helyettesítik. Ha egy egyszerű titkosírásban mondjuk az A, B, C, D… betűk helyett rendre a betűsorozat végéről visszafelé elővett z, y, x, w… párjaik állnak, akkor a „wzx” jelentése „dac”. A szubsztitúcióra is számos módszer alakult ki, a monoalfabetikus szubsztitúciónál például egy jelet egy adott másik jel helyettesít, a polialfabetikus formánál több szimbólum fejez ki egy betűt vagy számot.



A nagy elől, az Enigma

A sima szöveg a (be)kódolás (encode, encrypt) során alakul át rejtjelezetté, a titkosított információból pedig a visszafejtés vagy dekódolás (decrypt, decode) során lesz titkosítatlan tartalom. Mindkét tevékenység egy vagy több kriptológiai algoritmus szerint történik.

A titkosító módszerek többnyire kulcsot (key) használnak: ez az a – gyakran önmagában is titkos – kritikus információ, amelyet az algoritmusok paraméterként használva aktuálisan működnek. Ha a kriptográfiában több entitás is részt vesz – azaz valaki nemcsak saját felhasználásra titkosít –, akkor a több félnek kiosztott algoritmust protokollnak nevezik.

Ha egy adott kommunikációs folyamathoz nem kódolják az információt, akkor az „tiszta szöveg” (cleartext) formájában továbbítódik.

A titkosítás speciális formájánál, a szteganofráfiánál maga az információ nincs kódolva, de úgy csomagolták be, hogy a csomagolás gondoskodjon az elolvasás megnehezítéséről. Erre példa, amikor lefényképezik az üzenetet és szabad szemmel olvashatatlanná – szteganogrammá – kicsinyítik.

A digitális világ

A számítógépes kriptográfiai módszerek közvetlen elődei azok a tárcsás titkosítógépek voltak, amelyeket a 20. század elején találtak fel – egyik legismertebb és legkifinomultabb képviselőjük a németek által a II. világháborúban használt híres-hírhedt Enigma.

Az ezek talaján a múlt század közepétől kifejlődő digitális módszerek az addigiaknál nemcsak – a főleg mennyiségi változást jelentő – bonyolultabb eljárások kidolgozását tették lehetővé, hanem a binárisan tárolt adatok és a bitműveletek miatt minőségileg is új technológiák alakulhattak ki. Az egyik lényeges változás tehát az, hogy míg a hagyományos kriptológia szó, karakter vagy jel alapú tudomány, addig az elvontabb számítógépes eljárások a jelek bitformátumú leképezéséhez is hozzáférnek. A másik döntő mozzanat, hogy túlzás nélkül kijelenthetjük: a számítógépes környezetben alkalmazott kriptológia lett az informatikai biztonság alappillére, hiszen közvetlenül kapcsolódik hozzá az információbiztonság, a hitelesítés, a hozzáférés-kezelés és a hálózatbiztonság – hogy csak a legfontosabbakat említsük.

Míg a klasszikus kriptológiának fontos aspektusa volt a nyelvészet, addig a digitális kriptológiához olyan matematikai problémák kapcsolódnak szorosabban, mint az információelmélet, a műveletek bonyolultságának elvont tudománya, a statisztika, a kombinatorika, az absztrakt algebra és a számelmélet.

Tipikusan a digitális kriptológiánál szokás emlegetni még egy fogalmat, a kriptográfiai lenyomatot vagy kivonatot (hash), amelyet egy függvény úgy állít elő a tetszőleges hosszúságú kódolatlan szövegből, hogy abból fix hosszúságú, csak az adott szövegre jellemző eredmény keletkezik. A lenyomat alkalmas az információ hitelességének és épségének a vizsgálatára.

Kriptológiai rendszerek

A definíció szerint a kriptoszisztéma „olyan kriptológiai algoritmusok/protokollok – és adott esetben kulcskezelő mechanizmusok – összessége, amelyek va-

lamilyen alkalmazás keretei között támogatják azok használatát". Ezeket a struktúrákat több szempont szerint lehet osztályozni; a legelterjedtebb csoportosítás a titkosító kulcshoz való viszonyuk alapján különbözteti meg őket:

A cd-rom is titkosítandó

- a kulcsnélküli rendszerek nem használnak titkos paramétert/kulcsot;
- a titkos vagy privát kulcsú rendszerek működéséhez egy olyan titkos paraméterre van szükség, amellyel az összes résztvevő entitásnak rendelkeznie kell;
- a publikus kulcsú rendszerek olyan titkos paramétereket használnak, amelyeket a résztvevők nem osztanak meg egymással.

Az elméleti alapokból térjünk át az informatikai gyakorlatra. A témakör számos vonatkozásával foglalkoztunk, és még foglalkozunk is majd későbbi írásainkban. A továbbiakban néhány olyan gyakorlati kérdéskört tekintünk át, amelyek aktualitásuk vagy egyéb ok miatt érdekesebbek lehetnek.

Szervezeti titkosítás

A Privacy Rights Clearinghouse becslései szerint jelenleg a különböző szervezeteknél tárolt személyes adatok harmada van kitéve valamilyen kockázatnak. Lehet hibáztatni a hackereket és a gondatlan alkalmazottakat, de a fő ok, hogy maguknak a szervezeteknek vannak problémáik az adatok titkosításával. Márpedig ez nemcsak a fogyasztókat és a szervezetek jó hírnevét sodorja veszélybe, hanem manapság már törvénytelen is.

Sajnos sok esetben a szoftverek és más biztonsági eszközök sem nyújtanak megfelelő segítséget. Ettől függetlenül a szervezeteknek minden olyan adatot, amely alkalmas személyek, csoportok, szervezetek vagy bármilyen entitás azonosítására, védeni kell a jogosulatlan hozzáféréstől a létrehozása, forgalmazása, a rajta végzett műveletek és a tárolás során. Ebben a tekintetben nem fogadható el semmilyen kompromisszum. Különösen áll ez azokra az információkra, amelyek valamiért megbízhatatlan közegbe – internetre, hordozható eszközökre, laptopokra, USB-memóriákra, stb. – kerülnek, de még a biztonsági mentéseket is titkosítani kell!

Még a minimalista megközelítés esetén is feltétlenül titkosítandók a következők:

- vezetékes és vezetéknélküli adatátvitel;
- merev- és hajlékonylemezek;
- cd-rom és dvd;
- a biztonsági mentés médiája (szalag, worm stb.);
- elektronikus levelezés, gyorsüzenő és még az amúgy üldözendő P2P-rendszerek is;
- PDA-k és laptopok;
- cserélhető háttértárak – USB-memóriákat is beleértve;
- adatbázisok.

A titkosítás mellett erős hozzáférés-kezelő mechanizmusokat kell használni, amelyek további védelmet biztosítanak a kritikus adatoknak.

A titkosítási szabályzat

A titkosításra olyan megoldásokat kell keresni, amelyek adott körülmények között a legjobban megfelelnek a szervezet és a fogyasztók igényeinek. Mielőtt azonban ezeket munkába állítanánk, le kell fektetni a titkosítási szabályzatot. Ennek ki kell térnie az operációs és felügyeleti lépések mellett a felelősség kérdéseire, és figyelembe kell vennie a lehetséges konzekvenciákat is. A szabályzatnak tartalmaznia kell azt a vállalást is, amely adatszivárgás észlelésekor a jelentési kötelezettségekre vonatkozik – ezt a tárgykört egyébként is egyre inkább törvényekkel szabályozzák (a mondat első feléből az is következik, hogy az adatvesztést érzékelő monitorozó eszközöket is használni kell).

A titkosítás témaköréhez csak lazán kapcsolódik, de bizonyos esetekben szükség lehet adatok megsemmisítésére, és ezekre az esetekre is le kell fektetni a megfelelő szabályzatokat.

Eszközök

Sajnos nincs olyan megoldás, amely minden titkosítási igényt egymaga képes lenne kielégíteni. Az Egyesült Államok Szabvány- és Technológiaügyi Hivatalának (NIST) vannak erre vonatkozó ajánlásai. Ezekhez már csak azért is érdemes igazodni, mert – noha elsősorban az amerikai kormányzati intézményekre vonatkoznak – a többszörösen kipróbált és javasolt módszerek más országok és más területek szervezetei számára is hasznosak lehetnek. Maguk az eszközök öt fő kategóriába sorolhatók.

Az NIST kriptográfiai eszközökkel foglalkozó honlapja – *http://csrc.nist.gov/CryptoToolkit*
Teljeshháttértár-titkosító eszközök – *http://www.full-disc-encryption.com/Full_Disc_Encryption.html*

Állomány- és könyvtárszintű titkosítás. A logikai fájlszerkezetben szereplő állományok adatait védi. A védelem lehet a háttértár adatainak „on-the-fly" folyamatos titkosítása, vagy megvalósulhat jelszóval védett archívumok formájában. Kiterjedhet az összes állományra,

vagy korlátozni lehet bizonyos fájlokra. A téma szakértői szerint a fájlszintű titkosítók a legfejlettebbek, és ennek megfelelően az ilyen típusú protokollok – 3DES, AES, Diffie-Hellman, Blowfish, RSA stb. – a legérettebbek.

A könyvtárszintű titkosítók elvileg teljes könyvtárakat kódolnak, de a gyakorlatban ezek az eszközök is legtöbbször a mappák állományait egyedileg titkosítják.

A fájlszintű titkosítók gyakori gyengesége, hogy noha az értékes információk titkosítottak, a műveletekben sima szövegként szerepelnek, ezért visszamaradhatnak a rendszerben olyan ideiglenes állományok, amelyekből a titkosítatlan tartalmuk kinyerhető – ezen segítenek az önállóan is használható teljeskötet- és partíciótitkosítók, illetve a médiaszintű megoldások.

Teljeskötet- és partíciótitkosító, valamint médiaszintű megoldások. Ezek a legerősebbként számon tartott kódoló eszközök vagy a teljes adathordozót titkosítják, vagy pedig folyamatosan kódolják a tárolandó adatokat. A lehetőségek használhatók önálló alkalmazásként, lehetnek az operációs rendszer részei, de hardverszinten is megvalósíthatók – utóbbit egyre erőteljesebben támogatják a háttértárak és különösen a szalagos háttértárak fejlesztői is.

Mezőszintű és adatbázis-titkosítás. A kettő szorosan összefügg, amennyiben az adatbázisok titkosítása mezőszinten történik. Magukat az adatbázisokat lehet soronként vagy oszloponként is kódolni, de tipikusan az elemenkénti titkosítást részesítik előnyben. Az eljárás transzparensen, „röptében” működik: a tárolt adatok a művelet előtt automatikusan titkossá válnak, visszaolvasáskor pedig dekódolódnak. Ez persze jól bezavar az indexelésbe és a lekérdezésekbe – éppen ezért fontosak a mezőszintű technológiák. Utóbbiakból egyébként nem nagyon készítenek önálló, a teljes rendszer többféle adatbázisán használható terméket, hanem az adatbázismotorok fejlesztői maguk szolgáltatják azokat saját megoldásaik mellé (vagy egyedi programozásra van szükség).

Nő a kulcstároló hardverek szerepe

A kommunikáció titkosítása. Sokszor hangoztatott doktrína, hogy a nem biztonságos hálózaton – interneten – utazó adatokat védeni kell, de ez még a szervezeti hálózaton belüli forgalmazásra is igaz. A weben meghonosodott az SSL/TLS szabvány, a szervezeti hálózatokon és a VPN-ekben a leggyakoribb az SSL, SSH és az IPSec. A levelezésbiztonságról – figyelem: a „normál” levelezésen semmilyen titkosítás sincs! – a PGP vagy az S/MIME segítségével lehet gondoskodni, és természetesen védeni kell az üzenőrendszereket is.

Ha egy rendszer több platformján és sokféle eszközén kell az összes adatot megvédeni, akkor holisztikus megoldásokra van szükség. Jelenleg tökéletes, az összes felsorolt pontra érvényes megoldást nem nagyon lehet találni, de olyanok léteznek, amelyek képesek bizonyos területek kombinációit lefedni.

Egy dolgot mindenképpen tartsunk szem előtt: érdemesebb az összetettebb feladatokat ellátó eszközöket választani, mert könnyebb a karbantartásuk, és a költségek is kisebbek.

A királyság kulcsa

A titkosítóeszközöket sokféle szempont szerint lehetne tovább osztályozni, például a kódolás/dekódolás helye és az ahhoz használt kulcsok kezelése alapján. A szoftveres megoldások a számítógép memóriáját használják, a hardveres lehetőségek vagy saját operatív tárral rendelkeznek, vagy olyan memóriaterületeket használnak, amelyeket csak ők érnek el.

Számos termék a védett számítógépen tárolja a kulcsot. Ebben az esetben a kulcsok további – jelszavas vagy hardveres – védelmére van szükség. Manapság egyre nagyobb a kulcstároló hardvereszközök – okoskártyák, USB-tokenek – szerepe. Előnyük, hogy erős, kétfaktoros azonosítást tesznek lehetővé. Hasonlóan elterjedőben vannak a TPM-lapkák, amelyek a számítógépek alaplapján tárolják a kriptográfiás kulcsokat, és meglehetősen ellenállók a szoftveres támadásokkal szemben.

EFS és IPSec

Reményeink szerint nem önkényes választás, ha elterjedtségük és aktualitásuk okán a továbbiakban a Windows-rendszerek néhány konkrét vonatkozását tekintjük át.

A hálózatokon tárolt adatok titkosítására akkor is szükség lehet, ha a rend-

ESZKÖZHIÁNY

Az elmúlt két évben annyi érzékeny adatokat tartalmazó IT-eszközt veszítettek vagy loptak el, hogy szinte naponta lehetett hallani tudósításokat incidensekről.

