WWW.IT-SECURITY.HU

IV. ÉVFOLYAM 2. SZÁM 2007. FEBRUÁR 20.

IT-SECURITY

AZ INFORMATIKAI BIZTONSÁG LAPJA

AZ IT-BUSINESS MELLÉKLETE

Ez nem a te (hon)lapod!

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

TÖBB A LYUK, MINT A SAJT

Az internetpenetrációval párhuzamosan átjáróházzá váltak a weboldalak.

Egy magára valamit is adó honi vállalkozásnál axióma az internetes jelenlét. Persze kérdéses, ki mit ért jelenléten. Van, aki ezt a fogalmat egy névjegy jellegű megjelenéssel azonosítja, a többség azonban magának a cégnek az üzletmenetét is kisebb-nagyobb mértékben az internetre alapozza.

Az internet internacionális voltából adódóan ugyanakkor bárhonnan, bárkit megtámadhatnak. Feltéve, ha nem védi kellőképp magát. Pontosabban cégének „kirakatát", vagyis a honlapját. Merthogy elképesztően sérülékenyek a honlapok! A legfrissebb statisztikák szerint az átlagosan meglévő 66 sebezhető pont miatt a webhelyek 70 százaléka bizony meghackelhető. S ami sebezhető, azt többnyire meg is sebzik. Hogy miért? Mondjuk, üzleti információszerzés céljából. Vagy azért, mert egy technológia ellen forralnak bosszút a behatolók. Nemegyszer politikai indíttatású a honlap elleni támadás, olykor pedig egyszerű szakmai virtuskodásnak esik áldozatul egy-egy webhely.

Sokszor csupán puszta kíváncsiságból „néznek körül" a cég honlapjá(ba)n, s aztán merő jóindulatból elmesélik, hogy merre sétálgattak. Nem egy olyan történetet ismerek, amikor az informatikai tudással felvértezett egyetemista finoman csak annyit közölt a baráti körébe tartozóval: a haverjuknál a céges védelem olyan lyukas, mint az ementáli sajt. Jóindulattal ezt a fajta felderítést akár etikus hackelésnek is nevezhetnénk. Merthogy itt befejeződött a behatoló áldásos tevékenysége, s a cég nem kompromittálódott. Megmaradt az amúgy gondosan építgetett imázsa. A hozzá nem értő külvilág előtt.

Sziebig Andrea

Sziebig Andrea
főszerkesztő

IT-BUSINESS TODAY

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

Regisztráljon!

www.it-business.hu/hirlevel

TERMÉKHÍREK

MEGKÉRDEZTÜK

CÍMLAPON

Ez nem a te (hon)lapod!

A honlapfeltörések a mindennapok részei. Nem csoda, hiszen a webhelyek elképesztő mértékben sérülékenyek. Egy vizsgálat szerint a honlapok 70 százaléka felett vehetnék át a hackerek az ellenőrzést. Jelenleg több mint 200 ezer weblap-sérülékenység ismert; ezekből egy honlapra átlagosan 66 jut. A problémát ma már nem annyira az erőfitogtató, harsány honlap-elcsúfítások jelentik, hanem az alattomos, üzleti célú támadások.

14. oldal

ESZKÖZTÁR

KOMMUNIKÁCIÓ

MENEDZSMENT

Szemmel tartott Linux

Önálló eszközt igényel a hálózati kiszolgálógépek felügyelete.

Unbreakable Linux (Törhetetlen Linux) programjának résztvevői számára kínál átfogó vállalati felügyeleti megoldást az Oracle Management Pack for Linux nevű új szoftvercsomagja.

Az Enterprise Manager 10g felügyeleti termékre épülő kiegészítés kiszolgálóéletciklus-kezelést biztosít a Linuxhoz, és ezzel a gyártó szerint jelentősen csökkenti a Linux-környezetek összetettségét, illetve felügyeleti költségeit.

Ez nem az a film

A Management Pack for Linux felügyeleti csomaggal a rendszergazdák az adott alkalmazáskörnyezettől függetlenül – vagy azzal összefüggésben – végezhetik el a Linux-kiszolgálók jogosultságkezelését, működésfigyelését és adminisztrációját, valamint a hibajavítások telepítését.

Előnye a terméknek, hogy a Linux-kiszolgálók, valamint a rajtuk futó alkalmazások és adatbázisok felügyelete egyetlen integrált megoldás segítségével végezhető. Ezáltal a felhasználók teljes körű és valós idejű adatokat kapnak a Linux-környezetekről, ami egyrészt hatékonyabbá teszi az üzemeltetést, másrészt csökkenti az állásidőt és az azzal járó költségeket.

A Systems funkcióval a Linux-kiszolgálók a felügyelet szempontjából egyetlen, jól elkülönülő csoporttá szervezhetők a többi alkalmazás-

www.oracle.com

szerver-komponenssel együtt. Ennek köszönhetően megvalósítható az átfogó teljesítmény- és állapotkövetés, kiegészítve a mögöttes okok elemzésével az alkalmazások szolgáltatási szintjén.

Tóth István

Újabb rés az irodán

A sérülékenység túlmutat az Excelen.

A széles körben használt Office irodai csomagot érintő, nulladik napi sérülékenységről tett közzé információkat a Microsoft-fé-

Milyen alkalmazások érintettek?

le Security Response Center. A windowsos Office 2000-et, XP-t és 2003-at, valamint a maces Office 2004-et veszélyeztető hibát egy rosszindulatúan kialakított Excel-táblázat segítségével lehet kihasználni.

Szakértők véleménye szerint elképzelhető, hogy a sérülékenység túlmutat az Excelen, és más Office-alkalmazásokat is érint.

A most bejelentett Excel-hiba az ötödik nem javított biztonsági rés az Office-

www.microsoft.com

ban, amelynek létezését a Microsoft tavaly december óta elismerte. A javítás megjelenéséig az Office-t használók úgy védhetik meg magukat a fenyegetéssel szemben, hogy nem nyitják meg az elektronikus levelek mellékleteként érkező vagy az interneten letöltésre kínált Office-dokumentumokat.

ADATHALÁSZATI FRISSÍTÉS

Az Internet Explorer 7 phishing ellenes szűrőjének hibáját orvosló frissítést tett közzé mind az XP-s, mind a vistás változathoz a Microsoft. A cég mindazoknak ajánlja a frissítés azonnali letöltését, akik a böngésző rejtélyes lelassulását tapasztalják a sok keretet tartalmazó weboldalak meglátogatása közben. Ennek hátterében az áll, hogy az adathalászati szűrő ellenőrzi a weboldal tartalmát, ami a hibás működés miatt jelentősen megnöveli a számítógép processzorának terhelését.

MEGKÖSZÖNT TÁMOGATÁS

Illegálisan másolt Microsoft-szoftverek segítségével építette fel technológiai iparát Románia, mondta *Traian Basescu* román elnök *Bill Gatesnek*, az óriáscég alapítójának. Traian Basescu és Bill Gates a Microsoft globális technikai központjának megnyitóján találkozott egymással Bukarestben.

Az eseményt követő sajtótájékoztatón a szókimondó román elnök arról beszélt, a szoftverkalózkodás komoly szerepet játszott abban, hogy a fiatal generációk megismerték a számítógépeket. Bill Gates nem reagált az elhangzottakra.

Egyébként szakértők szerint a Romániában jelenleg használt szoftverek 70 százaléka kalózmásolat, és a román főváros irodaépületeiben még mindig találkozni a lopott programokat árusító nepperekkel.

Kevesebb a személyiséglopás

Megfelelő intézkedésekkel és a fogyasztói szokások megváltoztatásával visszaszoríthatók a bűncselekmények.

A Javelin Strategy & Research piackutató cég felmérésén alapuló előzetes adatok szerint meghozták az első eredményeket a személyiséglopás elleni összehangolt kormányzati intézkedések az Egyesült Államokban: ugyanis közel 12 százalékkal csökkentek tavaly az e bűncselekményből származó veszteségek.

Ami a konkrét számokat illeti: míg 2005-ben 55,7 milliárd dollárra becsülték az áldozatokat ért kárt, addig 2006-ban 6,4 milliárd dollárral 49,3 milliárd dollárra mérséklődött a veszteség (ami azért továbbra is elképesztően nagy összegnek számít).

Örvendetes tény ugyanakkor az is, hogy hozzávetőlegesen félmillióval kevesebben estek áldozatául e veszedelmes bűncselekménynek, ami még mindig az ország felnőtt lakosságának 3,7 százalékát érintette tavaly. Szakértők szerint a javulás hátterében a cégek és a fogyasztók megváltozott szokásai és fokozott óvatossága állnak.

A felmérés megállapította azt is, hogy leginkább a 18–24 éves korosztály csalható lépre a személyiségtolvajok által alkalmazott módszerekkel: ennek a korcsoportnak nem kevesebb mint 5,3 százaléka – vagyis minden huszadik fiatal felnőtt – válik áldozattá az Egyesült Államokban.

www.coworldcs.com
www.alphasonic.hu

Fogyasztói szokások

RUGALMAS BŐVÍTHETŐSÉG

Már Magyarországon is kaphatók a Coworld NDAS technológián alapuló, Sharedisk Home nevű külső hálózati tárolóeszközei a cég hazai forgalmazójánál, az Alphasonicnál. A kisirodáknak és otthoni felhasználóknak szánt berendezésekkel mind hálózaton keresztül, mind közvetlenül a számítógéphez csatlakoztatva gyorsan és biztonságosan növelhető a tárolókapacitás.

Az NDAS technológiájú merevlemezes tárolók más hálózati tárolóeszközökkel ellentétben nem az internetet használják az adatátvitelhez, hanem a számítógépek saját hálózatát, így az átviteli sebesség nem függ az internetkapcsolat sebességétől. További előny a nagyobb biztonság, mivel az internetről nem érhető el a tároló, a hálózaton belül pedig jelszó védi a hozzáférést.

Erős és egyszerű

Kémprogramok, vírusok és egyéb hálózati támadások elleni hardveres védelem.

Nagy- és középméretű vállalatok internet felőli védelmét ellátó appliance-t fejlesztett ki a Check Point, amellyel a hagyományosan nagyvállalati ügyfelekre koncentráló internetbiztonsági cég az egyre inkább gyarapodó kis- és középvállalati szegmens igényeit igyekszik kielégíteni.

Telepítés és felügyelet

A magyarországi értékesítés megkezdését megelőző sajtóbeszélgetésen a Check Point értékesítési és műszaki szakemberei az UTM–1 kiemelkedő tulajdonságai közül a telepítés és a központi felügyelet egyszerűségét emelték ki.

A tűzfal, a vírus- és kémprogram elleni védelem, valamint a web- és csomagszűrés mellett az UTM–1 Web Application Firewallját webkiszolgálók, VoIP-alkalmazások, azonnali üzenetküldők és pont–pont hálózatok kezelésére is felkészítették.

Az egység központi felügyeleti szoftvere, a Check Point Smartcenter további kiegészítők nélkül képes ellátni a központosított felügyeletet, az integrált SSL- és virtuális magánhálózati technológiák pedig távoli alkalmazottak hálózati csatlakozás biztonságossá tételére szolgálnak, miközben átlátható képet adnak az adminisztrátoroknak az infrastruktúráról.

Központilag felügyelhető

Egyszerűen bekapcsolódva

Mindezek mellett az UTM–1 termékek kihasználják a Check Point egységes biztonsági architektúráját: egyszerűen bekapcsolódnak a már telepített Check Point-környezetbe, aminek a rendszergazdák például a biztonsági események kezelése, a frissítések elosztása, a biztonsági házirend alkalmazása során látják előnyét. A frissítéskövetésre különféle licenceket ajánl a gyártó.

Kelenhegyi Péter

Megőrzött levelezés

A vállalati adatok szigorú szabályok szerinti kezelése komoly kihívás elé állítja az informatikusokat.

Minthogy a terrorizmus és a nemzetközi bűnözés visszaszorítása érdekében hozott kormányzati szabályozások kötelezően előírják bizonyos információk meghatározott ideig tartó megőrzését, elemzők szerint az elkövetkezendő években a szervezetek világszerte 7000 petabájtnyi adatot archiválnak majd.

A Symantec-féle Enterprise Vault 7.0 intelligens tartalomarchiválási megoldással a gyártó szerint költségkímélő módon archiválhatók az elektronikus levelezés mellett egyéb tartalmak is, betarthatók a megőrzési és megfelelési előírások, valamint a szoftvertámogatást nyújt az e-felderítéshez és a tudásmenedzsmenthez. A hatékony információkezelés megköveteli az adatok megfelelő kategóriákba sorolását, valamint a kategóriákra vonatkozó szabályok betartását. Az Enterprise Vault 7.0 új, intelligens kategorizálási megoldást nyújt, amely lehetővé teszi a tartalom megőrzését vagy eltávolítását annak üzleti értéke alapján.

Csökkentett postafiókméret

Az automatizált osztályozási motor csökkenti az archivált anyagok méretét és a keresési időt, és lehetővé teszi az e-mailek 50, előre meghatározott vagy korlátlan számú szabály szerinti megőrzését. A felhasználói osztályozási motor következetes adatmegőrzési programot biztosít azáltal, hogy minden egyes e-mailt osztályoz, amint azt létrehozták vagy elolvasták a Microsoft Office Outlookban.

A Microsoft Exchange Server 2007-tel együttműködő Enterprise Vault 7.0 csökkentett postafiókméretet biztosít, megszünteti a PST fájlok és kontingensek szükségességét, valamint gyorsabb mozgatást tesz lehetővé. A Windows Desktop Search (WDS) támogatása az első archiváláskor jelentősen növeli a hatékonyságot, mivel lehetővé teszi az állományok, valamint az archivált és élő e-mailek gyors keresését egy közös keresőeszköz alkalmazásával. Az Enterprise Vault korábbi változatai közel 5000 ügyfél mintegy 8 millió postafiókját kezelik világszerte.

Ugyancsak új termék a Symantec kínálatában a Veritas Storage Foundation 5.0 High Availability, amely az adatok és alkalmazások elérhetőségét biztosítja a Windows-környezetekben. Két vezető iparági megoldást – a Storage Foundation Windowshoz készült változatát és a Veritas Cluster Servert – ötvöz, amelyek a gyártó szerint együtt magasabb szinten biztosítják a tárolási menedzsment egyszerűsítését, a magas fokú elérhetőséget, valamint az olyan kritikus fontosságú Windows-alkalmazások helyreállítását, mint a Microsoft Exchange, az SQL Server és a SharePoint Portal Server.

Tóth István

TOVÁBBI TERJESZKEDÉS

Aláírta a végleges megállapodást a Symantec az Altiris felvásárlásáról. Az Altiris által gyártott IT-menedzsmentszoftverek lehetővé teszik a vállalkozások számára hálózat alapú végpontjaik egyszerű kezelését és kiszolgálását, a mobileszközöktől kezdve a kiszolgálógépekig és tárolókig. A megállapodásnak megfelelően az Altiris részvényesei 33 dollárt kapnak készpénzben részvényenként a nettó 830 millió dollár értékű tranzakció eredményeként. Az Altiris felvásárlásától a Symantec piaci pozíciójának megerősödését, valamint a vállalati végpontokat érintő megoldások magasabb szintre emelését várja.

AZONNALI VÉDELEM

A Windows Vista megjelenése előtt kompatibilissé tette az új operációs rendszerrel a Norton Internet Securityt, a Norton Antivirust és a Norton Confidentialt a Symantec. Az első két termék korábbi előfizetői jogosultak lesznek arra is, hogy letöltsék a Symantec Online Network for Advanced Response (SONAR) technológiát tartalmazó frissítést. A kártékony kódokat még a vírus- és kémprogram-definíciók megjelenése előtt kiszűrni képes technológiához a Wholesecurity felvásárlásával jutott a Symantec.

Lehúzott redőny

Minden lehetséges behatolási pontot figyelemmel kell kísérni a hatékony védelemhez.