Az Egyesült Államok Kereskedelmi Minisztériumának tavaly szeptemberi statisztikái szerint 1138 laptopot loptak és vesztettek el, vagy egyszerűen csak nem találnak a hivatalnak és szövetségi fiókszerveinek 30 ezer darabos táskagép-állományából. Az utolsó öt évre vonatkozó jelentés szerint a hiányzó eszközökből 249 tartalmazott érzékeny információkat, de a beszámoló szerint állítólag ezek valamilyen formában titkosítva vagy védve voltak.

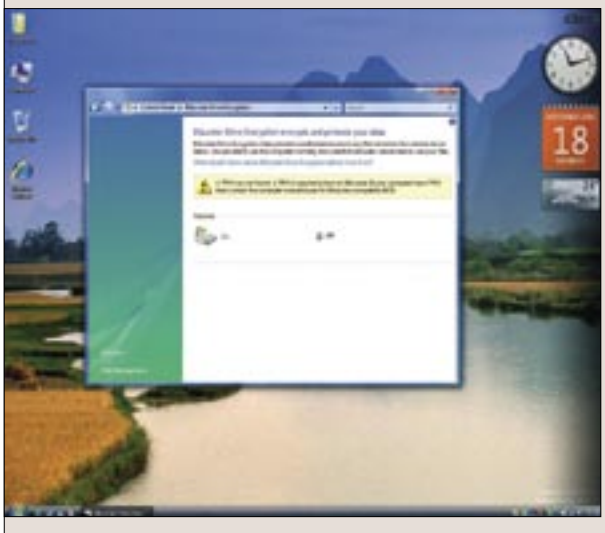
A hordozható IT-eszközök – USB-meghajtók, mobiltelefonok, PDA-k, laptopok, stb. – „közkedvelt” elvesztési helye a taxik hátsó ülése. A PointSec szerint csak a tavalyi év második felében és csak két amerikai nagyvárosban (San Francisco, Washington) összesen 12 ezer ilyen jószágot sikerült az utasoknak ottfelejteniük a kocsikban.

Egy Londonra vonatkozó hasonló felmérésből kiderül, hogy 2006 második félévében 55 ezer telefont, 5000-nél több PDA-t, 3000-nél is több laptopot és ezernél több USB-memóriát hagytak az utasok ugyancsak a taxikban, ami azt jelenti, hogy a taxizás jó üzlet lehet, mert például egy átlagos, a brit fővárosban tevékenykedő taxis évente két táskagépet vihet haza.

szer peremén minden szükséges óvintézkedést megtettünk a külvilág és a hackerek kíváncsiskodása ellen. Sokszor leírtuk már, hogy a belső védelem legalább ennyire fontos – azaz alapesetben szükség van bizonyos érzékeny információk titkosítására, hogy azokat ne érje el minden felhasználó. A modern Windowsok – a 2000 és az újabb változatok – megjelenésével az ezekhez szükséges eszközök bekerültek magába az operációs rendszerbe.

Az alkalmazott védelem miléntje az adatok állapotától függ. A tárolt adatok titkosságát az EFS (Encrypting File System) használatával érhetjük el, de ez nem képez védőburkot a forgalmazott adatoknak; azok tranzit közben olvashatókká válnak. A hálózatot figyelő eszközök elől az IPSec segítségével rejthetjük el az információkat, de az IPSec nem titkosítja a tárolt adatokat.

Noha maga a platform már rendelkezik ezekkel a titkosító képességekkel, több tényező miatt is kevesen élnek velük. Az egyik nyilvánvaló okot – a teljesítménycsökkenést – akkor tapasztaljuk, amikor a kettőt együtt használjuk: a rendszer érezhetően lelassul. A lassulás mértéke több faktortól függ – a hardvertől, a hálózat áteresztőképességétől, a titkosítás mértékétől –, de mindenképpen érezhető. Más kérdés, hogy az adatok kritikus volta esetén néha még a hosszú szüneteket is el kell viselni.



BitLocker – kiküszöböli a hiányosságokat

Maga az IPSec más protokollok együttese és két lehetséges működési módja a tunnel (csatorna) és a transzport üzemmód. Röviden: a tunnel mód a hálózatok (szerverek) közötti kommunikációra használatos, és ezt használják a VPN-ek is – ekkor az adatcsomag és az IP-fejléc is titkos. A transzport mód a hálózaton vagy csatornákon belüli forgalom titkosításakor működik, és ebben az esetben csak az adatok titkosak.

PER A BÖRTÖNBŐL

Idén márciusban egy többszörös fegyveres bűnelkövetés miatt letartóztatott férfi a rács mögül perbe fogta a Microsoftot és üzleti partnereit. *Michael Alan Crooker* szerint a szoftvercég és társai által reklámozott titkosítási képességeknek meg kellett volna akadályozniuk, hogy az FBI ügynökei lefoglalt számítógépén hozzáférjenek személyes állományaihoz. Mivel a hatóságok a titkosítás ellenére – féléves kemény munkával – megtalálták Crooker és barátnője közös szexvideóit és félreérthetetlen jeleit annak, hogy gyakran látogat pornóoldalakat, ezért a jóember azt nehezményezte, hogy „nagyon megszégyenült a nyilvánosság előtt".

További meglepő – de nem igazolt – fejlemény (pletyka?), hogy Crooker állítólag előzőleg már peren kívül megegyezett a gép szállítójával, mert az FBI-osok által feltört titkosító rendszert a cég szállította a számítógépéhez. Annyi mindenesetre bizonyos, hogy a per rövidre sikeredett, mert a bíróság három napon belül elutasította a megszégyenült rab vádjait.

A tárolt állományok fájlszintű titkosításának lehetőségét az EFS kínálja. A technológia a Windows 2000-ben történt bevezetése óta markáns átalakuláson ment át, de a lényeg minden változatnál az, hogy bekapcsolt állapotában transzparensen – azaz a felhasználó számára észrevétlenül – védi a tárolt állományokat, és végzi azok titkosítását tároláskor, illetve visszafejtését olvasáskor. Az EFS publikus kulcsú titkosítást (PKI) használ, és a gyakorlatban elég jó védelmet kínál, de mivel a kulcs szóló gépeken a felhasználó bejelentkezési adataiból származik, ezért „bruteforce" (nyers erős) támadásokkal lassacskán felőrölhető. A Vista megjelenésével ez a helyzet erőteljesen javult, amennyiben a felhasználók sokkal biztonságosabb okoskártyás bejelentkezése és a kártyán vagy USB-memórián tárolt kulcs használata is támogatott.

Két megjegyzés viszont idekívánkozik. Tévhit, hogy az EFS-t csak komplett PKI-szisztéma, azaz tanúsító szolgáltatások (CA) elérhetősége mellett lehet használni. Ha van ilyen a rendszerben, akkor használható az is, egyébként a rendszer a felhasználó azonosítóiból generálja az „öntanúsított" (self-signed) kulcsot.

Mint már írtuk, szóló gépeken lehetséges a nyers erős támadás, de EFS-titkosított média adatainak kinyeréséhez mindenképpen kellenek a kulcsok, ezért mondjuk a gépből kivett merevlemez titkosított adatainak kinyerése legalábbis nehézségekbe ütközik.

EFS és BitLocker

Ha már a Vistánál tartunk: az adatok titkosításának területén a platform más újdonságokkal is szolgál. Ezek legfontosabb képviselője a BitLocker – Vista Enterprise és Ultimate kiadások –, amely többféle (választható) üzemmódban működő teljes merevlemez-titkosítási lehetőségként képes az adatok merevlemezre írásakor a titkosításra, visszaolvasáskor pedig a dekódolásra. A BitLocker különösen az utóbbi időszak laptopelvesztési vagy -eltulajdonítási incidenseit tekintve hasznos védelmi lehetőség. A két képesség együttes használatával jól le lehet fedni a tárolt adatok titkosítási igényeit.

Az EFS nem nyújtott védelmet a rendszerkötet, a lapozófájl, az ideiglenes, de még a törölt állományok elérése ellen sem, márpedig ezekből korántsem túl bonyolult eszközökkel hasznos információkat lehet kibányászni. A BitLocker ezeket is védi.

- Az EFS csak a Windows betöltése után kezd el működni, a BitLocker az operációs rendszer szintje alatt, azaz már betöltés előtt is működik.
- Az EFS fájlszinten, a felhasználó engedélyein, hozzáférésén vagy a rendszerben élő tanúsító szerver információi alapján működik, a BitLocker alacsonyabb szintű és ezektől független mechanizmus – ez persze azt is jelenti, hogy az EFS jobban kézben tartható, de a BitLocker azokat a foltokat is lefedi, amelyeket az EFS nem.
- Az EFS-sel titkosított állományok nem fejthetők vissza, a BitLockerrel titkosí-

tott kötetekben az állománynevek még csak nem is látszanak.
- A BitLocker kisebb gyengesége, hogy a hibernált vagy felfüggesztett állapotból felélesztett PC szabadon hozzáférhető, mert ekkor a mechanizmus nem figyeli a kulcsot.
- Kisebb gyengeség az is, hogy a BitLocker csak a rendszerkötetet titkosítja, a többit nem – erre viszont ott van az EFS.
- A Microsoft szerint a BitLocker használata 9-11 százalékos teljesítménycsökkenéshez vezet. Ettől sokan tartanak, de mindenkit megnyugtatunk: több felhasználó és saját szubjektív tapasztalataink alapján a napi munkában ezt nem lehet megérezni – és egyébként is: ennyit megér.

Összefoglalva: a magát a Windowst, a lapozófájlt, az ideiglenes állományokat és általában a rendszerkötetet titkosító BitLocker kiküszöböli azokat a hiányosságokat, amelyek az EFS használatából fakadhatnak. A felhasználó/PKI központú EFS – amely a Vista esetében a külső okoskártyás és USB-kulcsok használatát is támogatja – biztosítja a többi logikai meghajtó titkosítását, miközben támogatja a szervezeti szintű menedzselhetőséget. A két képesség együtt betonbiztos védelmet kíván az asztali PC-k, de főként a laptopok bizalmas adatai számára.

Titkosítási gondok

„A titkosítás könnyű, a kulcskezelés nehéz” – a titkosítás létezik, használni kéne, de számos esetben az idézethez hasonló szállóigék szellemében problematikus az alkalmazása. Zárszóként közreadjuk Anton Chuvakin takaros csokorba szedett gondolatait a titkosítás körüli mizériákról.

A titkosítás könnyű és elfogadott, mégsem használják. Az internetes adatforgalomban még ma is sokan az olyan „simaszöveg-protokollokhoz” ragaszkodnak, mint a telnet vagy az FTP. Ezekhez hasonlóan még a kritikus tranzakciókat bonyolító webalkalmazásokban is gyakori az egyszerű HTTP protokoll használata. Miközben a tárolt adatok titkosítása sok helyen már megoldott, annyival fontosabbnak tartják a kommunikáció biztonságánál, hogy az utóbbiról egyszerűen elfeledkeznek.

Saját titkosításra van szükség. A legtöbb programozó nem rendelkezik az ehhez szükséges képességekkel. A kriptológia a matematikához és a fizikához hasonló komplexitású tudomány, ezért mélyebb ismeretek nélkül megfelelő titkosító mechanizmust kitalálni képtelenség – arról nem is beszélve, hogy ezek már önmagukban is bonyolultak, ezért az implementációjuk is nehéz.

Kódolt titkok. Egy titkosító algoritmus minősége nem azon múlik, hogy mennyire titkos vagy publikus, hanem leggyakrabban a kulcskezelésen. Ha a kulcs avatatlan kezekbe kerül, a játéknak vége. Ha a kulcsot vagy a jelszót belekódoljuk az algoritmus implementációjába, akkor tálcán kínáljuk fel a támadónak. Az ilyen beágyazott kódok hosszú távon nem rejthetők el, és gyakran jártak fatális következményekkel – erre a legújabb példa a hd-dvd kódolásának visszafejtése.

Kulcsok tárolása az adatok között. Az adatbázis-titkosítás most éli a reneszánszát. Védjük meg az adatokat, titkosítsuk őket! Igen ám, de hová tegyük a kulcsot? Természetesen ugyanabba az adatbázisba – és kész a katasztrófa. A jelenség egyik „briliáns” változatában az egyik adatbázis titkosítására szolgáló kulcsot ugyanannak a szervernek egy másik adatbázisában tárolják.

Az adat-visszaállítás elhanyagolása. Ez a probléma a titkosítást az ellen fordítja, akinek a hasznát kéne szolgálnia. Hiába vannak nagyszerűen megvédve és titkosítva az adatok akkor, ha elvész a kulcs, és nem lehet visszaállítani az információkat. A kulcskezelés a titkosítás mellett az adatok visszaállításának alfája és ómegája. Az adattolvajok elleni védekezés csak félsiker, az adatokat a „jó” titkosítástól is meg kell védeni.

Kelemen László

Az USB-kulcs is támogatott

ADATOK A KUKÁBAN

Egy tanulmány szerint a háztartásokban rengeteg olyan dokumentumot és adathordozót hajítanak ki a szemétbe, amelyekből a bűnözők pénzszerzésre alkalmas azonosítókhoz juthatnak hozzá. A brit rendőrség és fogyasztóvédelmi szervezetek által tavaly megvizsgált 120 háztartás felében dobtak a kukába bűnözők által használható információkat. A szigetország lakosainak a becslések szerint évente 1,7 milliárd fontba kerülnek az azonosítóik birtokában elkövetett csalások.

Tavaly szeptember elején a J. P. Morgan Chase Card Services vezérigazgatója, *Rich Srednicki* bejelentette, hogy a vállalat által üzemeltetett Circuit City kártyarendszer 2,6 millió volt és jelenlegi felhasználójának az azonosítóit tartalmazó mágnesszalagokat véletlenül kukába hajították. Rich Srednicki szerint a titkosítatlan adatokat tartalmazó tekercsek zárt dobozokban voltak, és reményei szerint a bejelentéskor már minden bizonnyal bezúzták őket.

Képviselők noteszgéppel

Korábban arra ügyeltek a képviselők, hogy senki ne vehesse ki táskájukból a titkos dokumentumokat. Ma noteszgépeikre vigyáznak, az azokon tárolt adatok védelmét különféle hardver- és szoftvereszközök látják el. Természetesen a képviselők közreműködésével.

A 2002–2006-os ciklus országgyűlési képviselői első, HP Compaq Evo 410C noteszgépüket 2003 tavaszán vehették át. A 2006-os ciklusváltáskor az új távmunka-eszköz az IBM X60-as noteszgép lett.

Napjainkban a parlamenti munkát nagymértékben segítik a hordozható számítógépek; a noteszgépekkel távolról is hozzáférhetnek a képviselők a hivatal belső anyagaihoz, továbbá számottevően csökkent a papírfogyasztás. A bárhova elvihető, kívülállók – családtagok, munkatársak – számára is hozzáférhető noteszgépek azonban kockázatokat rejtenek magukban. Körültekintő biztonságpolitikára, megfelelő biztonsági intézkedésekre és rendszerekre van szükség ahhoz, hogy a szerveren, illetve a noteszgépen tárolt adatokhoz ne férhessenek hozzá illetéktelenek.

A múlt: chipkártyás azonosítás

A képviselők 2003 márciusában testreszabott gépeket kaptak kézhez, és csak négyórás oktatást követően vehették azokat használatba – kezdi az elején *Kertészné Gérecz Eszter,* a Parlament informatikai főosztályának vezetője. Többféle hálózati csatlakozási lehetőséget biztosítottak a noteszgépekhez, egyaránt lehetett tehát kapcsolódni a Parlament helyi hálózatához, analóg, digitális és mobiltelefon-hálózatokhoz, valamint a szélessávú internethez.

MÁS GÉPRŐL IS

Várhatóan a képviselők ez év szeptemberétől nemcsak saját noteszgépükről, hanem más eszközökről is elérhetik az Országgyűlés belső informatikai szolgáltatásait. Ehhez be kell vezetni a tokenek one-time passwordös szolgáltatását, amelynek feltétele, hogy néhány háttérszoftvernél a legújabb verziókra térjenek át.

Minden képviselő PIN-kóddal védett chipkártyával azonosította magát. A chipkártyás autentikációnál kikötötték, hogy a tanúsítvány privát része sohasem hagyhatja el a kártyát. A tanúsítvány generálását akkoriban kizárólag Microsoft-termékkel lehetett megoldani. Gyakorlatilag ekkor került be a Parlament informatikai rendszerébe egy Microsoft 2000-szerverpár a Novell Netware, a Solarison futó Oracle adatbázis-környezet és a Linux alkalmazásszerverek mellé.

Chipkártya nélkül elindult ugyan a gép, de az operációs rendszert csak az azonosítást követően lehetett elérni.

A képviselők nem kaptak rendszergazdai jogokat, azaz rendkívül korlátozott volt azoknak az eszközöknek és szoftvereknek a köre, amelyeket saját maguk installálhattak. Ezzel gyakorlatilag elhárult az a veszély, hogy a magas jogosultságot igénylő, internetről letöltött vagy ellenőrizetlen forrásból származó szoftverek, anyagok felkerüljenek a noteszgépre.

Az igényelt installálás vagy probléma esetén a szervizesek be tudtak lépni a noteszgépbe, de nem férhettek hozzá a titkosított képviselői adatokhoz.

Minden noteszgép eltérő, rendkívül erős szervizjelszót kapott, amelyeket páncélszekrényben őriztek.

A képviselői adatok védelmét központilag menedzselt F-Secure rendszer látta el a víruskereső, tűzfal- és FileCrypto moduljaival. Ha tehát valaki a merevlemezt esetleg kiemelte volna a noteszgépből, akkor sem férhetett hozzá az adatokhoz.

A chipkártyákat évente kellett érvényesíttetni. Ilyen alkalmakkor a képviselők a számítógéppel együtt jelentek meg az Informatikai Ügyfélszolgálaton, amikor mód nyílt a noteszgépek állapotának ellenőrzésére és egyéb képviselői igények kielégítésére is.

Az Országgyűlés Hivatala (továbbiakban Hivatal) biztosítást kötött a képviselői noteszgépekre. A szerződések értelmében a képviselőknek ebben a biztosításban önrészük volt.

MEGKÉRDEZTÜK A KÉPVISELŐKET

Valóban megkönnyíti-e a munkát, kiváltja-e a rengeteg nyomtatott dokumentumot a noteszgép, illetve találkoztak-e olyan problémával, amely a gépen tárolt adatok biztonságát fenyegette volna? – kérdeztük a képviselőktől. E-mailben elküldött kérdéseinkre csupán nyolcan válaszoltak ugyan, de az ő munkájukat egyértelműen segíti a noteszgép. Van, aki még nem szokott hozzá, hogy mindenhova magával vigye a noteszgépet, mások viszont éppen az eszköz mobilitását emelték ki, mondván: ezt tartják legnagyobb előnyének.

A noteszgépek bevezetése óta a nyomtatott dokumentumok mennyisége nagyságrendekkel csökkent; ezt mindenki egyértelműen üdvözli. Bizonyos esetekben azonban nem kerülhető el a nyomtatás. Előfordul például, hogy egy hosszabb tárgyalás alatt lemerül a noteszgép akkumulátora, így jobb, ha kéznél van a nyomtatott dokumentum is.

A képviselők nem érzik veszélyben a gépen tárolt adataikat, bár van, aki nem tenne fel minden érzékeny adatot a noteszgépére.

Problémaként jelezte az egyik képviselő, hogy amikor előző noteszgépének merevlemeze meghibásodott, minden rajta tárolt anyaga hozzáférhetetlenné vált. Egy másik képviselő, akinek munkájába már szervesen beépült a noteszgép, megjegyezte: öröme akkor lenne teljes, ha a jövőben a képviselői indítványokat is lehetséges lenne kizárólag elektronikus úton benyújtani.

Jöttek a tokenek

A 2002–2006-os ciklus végén minden képviselőnek le kellett adnia noteszgépét. „Egyrészt egységes, másrészt a hároméves tapasztalat birtokában korszerűbb és jobb műszaki paraméterekkel rendelkező, felhasználóbarátabb környezettel rendelkező gépparkkal akartunk nekivágni a következő ciklusnak. A HP Compaq Evo noteszgépeket felértékeltettük, és a korábbi ciklus országgyűlési képviselői a műszaki bizományi által megállapított áron megvásárolhatták azokat. Az eladandó gépekről mindent letöröltünk, majd az OEM Windows XP operációs rendszer és egyéb hozzáadott OEM-termékek mellé csupán egy ingyenes OpenOffice-t telepítettünk a noteszgépekre” – tájékoztat a váltás részleteiről *Tóth János* osztályvezető.

A képviselők véleménye szerint kényelmetlenséget okozott a többjelszavas bejelentkezés, ezért az új megoldás kidolgozásakor az SSO (single sign-on) irányába mutató eszközt kellett keresni. Továbbá többen igényelték, hogy ne csak saját noteszgépükről, hanem más távoli számítógépről is be tudjanak jelentkezni az interneten keresztül az Országgyűlés belső informatikai szolgáltatásaira. A lehetőségek feltérképezését követően a Hivatal tokenes megoldás mellett döntött.

A jelenlegi rendszerben tehát a chipkártya helyébe a noteszgép USB-portjához csatlakoztatható Aladdin E-token lépett. A token a tanúsítványon kívül a jelszavakat is tárolja. Magát az eszközt egy bonyolult, minimum 8 karakter hosszú jelszó védi. A képviselőknek csak ezt az egy kódot kell megjegyezniük.

Az Aladdin E-token eszköz rendelkezik egy kis kijelzővel, amely lehetőséget biztosít az OTP (one-time password) alapú beléptetésre is.

„A heterogén környezet nem kedvezett a valódi, szoftveres SSO-nak, viszont az egyjelszavas bejelentkezés a token hardveres jelszótárával a felhasználó számára egy kvázi-SSO funkciót nyújt" – fogalmaz Kertészné Gérecz Eszter.

Központi menedzsment

A gépparkot továbbra is központilag menedzselik. Ha a noteszgép rákapcsolódik a Hivatal informatikai rendszerére (LAN, VPN), automatikusan megkapja a szoftverfrissítéseket, a menedzsment-beállításokat, a legújabb vírusvédelmet stb. Ha egy bizonyos ideig (kezdetben 90 nap volt ez a határ, ma 150 nap) nem jelentkezik be a hivatali rendszerbe, akkor a gép kitiltja magát a rendszerből. Ilyenkor két dolgot tehet a felhasználó: vagy bemegy az ügyfélszolgálatra, vagy telefonon kér segítséget. Az utóbbi esetben, ha a felhasználó internetes kapcsolatot létre tud hozni, akkor megkapja az egyszeri bejelentkezési lehetőséget. Csatlakoznia kell a VPN-hez, hogy a gép megkapja a szükséges frissítéseket.

Időközben az F-Secure beszüntette a FileCrypto rendszert, ezért az IBM X60-asokra a SafeBoot Device Encryptiont telepítették, amely egyébként a korábbinál erősebb biztonsági megoldás. Ez a titkosító a BIOS-indítás után rögtön üzembe lép. A titkosító feloldása nélkül tehát be sem lehet indítani az operációs rendszert. Ha kihúzzák a kártyát vagy a tokent, a gép azonnal zárolódik. Ha működés közben egy bizonyos ideig senki sem használja a noteszgépet, akkor a gép automatikusan lezárja magát.

Érzékeny adatok kizárólag VPN-en

Az üléstermek rekonstrukciójával együtt 1998-ban megtörtént a vezetékes LAN kábelezése. Eleinte a végpontok nem „éltek", de 2003-ban a képviselők már rá tudtak csatlakozni noteszgépeikkel a hálózatra.

Az Evók még nem, de az új noteszgépek már gyárilag wifi-képesek. Noha az ülésteremben mindenki használhatja a vezetékes LAN-t, több bizottsági helyiségben erre nincs mód. Mivel a képviselők, parlamenti titkárok, minisztériumi szakértők munkájához ma már nélkülözhetetlen az internet, folyamatosan nő a wifi-vel lefedett területek nagysága.

A Parlamentben két wifi-alhálózatot alakítottak ki. Az egyik „kvázi publikus" elérésű, amelynek hozzáférési és használati szabályait a fő felhasználók – parlamenti titkárok, újságírók – részére megfelelő helyeken publikálják. E hálózatból nem érhetők el az országgyűlés belső informatikai szolgáltatásai, ám nincs akadálya a böngészésnek, az e-mailek küldésének, fogadásának.

A másik a képviselői wifi-alhálózat, amely szigorú szabályrendszer szerint működő, több szinten védett hálózat. Csak olyan eszközök csatlakozhatnak rá, amelyek a 802.11x szabvány szerinti tanúsítvánnyal igazolják, hogy a Parlament eszközei. A hálózat hozzáférési szabályai nem publikusak. Amikor egy jogosult gép belép a hálózatba, VPN-en kapcsolódhat a Parlament belső rendszeréhez.

Többféle kapcsolódási lehetőség

PAPÍRTAKARÉKOSSÁG

A noteszgépek bevezetését követően számottevően csökkent az Országgyűlésben felhasznált papír mennyisége. Míg korábban minden képviselőnek futárpostával küldték ki a lakására az aktuális dokumentumokat, addig 2004 szeptemberétől ez az eljárás gyakorlatilag megszűnt.

Időközben elkészült a futárposta elektronikus változata. Olyan internetes alkalmazásról van szó, amely mindig az aktuális üléshétre vonatkozó elektronikus dokumentumokra hivatkozik, és ezek között rendkívül könnyű eligazodást biztosít.

A képviselők oktatásakor kitértek a WLAN-ok, azokon belül is a nyilvános hotspotok biztonságos használatára is. A Parlament belső informatikai szolgáltatásai természetesen bármilyen külső WLAN-ról is elérhetők, de az is magától értetődő, hogy a kapcsolat kizárólag VPN-en keresztül épülhet fel.

Fizikai biztonság

A képviselők noteszgépeik fizikai biztonsága érdekében kérésre Kensington zárat kapnak, amellyel le lehet lakatolni a gépeket. A lakatok tartalékkulcsait páncélszekrényben őrzik.

Mivel a gép eltűnése önmagában is tetemes kárt okoz (nem beszélve a noteszgépen tárolt, védett, de nem mentett adatokról) a képviselőknek javasolják, hogy lakatolják le a noteszgépet, ha a legkisebb veszélyt is sejtik. A biztonsági szakemberek azt sem tartják túlzásnak, ha valaki a szállodai szobájában a fűtőtesthez lakatolja a noteszgépét.

Jó tanács az is, hogy a tokent és a kártyákat akkor is vegyék ki a noteszgépből, ha csak egy rövid időre távolodnak el a géptől. Ezzel nemcsak az adatokat, hanem az eszközök fizikai állagát is védik. Egy USB-kulcsot vagy egy kilógó kártyát ugyanis nagyon könnyű elgörbíteni vagy letörni.

Mallász Judit

Élni és visszaélni

Bizalmas adatok a weben és a keresőkben.