A vállalati számítógépeket nem csak a helyi hálózatból és az internetről érkező támadásokkal szemben kell megvédeni, ugyanolyan veszélyt jelentenek a külvilággal kapcsolatot tartó különféle csatlakozók (soros, párhuzamos, USB, FireWire), a vezetéknélküli átvitelt biztosító adapterek (Bluetooth, wifi, infra) és a hordozható adattárolókat (cd, dvd, hajlékonylemez, szalagos kazetta stb.) fogadó meghajtók, amelyekhez a hozzáférést a legtöbb gépen semmi sem korlátozza.

www.devicelock.com

A felsorolt eszközök védelmére kifejlesztett DeviceLock program biztosítja a munkaállomások hálózaton keresztüli ellenőrzését, és megvédi a háttértárolókat a véletlen vagy szándékos formázástól. A jogosultságok gép és felhasználó szerint adhatók meg, és az eszközök ellenőrzése időhöz köthető. A legfrissebb, 6.1-es változat újdonságai között megemlítendő a billentyűleütéseket figyelő programok felismerése, a rendszergazdák bővített kezelési lehetőségei, valamint az auditrekordok automatikus összegyűjtése a távoli gépekről és központi tárolása a DeviceLock Enterprise Serveren.

Ellenőrzött adatmozgás

A kimenő információk nyomon követésével megakadályozható a kiszivárogtatás.

Beláthatatlan következményekkel járhat az értékes vállalati adatok elvesztése és illetéktelen kezekbe kerülése. Nem csupán az anyagi kár lehet jelentős, hanem csökkenhet az ügyfelek bizalma, ami a részvényárfolyam és a piaci érték csökkenéséhez vezet. Felmérések szerint csak az Egyesült Államokban több mint 100 milliónyi személyes adat került nyilvánosságra 2005 eleje óta biztonsági rések miatt.

A McAfee adatvesztés ellen védő Data Loss Prevention nevű terméke a gyártó szerint átfogó megoldást kínál a bizalmas adatok megőrzésére, mind a rosszindulatú támadások, mind a véletlen incidensek ellen. Lehetőséget nyújt a kimenő adatok ellenőrzésére levélküldéskor, azonnali üzenetváltásnál, nyomtatáskor, valamint USB-tárolók, optikai lemezek és egyéb eszközök használatakor.

A Data Loss Prevention tartalomtól és környezettől függően képes blokkolni a kritikus adatok átvitelét, másolt, kivágott, beillesztett, rejtett vagy tömörített állományokban is. A termékhez mellékelt szerverkomponens segítségével a rendszergazdák központilag ellenőrizhetik a kimenő adatok végpontját és a valós idejű eseményeket. A Data Loss Preventionnel rögzíthetők a végpontok, az adatkezelés és az adatátvitel pedig átlátható, jól körülhatárolt lépések sorozatává válik.

Szintén a McAfee-vel kapcsolatos hír: a webes keresés és böngészés biztonságosabbá tételére hivatott, eddig több mint 10 millió példányban letöltött McAfee Siteadvisor adathalászat elleni védelemmel bővült. A régebbi Siteadvisor-változat automatikusan bővül az új funkcióval. A Siteadvisor más fejlesztők programjainak kiegészítéseként is használható.

Tóth István

Szivárgás ellen

Tartalomszűréssel és titkosítással kombinálja a portok menedzsmentjét a Pointsec Device Protection.

Pendrive-okon, okostelefonokon, digitális kamerák és zenelejátszók tárolóin akár több gigabájtnyi adatmennyiséget is ki lehet csempészni a cégtől úgyszólván a rendszergazdák, informatikusok orra előtt.

Gyártója szerint a Pointsec Device Protectionnel a maga nemében egyedülálló módon, igen aprólékosan beállítható, milyen eszközök csatlakoztathatók a számítógéphez, és milyenek nem, az adattárolásra alkalmasak titkosítva legyenek-e, és azokon milyen adatok kerülhetnek ki a cégből, illetve milyenek juthatnak be oda.

www.filtermax.hu
www.pointsec.com

Tolvajkulcs köntösben

A Pointsec hazai képviselője szerint a magyarországi cégeknél még nemigen számolnak a nagy mennyiségű adat tárolására alkalmas hordozók veszélyeivel.

Nem meglepő tehát, hogy sokan csak a bizalmas adatok kiszivárgása után szembesülnek a problémával. Ezt tetézi, hogy a jogvédő szervezetek is mind élénkebb aktivitást mutatnak; így nem mindegy, milyen jogvédett zenék és filmek találhatók a vállalati számítógépeken. ■

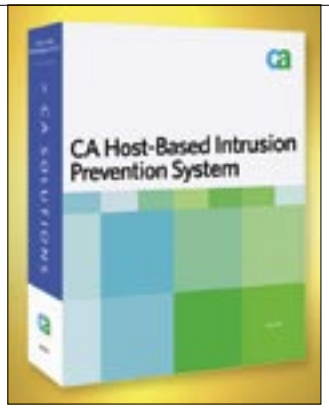
Példákból tanul

Host alapú, központosított behatolásvédelem.

Az összetett fenyegetések kivédéséhez olyan védelemre van szükség, amely egyesíti a fenyegetések megelőzését, és szorosan együttműködik a meglévő vírusellenőrző és kémszoftverelhárító technológiákkal. A CA szerint ilyen a 2007-es RSA konferencián bejelentett Host-Based Intrusion Prevention System (CA HIPS), amely a bejövő és kimenő forgalmat egyaránt figyeli, emellett lehetővé teszi a hozzáférés-felügyeleti irányelvek központosított adminisztrációját.

Meglévő minták és a felhasználók viselkedése alapján készíthetők el az irányelvek, s ezzel a „példákból tanuló” módszerrel megtakarítható az egyes szerepekhez, alkalmazásokhoz és/vagy erőforrásokhoz szükséges irányelvek külön-külön beállítása. Például az USB-tárolók használata bizonyos felhasználókhoz, alkalmazásokhoz vagy időpontokhoz köthető, de az LDAP-ban és a Microsoft Active Directoryban definiálhatók irányelvek megadott felhasználókhoz és csoportokhoz, illetve egyes biztonsági mechanizmusokhoz, például tűzfalakhoz, IDS-ekhez és IPS-ekhez, valamint az alkalmazások bizonyos típusaihoz is.

http://ca.com



Munkaállomásonként 40 dollár

Kelenhegyi Péter

Kezdődik minden elölről

Már nemcsak próbálgatják a nagyfelbontású filmek titkosításának feltörését.

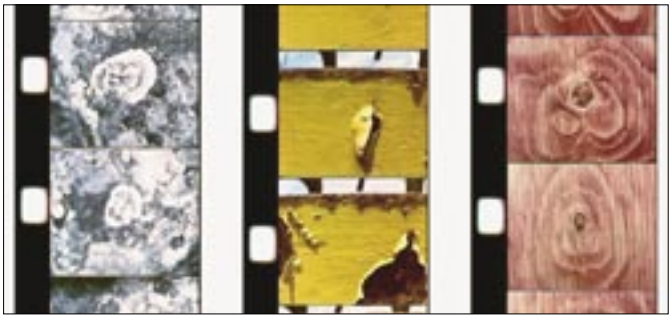
Elismerte az Advanced Access Content System (AACS) digitális jogokat kezelő (DRM) rendszer licencelésével foglalkozó szervezet – az AACS Licensing Administrator –, hogy a muslix64 néven azonosított hacker egy PC-s lejátszószoftver hibáját kihasználva megszerezte néhány nagyfelbontású film titkosításának feloldásához szükséges kulcsot. Ennek birtokában le tudja másolni a szóban forgó filmeket, függetlenül attól, hogy Blu-ray vagy HD DVD formátumúak.

www.aacsla.com

A hollywoodi stúdió a kulcs megváltoztatása mellett döntött a későbbiekben gyártásra kerülő példányok esetében.

Ugyanakkor egy másik – amezami fedőnévvel tevékenykedő – hacker muslix64 módszerénél egyszerűbben is fel tudja törni a Blu-ray és HD DVD médiák védelmét. Amezami ráadásul minden, a dekódoláshoz fontos titkosító paramétert is megtalált, és eljárása bármikor alkalmas lehet akár a megváltozott kulcsok kinyerésére is.

Tóth István



MEGKÖTÖTT KEZEK

Nem kutathat a rendőrség feltételezett bűnözők számítógépében az interneten keresztül az illetők tudta nélkül – mondta ki precedens értékű ítéletében a karlsruhei német szövetségi bíróság, amely szerint az ilyen módszerek bevezetéséhez jogi szabályozásra, azaz a parlament által elfogadott törvényre van szükség. Ennek kapcsán az online adatgyűjtés jogi szabályozását sürgette a német Szövetségi Bűnügyi Hivatal (BKA) elnöke, *Jörg Ziercke*, mivel véleménye szerint a titkos internetes nyomozás nélkülözhetetlen fegyver a nemzetközi terrorizmus és a szervezett bűnözés ellen vívott harcban. Hasonlóképpen foglalt állást a rendőrség szakszervezetének elnöke, *Konrad Freiberg* is, aki rámutatott, hogy a törvényhozóknak mielőbb jogi alapot kell biztosítaniuk a magántulajdonban lévő számítógépek titkos átkutatására.

Trükkös képek

Egyre kifinomultabb módszereket igényel a rejtőzködő levélszemét kiszűrése.

Kutatások szerint a képeket tartalmazó levélszemét egyre több bosszúságot okoz, mert kijátssza a hagyományos levélszemétszűrőket, ezzel pedig túlterheli a levelezőkiszolgálókat és a postafiókokat. Nap mint nap kéretlen levelek százmilliói lepik el a világhálót: a spam

www.maysoft.com

az összes e-mail 90 százalékát teszi ki. A kép alapú levélszemét az elmúlt fél év során terjedt el, jelenleg az összes levélszemét 35 százaléka ilyen típusú. S mivel a képek lényegesen nagyobb helyet foglalnak el, mint a szöveg, ezek a levelek adják a teljes spamsávszélesség 70 százalékát.

A Mayflower Software Lotus Domino rendszereken működő spamszűrője, a Spamsentinel V5 egyik újdonsága, hogy a korábbiaknál hatékonyabban azonosítja a kép formájában érkező kéretlen üzeneteket. A fejlesztők fő célkitűzése a 98,5 százalékos szűrési eredmény és a közel nullaszázalékos mértékű téves szűrés elérése, amit a hagyományos spamek esetében már megvalósítottak. A SpamSentinel további újdonságai között megtalálható a natív Linux-verzió megjelenése, valamint az Auto Installer funkció, amelynek révén a jövőbeli frissítések automatikusan telepítődnek, s ennek megtörténtéről a program e-mailben küld értesítést.

Minden Windowshoz

A rootkitek ellen is védeni kell.

Megjelent a NOD32 2.7 vírusellenes programcsomag magyar verziója, amely a Microsoft összes 32 és 64 bites operációs rendszere alatt – a Vista összes változatát is beleértve – használható. A 2.7-es változat egyik legfontosabb újdonsága a továbbfejlesztett rootkit-ellenes védelem, ami már nem csupán a rootkitek településének

www.nod32.hu

megakadályozására képes, hanem arra is, hogy heurisztikus technológiájának segítségével felismerje és blokkolja a számítógépre korábban feltelepült, aktív rootkiteket. Ily módon a NOD32 mindenféle rosszindulatú fenyegetés – vírusok, férgek és trójaiak, kémprogramok, kéretlen reklámprogramok, adathalász fenyegetések és rootkitek – ellen felveszi a küzdelmet.

A NOD32 korábbi magyar nyelvű változatai a következő hetekben automatikusan frissíteni fogják magukat a 2.7-es verzióra. Akik minél előbb szeretnének továbblépni az új változatra, a program weboldaláról tölthetik le a telepítő csomagot.

Felismer és blokkol

Kalózparadicsom

Továbbra is virágzik a zenék illegális terjesztése.

Hiába minden igyekezet a kiadók részéről az illegális zeneletöltés visszaszorítására, a kalózkodás eredményeképpen még mindig sok millió dollár veszteséget kénytelenek elkönyvelni a jogtulajdonosok. Az

iparág kétségbeesetten igyekszik pótolni a cd-k évek óta csökkenő eladásaiból származó bevételkiesést a legális letöltésekből befolyó összegekkel. Szakértők becslése szerint azonban havonta több mint 1 milliárdnyi zeneszámmal kereskednek illegálisan a neten, miközben a legális online eladások több mint 70 százalékát magáénak tudó iTunes zeneáruházban 2003-as indítása óta alig több mint 2 milliárdnyi dalt értékesítettek.

Felmérések szerint tavaly az illegális letöltések száma 24 százalékkal emelkedett.

Kernelszintű védelem

Napjaink biztonsági programjai egyre összetettebb szolgáltatásokat nyújtanak.

Az internetes fenyegetések fejlődésével az adatlopó szoftverek, a reklám- és kémprogramok, a vírusok és a rootkitek egyszerre fenyegetik a világhálóra kötött számítógépeket.

Az újratervezett Counterspy 2 kémprogram-eltávolító második kiadása voltaképpen egy vírusellenes program és egy kémprogram-kereső hibridje, amely az egyre kifinomultabb rosszindulatú kódok valamennyi fajtájától igyekszik megvédeni használóját.

Az új Firstscan technológia révén a Counterspy 2 a Windows betöltődése előtt, a Windows-rendszerhívások megkerülésével képes a károkozók eltávolítására, így a rendszerhívásokat meghamisítani próbáló rootkitek és kémprogramok nem tudnak rejtve maradni. A kernelszintű aktív védelemnek köszönhetően a program még a rendszerindulás előtt képes blokkolni a károkozókat, a nemkívánatos

www.sunbelt.hu

rendszermódosításokat pedig a károkozó azonnali felfüggesztésével tudja megakadályozni.

Tóth István

FOTÓ: IT-SECURITY

Ludman Zoltán IT-biztonsági konzultáns, HP Magyarország

Ellenőrzött betörések

Inkább egy liter verejték a gyakorlótéren, mint egy csepp vér a csatában – a régi katonai igazság szelleme vezeti azokat az informatikai vezetőket, akik egyfajta hadgyakorlatként, kontrollált körülmények között tesztelik védelmi rendszereiket. Az etikus hackelés nem hiányozhat az IT-biztonsági eszköztárból.

– A hackertámadás az informatikai vezetők rémálmai közé tartozik. Miért vállalkozik mégis egy cég arra, hogy megkísérelje feltöretni informatikai rendszereit?

– Saját hálózatukat, informatikai rendszereiket a szakemberek is hajlamosak biztonságosabbaknak ítélni, mint amilyenek azok valójában. Ezért is ajánlott egy kívülálló, független szakértővel is felülvizsgáltatni a rendszert, aki más szemszögből is szemügyre veszi az infrastruktúrát, hogy előjöjjenek az esetleges rejtett hiányosságok is. A már számos iparágban kötelező IT-biztonsági audit segít egzakt eredményeket kapni a rendszer működéséről, biztonságáról. Ellenkező esetben ezekre csak olyankor derül fény, amikor már megtörtént a baj. A vizsgálatok egyik speciális válfaja az etikus hackelés, behatolási (penetration) teszt.

Többet tudunk, mint egy átlagos számítógép-kalóz

– Ezek szerint az etikus hackelést egy átfogó biztonsági vizsgálat részének kell tekinteni? Érdemes-e önálló projektként futtatni?

– Mindenképpen célravezető lehet, ha a behatolási teszt egy szélesebb körű biztonsági ellenőrzés egyik állomása. A szabályzatokat, a struktúrát, a szabályrendszereket átvizsgálva már sok mindenre fény derülhet, de mint oly sok esetben, itt is jellemzően sok rejtett hiba, sérülékenység, biztonsági rés deríthető ki a tényleges átfogó felülvizsgálat alapján.