A Pallorium nevű internetes magánnyomozóiroda tulajdonosát, *Steven Rambamet* közvetlenül a tavaly júliusi Hope (Hackers of Planet Earth) konferencián tartandó értekezése előtt letartóztatta az FBI. Rambam az egyik Hope-delegátus, *Rick Dakan* engedélyével mindössze négy és fél órával a rendezvény előtt minden lehetséges és lehetetlen adatot – összesen 500 nyomtatott oldalnyi információt – összeszedett Dakanról úgy, hogy kizárólag az interneten keresgélt.

Az információk között volt Dakan biztosítási száma, életrajzi adatai – olyanok, amelyekre már ő maga sem emlékezett –, ismeretségi körének teljes felsorolása, közlekedési vétségei és még az is, hogy a barátai mikor és hogyan kerültek összeütközésbe a törvénnyel. A kutakodás az internetes magánszféráról tartandó előadásához szánt prezentáció része lett volna. Olcsó húzás lenne azon élcelődni, hogy biztos azért kapták el Rambamet, mert túl jól sikerült a keresgélés (egyébként tényleg jól sikerült). A bekasztlizás oka valójában egy korábbi, ettől az ügytől független eset volt, amelyben végül ejtették a Rambam elleni vádakat.

HOVÁ KELL CÉLOZNI?

Az amerikai elnök utazásaival és járműveivel kapcsolatos információkat mindig hétpecsétes titokként kezelik. Érthető hát, hogy a légierőnél jókora felfordulást okozott, amikor tavaly áprilisban kiderült: a két elnöki gép védelmi rendszereiről szóló információk – beleértve a rakétavédelmet és a testőrök ülésrendjét – voltak elérhetők az interneten. A sokáig látható dokumentumból az is kiderült, hová kellett volna célozni távcsöves puskával ahhoz, hogy felrobbanthassák az elnöki gép orvosi részlegének oxigéntartályát.

Kétélű fegyver

Az online keresők és maga az internet legnagyobb haszna kétségtelenül az információk gyors felkutatása és elérése. Nem számít, hogy mire van szükségünk, mert számítógép és internetkapcsolat segítségével pillanatokon belül hozzá lehet jutni bármilyen adathoz. Sokan azonban hajlamosak vagyunk feltételezni, hogy az

Minden információ fellelhető

internetet csak jó emberek használják. Meglepő, hogy a felhasználók és szervezetek lustaságból vagy egyszerűen csak tájékozatlanságból mennyi olyan információt tesznek fel az internetre, amelyek a keresőket kétélű fegyverré változtatják. Sajnos az adatszivárogtatók a legtöbb esetben a szervezetek rendszergazdái, akik elmulasztják megfelelő védelemmel ellátni a bizalmas adatokat.

Mágikus Google-opciók

Az inteneten tehát csaknem mindent fel lehet kutatni, és le lehet tölteni. A Google például egyrészt nagy tudású keresőrobotjaival rendszeresen és a lehető legalaposabban átkutatja, illetve indexeli a webhelyeket, másrészt olyan lehetőségeket kínál, amelyekkel speciális típusú adatok után lehet keresni, és ezzel vissza is lehet élni. Az alábbiakban bemutatunk néhány példát:

index of /password filetype:txt

Ez a keresés olyan .txt, azaz szöveges állományokat (filetype:txt) ad vissza eredményként, amelyekben szerepel az „index of” kifejezés, a találat szövegének része („/” operátor) a „password” szó magyarul jelszólistákat kapunk eredményül.

index of /password filetype:txt site:www.celhonlap.hu

Ez a Google-keresőkifejezés annyiban tér el az iméntitől, hogy a „site:” opció miatt csak a www.celhonlap.hu URL-en szereplő találatokat adja vissza, azaz a jelszólista-keresést leszűkítette egy internetes doménre.

intitle:érdekes intitle:adatok

vagy

allintitle:érdekes adatok

Csak olyan .html-lapok listáját kapjuk, amelyek címében (feliratában) az „érdekes” és az „adatok” szó is szerepel.

inurl:erdekes inurl:adatok

vagy

allinurl:erdekes adatok

Az eredmény csak azoknak honlapoknak a felsorolását tartalmazza, amelyek teljes internetes elérési útvonalában az „erdekes” és az „adatok” szavak is szerepelnek. Néhány teoretikus példa lehetséges eredményekre:

http://www.erdekes.hu/adatok.html

ITTHON IS ELKELNE

A kaliforniai TrustedID vállalkozás januárban olyan internetes szolgáltatást indított, amelynek segítségével gyanú esetén az Egyesült Államokban élő felhasználók utánanézhetnek, hogy szerepelnek-e valamilyen formában a weben – azaz közkinccsé váltak-e – személyes azonosítóik.

A StolenID Search már a kezdéskor egy olyan, kétmillió bejegyzést tartalmazó adatbázist használt, amelyben az „internet sötét bugyraiból” összegyűjtött bankkártya- és biztosítási számok találhatók. A TrustedID szerint a – természetesen https-t használó – szolgáltatás nem jelent biztonsági kockázatot, mert az adatokat nem kötik személyekhez, a találatokban csak az előfordulás ténye szerepel, és így az információk illetéktelenek számára használhatatlanok.

Nem kell nagy kreativitás

http://www.erdekes-adatok.hu/
http://www.honlapom.hu/erdekes-adatok.html

Védekezés

A felsorolt lehetőségek alapvetően hasznos eszközök, de rosszindulatú használatuk esetén nagy károkat lehet velük okozni. Szerencsére aránylag egyszerű megvédeni adatainkat vagy honlapjainkat a nem kívánt megjelenéstől.

Alapszabály: szükségtelenül ne tegyünk fel a webhelyünkre bizalmas, a keresők által is „látható" információkat.

A weblap gyökérkönyvtárában helyezzünk el egy olyan csupa kisbetűs „robots.txt" (nem „robot.txt" vagy „Robots.txt"!) nevű állományt, amely leszabályozza a keresőket. A keresők robotjai az állományban felsorolt könyvtárakat nem nézik át, és nem is indexelik, ezért azok tartalma a találati listákban sem jelenik meg. Az igazsághoz hozzátartozik, hogy némelyik renitens kereső nem mindig tartja magát ehhez a szabályhoz, ezért az engedélyek megfelelő beállításaival és/vagy jelszavak használatával a honlap érzékeny adatokat tartalmazó könyvtáraihoz tiltsuk le a keresők hozzáférését.

StolenID Search – *https://www.stolenidsearch.com/*
A robots.txt-ről – *http://www.searchtools.com/robots/robots-txt.html*
Google-keresési opciók – *http://www.google.com/help/operators.html*

További tanácsok

A következő szempontokat feltétlenül érdemes még szem előtt tartani bizalmas információkat is tartalmazó honlapok üzemeltetésekor. Az valójában mindegy, hogy a honlap látogatói adják-e meg az alábbi információkat, vagy a szervezet eleve tárolja, illetve máshonnan szerzi be, de az alábbi adatokat bizalmasnak kell tekinteni, és feltétlenül gondoskodni kell a védelmükről:

- taj-szám;
- személyiigazolvány-szám;
- jogosítványszám;
- személyi szám;
- születési hely és idő;
- anya leánykori neve;
- bankkártya-információk;
- mindenféle, de különösen banki hozzáférések azonosítói;
- cím és telefonszám.

Természetesen ezektől eltérő adatok is szóba jöhetnek; kérdéses esetben célszerű adatbiztonsági szakemberrel vagy jogásszal is konzultálni.

Maga a bizalmas adatokat tartalmazó webhely feleljen meg a következő kívánalmaknak:

- csak annyi és olyan bizalmas információt tároljon vagy kezeljen, amennyire és amilyenre valóban szükség van;
- a működtetéshez nem minden esetben szükségesek ténylegesen kritikus adatok – ha lehet, keressünk alternatívákat;
- a bizalmas információk kezelése feleljen meg a törvényi előírásoknak;
- az információk kezelésének mikéntjéről és az adatvédelmi intézkedésekről tájékoztatni kell a felhasználókat, és ki kell kérni a beleegyezésüket;
- a bizalmas adatokat titkosított – https – csatornákon kell forgalmazni;
- gondoskodni kell róla, hogy a kritikus információkhoz csak arra jogosult személyek férjenek hozzá;
- alapdolog, hogy a webszerver gyökérkönyvtárában tilos érzékeny adatokat tárolni;
- „védekezni" kell a keresők robotjai ellen;
- a honlapot, illetve a szervert el kell látni a megfelelő védelmi technológiákkal;
- gondoskodni kell a használt szoftverek szabályos sérülékenységkezeléséről;
- a webhely indítása előtt és működése közben is folyamatosan monitorozni kell annak biztonságát – naplóállományok szerepe;
- pontos intézkedési tervet kell kidolgozni arra az esetre – a jelentési kötelezettséget is beleértve –, ha valamilyen adatbiztonsági probléma lépne fel;
- a bizalmas információkat egy pillanattal sem szabad tovább megőrizni, mint ameddig valóban szükség van rájuk.

HONI TALÁLATOK

Nem igényel túlzott kreativitást, hogy valamely keresőbe a megfelelő szavakat beírva az internet magyar zugában sikeresen kutakodjunk bizalmas információk után. Az alábbiakban a keresett szavak és a hivatkozások, illetve az intézmények nevének elhallgatásával közreadunk néhány érdekesebb találatot:

- büntetőjogi felelősség vizsgálatához intézményi belső használatra szánt segédlet érdekes statisztikákkal;
- egyetemi tanári pályázat alkalmasságának megítélésére szolgáló vizsgálati lap;
- közbeszerzési pályázat elbírálási útmutatója;
- szűk körű tesztelésre szánt szoftver;
- üzleti és szállítási szerződések;
- cégátvilágítás dokumentációja;
- költségvetési tervek;
- informatikai rendszer részletes – támadások indítására elég jól használható – leírása;
- szervezet belső ellenőrzésének eredménye;
- belső használatra szánt piaci elemzés;
- célcsoportvizsgálat egy ugyancsak belső használatra szánt marketingjelentésben.

Nekünk a legjobban az a szabályzat tetszett, amelyben egy biztonsági cég alkalmazottai számára részletesen előírták, hogy milyen körülmények között, mekkora rákészüléssel és milyen útvonalon(!) kell a rendszeresen a gondjaikra bízott pénzküldeményeket szállítani.

A weben tárolt adatok biztonsága az adott honlapot működtető vagy birtokló szervezet felelőssége, de bármilyen kétség vagy probléma esetén ne habozzunk kikérni a megfelelő szakember tanácsát vagy külső auditorok segítségét!

Kelemen László

Rosszindulatú kriptológia

A kriptovírusok ellen nem létezik célzott védekezés.

A kriptológia és a kriptanalízis defenzív tudományok. A kriptológia célja az információk védelme, a kriptanalízisé az alkalmazott kriptográfiai módszerek gyengeségeinek a feltárása. Ugyanakkor magától értetődik, hogy utóbbi kétélű fegyver lehet, hiszen a kriptológia antitéziseként sokan a hackelés matematikai változatának tartják. A közfelfogás szerint a számítógépes kriptológia egyenlő az informatikai biztonsággal, de ahogyan a kriptanalízissel is lehet szándékosan károkat okozni, a kriptológia rosszindulatú alkalmazása is lehet romboló.

Jobban lopnak

Zavartalan dúlás

A kriptológia sajnos a rosszindulatú programok íróit is segítheti. A titkosított kórokozóknak védettebb a „magánszférája", zavartalanabbul tevékenykedhetnek, megvédhetők a visszafejtéstől és a tanulmányozásától, biztosítják készítőjük névtelenségét és a védett kommunikációt. A kódolt vírussal – a kriptovírussal – jobban lehet adatokat lopni, zsarolni, fejlettebb DoS-támadásokat lehet kivitelezni, javítani lehet azok hibatűrését, és sok más lehetőséget is kínálnak. A kriptovírusok olyan „aszimmetrikus kiskaput" nyithatnak a rendszeren, amelyről hiába tudja a biztonsági szakember, hogy létezik, nehéz pontosan lokalizálni; csak a rosszindulatú kód készítője tud rajta keresztül hozzáférni a kártékony ágenshez – szemben a hagyományos trójaiak hátsóajtajával, amelyet fel lehet deríteni, és elvileg más is használhatja.

Kriptokórokozók

A kriptovírus a definíció szerint olyan kártékony kód, amely publikus kulcsot használ. A kulcs általában a vírus írójánál van, de elképzelhető, hogy maga a kártevő generálja futásidőben. A kriptotrójaiak és a kriptoférgek ugyancsak kriptovírusok – azzal a kiegészítéssel, hogy ezek trójai- és féregtulajdonságokkal is rendelkeznek. A terület művelői fontosnak tartják megjegyezni, hogy a nem publikus, hanem szimmetrikus kulcsot használó vírusok nem tartoznak a definíció hatóköre alá. A szakemberek számára ez a megkülönböztetés különösen a polimorf vírusok esetében lehet fontos – a felhasználóknak teljesen mindegy, mert mindkettő rossz. (Amúgy polimorf vírus is lehet kriptovírus.)

A teóriától a védekezési kényszerig

A szerteágazó kriptovírus-koncepció olyannyira bonyolult, hogy kriptokártevők eleinte csak papíron, később izolált kísérleti körülmények között léteztek.

KRIPTOTÁMADÁSOK

Egyes nyílt támadási formáknál a kriptokórokozók az áldozat gépén véletlenszerűen vagy célzottan kódolnak állományokat, és a felhasználónak fizetnie kell a „túszul ejtett" információk visszaállításáért. A támadásféleség a kilencvenes évek közepétől csak elméletben létezett, aztán néhány éve megjelentek az ezt az elvet használó „ransomware-ek", a váltságdíjat követelő kártevők. Sokan éppen ezek nyomán kérdőjelezik meg a kriptovirológia mint tudomány létjogosultságát az IT-biztonságban, mondván, hogy a támadóknak ad ötleteket.

Más támadásoknál a kórokozó befészkeli magát az áldozat gépére, felkutatja a készítője számára értékes adatokat, majd elküldi a gazdájának. Speciális forma a kleptográfiai támadás, amely kriptoszisztémák ellen irányul, aszimmetrikus kiskaput használ, és célja a tárolt kulcsok eltulajdonítása.

Természetesen a kórokozók az elküldött információkat is titkosítják. Ez nemcsak önmagában nehezíti meg a felderítést, hanem egyrészt a támadók titkos „tudatalatti" vagy „küszöb alatti" csatornákat használnak, másrészt a kódolás miatt kisebbek az adatcsomagok, és az elenyésző mennyiségű forgalmazás közvetetten is rontja a detektálhatóságot.

A komplikációk miatt a vírusírók nehezen lendültek be, de lassacskán megjelentek a definíciónak eleget tevő vagy ahhoz közel álló vad formák – Ransom-A, Krotten-N, PGPCoder.D, CryZip stb. A kriptovirológia sajnos minden olyan szervezetet és felhasználót érint, amely vagy aki kritikus adatokat tárol a rendszerén – ehhez elegendő egyetlen „biztonságos" online vásárlás is. A szakértők szerint a kleptográfiás formáknak különösen az okoskártya-rendszereknél lesz majd jelentőségük.

A kriptovírusok különféle változatai ellen nem létezik célzott védekezés. A biztonságot ugyanazok az intézkedések növelik, mint más kórokozók esetében. A következők betartása mindenképpen ajánlott: meg kell győződni a futtatandó programok megbízhatóságáról, védeni kell a rendszert a behatolások ellen, vírus- és kártevőellenes eszközöket kell használni, gyakran kell biztonsági mentéseket végezni – és általában véve is vigyázni kell a biztonságra.

Kelemen László

Cyptovirology – *http://www.cryptovirology.com/*
VX Heavens – *http://vx.netlux.org/lib/?index=CR&lang=EN#start*

Hibajelentés

Áprilisi ijedelmek.

Az áprilisi bolondozás időnként túlmegy az ártatlan tréfa határain. Üres riogatásnak bizonyult a „Vista-bugok hete” nevű projekt, amelynek a Microsoft is majdnem bedőlt. A tréfás kedvű hackerek által indított kezdeményezéssel kapcsolatban a szoftveróriás szóvivője közölte, hogy készek minden problémát kivizsgálni. Az első nap jelentésére, egy hamis tűzfalgubancra egyébként számos elemző mellett a Symantec is rámozdult, de szakértői hamarosan közölték, hogy nem bizonyosodott be a hiba valódisága.

Akadtak komoly dolgok is: a táblázatunk első bejegyzésében leírt sebezhetőséget maga a Microsoft tartotta annyira fontosnak, hogy soron kívül adott ki hozzá javítást. Ez azonban néhány felhasználónak gondot okozott, mert problémák jelentkeztek a Realtek lapkakészletes hang- és hálózati komponensekkel. A Microsoft egy héten belül a javításhoz is közzétette a frissítést. Az események ismét ráirányítják a figyelmet a sérülékenységkezelés szabályainak betartására.

A Fortify dokumentálta az első komolyabb Web 2.0-val és Ajax-rendszerekkel kapcsolatos sebezhetőséget. A „JavaScript Hijacking” névvel önálló sérülékenységi kategóriának definiált – táblázatunkban nem szereplő – probléma révén kritikus adatokat lehet eltulajdonítani a mit sem sejtő felhasználóktól, mivel az adatátvitelre használt kód nemcsak a küldő/kiindulási weboldal, hanem más honlapok kontextusában is képes adatokat sugározni. A jelenség kifejezetten az Ajaxban írt, adatátvitelre JavaScriptet használó webalkalmazásokra (ilyen a Google online eszközeinek többsége) specifikus, és a Fortify által vizsgált 13 Ajax-rendszerből 12-ben fennáll. A Fortify külön érdeme, hogy dolgozatában javaslatot tesz a megoldás miként jére.

Táblázatunkat a Secunia információi alapján állítottuk össze.

Kelemen László

Secunia – *http://www.secunia.com*
Animált kurzor/Realtek-probléma – *http://support.microsoft.com/kb/935448*
A Fortify tanulmánya – *http://support.microsoft.com/kb/932246*
Vista-bugok hete – *https://www.securinfos.info/english/the-week-of-vista-bugs_day1.php*

FELFEDEZETT HIBÁK ÉS JAVÍTÁSAIK

Szoftver/Alkalmazás	Secunia-fokozat (1–5)	Secunia-azonosító	Leírás	Megoldási javaslat/további információ
Microsoft				
Windows 2000, XP, Server 2003 és Vista	5	24659	Az .ani (Animált kurzor információkat tartalmazó) állományok kezelési problémája rosszindulatú honlapok meglátogatásakor tetszőleges kód futtatására ad alkalmat.	Javítások letöltése és telepítése: http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx.
Microsoft Content Management Server 2001 és 2002	4	24819	A tartalomkiszolgáló szoftver problémái miatt oldalak közti átszkriptelésre és jogosulatlan rendszerelérésre nyílik lehetőség.	Javítások letöltése és telepítése: http://www.microsoft.com/technet/security/Bulletin/MS07-018.mspx.
Microsoft Windows XP Home és Professional	3	24822	Az UPnP (Universal Plug and Play) rendszerszolgáltatás sérülékenysége tetszőleges kód „lokális szolgáltatás” jogosultságokkal történő futtatásához vezethet.	Javítások letöltése és telepítése: http://www.microsoft.com/technet/security/Bulletin/MS07-019.mspx.
Microsoft Windows 2000, XP és Server 2003	4	22896	A Microsoft Agent (agentsvr.exe) speciálisan kialakított URL-ekkel aktivizálható problémája jogosulatlan rendszerelérést eredményezhet.	Javítások letöltése és telepítése: http://www.microsoft.com/technet/security/Bulletin/MS07-020.mspx.
Microsoft Windows 2000, XP, Server 2003 és Vista	4	24823	A kliens–szerver futásidejű alrendszer (CSRSS) nem megfelelő erőforrás-kezelése tetszőleges program Rendszer jogosultságokkal történő futtatását okozhatja.	Javítások letöltése és telepítése: http://www.microsoft.com/technet/security/Bulletin/MS07-021.mspx.
Multimédia				
Winamp 5.x	3	24766	A médialejátszó LIBSNDFILE.DLL moduljában felfedezett .mat (Matlab hangállomány) kezelési sebezhetősége miatt tetszőleges memóriát lehet felülírni zérusbájtokkal, és ez ugyancsak tetszőleges kódok futtathatóságát okozhatja.	A javításig csak megbízható .mat állományokat nyissunk meg: http://www.piotrbania.com/all/adv/nullsoft-winamp-libsndfile-adv.txt.
ACDSee 2.x–9.x változatok (Pro is) és ACDSee Photo Editor 4.x	3	24779	A képnéző és -kezelő termékekben felfedezett biztonsági hiba bizonyos .bmp állományok kezelésekor memóriaproblémákhoz vezethet.	A javításig csak megbízható .bmp állományokat nyissunk meg: http://ifsec.blogspot.com/2007/04/several-windows-image-viewers.html.
Egyéb				
Kaspersky Anti-Virus 4.x, 5.x, 6.x; Kaspersky Internet Security 6.x	4	24778	A védelmi rendszerek több problémája miatt rendszerinformációk szivároghatnak ki, jogosulatlan privilégiumokat lehet szerezni, és DoS-helyzetet lehet előidézni.	A vírusellenes motor 6.0.2.614-es változatának letöltése és használata: http://www.kaspersky.com/technews?id=203038693 és http://www.kaspersky.com/technews?id=203038694.
OpenOffice 1.x és 2.x	4	24588	Az ingyenes irodai alkalmazáscsomag több sérülékenysége tetszőleges kód futtatását és jogosulatlan rendszerelérést tesz lehetővé.	A 2.2-es változat letöltése és telepítése: http://l10n.openoffice.org/languages.html.

(Forrás: Secunia)

Van képük hozzá

Az új típusú spamtechnikák új szűrési módszerek bevezetését teszik szükségessé.

Újabb és újabb hullámokban lepi el a levélszemét az internetet, számottevően megterhelve az átviteli sávszélességet és a felhasználók idegrendszerét. Mivel jelentős többletkiadásokat okoz az internetszolgáltatóknak a megnövekedett forgalom kezelése, biztosak lehetünk abban, hogy ez megjelenik az internet-előfizetés árában is. Sokba kerülnek a kéretlen levelek a vállalatoknak is, mert ha nem akarják, hogy alkalmazottaik munkaidejük tetemes részét a spamek olvasásával és törlésével töltsék, gondoskodniuk kell a hatékony szűrésről.

A spam voltaképpen olyan illegális marketingmódszer, amelynek lényege, hogy az elektronikus levelezésben rejlő előnyök kihasználásával rövid idő alatt igen sok címzetthez lehet eljuttatni a reklámokat. Méghozzá ingyen, legalábbis a terjesztőknek nem kerül semmibe, a spam árát ugyanis végső soron a címzettek fizetik meg. A spammerek nem ellenőrzik a különféle módon – hírcsoportok és webhelyek átvizsgálásával, címlisták vásárlásával, legális levelezőkiszolgálók kisajátításával, címgenerálással – megszerzett e-mail-címeket, hanem válogatás nélkül bombázzák ezeket leveleikkel, mivel tudják: minél több levelet küldenek, annál nagyobb haszonra tehetnek szert.

Nehezen felismerhető

Így történhet meg, hogy bár a kéretlen levelekben található reklámok nagy részével az egyesült államokbeli internetezőket célozzák meg, azok a világ többi részébe is eljutnak, teljesen felesleges terhet róva a világhálóra.

A Symantec havonta közzétett spamjelentésének legfrissebb, márciusi kiadása szerint a világszerte elküldött összes elektronikus levél átlagosan 70 százaléka spam, és ez becslések szerint naponta átlagosan 50 milliárdnyi üzenetnek felel meg. A legtöbb kéretlen üzenetet Észak-Amerikából (40 százalék) és Európából (34 százalék) bocsátják útjára.

Grafikus reklámszövegek

Azonban a spam által az internetes közösségnek okozott kár messze túlmutat a sávszélesség lefoglalásából származó költségeken. A kéretlen leveleket előszeretettel használják az adathalászok is, akik az ezekben elhelyezett hivatkozásokkal csalják meghamisított webhelyekre a pénzintézetek ügyfeleit, hogy ott megszerezzék tőlük bejelentkezési adataikat vagy banksámlaszámukat. A spamterjesztők az ellenőrzésük alá vont több milliónyi zombigépből álló bothálózatokat használják leveleik célba juttatására; szakértők szerint egy tipikus botnet két óra alatt 160 millió üzenetet képes kiküldeni. De a zombivá válás is egy spam megnyitásával kezdődik: a felhasználó óvatlanságból elindít egy kéretlen levél mellékleteként érkező rosszindulatú kódot.

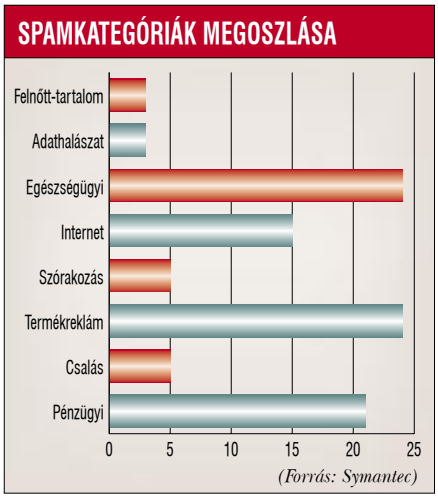
Karakterből grafika

Régebben a kéretlen levelek egyszerű karakteres üzeneteket tartalmaztak. Mivel azonban a szövegfelismerésben a szűrőprogramok meglehetős jártasságra tettek szert, kicselezésükre a számítógépes bűnözők létrehozták a közlendő reklámszöveget grafikus formában megjelenítő, úgynevezett képes spamet. Az új álcázási módszereknek köszönhetően ez az utóbbi pár hónapban olyan fényes karriert futott be, hogy februárban már az összes levélszemét 38 százalékát alkotta. Mivel a kéretlen levelekben elhelyezett grafikák lényegesen nagyobb helyet foglalnak el a szövegnél, a képes spam terjedése újabb csapást mért az internet sávszélességére: egyes becslések szerint az új típusú üzenetek annak nem kevesebb mint 70 százalékát foglalják le.

Az első képes spamek többnyire egy .gif formátumú grafikán jelenítették meg a reklámszöveget, amelyhez a további információkra kíváncsi felhasználók kiszolgálására mellékeltek egy webcímet. Ezzel az egyszerű trükkel a hackerek képesek voltak hatástalanítani az alapvetően a szövegek elemzésére kifejlesztett, hagyományos spamellenes eljárásokat, a szófel-

ismerést és a minta alapján való szűrést. Ezek nem tudták azonosítani a képben a szöveget, és simán átengedték a spamet.

Mivel azonban a képbe ágyazott hivatkozások egyszerűen felismerhetők, a szűrőprogramok fejlesztői olyan feketelistákat készítettek, amelyek tartalmazták a rosszindulatú webhelyekre mutató hivatkozásokat. Ezeknek a listáknak a segítségével aztán blokkolhatók lettek a képes spamek is.



A bűnözők válasza a hivatkozás nélküli képes spam lett, amely szöveges üzenetben kéri a címzettet a megadott hivatkozás böngészőbe való begépelésére, megakadályozva ezzel a feketelisták használatát.