Ugyanakkor az etikus hackelés külön projektként is megállhatja a helyét, és nagyon hasznos eredményekkel szolgálhat a hálózat, a rendszerek pillanatnyi biztonsági állapotáról. A hangsúly itt a „pillanatnyin” van: mivel a hálózati környezet folyamatosan változik, a behatolási tesztet is rendszeres időközönként (ideális esetben évente) meg kell ismételni.

– Milyen hibák, sérülékenységek felderítésére alkalmas egy behatolási teszt?

– Számos olyan elem van, amely hozzájárulhat egy hálózat sérülékenységéhez, és ezeknek csak egy része függ a szoftverektől vagy a hardverektől. A legjellemzőbb hiányosságok a vizsgált rendszerekben a tervezés hibáiból, a nem megfelelően végiggondolt kiépítésből, a szegmentáció, illetve az egyes komponensek (tűzfalak, behatolásmegelőző rendszerek) hiányából, nem megfelelő konfigurációjából adódnak. Gyakran tapasztaljuk, hogy kritikus fontosságú kiszolgálókat nem megfelelően védenek a hálózat többi részétől: olyan hálózati szegmensben működnek, ahova azoknak a felhasználóknak is szabad bejárásuk van, akiknek semmi közük az adott kiszolgálóhoz és a rajta futó alkalmazásokhoz – ez pedig egyértelműen kockázati tényező.

Hasonlóképpen komoly problémák forrása lehet a hiányosan vagy roszszul konfigurált vezetéknélküli hálózat, amely a megfelelő hatótávolságon belül akár a teljes belső hálózatot elérhetővé teheti idegenek számára, anélkül, hogy a fizikai védelmen át kellene jutniuk (a megfelelő azonosítás, titkosítás hiánya vagy nem megfelelő volta). Ma már rendelkezésre állnak a megfelelő eszközök ezek elkerülésére: használhatjuk a WPA-t, amely 128 bites titkosítást használ, vagy alkalmazhatjuk a WPA2-t AES (Advanced Encryption Standard) titkosítással – természetesen a jelszó-házirend helyes megválasztása és betartása mellett.

Szomorú tapasztalat az auditfolyamatok során, hogy bár sok cég rendelkezik kellő alapossággal megtervezett és megírt biztonsági szabályzattal, azt nem a kellő szigorral tartják be (például a jelszó- vagy a jogosultságkezelés terén), ezáltal olyan, mintha nem is lenne.

Természetesen a nem megfelelően konfigurált eszközök is számtalan behatolási lehetőséget kínálnak a támadóknak. Gondot okozhat, ha nem telepítik a szükséges frissítéseket és javítókódokat (bár speciális, mondjuk, banki alkalmazások esetében ez nem triviális folyamat),

vagy ha feleslegesen futó alkalmazásokat hagynak az adott szervereken (ezek alapértelmezett telepítéskor kerülhetnek fel a gépekre mind Microsoft-, mind Unix-környezetben). Ezeknek az árván hagyott alkalmazásoknak a patchelése sokszor elmarad, ami könnyű bejutási pontot jelenthet az adott kiszolgálóra. A titkosítást nélkülöző hálózati kommunikációs protokollok (ftp, http, telnet) is nagyban csökkenthetik a hálózat biztonságát; az ilyen hálózati forgalom monitorozása során a támadó értékes információkhoz (felhasználónév/jelszó) juthat hozzá.

– Hogyan dolgozik az etikus hacker? Úgy kell elképzelni, mint az igazi számítógépkalózt: ül valahol a gépe előtt, és keresi a gyenge pontokat?

– Többféle tesztet is takar az etikus hackelés kifejezés, és ezek közül az úgynevezett „black box" teszt az, amely a leginkább hasonlít a fenti forgatókönyvre. Ilyenkor a tesztelést végző szakembernek gyakorlatilag semmilyen előzetes információ nem áll a rendelkezésére a vizsgálandó hálózatról vagy szerverről, és így kell a lehető legtöbb rejtett információhoz jutnia, minél több sérülékenységet kiderítenie.

Egy másik változat a „white box" teszt, amikor többféle információ is a szakember rendelkezésére áll. Ezzel a számítógépes kártevők egy másik nagy csoportjának a viselkedését lehet szimulálni: a bosszúálló vagy csak kíváncsi belső munkatársét. Ő már rendelkezik valamilyen hozzáférési jogosultsággal, bizonyos szinten ismeri a hálózat felépítését, esetleg azt is tudja, hogy milyen típusú szerverek működnek a háttérben. A kettő között persze lehet átmenet is, attól függően, mennyi információt kap a tesztelő.

FOTÓ: IT-SECURITY

Mind a két esetben beszélhetünk még külső és belső tesztről is, a szolgáltatás jellegétől függően. Ha olyan szerverről van szó, amely az internet felé kínál szolgáltatásokat, akkor értelemszerűen külső vizsgálattal kell kezdeni, még akkor is, ha tűzfal mögött van.

– Milyen támadásokat próbálhat ki egy etikus hacker?

– Ezt a kérdést még a felmérés kezdete előtt tisztázni kell. Megpróbálhat jogosultságokat megszerezni, sérülékenységeket kihasználni (buffer overflow, null session share, code execution), adatokat „lopni", átvenni az ellenőrzést egy gép vagy egy hálózati szegmens felett, esetleg szolgáltatásmegtagadási támadást (DoS) indítani a hálózat vagy egy szerver ellen. Ilyenkor természetesen azt is figyelembe kell venni, hogy mi lehet egy-egy támadás következménye. Egy szolgáltatásmegtagadási támadás például időlegesen elérhetetlenné teheti azt a kiszolgálót, amely ellen irányul, ezért az ügyfélnek kell mérlegelnie, hogy mikor, melyik szerveren és milyen időtartamú szolgáltatáskiesést tud elviselni. Az ilyen jellegű tesztek egyeztetett leállási időn belül történnek, amely nem befolyásolja a felhasználók munkavégzését. A vizsgálat történhet egy erre a célra létrehozott, az eredetivel mindenben megegyező környezetben is (sandbox), kifejezetten kritikus rendszerek esetében.

Választ lehet adni arra, mi sérülékeny az adott hálózatban

– Vajon titokban kell-e tartani az etikus hackelés tényét a dolgozók és az informatikai munkatársak előtt?

– Ez a vizsgálat céljától függ. Ha csak az illetékes vezető tud a tesztről, akkor az etikus hackelés a belső informatikai vagy IT-biztonsági csapat ellenőrzésére is használható. Sokatmondó, hogy az erre szolgáló eszközök (tűzfalak, behatolásmegelőző rendszerek) küldenek-e riasztást, a rendszergazdák észreveszik-e, hogy támadás indult az általuk felügyelt rendszerek ellen, mikor veszik észre, mit tesznek ebben az esetben, milyen visszajelzések érkeznek tőlük, milyen mértékben tartják be az erre az esetekre megállapított szabályokat.

Hasonlóképpen adott a lehetőség, hogy az etikus hackelés társuljon egy „social engineering" vizsgálattal is. Ilyenkor nem csupán az informatikai környezetet tesztelik, hanem minden biztonsági rendszer leggyengébb elemét, az embert is. Ezzel ellenőrizni lehet, hogy a munkatársak betartják-e a lefektetett irányelveket, tisztában vannak-e a biztonság fontosságával, menynyire hiszékenyek, ha ismeretlenek keresik őket telefonon vagy akár személyesen. Kiadnak-e kritikus információkat (például a jelszavukat telefonon), ha valaki egy hihető mesével áll elő?

– Milyen eszközöket használnak a teszteléshez? Ugyanazokkal a szoftverekkel dolgoznak, mint egy igazi hacker?

– Mindig az adott feladat határozza meg, hogy milyen eszközökhöz nyúl a tesztet végző személy vagy csapat. A felhasznált eszközök függnek a hálózati eszközöktől, valamint a struktúrától, a „megtámadandó" szerverek operációs rendszerétől, a szoftverkörnyezettől, a vizsgált szolgáltatásoktól, lehetséges védelmi komponensektől. Vannak köztük hálózati szkennerszoftverek, amelyekkel sérülékenységeket lehet felderíteni, vagy a környezetet lehet nagy mélységben megismerni. Az észlelt hiányosságok, sérülékenységek alapján lehet különféle módszereket alkalmazni ezek kiaknázására. E módszerek egy része az interneten is fellelhető tudás – nem véletlenül, hiszen egy valódi támadónak is ezek állnak rendelkezésére –, egy másik része pedig belső fejlesztés, kutatás eredménye. Ezért bizonyos szempontból többet tudunk, mint egy átlagos számítógépkalóz.

– Milyen eredményeket várhat el egy ügyfél az etikus hackelés elvégzésétől?

– Egy alaposan elvégzett vizsgálat tiszta képet nyújt az ügyfélnek a vizsgált komponensről vagy hálózatról. A teszt sikerességét nem azon kell leméri, hogy mennyi kiszolgálót vagy hálózati eszközt sikerült feltörnie a vizsgálatot végző csapatnak. A sikert az jelenti, hogy pontos választ lehet adni arra, hogy mi sérülékeny az adott hálózatban.

Az etikus hackelés azonban nem áll meg a sérülékenységek felderítésénél. A vállalás szerves részét alkotja, hogy a tesztelők megoldási javaslatokat adnak a hibák kijavítására. A probléma jellegétől függően a megoldás lehet a hálózat átstrukturálása, a felesleges programok eltávolítása, az elavultak frissítése, a megfelelő javítókódok telepítése, tűzfalak vagy behatolásmegelőző rendszerek beépítése, és még számos egyéb.

Schopp Attila

Ez nem a te (hon)lapod!

A grafiti az ókortól a „kultúra” része. Néha egy kicsit szabályozottabb, művészibb, de gyakrabban jut eszünkbe az a vandalizmus, amelynek célja a „művész” kétes képességeinek a fitogtatása. Az internetkorszakban az online folklór is megörökölte a falfirkát – elcsúfított, meghackelt honlapok formájában.

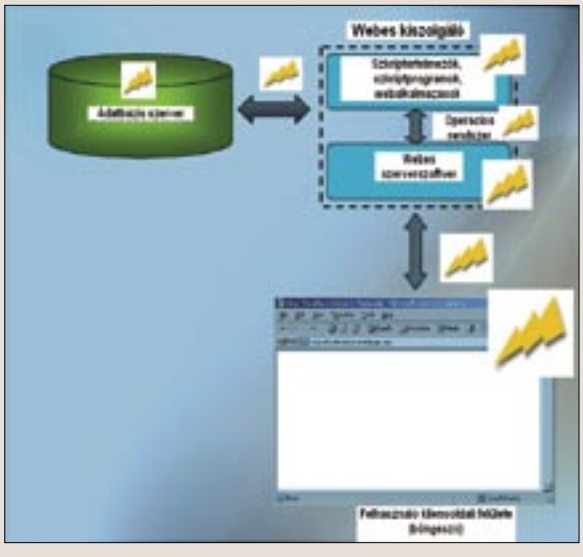
Az online vandálok obszcén képeinek és zavaró, nem ritkán trágár feliratainak célja a magamutogatás, erőfitogtatás és a botrányokozás mellett lehet például világnézeti, vallási, politikai – anarchista vagy terrorista – nézetek hangoztatása is. A mai pénzcentrikus támadásokban azonban megjelent az üzleti motívum is, hiszen egy szervezetet az interneten a honlapja reprezentál, az üzleti partnerek, az ügyfelek és a fogyasztók pedig gyorsan elvesztik a bizalmat abban az intézményben, amelynek a webhelye valóságos átjáróház.

A hackelés nemcsak a respektust rontja, hanem a következményeinek a felszámolása leállással, járulékos munkával – közvetett üzleti károkkal – jár. Az igazi baj azonban nem a látható honlapdúlásokkal van. Sokkal kellemetlenebbek azok a „láthatatlan” támadások, amelyeknek nincs szembeötlő jelük, de a webhelyek és a rajtuk zajló internetes tranzakciók manipulálása révén a közvetlen anyagi haszonszerzés a céljuk.

A webszerverek ellen intézett támadások puszta ténye önmagában többletkiadásokat okoz, hiszen készülni kell rájuk, követni kell a sérülékenységeket, és karban kell tartani a honlapokat.

Minden támadható

Az egyre szervezettebb támadások bizonyítják, hogy az online üzlet legkritikusabb területe a webes biztonság. Ha a szerver vagy a honlap kompromittálódik, akkor a támadó – még jól beállított tűzfal, karbantartott operációs rendszer és szoftverek mellett is – korlátlanul hozzáférhet az adatokhoz. A hackerek sajnos több ponton is réseket találhatnak, és az egyik alapvető kérdés: melyek az esendő komponensek?



Minden támadható

Sajnos mindegyik – azaz egy átlagos, korszerű, dinamikus webszerver esetében az alábbi alrendszerek:

Operációs rendszer. A legegyszerűbb támadások során a támadó azt használja ki, hogy a telepítéskor az operációs rendszer – Linux, Unix, Windows stb. – beállításait változatlanul hagyták. Ezekhez még sérülékenynek sem kell lennie, de ha még a platform rendszeres biztonsági frissítése is elmarad…

Webes szerverszoftver. Általában állandóan futó szolgáltatás, amely a felhasználók böngészői által kiadott webes kérelmekre figyel és válaszol; a legelterjedtebb az Apache és a Microsoft IIS. Ezeknek is lehetnek biztonsági problémáik: például távolról hozzáférést lehet szerezni az operációs rendszerhez olyan emelkedett jogosultságok mellett, amelyek tágabb mozgásteret adnak az egyszerű böngészéshez szükségesnél.

Szerveroldali szkriptértelmező. A modern honlapok általában helyzetérzékenyek, a könnyű karbantarthatóság miatt gyorsan követik a változásokat, és interaktívak. Erről a statikus html-formátum helyett olyan parancs- vagy szkriptnyelvek – például Php, Perl, Asp, Asp.Net, Jsp, Cgi – gondoskodnak, amelyek dinamikusan, a lekéréseknek megfelelően generálják a felhasználó böngészője által aktuálisan értelmezendő, és a megjelenítést végző html-kódot. A dinamikus nyelvekről is derülnek ki hibák, ezeket is karban kell tartani. Különösen kritikus, hogy ezek felelnek a felhasználóktól érkező adatok feldolgozásának alapszintjéért, és ezt nagyon biztonságosan kell végezniük.

Adatbázismotor. A honlapok dinamizmusáért, az egyénre és helyzetre szabott tartalomért felelős másik komponens további fontos feladata – a honlap megjelenését vezérlő adatok tárolása mellett – az üzleti, felhasználói és tranzakciókkal kapcsolatos információk tárolása és kezelése valamilyen adatbázisban. Az adatbázisokat működtető motorok – Microsoft SQL, MySQL, Oracle stb. – több szinten is támadhatók.

A kommunikációhoz szükségük van nyitott portokra, amelyek ellenőrzését az operációs rendszer védekező mechanizmusainak megkerülésével megpróbálhatják megszerezni. A nyitott portok

Ma már nem csak erődemonstráció

mellett az adatbázismotor is szoftver, lehetnek hibái, sérülékenységei, elmaradt biztonsági javításai, de lehet gyenge a jelszava, vagy – ami még rosszabb, de sajnos nagyon gyakori – változatlanok maradhatnak az alapértelmezett gyári adminisztratív hozzáférés azonosítói.

Bár nem fizikai entitás, de kiegészítésül röviden megemlítjük, hogy jellegüknél és biztonsági szerepüknél fogva fontos biztonsági szerepet töltenek be a kommunikációs protokollok is.

A felsorolásban nem foglalkoztunk a szerver elhelyezési körülményeihez kapcsolódó fizikai biztonsággal, és feltételeztük, hogy a hardver hibátlan, de egy dolog már nyilvánvaló: figyelni kell a sérülékenységekre, a kockázatokra és a fenyegetésekre; rendszeresen biztonsági mentéseket kell végezni, és telepíteni kell a fejlesztői javításokat – természetesen a megfelelő szabályok szerint.

A sebezhetőségekre általában igaz az, amit tavaly márciusi számunkban írtunk, és a kihasználás általános menetét illetően utalunk az ott leírtakra (*IT-Security* 2006/3., Sérülékenység).

Webalkalmazások

A kiszolgáló alapvető egységei felett a felhasználók böngészői elsődlegesen az említett komponenseket használó – a már említett dinamikus parancsnyelven írt – programokhoz, a webalkalmazásokhoz csatlakoznak. Ezek a felsorolt komponensek feletti szinten működtetik magát a honlapot, elvégzik a megjelenítést és a felhasználó inputok feldolgozását, illetve továbbítását, továbbá ezeknek a moduljai vezénylik le az online tranzakciókat is.

Több definíciójuk létezik, keretes írásunkban soroltunk fel néhányat.

A webakalmazások képesek rá, hogy kliensoldali parancssorozatokat futtassanak a böngészőben azokon a kliensoldali szkriptnyelveken, amelyeket a böngésző is megért (a böngésző által értelmezett szkriptnyelvek nem azonosak a szerveroldalon használt dinamikus szkriptnyelvekkel!).

Fontos distinkció az előző pontban felsoroltak és a webalkalmazások között, hogy a szerverhez tartozó komponensek általánosabban elterjedtek, ismertebbek és jobban figyelnek rájuk. Ez megnyilvánul a fejlesztői vagy közösségi hibakeresésben és a szélesebb körű támogatottságban – és természetesen a nagyobb fenyegetettségben is. A webalkalmazások viszonylagosan egyedibb fejlesztések eredményei, készítésük során messzemenően betartandók a biztonságos programozásra vonatkozó ajánlások (*IT-Security*, 2006/10., Tiszta források nyomában).

A webalkalmazás-modell egy kicsit megbolygatja az eddigi tagolást, amennyiben három rétegről szokás beszélni:

- az első réteg a böngésző és az általa megjelenített/kezelt felhasználói felület;
- a második réteg a tartalomgeneráló technológia – a webes kiszolgáló vagy alkalmazásszerver a rajta futó szerverszoftverrel, dinamikus szerveroldali parancsnyelvmotorral és az operációs rendszerrel – ide kapcsolódnak a webes alkalmazások is, amelyek lehetnek külön kiszolgálón;
- a harmadik réteg az adatbázis (kiszolgáló).

Ebben a modellben a felhasználó által kezdeményezett, a böngésző és web-

szerver által közvetített kérelmek a webalkalmazásokhoz jutnak, és azok dolgozzák fel őket. A webalkalmazás a kérelem kiszolgálása közben elvégzi a megfelelő adatbázis-műveleteket, majd az eredményt visszaküldi, és az honlap formájában megjelenik a böngészőben. A webalkalmazások biztonsága azért különösen fontos, mert ezek jelentik az átjárót az adatbázisban tárolt kritikus információk és az olyan egyedi programok felé, amelyeket nem feltétlenül a védelmi szempontok figyelembevételével fejlesztettek – és persze maguk a gombamód szaporodó webalkalmazások sem mindig tükrözik azt a programozói gondosságot, amely a tökéletes biztonság letéteményese lenne.

Hangsúlyozzuk: a webalkalmazásokban különösen kritikus a sérülékenységek felderítése és kijavítása, tovább a felhasználóktól származó inputok ellenőrzése, ide értve az URL-kérelmek által közvetített parancsokat is.

Az általános áttekintés után lássunk néhány konkrét támadásféleséget.

SQL-injektálás

A Web Application Security Consortium tavaly nyári adata szerint az összes incidens 9 százaléka SQL-befecskendezés következménye, és egy további adat szerint a honlapok fele fogékony rá.

Normális esetben a webhelyek mögöttes adatbázisával a felhasználók többszörös áttételeken keresztül kommunikálnak, saját oldalukon a webes böngésző segítségével, a böngésző pedig azzal a szerveren futó alkalmazással van kapcsolatban, amely működteti a honlapot, és közvetlenül kapcsolódik az adatbázishoz. Az SQL-befecskendezésnél a támadó SQL-parancsokat próbál átpaszszírozni a böngészőn és az alkalmazáson keresztül azért, hogy azokat az adatbázison futtassa. Ha az ellenőrző mechanizmus az ilyen kísérleteket nem gyomlálja ki, azaz nem szanálja a beadott malignus utasításokat, akkor a támadó megszerezheti a rálátást az adatbázisra, vagy meg is változtathatja azt.

A támadó utasítások – kedvezőtlen esetben – „bemehetnek” egyszerű bejelentkező oldalakról, űrlapokról, keresési és webes vásárlási formulákról, azaz általában minden olyan beviteli mezőről, amely egy online üzleti alkalmazásnak egyébként szerves része, mert ez az ügyfelekkel való kapcsolattartás fontos eszköze.

Egy egyszerű bejelentkezőoldalon a felhasználó az azonosító–jelszó párossal

Elsődleges védelem: a felhasználói input szűrése

tud hozzáférni bizonyos korlátozott tartalmakhoz – például a személyes adataihoz vagy egy fórumhoz. Amikor ezeket beírja, a lapot működtető alkalmazás SQL-lekérdezésekkel ellenőrzi azokat az adatbázisban. Sikeres ellenőrzés után a felhasználó jogosultságot szerez a korlátozott tartalmak elérésére.

SQL-injektálásnál a támadó olyan SQL-parancsokat ír be – illeszt, „injekcióz” vagy „fecskendez” – a beviteli mezőkbe a bejelentkezési adatok helyett, amelyekkel az azonosító mechanizmust akarja megkerülni. Ez csak akkor lehetséges, ha a bevitt adatokat az alkalmazás megfelelő ellenőrzés nélkül továbbítja az adatbázismotorhoz.

Az SQL-injektálás részben a szkriptértelmező kontextusában működik, hiszen az értelmezi és SQL-utasítás formájában továbbítja a beírtakat, másrészt az adatbázistáblák és -rekordok elnevezéseinek kitalálásához az esetek egy részében némi kreativitás is szükséges – mint az élet igazolja, nem túl sok – a közvetlen SQL-kérelmek kiadásához.

Az SQL-rendszerek általában körbe vannak bástyázva megfelelő védelmi vonalakkal – tűzfalakkal, behatolásvédelmi rendszerekkel – , de ezeknek lehetővé kell tenniük, hogy a webhelyet működtető alkalmazás a nyitott portokon legitim módon kommunikáljon az adatbázissal. Ha egy webhely valamely lapján egy beviteli mező ellenőrzése nem megfelelő, akkor a támadó a járulékos SQL-parancsokkal mintegy „kibővíti” a honlap funkcióját úgy, hogy egy saját igényeinek megfelelő csatornát „fúr bele” az alkalmazásba.

Az SQL-parancsbeillesztés gyakran használt támadási forma, ugyanakkor elég nehéz megítélni, hogy egy konkrét honlap sérülékeny-e ebből a szempontból, ráadásul a sebezhetőség mértéke is változó. Ha azonban egy rendszer fogékony az SQL-parancsokra, akkor a támadó úgy szerzi meg az adatbázis bejegyzéseit, ahogyan csak akarja, és úgy írja át azokat, ahogyan neki tetszik.

Sajnos az ügyesebb támadók sokáig rejtetten tevékenykedhetnek, mert elég nehéz őket lefülelni.

Az SQL-injektálás elleni védekezés nem túl nehéz, de a tűzfalak és a behatolásvédelmi rendszerek itt nem számítanak sokat, hiszen a honlapnak elérhetőnek kell lennie, és a csatornáknak is nyitva kell maradniuk. Noha egyébként kritikus, de ebben a vonatkozásban alárendelt a sérülékenységkezelés szerepe is. Https-kérelmek esetén a behatolásvédelmi rendszerek nem védenek, de egyébként (sima http) képesek kiszűrni az SQL-beillesztő próbálkozások nagy részét, az elsődleges védelmet azonban a felhasználói inputok szűrése jelenti.

Cross Site Scripting

Az oldalak közötti átszkriptelés (css, de inkább xss-ként emlegetik) az általános

A WEBHELYEK LEGGYAKORIBB TÁMADÁSVEKTORAI

- URL- és felhasználók által szerkesztett paraméterek
- Rejtett mezők
- Megszakadt hozzáférés, session-kezelés
- Puffertúlcsordulás
- SQL- és szkriptparancsok
- Hiba- és kivételkezelési problémák
- Hálózatvédelmi problémák
- Helytelen SSL-használat
- Gyenge jelszavak
- Adattárolási és védelmi problémák
- A hozzáférés-ellenőrzés gyengesége
- A helytelen felhasználókezelés

vélekedés szerint az incidensekben detektált 27 százalékos előfordulási arányával a leggyakoribb támadás, és a webhelyek nagyjából harmada fogékony rá. Több típusa van, némelyikre nem is igazán illik az eredeti elnevezés.

A régi, jóféle statikus html-oldalakkal nincs semmi gond, mert a webhely tökéletesen ellenőrzi, milyen módon értelmezi a felhasználó böngészője a kódot. A gond azokkal a dinamikusan generált oldalakkal van, amelyek html-kódot és más felhasználók által szerkesztett szöveget keverten jelenítenek meg. A webhely ilyenkor nem uralja teljes mértékben a kliensoldali megjelenítés mikéntjét, és a felhasználók által szerkesztett szövegekbe ágyazott rosszindulatú tartalom beágyazódik a továbbiakban generált dinamikus oldalba. Sem a szerver, sem a kliens nem rendelkezik elegendő információval ahhoz, hogy védelmi intézkedéseket foganatosítson.

Adva van a kliensoldalon egy parancs- vagy szkriptértelmezésre képes böngésző, és a sérülékeny oldal generált dinamikus tartalma azzal a megjelenítendő szöveggel, amely más felhasználói inputból származik, és rosszindulatú JavaScript-, VBScript-, ActiveX-, html- vagy Flash-kódot tartalmaz. A malignus kliensoldali szkript vidáman lefut a mit sem sejtő felhasználó gépén; begyűjthet személyes információkat, monitorozhat vagy manipulálhat cookie-kat, legitim felhasználói akcióknak látszó kérelmeket kezdeményezhet, vagy bármilyen más rosszindulatú kódot letölthet/telepíthet/futtathat.

Némi bíbelődéssel – és a böngésző- és szerveroldali szkriptnyelv ismeretével – a honlapokról speciálisan formázott „xss URL-ekkel” kideríthető, milyen mértékben és hogyan eresztik át vagy fogadják el a szövegbe ágyazott szkriptutasításokat. Potenciálisan minden olyan webhely fogékony lehet az xss-re, amely a felhasználók által beadott/szerkesztett szövegeket tárol az adatbázisában.

Az xss-támadások elleni védelem nem túl nehéz. Azt már láttuk, hogy megjelenítéskor nem lehet túl sok mindent kezdeni, de a webes inputokkal igen, csak ez némi programozói „izommunkával” jár. A felhasználók által beadott szövegekből tárolás előtt egyszerűen ki kell szűrni a szkriptutasításokat, és kész. Nem kell megijedni; a vizsgálatot nem kell elvégezni az összes lehetséges parancsra, hanem csak azok jellegzetes metakaraktereire – például <, >, #, & stb. –, viszont az ellenőrzést az ASCII és a hexadecimális kódformákon is végre kell hajtani.

NÉHÁNY WEBALKALMAZÁS-DEFINÍCIÓ

- „Webalkalmazásnak tekinthető minden olyan kliens–szerver interakció, amelyben kapcsolat létesül a felhasználó és a webszerver között.”
- „A webes alkalmazások internetes kiszolgálókon tárolt, webes úton terjesztett, rendszerint egy vagy több honlap kombinációjaként megjelenő szoftverek, melyek a böngészővel integránsan működnek.”
- „A webalkalmazások név minden webbel kapcsolatos entitást magába foglal, beleértve az internetes böngészőket és más kliensoldali szoftvereket, amelyek képesek a web elérésére; ugyancsak beleértve a webes kiszolgálón tárolt és ott futó szoftvert, illetve a felhasználó gépére letöltődő szoftvert is.”

CRLF-beillesztés

A „sor vége”, vagy „kocsi vissza + soremelés” az ősidők távírószerű termináljaitól származó örökség. Azok már eltűntek ugyan a süllyesztőben, de az ASCII 13 + 10 kódpáros – vagy <CR><LF> vagy „hexában” 0dH, 0aH vagy egyszerűen „\n” – megmaradt tagolójel a szövegekben a sorvég vagy más esetekben a parancslezárás, illetve a felhasználói input végének jelzésére.

Távírós örökség – eltűntek a süllyesztőben

A viszonylag nem túl közismert CRLF-támadásokra leggyakrabban idézett példa a naplóállomány-manipuláció. Ha a támadó egy beviteli mezőbe ezt írja be:

SQL teszt<CR><LF>SQL adatbázis: helyrehozhatatlan hiba

a naplóban ez látszik majd:

SQL teszt
SQL adatbázis: helyrehozhatatlan hiba

Az adminisztrátor ezután órákat tölt a nem létező probléma felderítésével, miközben a támadó más módon rohanja le a rendszert.

Egy másik (linuxos) példában a bemenet lehet ilyen is:

bankkartyaszamok.txt<CR><LF>rm -rf /

A sérülékeny rendszer először az „ls -a bankkartyaszamok.txt” paranccsal kilistázza az ügyfelek kártyaadatait, de nagyjából ez volt az utolsó „értelmes” ténykedése, mert ezután törli a „root” partíciót.

Látjuk, hogy itt is a felhasználói bevitel megfelelő ellenőrzésével lehet elkerülni a bajokat. Nincs szükség másra, mint a CRLF-jelzés lehetséges metakaraktereinek szűrésére – ezért is soroltunk fel emlékeztetőül néhány írásmódot.

Directory Traversal

A „könyvtárátkelésnél” olyan http-aknákat használnak ki, amelyek a hackerek számára lehetővé teszik, hogy védett könyvtárakhoz is hozzáférjenek, és a webszerver gyökérkönyvtárától eltérő helyeken parancsokat futtassanak. Normálisan az átlagos látogatók csak a szerver logikai gyökerére – például Windows alatt ez fizikailag alapértelmezésben a C:\inetpub\wwwroot könyvtár – látnak rá, a máshol elhelyezkedő állományok hozzáféréseit az elérési listák (ACL-ek) szabályozzák, de az átlagfelhasználó számára mindenképpen tiltják.

Ha létezik ilyen sérülékenység a szerverszoftverben vagy az alkalmazásban, akkor minimális „helyismerettel” és némi találékonysággal a böngésző segít-

ségével is ki lehet lépni a gyökérből, és hozzá lehet férni a rendszer más részeihez – ennek lehetséges következményeit pedig már nem kell hangsúlyozni.

Egy az archívum elérésére vonatkozó dinamikus html-kérelem általában így néz ki a böngésző címsorában:

http://www.telapod.hu/show.asp?view=archivum.html

Egy sérülékeny szerver viszont ennek a kérelemnek a „korrekt” kiszolgálására is képes:

http://www.telapod.hu/show.asp?view=../../../../../Windows/system.ini

Ugye, nem kell kommentálni? Akkor lássunk egy még szörnyűbbet:

http://www.telapod.hu/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:
(a %5 a „\” jele)

Ez az URL csak könyvtárlistát készít, a „dir” helyett bármi más is állhat – az olvasó fantáziájára bízzuk.

Szerencsére a modern szerverszoftverek általában nem nagyon hagyják az ilyen garázdálkodást, a régebbi rendszereknél azonban mindenképpen kötelező, az újabbaknál pedig ajánlott kiszűrni az efféle kódokat – persze nem szabad elfeledkezni a biztonsági frissítésekről sem.