Kézenfekvő ötlet volt a képes spam kiszűrésére a kép minta alapján való azonosítása: ehhez elegendő elcsípni egy példányt, annak jellemzőit megtanítani a szűrőprogramnak, ami aztán leleplezi majd a többi üzenetet. Ezt a védekezési módszert a hackerek az üzenetek automatikus generálásával hatástalanították, amelynek eredményeképpen ugyanazt a szöveget tartalmazó, de méretben, illetve a szöveg tördelésében, színében vagy más jellemzőjében eltérő, egyedi képek jöttek létre.

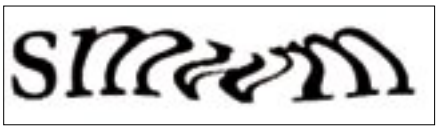
Álcázott spam: hivatkozás nélkül

Körmönfontabb trükkök

A kéretlen reklámlevelek elleni programok további összezavarására a spamterjesztők véletlenszerűen elhelyezett karaktereket és pöttyöket alkalmaznak, vagy megváltoztatják a szöveg hátterét. Az ilyen fogások segítségével ugyanabból a grafikus üzenetből teljesen egyedi képeket hoznak létre, kizárva a minta alapján történő felismerést.

Ugyancsak hatásos módszer a színek és szövegtorzítások kiterjedt alkalmazása, amely a megegyező színű és határozott körvonalú karakterek felismerésére kifejlesztett, s nemrégiben a szűrőprogramok részévé vált optikai karakterfelismerés dolgát nehezíti meg. A különböző színű képpontokból felépített betűkkel és az eltérő színű karakterekből álló szöveggel – bár ezek szemmel jól láthatók – komolyan meggyűlik a bajuk a karakterfelismerő eljárásoknak. Csakúgy, mint a ritkán használt betűtípusokkal, a hosszában két részre vágott szövegrészekkel, valamint a legkülönfélébb módokon torzított alakú karakterekkel és sorokkal.

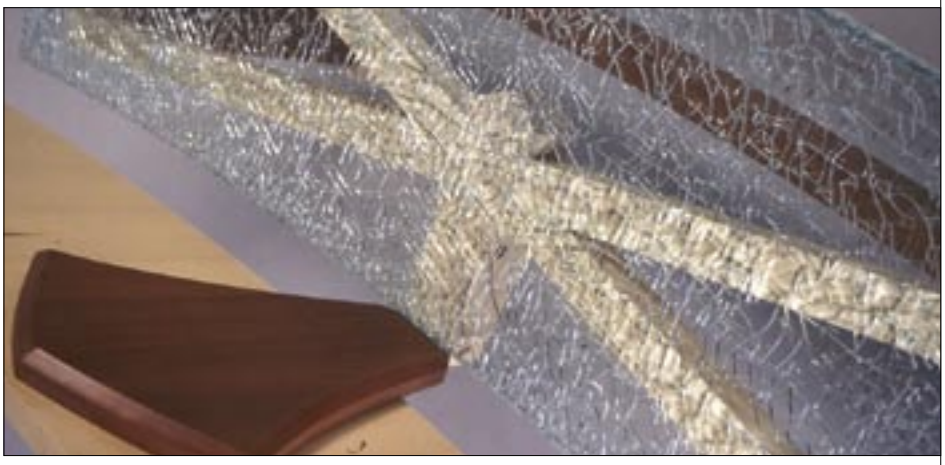
A spamkészítők már felfedezték maguknak a Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) biztonsági technológiát is, amellyel többek között webes szolgáltatások regisztrációs oldalain találkozhatunk. A csak emberek által felismerhető karaktereket megjelenítő Captcha az automatizált gépi bejelentkezést hivatott megakadályozni. A technológia segítségével torzított szöveg azonosítása kemény próba elé állítja a spamszűrőket.



Géppel szinte olvashatatlan

Bevált fogás a reklámszöveget tartalmazó kép olyan mértékű elrontása, ami még nem akadályozza meg a grafika megjelenítését a levelezőprogramban, de a spamszűrő alkalmazás észlelőmodulja számára megnehezíti annak beolvasását.

Nem könnyű azonosítani a darabokra vágott képeket sem. A hackerek egy html formátumú levélben jelenítik meg a szétszabdalt képes spam részeit, amelynek egymáshoz rendelése nehéz feladat elé állítja a karakterfelismerést. Szélsőséges esetben az üzenet minden egyes betűjét külön képként továbbítják.



Nem könnyű azonosítani

Szintén a felszabdalás egyik formája a szöveg megjelenítése animált .gif formátumban. Az ily módon prezentált üzenetek több, részben átlátszó képkockából épülnek fel, és ezek külön-külön nem szolgáltatnak elegendő információt a reklámlevéllé minősítéshez. A felismerés további nehezítése érdekében az animált .gif-ek álcázását a fentebb tárgyalt módszerekkel kombinálják.

Tóth István

Mobilok, védőőrizetben

Vannak tevékenységek, amelyeknél létfontosságú a bizalmas információk megőrzése.

Nem titok, hogy a telefonok lehallgathatók. A legtöbben tisztában vannak ezzel – nem telefontéma, szokás mondogatni –, de mivel nincs különösebb rejtegetnivalójuk, nem sokat törődnek a magánéletükre leselkedő potenciális veszélyekkel. A teljes igazsághoz persze az is hozzátartozik, hogy a telefonlehallgatás nem kizárólag a tilosban járók tevékenysége: a nyomozóhatóságok ugyancsak előszeretettel alkalmazzák bizonyítékok gyűjtésére. Természetesen ma már csak szigorúan szabályozott módon, a szükséges engedélyek birtokában tehetik ezt meg, az érintett szolgáltatók tudtával és közreműködésével.

A mobiltelefonok kommunikációjukhoz a távközlési hálózat hozzájuk legközelebb eső bázisállomását használják, így tulajdonosuk tartózkodási helye megállapítható. Azt viszont már kevesebben tudják, hogy megfelelő technikai felszerelés birtokában a mobilbeszélgetések is lehallgathatók, dacára annak, hogy titkosítják a kommunikációt. Persze a kíváncsiskodóknak lényegesen felkészültebbeknek kell lenniük, mint vezetékes telefonok esetében, hiszen ezeknél elég lehet egyszerűen rácsatlakozni a megfigyelt állomás vonalára a telefonszolgáltató hozzáférhető helyen elhelyezett elosztóján.

Támadási pontok

A mobilhálózatok egyik nagy hiányossága, hogy bár a telefonnak azonosítani kell magát a hálózat felé, az ellenkező irányú azonosítást nem követeli meg a GSM-szabvány. Ezt használja ki a SIM-kártyákon tárolt, azok aktiválásához szükséges IMSI (International Mobile Subscriber Identity) számot elfogó berendezés, az

www.cryptophone.com

úgynevezett IMSI-catcher, amelyet a közelében lévő telefonok tévesen legális bázisállomásként érzékelnek. A GSM-titkosítást kikapcsoló IMSI-catcher voltaképpen egy „man in the middle” jellegű támadást hajt végre: áthaladnak rajta az átvert mobilról indított hívások, amelyeket aztán a mobilhálózatra továbbít.

Biztonsági szakértők szerint azonban a bekapcsolt titkosítás sem képes megakadályozni a beszélgetések lehallgatását. A GSM-szabványban leírt algoritmusok titkosító kulcsa pusztán az elfogott, titkosított adatok birtokában is pillanatok alatt megfejthető. Európában voltak próbálkozások az erősebb titkosítási eljárások bevezetésére, ezek azonban sorra elbuktak azoknak az országoknak az ellenállásán, amelyek hatóságai a terrorizmus és a szervezett bűnözés elleni küzdelem hatékonyságának növelése érdekében nagy számban hallgatnak le telefonokat.

Megoldás lehet a kommunikáció védelmére a használtan vásárolt feltöltőkártyás telefon, mert bár ez is lehallgatható, azt nem lehet tudni, hogy ki kezdeményezte a hívást. Egyszer és mindenkorra vége szakad azonban az anonimitásnak, ha a titkolódzó személyt egy adott telefonhoz sikerül társítani, a készülékbe „égetett” egyedi IMEI-azonosító alapján ugyanis ezután egyszerűen nyomon követhető lesz, és ezen a SIM-kártya cseréje sem segít. Ilyenkor nem marad más hátra, mint a telefon cseréje.

A paranoiás hangulat fokozására itt jegyezzük meg, hogy egyes mobiltelefonok még kikapcsolt állapotban is sugároznak rádiójeleket, így megállapítható a tartózkodási helyük. Sőt, olyan esetről is olvashatunk a neten, amelynek során a hatóságok állítólag távolról bekapcsolták egy figyelt személy mobiljának mikrofonját, és így hallgatták le a beszélgetését. Ezek a „fenyegetések” az akkumulátor eltávolításával védhetők ki.

Van megoldás

De mit tehetnek akkor azok az üzletemberek, bankárok, fehérgalléros és közönséges bűnözők, ügyvédek, üldözési mániában szenvedők és hasonlók, akik nem tudnak lemondani a mobiltelefon használatáról, viszont mindenképpen el akarják kerülni, hogy beszélgetéseiket illetéktelen fülek is hallgassák.

A megoldást számukra a végponttól végpontig terjedő titkosítást megvalósító, speciális biztonsági mobilok jelentik, amelyek méregdrágák – de a célcsoportnak nyilvánvalósan nem okoz különösebb gondot a megvásárlásuk –, és csak az ugyanattól a gyártótól származó termékek kompatibilisak egymással.

Itt van például a berlini székhelyű német GSMK cég, amely a saját fejlesztésű CryptoPhone technológiát alkalmazó telefonokat – két mobil, egy műholdas és egy vezetékes modellt – kínál. A gyártó szerint ezek a 256 bites kulcsú AES és Twofish titkosítást használó készülékek egymás közötti kommunikáció esetén mind a telefonhálózatban, mind a levegőben az illetéktelenek számára hozzáférhetetlen beszédátvitelt biztosítanak. A cég webhelyén olvasható tájékoztatóban az áll, hogy a CryptoPhone-ok a világ nagy részén, így többek között az Európai Unióban és az Egyesült Államokban korlátozás nélkül használhatók. A vásárlói bizalom erősítésére szolgál, hogy a készülékekben alkalmazott szoftverek forráskódja bárki által szabadon letölthető.

FORRÁS: GSMK

Megóv a lehallgatástól

A GSMK-nál gondoltak azokra is, akiknek a partnerei nem engedhetik meg maguknak a költséges biztonsági telefonokat. A vezetékes és GSM-modemekkel egyaránt kompatibilis, ingyenes CryptoPhone for Windows program révén nemcsak a cég által gyártott telefonokkal folytathatók titkosított beszélgetések, hanem a programot futtató más számítógépekkel is.

Tóth István

IT-BUSINESS TODAY

- felsővezetőknek, döntéshozóknak
- az elmúlt 24 óra legfontosabb hazai és nemzetközi ICT hírei
- ingyenes napi hírlevél

Regisztráljon!

www.it-business.hu/hirlevel

Második menet

Javuló helyzet az Ügyfélkapuban.

Egy hónappal első cikkünk megjelenése után megnéztük, milyen változások álltak be a magyar e-ügyintézés főbejáratában és körülötte.

Már az első változás impresszív: az egy perc körüli oldalletöltési idő lement 3-5 másodpercre.

Következett a próba az elektronikus aláírással történő regisztrációval… azaz következett volna, de a kapu üzemeltetői e téren is javítottak, és időközben elejét vették a többszöri regisztráció lehetőségének. A rendszer most már érzékeli az azonos adatokat és közli:

„A regisztráció nem fogadható be, mivel a megadott természetes személyadatokkal van már regisztráció a rendszerben. (Üzenetkód: 41)”

Nem is tudjuk, hogy működik-e a lehetőség, de ez így van rendjén.

Csak halkan jegyezzük meg, hogy az ezzel kapcsolatos egy hónappal ezelőtti érdeklődő felhasználói e-mailekre még nem érkezett válasz. További csendes észrevétel, hogy az okmányirodákba most is csak egy héttel későbbi időpontok közül választhatunk, de ne legyünk maximalisták – már csak azért se, mert az okmányiroda most már kiválasztható a „Hivatalkereső” és az „Okmányirodák” menüpontoknál is.

Http-fejléc

A Kapu őrei erre is odafigyeltek. Bár az óra továbbra is GMT-ben mér, és a számlálója most két(?) órával mutat kevesebbet a számítógép közép-európai értékénél, de már nem látszik az Apache-szerver verziószáma. A szoftver kétéves korára utaló változat így már nem csiklandozza a hacker-fantáziát, de kérdés, hogy a változatra utaló jelzés hiánya milyen mértékben „birizgatív”. Aprócska további változás, hogy a fejléccel együtt most már egy munkamenet-azonosító cookie-t is kapunk, ami a biztonság szempontjából kellemes fejlemény.

Nem mellékesen

A felhasználóhitelesítésért és az elektronikus aláírás ellenőrzéséért felelős motort szállító E-Group felvette velünk a kapcsolatot. Mivel nem ők üzemeltetik a leszállított rendszert, így a korábbi cikkben leírt konkrét hibajelenség okát nem tudták megvizsgálni. Ugyanakkor elmondták, hogy egészében véve elsősorban azért rogyadozik a rendszer e-aláírási ága, mert a motiváció hiánya miatt elenyészően kevés ügyfél rendelkezik megfelelő elektronikus tanúsítvánnyal. Ugyanis minden, Ügyfélkapun keresztül elérhető szolgáltatás jelszavas azonosítással is igénybe vehető – és a felhasználók nemhogy a magasabb biztonságot nem igénylik, de még a jelszavukat is könnyedén továbbadják sokszor.