Az azonosítás meghackelése

A támadó magát felhasználónak álcázva azonosítja magát egy rendszer felé, így megszerzi azokat a jogosultságokat, amelyekkel az adminisztrátor az adott felhasználót felruházta – legrosszabb esetben adminisztrátori jogokkal.

A http-protokollban többféle azonosítómódszer használható – név–jelszó, NTLM, tanúsítványok, passportok stb. Ezek a technológiák a http felett (vagy az SSL/TSL felett) működnek a lekérés/válasz forgalmazás beágyazott hitelesítő technológiájával. A probléma technológiailag nem is annyira az operációs platform vagy a szerverszoftver biztonsági hibája, hanem az azonosítók, tanúsítványok stb. biztonságos tárolásával függ össze, és azzal, hogy a támadó hogyan fér hozzájuk. Az efféle támadásokat legegyszerűbben a gyenge jelszavak teszik lehetővé, de léteznek olyan szótár alapú vagy „brute force” („nyers erős”) automata eszközök – WebCracker, Brutus –, amelyekkel gyenge rendszerek esetében csak idő kérdése a hozzáférés megszerzése.

Az automatizált támadások ellen védekezni például úgy lehet, hogy a támadóeszköznek a jól ismert 400-as hibajelzés helyett a „HTTP 200 OK” választ adjuk sikertelenség esetén is. Egy másik jó védekezés a bejelentkezéskor véletlenszerű színű és formájú karaktersorozatok képes megjelenítése és az ábra megfelelő betűinek bekérése.

Lényeg, hogy a kép az optikai karakterfelismerők számára kezelhetetlen legyen.

A WEBSZERVEREK BIZTONSÁGÁT ELLENŐRZŐ NÉHÁNY ESZKÖZ

Általános biztonsági pásztázók:
Cerias
Foundstone
ISS InternetScanner
Lightning Console
Nessus Security Scanner
NetIQ Security Analyzer
NMap Network Mapper
Qualys Free Security Scans
Qualys Guard
Saint
Sara
Secure-Me
SecurityMetrics Perimeter Check
Stat Scanner
Webalkalmazások ellenőrzésére is alkalmas lehetőségek:
Acunetix Web Vulnerability Scanner
Codenomicon Http Test Tool
Core-Impact
N-Stalker
Watchfire AppScan
WebInspect

Google-os hackelés

A támadó valamilyen internetes kereső – nem feltétlenül a Google – segítségével próbál meg kiaknázható szervereket felkutatni. Értékes találatnak számítanak:

- biztonsági- és sérülékenységekről szóló értesítők,
- a túl informatív hibaüzenetek,
- a jelszavakat tároló állományok,
- a rosszul védett/értékes adatokat tartalmazó könyvtárak.

Néhány biztonsági szakértő/hacker (?) – néha elég nehéz a különbségtevés – külön online adatbázisba (ilyen például a Google Hacking Database) gyűjtögetik lekérdezhető formában az ilyen vonatkozású találatokat, de a keresők üzemeltetői ma már megpróbálják blokkolni a támadásra is használható információkat.

Közben azonban elindult a Google kódkereső szolgáltatása, amely eredeti – a programozást segítő – célja mellett sajnos az interneten fellelhető programlisták hibavadászatára is alkalmas. A védekezés egyébként pofonegyszerű: ha a „http:www.tegeceged.hu/problemas.php” URL sérülékenynek van feltüntetve valamely keresőben, akkor a problémás oldalt meg kell szüntetni, vagy ki kell javítani.

Hol a hiba?

Az eddigiekben csak a leggyakoribb támadásféleségeket tekintettük át, de egyrészt van még belőlük, másrészt az egyre leleményesebb hackerek naponta újabb trükkökkel próbálkoznak.

A réseket kétségtelenül nehéz megtalálni, de nem lehetetlen – és inkább mi találjuk meg, mint egy esetleges támadó. A webszerverek és webes alkalmazások védelmének megítélésére a webes biztonsági audit szolgál. Ide értjük a hozzáférések, az architektúra, a szolgáltatások, a protokollok, a titkosító mechanizmusok ellenőrzéseit. Az audit kiterjed továbbá az adatbázisokra, az operációs rendszerre, a fájlrendszerre, könyvtárakra és állományokra, a felhasználói szintekre és felhasználókra, valamint a jelszavakra. Az ellenőrzés során foglalkozni kell a beállításokkal és a rendszernaplókkal – különös tekintettel a szolgáltatások és portok, illetve a biztonsági alrendszerek beállításaira és feljegyzéseire. Nem szabad elfeledkezni a szoftverekről; futó állományokról és különösen a webalkalmazásokat felépítő egyedileg fejlesztett programokról. Noha írásunk nem a böngészőre koncentrál, de egy szervezet rendszerének felülvizsgálatakor tüzetesen ellenőrizni kell a felhasználók által használt böngészők beállításait is.

Az audit eredménye ideális esetben nem a hibák egyszerű felsorolását tartalmazza, hanem magukat a megoldási javaslatokat is.

Az iménti felsorolás tetemes munkát jelent – különösen, ha tudjuk, hogy az idézett pontok mindegyike mögött további ágas-bogas vizsgálatok húzódnak meg –, de szerencsére ezekre léteznek kész eszközök – kereskedelmi és ingye-

nes szoftverek, illetve szolgáltatások egyaránt –, amelyek lényegesen egyszerűbbé teszik az életet.

Tanácsok

A webszerverek biztonságával foglalkozó írások jókora köteteket töltenek meg. Van azonban néhány tanács, amelyek betartásával a kiszolgálók működtetői eleget tesznek az alapvető védelmi követelményeknek:

Ne futtassunk felesleges szolgáltatást, értelmezőt – röviden szoftvert! Ha nincs szükség a szerveren, mondjuk FTP-lehetőségre, akkor ne is telepítsük, és ugyanígy ne adjunk felesleges támadáspontot a hackereknek a szükségtelen vagy nem használt dinamikus szkriptértelmezők felesleges telepítésével!

Figyeljük a fejlesztők értesítőit! A legcélszerűbb, ha feliratkozunk azokra a hírlevelekre, amelyeket a szerverünkön futó szoftverek készítői bocsátanak ki a felfedezett biztonsági problémákról és javításokról. Ajánlott a független internetes hibakeresők – CERT, Secunia, FrSIRT stb. – rendszeres látogatása is.

Telepítsük a biztonsági frissítéseket és javításokat! Mindig tartsuk azonban szem előtt a sérülékenységkezelés szabályait!

Rendszeresen készítsünk biztonsági mentéseket! Itt is utalunk a vonatkozó szabályok betartására (lásd: *IT-Security,* 2005/9., Minden esetre).

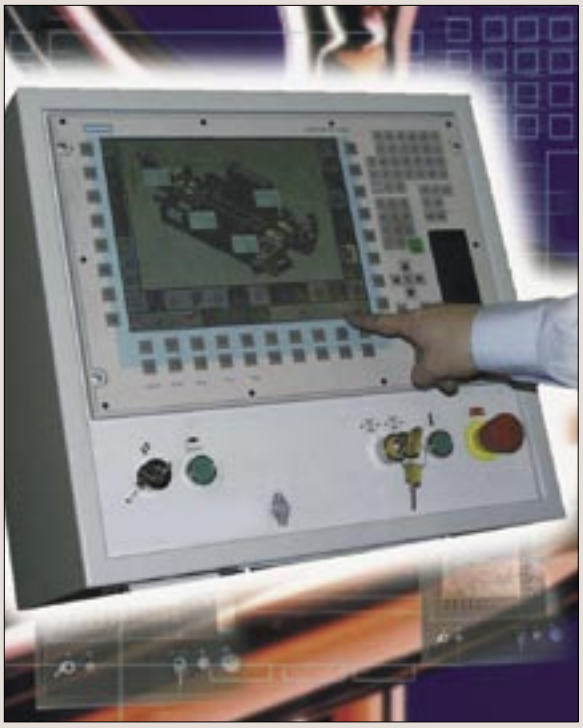
Tegyük napi gyakorlattá az erős jelszavak használatát! Az egyszerű, könnyen kitalálható azonosítók használatát kerüljük – különösen az adminisztratív hozzáféréseknél. Másfelől ne adjunk ki olyan bonyolult jelszavakat, hogy a felhasználók kénytelenek legyenek cetlikre leírni azokat. Feltétlenül változtassuk meg a szervereken használt különféle rendszerekhez mellékelt alapértelmezett gyári hozzáférések azonosítóit. Az érzékeny komponensek és adminisztratív hozzáférések minden esetben legyenek erős jelszavakkal védettek.

Használjunk biztonságos protokollt (SSL, TSL) – menjünk át https-be!

Web Application Security Consortium – *http://www.webappsec.org/*
Biztonsági tippek webes fejlesztőknek – *http://www.squarefree.com/securitytips/web-developers.html*
Biztonsági audit: GYIK – *http://www.pramati.com/docstore/1230042/wwhelp/wwhimpl/common/html/wwhelp.htm?context=security&file=sec_audits.htm*

Legyünk tisztában a rendszerrel! A legtöbb webes kiszolgálón több fejlesztő alkalmazásai futnak. A készítők bizonyos szabadságot élveznek ezek telepítésében, de figyelni kell rá, hogy mit tesznek fel, a szoftvereikben milyen hibák lehetnek, mihez és hogyan férnek hozzá.

Használjuk az operációs rendszer engedélyezési mechanizmusait! A webszerver komponensei és különösen alkalmazásai általában bizonyos felhasználókhoz rendelt jogosultságokkal futnak. Gondoskodjunk róla, hogy csak a szükséges legkisebb jogosultságok legyenek nekik kiosztva.



Legyünk tisztában a rendszerrel

Figyeljük a rendszernaplókat! A kiszolgálón – ideális esetben – minden kérelemnek és tevékenységnek nyoma marad a rendszernaplókban. Ezek monitorozása elengedhetetlen

Szükség esetén automatizáljuk a felügyeletet!

Osztályozzuk és különítsük el az adatokat! Tegyünk különbséget a nyilvános és bizalmas információk között! Az érzékeny adatokat tároljuk elkülönítve; szükség esetén a „külső” és „belső” adatok közé állítsunk dedikált védelmi „falakat”.

Körültekintően konfiguráljuk a kiszolgálónkat! A futtatható állományok hatókörét korlátozzuk a szükséges területekre! Vigyázzunk rá, hogy a szervert/alkalmazásokat működtető szkriptállományok ne legyenek kívülről elérhetők. A szükségtelen tulajdonságokat – például könyvtárak indexelése – kapcsoljuk ki. Használjuk a fejlesztők biztonságfokozó, „hardening” eszközeit!

Végezzünk biztonsági teszteket! Ez a szerverek minden komponensénél elengedhetetlen, de különösen fontos a webalkalmazásokat felépítő dinamikus parancsállományok vagy „programok” esetében. Extrémen kritikus a felhasználóktól származó adatok validálása és az ezzel kapcsolatos gyengeségeket észlelő webalkalmazás-pásztázók szerepe.

Használjunk biztonsági megoldásokat! Sokak szerint legfontosabb a tűzfalak és a behatolásvédelmi rendszerek, de nem becsülhető le az internetes kártevők elleni védelem eszközei, nagy rendszerekben pedig a biztonsággal kapcsolatos automatizált védelmi megoldások – napló- és eseménykezelő rendszerek – szerepe sem. A biztonsági eszközökre különösen érvényesek a konfigurálásnál és a naplózás monitorozásánál leírtak. Használjunk továbbá webalkalmazás-tűzfalakat (lásd: *IT-Security,* 2006/9., Foltozunk vagy falazunk?).

Ha már megesett…

Kétségtelen, hogy ha egy webes kiszolgáló/alkalmazás kompromittálódik, az nem tesz jót a működtető szervezet hírnevének, és anyagi károkkal is jár. Talán ennél is nagyobb baj lehet, hogy az online üzletben érintett partnerek, felhasználók adatai és anyagi javai egyaránt veszélybe kerülnek.

Ilyenkor nincs mese, le kell nyelni a békát. Elő kell venni és alkalmazni kell az incidenskezelési tervet, amelynek remélhetőleg az is része, hogy az érintetteket értesíteni kell. A hallgatás csak még tovább ronthat a renomén – arról nem is beszélve, hogy erre a szervezeteket ma már sok helyütt törvény is kötelezi.

Kelemen László

Terjed a spamdexing

Leleményes programozók – növelendő az internetes marketing hatékonyságát – megpróbálják megtéveszteni a felhasználókat.

Az internetmarketing akkor hatásos, ha a szóban forgó weboldalt sok látogató éri el. Az is fontos szempont, hogy a weblap lehetőleg az elsők között szerepeljen, ha a felhasználó témába vágó keresést indít. Ennek érdekében a programozók különböző programozási, eljárási trükköket vetnek be. Legálisakat és illegálisakat egyaránt. A legális megoldásokat nevezi a szakirodalom Search Engine Optimalizationnek (SEO). Az illegális módszerek között egyre gyakrabban találkozhatunk az úgynevezett spamdexinggel.

DEFINÍCIÓK

Spam. Tömeges, a fogadó által nem igényelt, többnyire hirdetés vagy felhívás tartalmú levél elküldése a címzettekhez.

Indexelés. Egy adott adatstruktúrában specifikus információra való gyors keresést lehetővé tevő megoldás (például az interneten).

Spamdexing. Spam + indexing.

A spamdexing a weboldalak olyan jellegű, indexeléssel történő manipulációja, amelynek révén a weboldal alkalmassá válik a legtöbb felhasználó megtévesztésére. A felhasználó a keresés során olyan tartalmakhoz – spam tartalmú weboldalakhoz, túlértékelt forrásokhoz – jut hozzá, amelyeket valójában nem keresett.

Várható, hogy a spamszűrők terjedésével a spammerek egyre gyakrabban alkalmazzák a spamdexinget.

Fehér, szürke, fekete

A gyakorlatban nem teljesen egyértelmű, hogy mi számít legális eljárásnak, tehát SEO-nak, és mi tartozik a spamdexing körébe. Általánosságban elmondható, hogy a SEO megerősíti, kiegészíti a felhasználó tapasztalatait, míg a spamdexing épp ellenkezőleg működik, és inkább félrevezeti a felhasználókat. A kép azonban a gyakorlatban nem ilyen tiszta: mindkét oldalon elég széles szürke sávval találkozhatunk az egyértelműen legális (fehér) és illegális (fekete) eszközök között.

A SEO olyan elemeket tartalmaz, amelyek olvashatóvá teszik az oldalakat a keresőmotorok számára. Kiemelik azokat a témákat, amelyek kapcsolódnak az illető tartalomhoz, termékhez vagy iparhoz. Az alapvető optimalizálás csupán arról gondoskodik, hogy a weboldal ne váljon érdemtelenül a webnek a keresőmotorok számára rejtve maradó, láthatatlan részévé. A fejlettebb optimalizálásba már olyan eszközök is beletartoznak, amelyek segítségével a keresés az oldal minden elemére kiterjed.

Az oldalak optimalizálása előtt meg kell határozni a kulcsszavakat, valamint azt, hogy melyik SEO-módszer tűnik a legalkalmasabbnak. Ez a kutatómunka magában foglalja a tárgyhoz tartozó kulcsszavak kiválasztását, a kulcsszavak népszerűségének meghatározását, a verseny mértékének megbecsülését, továbbá annak eldöntését, hogy mely kulcsszavakat tudja a leginkább támogatni a minőségi tartalom.

Amit a közönség fontosnak tart

Ahhoz, hogy egy weboldal a keresőmotor számára a lehető leglátható bbá váljon, meg kell érteni, hogy a célközönség milyen módon keresi a weben az aktuális információt. Amikor például termékeket vagy szolgáltatásokat keres, akkor egy szó- vagy kifejezéssort gépel be a keresőmezőbe.

Ahhoz, hogy a keresőmotor valóban megtalálja a keresett weblapot, az oldalnak olyan kulcsszavakat kell tartalmaznia, amelyeket a célközönség begépel a keresőmezőbe. A rendszer akkor működik jól, ha a keresőmotor ugyanazt a szöveget tekinti a legfontosabbnak, mint a célközönség. Tehát azt, amit a célközönség a weblapra kattintva először elolvas.

Ott kezdődik a baj – a SEO ott válik spamdexinggé –, amikor a keresési algoritmus lényegtelen, elsősorban kereskedelmi célokat szolgáló weboldalakat helyez előtérbe.

Vannak keresőmotor-adminisztrátorok, akik szerint a SEO minden olyan formája spamdexing, amely javítja egy weboldal helyezését a találati listán. Ezzel ellentétben az utóbbi időben meglehetősen széles körű egyetértés alakult ki arról, hogy mi számít elfogadható, illetve elfogadhatatlan eszköznek.

Az egyik legetikusabb SEO-módszernek az számít, amikor valaki értékes tartalmat helyez el saját weboldalán, és erre sok más weboldal önkéntesen átirányítja saját látogatóit. Ugyanakkor egyesek megkérdőjelezik az etikusságát annak, ha egy weblap más, témába vágó weblapokat tájékoztat saját tartalmáról, és linkeket kér. Minden valószínűség szerint senki sem tekinti etikátlannak, amikor valaki olyan releváns szókészletet helyez el weboldalán, amelyre célközönsége gyakran keres rá.

Magától értetődően etikus (sőt egyenesen ajánlott) módszer, amikor a weblaphoz oldaltérképet mellékelnek; ide vagy a kezdőlapon vagy akár minden oldalon mutat egy link. Ez a megoldás garantálja, hogy ha egyszer a kereső megtalálta a webhelyet, akkor a hozzá tartozó összes oldalt áttekinti és indexeli.

FORRÁS: COPPERSTATE.ORG

Ez is repülő, bár lehet, hogy mást kerestünk

Vitatott módszer

A SEO egyik legvitatottabb – ugyanakkor meglehetősen gyakori – formája az úgynevezett cloaking (takarás). Ez a módszer a keresőmotorok megtévesztésére alapoz. Más tartalmat mutat a keresőnek, mint a

FORRÁS: TOMSASTROBLOG.COM

Vigyázat! A világ minden táján vannak leleményes programozók

felhasználónak (általában IP alapján válogat). Azaz: a cloaking tulajdonképpen jogtalan kísérlet lehet a keresőmotorok félrevezetésére a tartalmat illetően, egy bizonyos webhelyen. Ugyanakkor a cloaking révén a felhasználó olyan, a keresettel többé-kevésbé egyező tartalomhoz is hozzáférhet, amit a keresőmotorok nem tudnak feldolgozni vagy elemezni.

Egy másik etikus felhasználása a cloakingnak, amikor vakok vagy más fogyatékkal élő emberek számára nyújt webhozzáférést. Annak eldöntésére, hogy a cloaking etikus vagy nem, jó viszonyítási pont a következő: ha kibővíti a hozzáférhetőséget, akkor etikus, ha nem, akkor spamdexing.

Tartalom-spam

A programozók szinte kifogyhatatlanok az ötletekből, így számtalan trükköt vetnek be. A spamdexing egyik leggyakrabban alkalmazott fajtája a tartalom-spam (content spam), amin belül további alkategóriákat különböztethetünk meg.

Itt van rögtön a rejtett vagy láthatatlan szöveg, amikor a weboldalon olyan módon helyezik el a kulcsszavakat, hogy ne látszódjanak a felhasználó számára, de a keresőmotorok (web crawler) megtalálják azokat. Ilyen például a háttérrel azonos vagy majdnem azonos betűszín használata, a miniatűr (gyakorlatilag láthatatlan méretű) betűk használata vagy a kulcsszavak html kódban történő (no frame section) elrejtése.

A tartalom-spam másik „közkedvelt” formája a kulcsszóhalmozás (keyword stuffing). Lényege, hogy a szükségesnél jóval több kulcsszót használnak a szövegben (látható vagy láthatatlan módon). A korábbi keresőmotorok egyszerűen megszámolták, hány kulcsszó található a szövegben, így bedőltek ennek a trükknek. A mai motorok már képesek az egészséges arány meghatározására.

Szintén a tartalom-spamek közé sorolható a metatag-halmozás (meta tag stuffing), amikor a metatagekben használt kulcsszavak száma a szükségesnél sokkal nagyobb értéket ér el. Ide sorolhatók még a gateway- vagy doorway-oldalak: ezeken történnek a már említett halmozások. Az ilyen oldalak közepén „Click here to Enter” felirat található. Rákattintva a felhasználó egy teljesen korrekt és etikus oldalra jut.

Végül, de nem utolsósorban a tartalom-spamek közé tartoznak az úgynevezett scraper site-ok, amelyek más, releváns tartalmú oldalakról gyűjtik egybe az információt, és továbbítják a spammer által kívánt oldalra.

SIKERTÉNYEZŐK

A spamdexing felfutása a kilencvenes évek közepén több, akkoriban vezető keresőmotor használhatóságát rontotta. Eközben a Google – ismertség alapú PageRank linkelemző rendszerének köszönhetően – jobb keresési eredményeket ért el, továbbá sikeresen vette fel a küzdelmet a kulcsszó-spamminggel szemben. Az eredmény nem maradt el: a Google a kilencvenes évek végétől világviszonylatban a meghatározó keresőnek tekinthető.

Jóllehet a spamdexing a Google-t nem tette használhatatlanná, vannak olyan kifinomult eljárások, amelyek ellen ez a keresőmotor sem teljesen védett. Ezek nyomán született meg a „Google bombing” kifejezés. E körben ártalmatlan, ám bosszantó csínytevésekkel találkozhatunk (tréfás kedvű spammerek például megoldották, hogy a „miserable failure” kifejezést begépelve a keresőbe, a látogató a Fehér Ház honlapján *George W. Bush* önéletrajzánál találta magát), de előfordulhat az is, hogy szándékosan, kereskedelmi előnyökért befolyásolják a rangsorolást.

Link-spam

Nemcsak a tartalomba rejthetők el spamek, hanem találkozhatunk úgynevezett link-spamekkel is. Mire kell itt gondolni? Például linkfarmokra – egymásra mutató linkek spammer-szövetségére, rejtett linkekre, amikor láthatatlan marad a linkek elhelyezése. De említhetjük a Sybil attacket, amikor ugyanannak a weboldalnak a készítője több olyan oldalt állít elő, amelyek egymást erősítő információkat tartalmaznak, növelve ezzel egymás hitelességét.

A Wiki-spam azt jelenti, hogy a Wiki használatával, annak szabad szerkeszthetőségét kihasználva linkeket helyeznek el benne. Furfangos programozók a szerkeszthetőség kihasználásával a blogokat is spammelik.

SEGÍTSÉG

A spamdexinggel készült oldalak jelentése:

http://www.google.com/contact/spamreport.html

http://add.yahoo.com/fast/help/us/ysearch/cgi_reportsearchspam

http://feedback.search.msn.com/eform.aspx?productkey=searchweb&page=search_feedback_form

És akkor még itt van a page hijacking! Ez az eljárás a keresőmotor megtévesztésén alapul. Olyan weboldalt hoznak létre, amely a megtévesztésig hasonló az eredeti site-hoz.

Említést érdemel még a referer log spamming, azaz a weblapok közötti linkelés alapján történő rangsorolás, valamint a lejárt domének megvásárlása.

Hogyan védekezzünk?

A felhasználó a spamdexinggel szemben gyakorlatilag kétféle módon védekezhet. Először is körültekintően használja az internetet, másrészt figyelemmel kíséri a spamdexinggel készült oldalakról szóló jelentéseket. A webes közösséggel jót tesz a felhasználó, ha maga is jelenti az ilyen jellegű oldalakat a legnagyobb keresőknek.

Mallász Judit

Személyes érintés

Az ujjlenyomat-olvasóval felszerelt USB-memóriák többféle biztonsági szolgáltatást kínálnak.

Sokan hordoznak bizalmas adatokat munkahelyük és otthonuk között USB-meghajtón, pedig ennek esetleges elvesztése vagy – akár csak egy rövid időre is – illetéktelen kezekbe kerülése beláthatatlan következményekkel járhat. Mivel az aprócska tárolóeszközre szinte lehetetlen 100 százalékos biztonsággal ügyelni, nincs más megoldás az adatok védelmére, mint a titkosítás.

Ennek egyik legújabb, igen erős formája a ujjlenyomatos védelem, amely az utóbbi években kezdett feltűnni a legkülönfélébb berendezéseken – noteszgépeken, asztali PC-ken, egereken, USB-memóriákon.

Természetesen az ujjaink végén található barázdák nem személyazonosítási célra alakultak ki az evolúciós fejlődés során, hanem az eszközök használatában segítették őseinket azáltal, hogy biztonságosabbá tették a tárgyak megragadását. Mivel azonban a barázdák rajzolata meglehetősen egyedire sikeredett, a nyomozási módszerek kifinomodásával ujjainknak ezt a sajátosságát a bűnözők azonosítására kezdték használni. Újabban pedig az ártatlan többség biometrikus azonosításának és a rosszban sántikálók kiszűrésének egyik fontos eszközévé vált az ujjlenyomat – gondoljunk csak az Egyesült Államokba való belépéskor foganatosított eljárásra.

Azonosítási titkok

Az ujjlenyomatos védelemmel ellátott USB-memóriákba épített beolvasó elektronika egyrészt rögzíti az adatokhoz hozzáférni igyekvő személy ujjának képét, másrészt ezt a képet összehasonlítja a belépésre jogosult felhasználó korábban beolvasott ujjlenyomatával.

A két leginkább elterjedt megvalósítás az optikai és a kapacitív szkennelés. A digitális fényképezőgépekben használatos érzékelőkhöz hasonlóan működő optikai szkenner esetében az üveglapocskára helyezett ujjunkat a berendezés saját fényforrása megvilágítja, majd az érzékelő rögzíti ujjunk képét. Mielőtt a szkenner ezt összehasonlítaná az adatbázisában tárolt ujjlenyomattal, megvizsgálja a kép fényességviszonyait és élességét, a túlságosan sötét vagy túlságosan világos, illetve életlen felvétel ugyanis nem alkalmas az azonosításra. Ilyenkor a szkenner módosított megvilágítással megismétli a beolvasást.

A kapacitív szkennerek ugyancsak képet hoznak létre az ujjlenyomatot alkotó rajzolatról, ezt azonban nem fény, hanem elektromos töltések segítségével teszik, kihasználva azt a jelenséget, hogy a bőr kiemelkedéseinél nagyobb kapacitás mérhető, mint a bemélyedéseknél. A módszer nagy előnye az optikai szkenneléssel szemben, hogy csak az igazi, háromdimenziós felületű ujjakról tud képet készíteni, így sokkal nehezebb kicselezni.

Az azonosítási folyamat második részében a beolvasott képet a rendszer összehasonlítja a jogosult felhasználó ujjlenyomatával, ez azonban nem olyan egyszerű eljárás, mint amilyennek elsőre gondolnánk. Nem elég egyszerűen egymásra helyezni a két képet, egyrészt mert az esetleges szennyeződések miatt nehéz pontosan pozícionálni azokat, másrészt a teljes ujjlenyomatok összevetése nagy feldolgozási teljesítményt igényel. Ezért az összehasonlításhoz az ujjlenyomatok kitüntetett pontjait használják, például azokat a helyeket, ahol a vonulatok végződnek, kezdődnek vagy szétágaznak.

Az ujjlenyomatos azonosítás legfontosabb előnyei közé tartozik, hogy igen nehéz a hamisítás. Egy ujjrajzolatot nem lehet úgy megsaccolni, mint egy jelszót, és elfelejteni sem lehet. A még oly tökéletesnek tűnő módszernek is megvannak azonban a hátrányai. Az optikai szkennerek az ujjlenyomatok képét is hitelesnek fogadhatják el, a kapacitiv rendszerű beolvasókat pedig egy megfelelően elkészített műujjal vagy durvább esetben egy levágott igazi ujjal lehet megtéveszteni. Ezt a trükköt a véráramlást mérő érzékelővel lehet kiküszöbölni, azonban egy hús-vér ujjra helyezett műlenyomattal ez a védelmi funkció is kikerülhető.

Személyes érintés

Mielőtt használatba vennénk egy ujjlenyomat-olvasóval felszerelt USB-memóriát, meg kell ismertetnünk vele ujjlenyomatunkat. A tanulási folyamat több beolvasási lépésből áll, és célszerű több ujjunk lenyomatát rögzíteni, ha ugyanis valamelyik ujjunk megsérül, nem tudunk hozzáférni adatainkhoz. Az USB-meghajtók többnyire lehetővé teszik egy adat-visszaállító jelszó megadását is; ennek akkor vehetjük jó hasznát, ha az ujjainkkal valamilyen ok folytán nem jutunk eredményre. Ha az eszközt átadjuk vagy eladjuk valakinek, a rögzített ujjlenyomatok törölhetők, és az új tulajdonoséival helyettesíthetők.

Belépés ujjlenyomattal

A bekapcsolt számítógéphez való jogosulatlan hozzáférést ugyancsak megakadályozhatjuk az USB-memória képernyőkímélő funkciójával, amelyből csak a hiteles ujjlenyomattal lehet kilépni.

Az ujjlenyomatos védelemmel ellátott USB-meghajtók további szolgáltatási között – gyártótól függően – megtalálható a Windowsba és más jelszót igénylő alkalmazásokba, illetve webhelyekre való ujjlenyomatos belépés, aminek óriási előnye, hogy nem szükséges megjegyeznünk a sokféle jelszót.

Tóth István

Védett PC-k

Gyárilag telepített biztonsági eszközök segítik a vállalati titkok megőrzését.

Komoly bonyodalmak származhatnak abból, ha a vállalati PC-ken tárolt adatok elvesznek, vagy illetéktelen kezekbe kerülnek. Különösen az iroda védettségéből gyakran kikerülő hordozható számítógépekre leselkednek veszélyek.

Léteznek eszközök az információk megóvására, azonban nem könnyű feladat ezek összegyűjtése és a különféle modulokból egy mindenre kiterjedő, működőképes biztonsági rendszer házilagos kiépítése. Szerencsére így vélekednek erről a nagyobb gyártók, köztük a HP is, és speciálisan az üzleti felhasználóknak készített teljes körű védelmi szolgáltatásokkal vértezik fel a vállalatoknak szánt számítógépeiket. A rendszergazdának már csak a szükséges funkciók bekapcsolásával és igény szerinti konfigurálásával kell törődnie.

www.hp.com/

A HP által kifejlesztett ProtectTools többszintű moduláris adatvédelmi rendszer szolgáltatásai rugalmasan testre szabhatók, így egyszerűen beállítható a kívánt biztonsági szint. A többféle védelmi technológiát egy csomagba integráló ProtectTools elsődleges feladata az ügyfélgépek megóvása a rosszindulatú támadásoktól, azáltal azonban, hogy az ügyfélgépek nem szolgálhatnak kiindulási pontként a vállalati hálózat elleni támadáshoz, a rendszer voltaképpen a teljes céges informatikai infrastruktúrát védi.

Hordozható biztonság

Igen kínos következményei lehetnek egy noteszgép elvesztésének vagy ellopásának, elég csak a sajtóban rendszeresen megjelenő hírekre gondolni, amelyek olyasmikről számolnak be, hogy például X óriáscég több tízezer alkalmazottjának adatai voltak az egyik alkalmazott által elhagyott laptopon. Ezután következik a cég illetékeseinek kínos magyarázkodása arról, hogy minden szükséges intézkedést megtettek a vállalati adatok védelme érdekében, de hát az „emberi tényezőt" nem lehet teljesen kiküszöbölni.

Bár a ProtectTools a könnyelműséget, hanyagságot nem tudja megakadályozni, azt el tudja intézni, hogy egy elveszett noteszgép adataihoz ne lehessen hozzáférni.