FELEDÉKENY KÖNYVELŐK

A vállalkozások nagy része külső félre bízza a könyvelést és az ezzel kapcsolatos elektronikus ügyintézést. Az ilyen ügyfeleik adóügyeinek intézésekor a könyvelők két módszer közül választhatnak:

- saját nevükkel vagy a könyvelőcégük nevében tevékenykednek;
- a cég képviselőjének azonosítóit használva járnak el az ügyfél nevében.

Mivel az első módszernél minden felelősség a könyvelőké, ezért az ügyfelek botlásai esetében is nekik kellene viselniük minden felelősséget, így késedelmes vagy hibás befizetésnél az anyagi következményeket is. A magyar ügyfelek márpedig botlanak – nem is keveset –, ezért az általunk megkérdezett könyvelő véleménye szerint az esetek döntő többségében a könyvelő elvárja, hogy az ügyfél átadja számára a bevallás elküldéséhez szükséges felhasználónevét és jelszavát.

A megfelelő megállapodások mellett a módszer törvényes, de vannak vele gondok: az egyik az, hogy így a könyvelő hozzáfér kliense minden Ügyfélkapun elérhető adatához – így például a teljes betegéletútjához is. A másik probléma az, hogy ezt a tényt a könyvelők néha „elfelejtik” közölni az ügyfelekkel.

Az E-Group azonosító rendszerének működése

Az E-Group egyébként szorgalmazza és támogatja a közhivatalok elektronikus ügyintézési rendszereinek kialakítását és integrálását a központi rendszer szolgáltatásaihoz, ami ma már nemcsak a központi bejelentkeztetést jelenti, hanem egy postafiókszerűen működő tárhelyfunkciót is. Ilyen helyzetekre vannak kész – a vonatkozó 2004. évi CXL. törvénynek megfelelő – megoldásaik.

Köztes állapot

Az e-aláírás egyébként biztosan nem lesz mindig mostohagyerek, bár lehetőségei a magyar e-ID kártyarendszer elindulásakor teljesednek majd ki igazán. Ebben a rendszerben intelligens kártyán tárolják majd a személyes azonosításhoz, elektronikus aláíráshoz és rejtjelezéshez szükséges kulcsokat, tanúsítványokat; továbbá esetlegesen jogosítvány, tömegközlekedési, elektronikus pénztárca és az egészségügyi ellátáshoz szükséges funkciók is kerülhetnek rá. A még csak homályosan körvonalazott rendszer megvalósulása esetén ez a kártya biztosítaná az Ügyfélkapu használatához szükséges azonosítást is.

Magyar Elektronikus Ügyfélkapu – *www.magyarorszag.hu*
E-Group – *www.egroup.hu*

Persze erre még kicsit várni kell, de a hírek szerint a közigazgatási informatikáért – és így az Ügyfélkapuért is – felelős Miniszterelnöki Hivatalban már addig is gőzerővel dolgoznak azon, hogy az elektronikus azonosítás egy köztes – stabil, költséghatékony és a jelszavas azonosításnál biztonságosabb – lehetőségét a Kapu vonatkozásában megteremtsék.

Kelemen László

ESEMÉNYNAPTÁR

Időpont	Megnevezés	Helyszín	Web	Részvételi díj	Leírás
Április 24–26.	Infosecurity Europe 2007	Grand Hall, Olympia, London	*www.infosec.co.uk*	20 font	Az egyik legjelentősebb IT-biztonsági kiállítás, ahol bemutatják az iparág legújabb termékeit és szolgáltatásait, oktatási programmal és kiállítással egybekötve.
Április 24–27.	MIPS 2007	SC Olympisky, Moszkva	*www.mips.ru/eng/*	Ingyenes belépő a honlapról kinyomtatható	Idén 13. alkalommal rendezik meg Oroszország legnagyobb biztonsági és tűzvédelmi konferenciáját és kiállítását. Az idei évben öt ország jelenik meg nemzeti standdal: Nagy-Britannia, Olaszország, Kína, Korea és Tajvan.
Április 24–27.	Fire & Safety Expo	Daegu Exhibition & Convention Center, Daegu, Korea	*www.fireexpo.co.kr/*	Az előzetes regisztráció ingyenes	A kiállítás a teljes biztonsági piacot lefedi; 20 ország 200 kiállítójának részvételével bemutatják az iparág jelenlegi helyzetét és jövőbeli trendjeit. A kiállításhoz konferenciák, előadások is társulnak.
Április 26–28.	2007 SIAM International Conference on Data Mining	Minneapolis, Minnesota, Egyesült Államok	*www.siam.org/meetings/sdm07/*	150–620 dollár	Az adatbányászattal foglalkozó nemzetközi konferencia három fő területe: metodológiák és algoritmusok; alkalmazások, esettanulmányok; humán faktor, etikai kérdések.
Május 6–8.	Middle East & Africa Smart Card Exhibition & Conference	Kairó, Egyiptom	*www.egytec.com/Cardex/index.html*	585–975 euró	Az ötödik alkalommal megrendezendő Card-EX 2007 konferencián szó lesz a bankkártyák és a smart-cardok legújabb fejlesztéseiről, biometrikus azonosításról, PKI-ról, IT-biztonságról, az e-kormányzat, e-fizetés, e-bankolás technológiáiról.
Május 7–9.	ISPEC 2007	Hongkongi Egyetem, Kína	*www.cs.cityu.edu.hk/~ispec2007/*	2500–5000 hongkongi dollár	A konferencia előadásain foglalkoznak az információbiztonság legújabb technológiáival és alkalmazásaival, kitérnek a kriptográfiai alkalmazásokra, a biztonsági szabványokra, a biztonsági szabályzatra, a jogi kérdésekre, illetve a biztonsági megoldások IT-rendszerbe illesztésére is.

OKTATÁS, TANFOLYAMOK

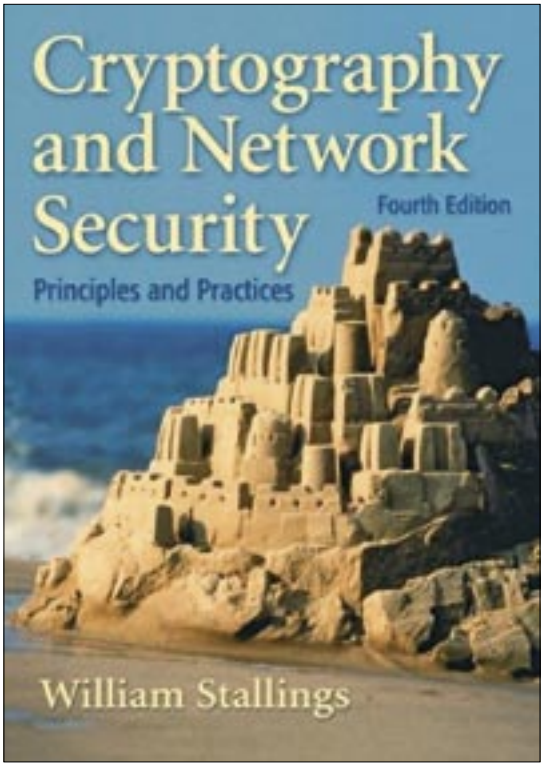
Tanfolyam címe	Leírás	Időpont	Időtartam	Részvételi díj	Webcím	Helyszín
ISO 27001:2005 Információbiztonsági rendszerek szakértője	A tanfolyam megismertet az információbiztonsági alapfogalmakkal, az ISO 27001:2005 szabvány alapkövetelményeivel. További témák: Rendszer- és folyamatszemlélet – PDCA ciklus az információbiztonság területén; Óvintézkedések, kontrollok; Kapcsolódás más szabványokhoz; Kockázatelemzés és kockázatkezelés; Alkalmazhatósági nyilatkozat; Az információbiztonsági rendszer dokumentációja és feljegyzések.	Április 24.	3 nap	140 000 forint + áfa	*www.training.hu.sgs.com*	Budapest, Sirály u. 4.
Balabit Certified Zorp Expert Upgrade	A tanfolyam célja bemutatni a Zorp üzembe helyezése és üzemeltetése szempontjából fontos témaköröket. A tanfolyam anyaga a Zorp Expert tanfolyam anyagára épül, de nem tartalmazza az előző tanfolyamokon már bemutatott részeket. Tematika: Haladó hálózati beállítások (advanced routing), IPSec VPN beállítása ZMC segítségével, Zorp Cluster konfigurálása, Autentikáció, a ZAS és a Satyr használata, Haladó Zorp Proxy-konfiguráció.	Május 2.	2 nap	80 000 forint + áfa	*www.wsh.hu*	Budapest, Teve u. 1.
PKI – Nyílt kulcsú titkosítás a gyakorlatban	Amióta törvény mondja ki, hogy az elektronikus aláírás egyenértékű a többi aláírástípussal, megnyílt annak a lehetősége, hogy titkosított és hitelesített levelek útján kommunikáljanak a partnercégek – amihez szükség van kulcspárra, tanúsítványra, és megfelelő tudásra. Ez a tanfolyam az RSA-algoritmustól indul el, tárgyalja – és gyakorlati példákon keresztül mutatja be – a Certificate Server és az X.509 tanúsítvány témáját is.	Május 7.	4 nap	195 000 forint + áfa	*www.net-academia.net*	Budapest, Andrássy út 62.

Hivatkozási alapul szolgálhat

Minden könyvet aszerint kell megítélni, kinek szánta a szerző.

Míg gyermekkönyvek esetén viszonylag könnyű az írónak kiszolgálnia leendő olvasóinak ízlését, a műszaki irodalomban ez sokkal nehezebb. Mint a világon mindennek, ennek is a pénz az oka. A legtöbb szerző nagyszerű könyvet tudna írni pályatársai és tanárai számára, hogy a szakma nagy konferenciáin elismerő pillantásokat zsebeljen be érte. Azoktól, akik kaptak a tiszteletpéldányból. Megvenni ugyanis kevesen fogják dédelgetett alkotásukat.

Ezeket hívjuk tudományos műveknek, és szerzőik láthatóan nem az eladott példányszám után kapják a fizetésüket. Sokkal valószínűbb, hogy egy nagy egyetem vagy kutatóintézet professzorai ők – közepesen jó fizetéssel és kedvező nyugdíjkilátásokkal –, különben senki nem adná ki szerzeményüket, amely a legnagyobb példányszámban könyvtárakba kerül majd.



Némi tanári véna

Vannak könyvek, amelyek szintén a szakmának íródnak, de nem csupán az annak csúcsán tényked tucatnyi akadémikusnak, hanem a dolgozó mérnököknek, akik munkájuk során jól használhatják a kötetben összegyűjtött információkat. Ezek a műszaki szakkönyvek általában kézikönyv jellegűek, és a kezelhetőség érdekében jól szervezetten, erősen tagolt a felépítésük. Ezek a könyvek tipikusan kevés folyó szöveget tartalmaznak, hiszen nem történeteket mesélnek el. Szerzőik pedig gyakorló szakemberek, némi tanári vénával, akik egy jól sikerült, hosszú életű mű eladásai után szépen kiegészíthetik jövedelmüket.

És van persze az informatika térhódításával párhuzamosan kialakult, egyre nagyobbra hízó kategóriája a népszerű-műszaki irodalomnak, amely számtalan „megélhetési" slágerszerzőt tart el. Ők tipikusan rendkívül jó előadók, akik valami oknál fogva híresek lettek, hírnevüket pedig a nép okítására, szakmájuk népszerűsítésére és közérthetővé tételére szeretnék fordítani. És persze meg is akarnak gazdagodni. Az ő könyveik – ne legyünk naivak, ezeket a könyveket egy egész stáb írja – arról ismerszenek meg első látásra, hogy sok bennük a folyó szöveg, a címek nagyok, a borító figyelemfelkeltő és tetszetős. Természetesen őket sem szabad elítélni, hiszen egyrészt: van ez a kereslet-kínálat nevű törvényszerűség; vagyis az ember csak azt tudja eladni, amit egy másik ember meg akar venni. Másrészt, az információtechnológia rohamosan részévé válik szinte minden ember életének – legalábbis a fejlett országok zártkörű klubjában –, így igenis szükség van ezekre a könyvekre, amelyek szemléletet adnak, például az IT-biztonság tekintetében. E hasábokon is ajánlottunk már nem egy ebbe az utolsó csoportba sorolható művet, hiszen az informatikai vezető tipikusan olyan ember, akinek erre a felszínes tudásra van szüksége, viszont több tucatnyi területről.

Szeretjük tehát a népszerű-műszaki irodalmat, mint ahogy esténként is szívesebben nézünk egy könnyen emészthető kalandfilmet, mit egy Oscar-díjas családi drámát.

Legyen ott a polcon!

Viszont, jelen kötetünk egyértelműen nem ez utóbbi kategóriába esik; sokkal inkább remek mérnöki szakkönyv. Sőt, mondjuk ki: egy alkalmazott kriptográfiai kézikönyv, amit nem is lehet – és felesleges is volna – elolvasni. Legyen ott a polcán mindenkinek, aki ezzel foglalkozik, de csak akkor vegye le, ha keres egy képletet, vagy ha meg akarja érteni, hogyan működik egy-egy algoritmus. Definíciók tekintetében is maradandót alkotott a szerző, ami elsősorban abban segítheti a szakmát, hogy egy szóképen mindenki ugyanazt a fogalmat értse. A könyv nemcsak nyomtatásban, hanem a szoftverekben már megszokott „súgó" formátumban elektronikusan is elérhető, amely jól jelzi, *William Stallings* egyértelműen olyan kötetnek szánta művét, amely voltaképpen minden szakmában létezik: egy megkérdőjelezhetetlen viszonyítási és hivatkozási alapnak.