A védelem első szintjét a rendszerindítást megelőző hitelesítés alkotja, ennek köszönhetően meghiúsítható a jogosulatlan hozzáférés az operációs rendszerhez. A hitelesítés eszköze lehet smart kártya vagy Java-kártya, amelyek használatához megfelelő kártyaolvasóra van szükség. Ezt vagy beépítve tartalmazza a számítógép, vagy noteszgépek esetében a PC-kártyaréshez, asztali PC-knél pedig USB-porthoz csatlakoztatható. Mindkét hitelkártya méretű hitelesítő eszközhöz jelszó és PIN-kód tartozik, és mindkettő használható a Windowsba való belépés engedélyeztetésére is.

Páncélozott iroda

A számítógép alaplapjára rögzített Trusted Platform Module (TPM) biztonsági lapkán alapuló ProtectTools védelmi szolgáltatás a DriveLock, amely akkor is megvédi az ellopott noteszgép merevlemezét a jogosulatlan hozzáféréstől, ha azt áthelyezték egy másik számítógépbe.

További védelmet nyújt a merevlemezen tárolt adatok titkosítására szolgáló Personal Secure Drive funkció, amely olvashatatlanná teszi a bizalmas vállalati információkat a jogosulatlanok számára. A titkosított lemezkötet méretét csak a meghajtó kapacitása korlátozza. A Personal Secure Drive szolgáltatás hordozható tárolóeszközökön, például USB csatolású merevlemezeken és memóriákon is használható.

De nem csak az irodán kívül kerülhetnek veszélybe a bizalmas adatok, a védettnek tűnő környezetben is érhetik kellemetlen meglepetések az alkalmazottakat, belső és külső kíváncsiskodók részéről egyaránt.

Nézzük például azt az esetet, amikor meg akarjuk akadályozni, hogy a bizonyos adatokhoz engedéllyel hozzáférő adóellenőr vagy belső kolléga kinyomtathassa vagy külső adathordozóra (cd-re, USB-memóriára stb.) menthesse az információkat. Pontosan erre szolgál a ProtectTools Device Access Manager szolgáltatása, amelynek segítségével a rendszergazda korlátozhatja az úgynevezett írható eszközök használatát.

A vállalati gépekhez – a vezetők dokumentumaihoz, a fejlesztők anyagaihoz, a pénzügyi adatokhoz, az ügyfél-információkhoz – a hálózaton belülről vagy külső kapcsolaton keresztül jogosulatlanul hozzáférni igyekvők ellen ugyancsak több

Azonosítás Java-kártyával

védelmi funkciót kínál a ProtectTools. Ezek között megtalálható a fentebb már említett rendszerindítás előtti hitelesítés, a kritikus erőforrások elérését megakadályozó Device Access Manager és a titkosítást végző Personal Secure Drive szolgáltatás.

Ha egy támadó mégis be tudna jelentkezni egy számítógépre, a Credential Manager meggátolja abban, hogy a jelszavakhoz és a jelszóval védett alkalmazásokhoz hozzáférjen.

A jelszavak egyszerű használatáról és további védelméről az Embedded Security for HP ProtectTools modul gondoskodik, amely védett tárolót létesít a különféle helyi és internetes szolgáltatások eléréséhez használt azonosítók és jelszavak számára. Így a vállalati felhasználók gond nélkül hozhatnak létre erős jelszavakat, mivel sem megjegyezniük, sem leírniuk nem szükséges azokat.

Tóth István

Hibajelentés

Elégedetlenkedés, paranoia vagy kóros bizonyítási vágy.

A sérülékenységeket tekintve kemény hónap áll mögöttünk: alig ért véget az Apple-hibák hónapja, máris jött Valentin nap előestéjén az elemzők által előszeretettel „piszkos 12-ként” emlegetett tucatnyi biztonsági javítás a Microsoft operációs és irodai rendszereihez. Ezeket már csak azért is ajánlott mihamarabb telepíteni, mert néhány közülük aktívan támadott, súlyos sebezhetőségeket javít.

A közeljövőben a PHP-s honlapokat működtető rendszergazdák szoronghatnak, mert a „Hardened PHP project” és a „PHP Security Response Team” (PSRT) alapítója, *Stefan Esser* márciusban irgalmatlanul elindítja a „PHP-hibák hónapját”. A PSRT-ből személyes és szakmai okokból kivált guru megígérte: ha már belevág, nem kegyelmez az SQL-rendszereknek sem.

Az is kiderült, hogy nemcsak a szoftverek lehetnek hibásak, hanem az emberi „bugok” is okozhatnak gondokat. Ezt persze eddig is tudtuk, de a Carnegie Mellon Egyetem és az Egyesült Államok titkosszolgálatának közös felmérése számszerűsítette, hogy a belső IT-szabotázsok közel 100 százalékban az instabil rendszergazdák elégedetlenkedéseire, paranoid alkatára vagy kóros bizonyítási vágyára vezethetők vissza.

Secunia: ***http://www.secunia.com***

A világban más jellegű sebezhetőségekkel is találkozhattunk: a Cambridge Egyetem két munkatársa kiválóan bebizonyította, hogy a fizetőterminálok is sérülékenyek. Először arra programoztak át egy okoskártyás+PIN-kódos EMV-fizetőautomatát, hogy Tetrist lehessen vele játszani. Az érintettek – a bankok – először meglehetősen lagymatagon reagáltak. Az APACS fizetőrendszer üzemeltetője egyenesen kijelentette, hogy ez csak laboratóriumi körülmények között lehetséges.

A két úrnak több sem kellett, és röpke egy hónapnyi szorgos munka után egy demonstratív prototípus-támadásban kicsit keményebb forgatókönyvet mutattak be. A szigorúbban megbütykölt automata egy éttermi fizetés során a vendég tranzakciójának módosított adatait átirányította egy ékszerüzlet fizetőterminálja, és a gyanútlan áldozat 40 helyett 4000 dollárral lett szegényebb. Persze ezekhez az akciókhoz az eszközbe is bele kellett nyúlni, de az esetek felhívják a figyelmet a fizikai eszközök elégtelen „hardening-jéből” fakadó sérülékenységeire és arra is, hogy nem minden az, aminek látszik!

Kelemen László

FELFEDEZETT HIBÁK ÉS JAVÍTÁSAIK

Szoftver/Alkalmazás	Secunia-fokozat (1–5)	Secunia-azonosító	Leírás	Megoldási javaslat/további információ
Microsoft				
Office 2000, 2004 for Mac, Word 2000	5	23950	A rosszindulatú kifejezéseket tartalmazó dokumentumok vizsgálatakor aktivizálható, pontosan nem sepcifikált probléma miatt tetszőleges kód válik futtathatóvá.	Frissítések letöltése és telepítése Windows (http://www.microsoft.com/downloads/details.aspx?FamilyId=F1E61E6A-BE3D-4536-AF76-A11D5-CE67199); Mac (http://www.microsoft.com/mac/).
A Windows 2000, XP és Server 2003 platformok	4	22452	Az ADODB.Connection ActiveX-vezérlő hibája olyan memóriakorrupciót okozhat, amelyet távolról kiaknázva – például rosszindulatú honlapról – tetszőleges kód futtatására lehet felhasználni.	Frissítések letöltése és telepítése (http://www.microsoft.com/technet/security/Bulletin/MS07-009.mspx).
Az Office 2000, XP, 2003, 2004 for Mac összes programja – ide értve az InfoPath, Project, Publisher, FrontPage és Visio változatokat is	5	24008	Az érintett irodai programokban két olyan súlyos sebezhetőségre derült fény, amelyek kihasználásával távolról tetszőleges programokat lehet futtatni a felhasználók rendszerein.	Frissítések letöltése és telepítése (http://www.microsoft.com/technet/security/Bulletin/MS07-015.mspx).
A Windows 2000, XP és Server 2003 platformok	4	24136	A HTML-súgó ActiveX HhCtrl.OCX-vezérlőjének paraméter-ellenőrzési gyengeségét az érintett platformok alatt távoli kódfuttatásra és jogosulatlan rendszerelérésre lehet kiaknázni.	Frissítések letöltése és telepítése (http://www.microsoft.com/technet/security/Bulletin/MS07-008.mspx).
A Windows Vista alatt futó Antigen, Windows Defender és ForeFront programok, illetve Windows Live OneCare	4	24146	A Microsoft kártevővédelmi motorjában bizonyos pdf-állományok ellenőrzésekor egészszám-műveleti hibát lehet előidézni, és a következményes puffertúlcsordulást tetszőleges kód futtatására lehet felhasználni.	Frissítések letöltése és telepítése (http://www.microsoft.com/technet/security/Bulletin/MS07-010.mspx).
A Windows 2000, XP és Server 2003 platformok (a hibáktól függően a Visual Studio .Net fejlesztőrendszerek és az Office-ban és azóta megjelent kiadásai is érintettek)	3	24147, 24150, 24152	Rendre a Windows OLE Dialog, az MFC OLE Dialog és a RichEdit OLE Dialog komponensek rosszinulatú rtf-állományokba ágyazott OLE-objektumokkal kiváltható sérülékenységei megnyitják a kaput tetszőleges kód távoli futtatása előtt.	Frissítések letöltése és telepítése (http://www.microsoft.com/technet/security/Bulletin/MS07-011.mspx); (http://www.microsoft.com/technet/security/Bulletin/MS07-012.mspx); (http://www.microsoft.com/technet/security/Bulletin/MS07-013.mspx).

Szoftver/Alkalmazás	Secunia-fokozat (1–5)	Secunia-azonosító	Leírás	Megoldási javaslat/további információ
Internet Explorer 5.01, 6.x, 7.x	4	24156	A böngészőben több olyan sebezhetőségre derült fény, melyek távoli kihasználásával tetszőleges kódot lehet futtatni az érintett rendszereken.	Frissítések letöltése és telepítése (http://www.microsoft.com/technet/security/Bulletin/MS07-016.mspx).
Apple				
Flip4Mac Windows Media Components for QuickTime 2.x	4	23958	A Windows Media Video (WMV) fájlok feldolgozásakor jelentkező memóriakezelési gyengeség miatt tetszőleges kód futtatása válik lehetővé.	A javítás megjelenéséig csak megbízható médiaállományokat célszerű megnyitni (http://projects.info-pull.com/moab/MOAB-27-01-2007.html).
Linux, Unix alapú platformok				
Suse-változatok	3	23984	A Novell által kibocsátott összesített biztonsági frissítőkészlet több – jogosulatlan információ- és rendszerelérést, DoS-helyzetet és a rendszer más jellegű veszélyeztetését eredményező – szoftverhibát javít.	A fejlesztő útmutatója szerint telepíteni kell a frissítőcsomagot (http://lists.suse.com/archive/suse-security-announce/2007-Jan/0015.html).
Sun Solaris 10	3	23982	A bejövő ICMP pingek feldolgozásakor jelentkező nem specifikált hiba révén DoS-szituációt lehet teremteni.	A fejlesztő útmutatója szerint el kell végezni a platformfüggő javítást (http://sunsolve.sun.com/search/document.do?assetkey=1-26-102697-1).
Egyéb				
A Trend Micro gyakorlatilag összes biztonsági megoldása	4	24087	A szoftverek UPX tömörítésű futtatható állományok ellenőrzésekor jelentkező problémáját tetszőleges kódfuttatásra, DoS-helyzet kialakítására vagy a rendszer lefagyasztására lehet felhasználni.	A 4.245.00 vagy újabb szignatúraállomány letöltésével a probléma korrigálható (http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034289).

(Forrás: Secunia)

Félregépelt doménnevek

Egyetlen betű eltévesztése – jó esetben – mindössze bosszúságot okoz. Megtörténhet azonban, hogy a nem kellően óvatos felhasználót komoly anyagi kár éri.

Kivel ne fordult volna már elő, hogy elgépelte a keresett weboldal doménnevét? Mellényúlt a billentyűzeten, vagy esetleg nem tudta pontosan, hogy milyen néven regisztrálták a vállalatot. Az esetek többségében ilyenkor nem történik nagy baj. Vagy nem jut az ember sehova, vagy egy teljesen más, érdektelen honlapon találja magát. Ezt észlelve nincs más tennivaló, mint újra begépelni az URL-t.

Megtörténhet ugyanakkor, hogy a keresett doménnévhez nagyon hasonló, attól csupán egyetlen betűvel eltérő kifejezést megadva olyan oldalra jut a látogató, ahol számos kellemetlenség, szélsőséges esetben komoly anyagi kár érheti. Természetesen csak akkor, ha nem elég körültekintő.

Apró csínytevések

Nézzük először a legártalmatlanabb félrevezetést, azt, amikor valaki egy széles körben ismert és sokat látogatott oldal webcímétől alig különböző címre valamilyen információt, hirdetést helyez el. Találkozhatunk olyan esetekkel, amikor valaki így akarja felhívni a figyelmet például a környezetvédelem fontosságára vagy a jegesmedvék megmentésére, de sokkal gyakoribb a közvetlen termékhirdetés.

Az ilyen típusú „csalogatástól” természetesen nem várható, hogy az oldal látogatottsága számottevően megnő, de kétségtelen, hogy valamelyest szaporodik a kattintások száma. A félrevezető haszna tehát nem túl nagy, kérdés, mennyire károsítja meg ezzel az ismert site üzemeltetőjét.

Nem túlságosan, hiszen az ember rövid időn belül rájön, hogy rossz helyen jár. Legközelebb már körültekintőbben gépeli be a doménnevet, illetve ha kétségei támadnak, akkor legjobban teszi, ha valamelyik keresőhöz fordul – hívja fel a figyelmet *Martos Balázs*, az Internetszolgáltatók Tanácsának (ISZT) elnökségi tagja.

Tisztességtelen verseny, sőt, bűncselekmény

A nagyobb problémák akkor kezdődnek, amikor az URL félregépelését követően a látogató az eredeti oldalhoz hasonló termékekkel, szolgáltatásokkal találkozik. Ha például egy számítógépeket kínáló portálról egy másik, szintén számítógépeket árusító oldalra csalják a gyanútlan, melléütő látogatót, akkor az már versenyjogi problémákat vethet fel. Megalapozottnak tűnik a szándékos megtévesztés, ha a két weboldal külső megjelenésében is nagyon hasonló, esetleg közel azonos.

Még komolyabb gondot jelent, sőt, a bűncselekmény gyanúját is felveti, ha a megtévesztés banki, pénzintézeti portálokat érint, illetve a hamis oldal valamelyik bank vagy pénzintézet portáljaként tünteti fel magát. „A csalás súlyosságát alapvetően a tartalom határozza meg. Az a legsúlyosabb eset, amikor a félrevezető oldalon olyan tartalom jelenik meg, ami anyagi kárt okozhat a felhasználónak, illetve az eredeti site üzemeltetőjének. Képzeljük csak el, ha valaki bankjának internetes oldalán akar számlaműveleteket végrehajtani, és egy félregépelés folytán egészen másutt találja magát. Erről azonban – a csalárd oldal üzemeltetőjének machinációi folytán – nem szerez tudomást. A legtöbb ember nem nézi meg tüzetesen a már sokszor felkeresett banki oldalt, nem veszi észre a csalást, és megadja azonosítóját, jelszavát, és ezzel tökéletesen kiszolgáltatja magát. Tulajdonképpen a félregépelésre épí-

FOTÓ: FUJITSU SIEMENS

Gépelési hibák márpedig becsúszhatnak

tő phishingről van itt szó, ami hihetetlenül nagy anyagi károkat okozhat. Az ilyen csalásokra a jog minden lehetséges eszközével nagyon keményen kellene lecsapni” – mutat rá Martos Balázs.