És bár van még egy-két pályázó erre a posztra, egyáltalán nem lepődnénk meg, ha a jövőben két IT-biztonsággal foglalkozó mérnök folyosói vitájára a Cryptography and Network Security Principles and Practices fellapozása tenne pontot.

Sós Éva

KÖNYV-JELZŐ

Cím: Cryptography and Network Security Principles and Practices, Fourth Edition
Szerző: William Stallings
Kiadó: Prentice Hall
Terjedelem: 592 oldal

Fogalomtár I.

Az IT-biztonság területén különösen sok olyan kifejezés van, amelyet még a hazai szakmai anyagokban is csak angolul találunk meg.

A következőkben néhány angol szót, illetve kifejezést sorolunk fel, azok magyar fordításával, rövid meghatározásával együtt. A listát ábécébe rendeztük, az egyszerű képzős alakokat és az egy-egy szóhoz kapcsolódó kifejezéseket csoportosítottuk. Emiatt van olyan kifejezés, amely két helyen is megjelenik. A fordításnál az MSZ ISO/IEC 17799:2002 biztonsági szabvány szógyűjteményét vettük alapul.

Authentication: hitelesítés
Általánosságban azt a tevékenységet jelenti, amelynek során eldöntjük, hogy valami hiteles, azaz valódi. Az informatikában a digitális személyazonosság ellenőrzésére szolgáló folyamat jelölésére szolgál, azaz a hálózatba (weboldalra) bejelentkező (log in) felhasználó személyazonosságát ellenőrzi. Erre a célra az elmúlt évek folyamán sokféle eljárást dolgoztak ki.

A legegyszerűbb esetben felhasználónév–jelszó kombinációt alkalmaznak – a legtöbb helyen ma is ilyen hitelesítéssel dolgoznak. Nagyobb biztonságot jelent a tanúsítvány, az intelligens kártya vagy a biometrikus azonosítás alkalmazása. Szükség lehet ugyanakkor hitelesítésre fordított irányban is, ekkor a felhasználó győződhet meg arról, hogy valóban a kívánt hálózatra csatlakozott-e.
Authentic: hiteles
Authenticate: hitelesít
Authenticity: hitelesség
Authentication control: a hitelesítés ellenőrzése
Biometric authentication: biometrikus hitelesítés
Message authentication: üzenethitelesítés
Node authentication: csomópont-hitelesítés, a csomópont hitelesítése
User authentication: a felhasználó hitelesítése

Certificate: tanúsítvány
A „személyi igazolvány”, vagyis azonosító okmány digitális megfelelője, amelyet titkosító rendszerben valamilyen nyilvános kulccsal együtt alkalmaznak. A tanúsítványt valamely megbízható harmadik fél, az úgynevezett tanúsító szervezet (Certification Authority) bocsátja ki. Ez a szervezet igazolja (ellenőrzi), hogy a kulcs valóban az adott céghez/személyhez tartozik-e.
Certification: tanúsítás
Certification Authority (CA): tanúsító szervezet (CA); tanúsító hatóság; (általában) hitelesítésszolgáltató (csak ha nincs ellentmondásban az „authenticator” vagy az „authentication service provider” jelentéssel)
Public key certificate: nyilvános kulcsú tanúsítvány

Cryptography: titkosítás, titkosítás mint tudomány
Az adatok titkos kóddá alakítása nyilvános hálózaton való továbbítás céljából.

Egy mára önállóvá vált, matematikai alapokra épülő, interdiszciplináris jellegű, de elsősorban informatikai tudományág, amely a rejtjelezéssel, titkosításokkal, kódolással, azok előállításával és megfejtésével foglalkozik.

Egy kommunikációs folyamat során továbbított nyilvános üzenetet akkor nevezünk titkos(ított)nak, ha a feladó olyan formá(tum)ban küldi, amelyet olvasni vagy fogadni esetleg többen is tudnak, de megérteni csak a fogadók egy megcélzott csoportja.

A nyilvános hálózaton továbbított adatokat, az egyszerű szöveget (plaintext) alakítják át kóddá, valamilyen titkosító algoritmus (encryption algorythm) alapján. A titkosított adatfolyamot a célponton visszafejtik (decrypt).
Cryptography legislation: kriptográfiával kapcsolatos jog
Cryptographic: kriptográfiai
Cryptographic controls: kriptográfiai óvintézkedések
Regulation of cryptographic controls: kriptográfiai óvintézkedések szabályozása
Cryptographic key: kriptográfiai kulcs
Cryptographic policy: kriptográfiai (titkosítási) szabályzat
Cryptographic service: kriptográfiai szolgáltatás
Cryptographic techniques: kriptográfiai technikák (módszerek)

Decryption: visszafejtés
Decipher: megfejt (rejtjelezést, elrejtést)
Decrypt: visszafejt (titkosírást)

Encryption: titkosítás
Encipher: rejtjelez
Encrypt: titkosít
Encryption algorithm: titkosító algoritmus
Encryption system: titkosító rendszer
One-way encryption algorithm: egyirányú titkosító algoritmus

Key: (titkosítási) kulcs
A kulcs a rejtjelző eljárás paramétere, amelyet csak a küldő és a címzet(tek) ismernek. A kulcs numerikus kód, amelynek alapján adatokat biztonsági célból titkosítanak. A titkosító algoritmusokban alkalmazott kulcs általában 40–256 bites bináris szám. Minél több bináris jegyből áll, azaz minél hosszabb a kulcs, annál több a lehetséges kombináció, tehát annál nehezebb feltörni a kódot.

Hardveres titkosító eszköz

Key generation: kulcsképzés, kulcselőállítás
Key information: kulcs(ra vonatkozó) információ
Key lock: kulcs-retesz
Key management: kulcsgondozás
Key update: kulcsfrissítés, kulcsaktualizálás
Private key: magánkulcs
Protocol encryption key: protokolltitkosító-kulcs
Public key: nyilvános kulcs
Secret key: titkos kulcs

Összeállította: Matula Zsolt

Mit olvas a szakértő?

Belső portálok és gyártói oldalak.

FORRÁS: AVAYA

Balog Attila

Hetedik éve dolgozik rendszermérnökként az Avaya magyarországi terméktámogató központjában *Balog Attila*. Feladata a tanácsadás és távoli segítségnyújtás elsősorban európai, közel-keleti és afrikai ügyfelek számára.

Munkája során egyre gyakrabban találkozik az ügyfeleknek az Avaya termékeivel kapcsolatos biztonsági kérdéseivel és egyedi igényeivel. Mivel az Avaya termékei Red Hat Linux, Microsoft Windows, Sun Solaris és SCO Unix operációs rendszereken futnak, és olyan technológiákat használnak, mint a Java, a PHP vagy éppen a PostgreSQL adatbázis, az Avaya olyan csoportot állított fel, amely a termékek alap-építőköveiként használt technológiákkal kapcsolatos biztonsági riasztásokat bevizsgálja és négy különböző kockázati kategóriába sorolja.

A riasztások leírását és az azokkal kapcsolatos teendőket az Avaya egy belső portálon adja közre (a legmagasabb kockázati besorolás esetében a cég vállalja, hogy az úgynevezett Security Advisory dokumentumot 24 órán belül közzéteszi). Nem véletlen, hogy Balog Attila számára is ez a portál minden IT-biztonsággal kapcsolatos tájékozódás kiindulópontja. Hasonlóan fontos információkkal szolgál egy másik Avaya-portál (SAC) is, amely az ügyfeleknél üzemeltetett eszközök távoli elérésére és az azoktól fogadott riasztások kezelésére szolgál.

Schopp Attila

A LEGJOBB FORRÁSOK

Hírforrás	URL	Jellemzők
Gyártók és kormányok biztonsággal foglalkozó portáljai		
Avaya ASA	*http://support.avaya.com/japple/css/japple?PAGE=avaya.css.OpenPage&temp.template.name=SecurityAdvisory*	Avaya Security Advisories portál
Avaya SAC	*http://support.avaya.com/sac*	Avaya Secure Access and Control portál
US-CERT	*http://www.us-cert.gov*	Általános riasztások kereshető formátumban
Red Hat Network	*http://rhn.redhat.com*	Red Hat Enterprise Linux-rendszerrel kapcsolatos biztonsági riasztások és javítások
Microsoft Security Bulletins	*http://www.microsoft.com/technet/security*	Microsoft-termékekkel kapcsolatos riasztások kereshető formátumban
SCO Security Advisories	*http://www.sco.com/support/security*	SCO Unix-rendszerrel kapcsolatos riasztások
Google linkgyűjtemény	*http://www.google.com/Top/Computers/Security/Advisories_and_Patches/Vendor_Releases/*	Google-linkgyűjtemény különböző gyártók biztonsági figyelmeztetéseihez és javításaihoz
Internetes magazinok, tudástárak		
NetAcademia Tudástár	*https://www.netacademia.net/tudastar/*	Microsoft-termékekkel kapcsolatos cikkek, tippek és trükkök
HWSW Informatikai Hírmagazin	*http://hwsw.hu*	Biztonsági kérdésekkel is foglalkozó magyar portál
IT-BUSINESS	*http://www.it-business.hu*	Magyar hírek

AZ INFORMATIKAI BIZTONSÁG LAPJA

SZERKESZTŐSÉG
Főszerkesztő
Sziebig Andrea – *asziebig@vogelburda.hu*
Felelős szerkesztő
Kelemen László – *kelemen@hungary.com*
Vezető szerkesztő
Varga János – *jvarga@vogelburda.hu*
Szerkesztőbizottság
Bártfai Attila – *attila.bartfai@hp.com*
Konkoly Thege Szabolcs – *szabolcs_konkolythege@symantec.com*
Papp István – *ipapp@avaya.com*
Papp Péter – *papp.peter@kancellar.hu*
Szabó Gábor– *gabors@microsoft.com*

Munkatársak
Kelenhegyi Péter – *pkelenhegyi@vogelburda.hu*
Mallász Judit – *jmallasz@vogelburda.hu*
Mészáros Csaba – *mcsaba@vogelburda.hu*
Schopp Attila – *aschopp@vogelburda.hu*
Sós Éva – *pingvin@terminal.hu*

Tervezőszerkesztők
Bujdosó Anikó – *abujdoso@vogelburda.hu*
Papp Gyula – *gypapp@vogelburda.hu*

Korrektor
Bende Magdolna – *mbende@vogelburda.hu*

Fotó
Jekler Gábor – *gjekler@vogelburda.hu*

Lapterv
Kocsis Gábor – *emotion@axelero.hu*

Grafika
Szántói Krisztián – *estharang@index.hu*

Online hírlevél
Kelemen László – *kelemen@hungary.com*
Mészáros Csaba – *mcsaba@vogelburda.hu*

Szerkesztőség és kiadó címe:
Vogel Burda Communications Kft.
1088 Budapest, Kéthly Anna tér 1.
Tel.: 888-3400, fax: 888-3499

KIADÓ
Kiadja a Vogel Burda Communications Kft.

A kiadásért felel
Walitschek Csilla ügyvezető igazgató
cswalitschek@vogelburda.hu
Tel.: 888-3450, fax: 888-3499

Hirdetési igazgató:
Farkas Viola – *vfarkas@vogelburda.hu*
Tel.: 888-3450, fax: 888-3499

Médiareferensek:
Németh Krisztina – *knemeth@vogelburda.hu,* tel.: 888-3468
Oláh Bernadette – *bolah@vogelburda.hu,* tel.: 888-3475
Rátóti Sarolta – *sratoti@vogelburda.hu,* tel.: 888-3453
Szendrey Szilvia – *szendrey@vogelburda.hu,* tel.: 888-3455
Fax: 888-3459

Terjesztési igazgató:
Walitschek Ottó – *owalitschek@vogelburda.hu*
Tel.: 888-3420, fax: 888-3499

Hirdetési koordinátor:
Szőke Erika – *eszoke@vogelburda.hu*
Tel.: 888-3411, fax: 888-3459

Nemzetközi hirdetésfelvétel:
Eric N. Wicha – *ewicha@vogelburda.com*
Vogel Burda Holding
Poccistrasse 11, D–80336 München
Tel.: +49 89 74642-326, fax: +49 89 74642-325
A hirdetések körültekintő gondozását kötelességünknek érezzük, de tartalmukért felelősséget nem vállalunk.

Marketing:
Gajdos Barna – *bgajdos@vogelburda.hu,* tel.: 888-3494

TERJESZTÉSI ADATOK
Ügyfélszolgálat
Tel: 888-3421, 888-3422
Fax: 888-3499
H–P: 9–17 óráig
E-mail: terjesztes@vogelburda.hu
Honlap: www.itmediabolt.hu

ITmédiaBoltok
1054 Budapest, Bajcsy-Zsilinszky út 60.
Tel: 373-0582 H–P: 8–20, Sz: 10–16 óráig

1036 Budapest, Lajos utca 47/a.
Tel: 242-0083 H–P: 9–19, Sz: 10–16 óráig

1117 Budapest, Karinthy Frigyes út 5.
Tel: 361-3408 H–P: 9–19, Sz: 10–16 óráig

Nyomda:
Pauker Nyomdaipari Kft.
1047 Budapest, Baross utca 11-15.
Felelős vezető: Vértes Gábor ügyvezető igazgató
Telefon: 272-2290, Fax: 370-2720
E-mail: nyomda@pauker.hu

Megújult!

www.IT-BUSINESS.hu

Archívum
Karrier
Fotósarok
Eseménynaptár
IT-BUSINESS Club

Magazin előfizetés
Ingyenes hírlevél regisztráció

VOGEL BURDA COMMUNICATIONS