Több doménnév regisztrálása

Azt természetesen egyik weboldal üzemeltetője sem akadályozhatja meg, hogy a felhasználók elgépeljenek egy-egy betűt. Vannak azonban olyan módszerek, amelyekkel csökkenthetik a félrevezetés esélyét. Az ISZT mindenekelőtt azt ajánlja, hogy minden cég gondolja végig a tévesztési lehetőségeket, majd regiszt-

ÉVENTE 50 EZER

Jelenleg körülbelül 280 ezer a .hu alatt bejegyzett doménnevek száma. Tavaly körülbelül 50 ezres volt a növekedés.

rálja a legvalószínűbben félreütött neveket is. Előfordulhat például, hogy a cégnév hangzása és írása nem egyezik meg. Ilyenkor a hangzásnak megfelelő nevet is célszerű regisztrálni. Zavart okozhatnak a kettőzött betűk, különös tekintettel a magyar fül számára idegen, bonyolult neveknél. Ilyenkor is ajánlott a helyes mellett több szóba jöhető változat regisztrálása.

Nyilvánvalóan nem lehet minden esetet figyelembe venni, a cégek nem tudják bebiztosítani magukat az összes elgépelés ellen, hiszen rengeteg a tévesztési lehetőség. Elsősorban a hosszú neveknél követhető ez a gyakorlat, a rövid, néhány betűs neveknél sokkal kevésbé.

Elektronikus aláírás, biztonságos kommunikáció

Saját magát és felhasználóit is megvédheti a honlap üzemeltetője, ha elektronikus aláírást és biztonsági tanúsítványt alkalmaz. Martos Balázs szerint nagyon fontos volna, hogy az internethasználók csak titkosított, tanúsítvánnyal ellátott oldalakon végezzenek minden olyan műveletet, ahol érzékeny, személyes adatokat adnak meg, valamint pénzügyi tranzakciókat hajtanak végre. Mindenkinek oda kellene figyelnie, hogy az ilyen típusú weboldalakhoz csak https- (secure) kapcsolattal lehessen csatlakozni. Ellenkező esetben az ügyfél adatai nyílt szövegként haladnak a hálózatban.

„Szomorúan látom, hogy sok bank, pénzintézet és e-kereskedelmet folytató site nem https-kapcsolattal, továbbá tanúsítvány nélküli oldallal várja a látogatókat. A normál kommunikációnál a felhasználó kevésbé lehet biztos benne, hogy valóban azzal a szolgáltatóval lépett kapcsolatba, amelyikkel akart. Az elirányítás egyik módja a doménnév-elütés, de számos egyéb támadással is találkozhatunk. Így például az internet másik protokollszintjén csomagokat lehet elirányítani, vagy akár egy közbeékelődő hamis site-ot is felállíthat a támadó” – fogalmaz Martos Balázs.

A szakember szerint minden olyan honlapon, ahol pénzmozgás van, illetve érzékeny adatokat (jelszót, bankkártya-adatokat stb.) adnak meg az ügyfelek, védett kommunikációs módszereket kellene alkalmazni.

Ez ma már egyáltalán nem minősül technikai problémának. A böngészőket

A biztonság lehetősége adott

felkészítették a feladatra, és szerveroldalon is adott a lehetőség. Gyakorlatilag anyagi terhe is csekély az effajta védelemnek. Az a néhányszor ezer, esetleg tízezer forint, amit a tanúsítványért fizetni kell, eltörpül az esetleges károk mellett. Mégis viszonylag kevesen élnek ezzel a lehetőséggel. Vélhetően azért, mert egyszerűen nem is gondolnak rá. „Talán a fele sem alkalmazza a védett kommunikációt azok közül a site-ok közül, amelyeket látogatok” – mutat rá Martos Balázs.

Arról, hogy biztonságos-e egy weblap vagy sem, rendkívül könnyen meggyőződhet a felhasználó. A böngészők általában egy kis ikonnal (például lakattal) jelzik a https-kommunikációt. Előugró ablak csak akkor figyelmezteti az embert, ha az illető weboldal olyan tanúsítványt alkalmaz, amely mögött nincs széles körben elfogadott hitelesítési lánc. Ilyenkor a böngésző megkérdezi a felhasználót, hogy folytatja-e a műveletet.

Ha valamiféle gyanú merül fel az oldal üzemeltetőjét, illetve a tanúsítvány valódiságát illetően, akkor a megfelelő menüpontnál bővebb információt kaphat a felhasználó.

Két hét várakozási idő

Jóllehet elsősorban a cégeknek kell körültekintően eljárniuk a doménnevek kiválasztásánál, Magyarországon az ISZT a maga eszközeivel megpróbálja csökkenteni a csalási lehetőségeket. Ezt a célt szolgálja az a kéthetes várólista, amire a regisztrációt megelőzően felkerül minden egyes nem-prioritásos, .hu alatti doménnév. A listát védjegyekkel, szerzői jogokkal stb. foglalkozó szakértők is folyamatosan figyelik. Ha bárki gyanús névre bukkan, akkor panaszt tehet.

„Sok esetben nem könnyű felfedezni a csalárd szándékot. Többnyire csak később, a weblapon elhelyezett tartalomból, a használatban derül ki, hogy valaki tényleg az összetéveszthetőséget akarja-e meglovagolni, vagy szó sincs ilyesmiről. Közismert cégeknél, márkák-nál, termékeknél, szolgáltatásoknál jobb a helyzet, ilyenkor adminisztrátoraink – és az egyszerű fogyasztók is – könnyebben észreveszik a hamisságot. Sokkal nehezebb azonban rábukkanni a csaló szándékra, ha maga a terület kevéssé ismert. Az magától értetődik, hogy minden olyan esetre fokozottan odafigyelünk, amikor valamilyen pénzintézet lehet az érintett” – fogalmaz Martos Balázs.

Mallász Judit

SZABVÁNYOS KARAKTERKÉSZLETEK

Két évvel ezelőtt, amikor a magyar ékezetes domménneveket bevezették, nagyon sokan érdeklődtek. Eleinte többen éltek a lehetőséggel, de aztán alábbhagyott a lelkesedés. Ma a teljes regisztrált állománynak mindössze 1-2 százaléka ékezetes.

Az érdektelenség egyik oka, hogy a legelterjedtebb böngésző, az Internet Explorer normál verziója egyelőre nem támogatja az IDN-eket (Internationalized Domain Name). Az IDN-ek egyébként az ASCII-n kívüli összes karakterkészletet tartalmazzák, teljesen szabványosított módon.

Megjegyzendő, hogy több böngésző, így például a Mozilla, a Netscape és az Opera már támogatja az IDN szabványt. Hírek szerint rövidesen az Internet Explorert is felruházzák ezzel a tulajdonsággal.

Rugalmas tárolók

A vezetéknélküli adatátvitelre alkalmas, hálózatra csatolt tárolóeszközök egyelőre különleges igényeket elégítenek ki.

A network-attached storage (NAS hálózatra csatolt tároló) technológia lényege, hogy az adattárolás a hálózathoz közvetlenül csatlakozó eszközökön, nem pedig a kiszolgálógépekben található merevlemezeken történik. A NAS-tároló Ethernet-kábelen keresztül kapcsolódik a vállalati hálózathoz, és a legtöbb esetben külön IP-címet kap, vagyis a hálózatnak független elemeként működik.

A technológia számos előnnyel rendelkezik a hagyományos hálózati adattároláshoz képest. Mivel a tárolás nem a kiszolgáló merevlemezén alapul, a tárkapacitás nem függ attól, hogy hány merevlemez-meghajtó fér el a kiszolgáló házában. A hálózati tárkapacitás NAS-eszközökkel tetszés szerint bővíthető a kívánt szintig, és egy berendezésen belül elegendő számú meghajtó helyezhető el RAID-es konfiguráció kiépítéséhez.

Sokoldalú wireless NAS az Iomegától

Az információk átmeneti tárolásához és ennélfogva az adatátvitel gyorsításához a NAS-eszközöket kapacitásuktól függő méretű memóriával szerelik fel a gyártók. A NAS tehermentesíti a kiszolgálógépet, és mivel attól külön működik, kevésbé érintik a rendszer összeomlásából és a biztonsági fenyegetésekből eredő gondok. Ha pedig a NAS-rendszerrel kapcsolatban lépnek fel problémák, egyszerűbb felépítése miatt a különálló tárolóeszközt sokkal gyorsabban lehet diagnosztizálni és újraindítani.

Sok NAS-berendezésen saját operációs rendszer fut, kezelésüket pedig webes felületen keresztül lehet végezni a mellékelt segédprogramokkal. A tárolóeszközök állapotát, az esetleges hibák diagnosztizálását és a konfiguráció megváltoztatását megfelelő jogosultsággal a hálózat bármely munkaállomásáról végre lehet hajtani.

A NAS-tárolók legfőbb jellemzője az alkalmazott merevlemezek típusa (SCSI, SATA), a tárolókapacitás és a bővíthetőség mértéke. A kisebb igényeket kielégítő berendezések kapacitása 1-2 terabájt, a közepes kategóriába a 30 terabájtig terjedő kapacitású rendszerek tartoznak, míg a csúcsmodellek tárolókapacitása meghaladja a 100 terabájtot. A gyorsabb adatátvitel érdekében sok modell gigabites Ethernet-összeköttetésen keresztül is használható.

Speciális igényekre

Mind népszerűbbé válnak a vezetéknélküli hálózatok, így nem csoda, hogy a vezetéknélküli technológia megjelent a NAS-ok világában is. Az úgynevezett wireless NAS-berendezések kétféleképpen használhatók: vezetéknélküli hozzáférési pontként, illetve hagyományos módon, kábelezéssel a hálózatba kötve. Vezetéknélküli átvitel esetén a tároló lényegesen alacsonyabb adatátviteli sebességet nyújt, mint hagyományos üzemben, igaz, kisebb munkacsoportok esetében ez nem okoz gondot. Különféle biztonsági problémák is fellépnek a vezetéknélküli adatátvitelkor.

Hogy mégis mi a létjogosultsága ennek a hibrid eszköznek? Speciális igények kielégítésére hozták létre, van ugyanis néhány olyan szituáció, amikor igen hasznos lehet. Ha például egy olyan helyiségben kell nagykapacitású tárolóeszközt telepíteni, ahol a hagyományos kábelezésre nincs mód. Vagy ha egy ideiglenesen használt irodában van szükség adattárolóra, és az átviteli sebességgel kapcsolatban nem merül fel különösebb igény, egy vezetéknélküli NAS-eszköz olcsó és kielégítő megoldás lehet. Ugyancsak jó hasznát vehetjük egy vezetéknélküli NAS-berendezésnek egy olyan irodában, ahol több noteszgépet kell vezetéknélküli kapcsolattal a vállalati hálózathoz csatlakoztatni, és helyi tárolóeszközre ugyancsak szükség van.

Biztonsági kérdések

A vezetéknélküli NAS-okkal kapcsolatos kockázatok gyakorlatilag megegyeznek a vezetéknélküli hálózatok biztonsági problémáival. Szerencsére léteznek hatékony módszerek a fenyegetések elhárítására, így megfelelő konfigurálás esetén ezek a tárolóeszközök is biztonságosan használhatók.

Az IEEE 802.11 szabványú vezetéknélküli hálózatokhoz eredetileg kifejlesztett Wired Equivalent Privacy (WEP) eljárás titkosítási hiányosságai miatt nem használható biztonságosan az adatátvitel védelmére, a megfelelő eszközökkel felszerelt támadók ugyanis némi technikai tudás birtokában jogosulatlan hozzáférést szerezhetnek a WEP-et használó vezetéknélküli hálózatokhoz. A WEP csupán 40 bites kulcsokat alkalmaz, ugyanazt a kulcsot használja minden hálózati felhasználó, s ez a kulcs mindaddig nem módosul, amíg a rendszergazda meg nem változtatja azt a WLAN-hoz csatlakozó minden berendezésen, ami a hálózat növekedésével egyre több időt vesz igénybe. Kutatások megállapították, hogy elegendő mennyiségű hálózati forgalom összegyűjtésével egy hacker háromféle módon jelenthet veszélyt a WEP-titkosítást alkalmazó vezetéknélküli hálózatra. Egyrészt az átvitt adatok lehallgatásával és titkosításának dekódolásával, másrészt az átvitt információ megváltoztatásával, harmadrészt pedig a hálózathoz való hozzáféréssel. Egy nagy forgalmú vállalati vezetéknélküli hálózatban csupán néhány óra szükséges a titkosítás feltöréséhez. Az is megkönnyíti a támadó dolgát, hogy a WEP-et nem látták el azonosítási mechanizmussal, pedig ez biztosítaná, hogy csak az használhassa a hálózatot, aki erre jogosult.

A WEP hiányosságainak megszüntetésére hozták létre a szabványalkotók a Wi-Fi Protected Access (WPA) specifikációt – pontosabban annak második ver-

zióját, a WPA2-t –, amely megszünteti a WEP összes sérülékenységét, és védelmet nyújt a legkifinomultabb támadásokkal szemben is. A titkosításra a 128 bites kulcsú Temporal Key Integrity Protocolt (TKIP) használja, a felhasználók azonosítására pedig bevezeti a 802.1X hitelesítést és az Extensible Authentication Protocolt (EAP).

Lényegesen fejlettebb titkosítást használ a WPA2, mint kudarcot vallott elődje, az alkalmazott dinamikus kulcsok menetenként és felhasználónként változnak, és a kulcsok szétosztása automatikus. A TKIP kulcshierarchiája és -kezelése kiküszöböli a WEP-re jellemző megjósolhatóságot. A kulcs méretének és a használt kulcsok számának nagymértékű növelésével, valamint az integritás vizsgálatával a TKIP lényegesen megnehezíti a vezetéknélküli hálózatban továbbított titkosított adatok dekódolását.

Kis odafigyeléssel biztonságossá tehető a vezetéknélküli adatátvitel

Vezetéknélküli tárolóközpont

Több gyártó kínálatában találunk vezetéknélküli átvitelre képes, hálózatra csatolt tárolóeszközöket. Ilyen például a négy darab, RAID-tömbbe kapcsolható, 250 gigabájtos meghajtót tartalmazó Iomega-féle StorCenter Wireless NAS 1TB, amelyet 10/100/1000 megabites Ethernet-csatoláson vagy 802.11g szabványú vezetéknélküli kapcsolaton keresztül köthetünk a hálózatba, vagy csatlakoztathatunk PC-hez. A kis cégek és otthoni felhasználók által egyaránt jól hasznosítható eszközt archiválási, valamint nyomtató- és médiakiszolgálási célokra szánja a gyártó. További merevlemezek és nyomtatók csatlakoztatására szolgál a StorCenter hátlapján elhelyezett két USB-port. Vezetéknélküli üzemmódban mind a WEP-, mind a WPA2-titkosítás használható.

A StorCenterhez mellékelt Iomega Automatic Backup Pro programmal a hálózati számítógépekről ütemezett archiválásokat készíthetünk (a kijelölt mappák növekményes archiválásától kezdve a teljes rendszerről való másolatkészítésig), amelyeket aztán katasztrófa esetén az adatszerkezet visszaállítására használhatunk. Természetesen a StorCenter tartalmáról is készíthetünk másolatot a hozzá csatlakoztatott merevlemezre vagy egy másik NAS-eszközre. Ami a médiakiszolgáló funkciót illeti, az Iomega UPnP adapteren keresztül televízióhoz csatlakoztatható készüléke kiválóan alkalmas videók, zenei állományok és fényképek központi tárolására.

Tóth István

Bizonyíték a semmiből

Vezetéknélküli támadók nyomában.

A 802.11 specifikációkon alapuló hálózatok gyors terjedése meglehetősen populáris támadásvektorrá tette a vezetéknélküli kommunikáció csatornáit. Ugyanakkor a technológia komplexitása miatt nehéz a biztonsági incidensek kezelése, illetve súlyosabb esetben a nyomozati munkát végzők és jogalkalmazók helyzete.

Wireless Forensics

A „vezetéknélküli nyomrögzítés” olyan önálló diszciplína a számítógépes és azon belül a hálózati kriminalisztika tárgykörében, amelynek célja a vezetéknélküli kommunikációra vonatkozó információk begyűjtése és elemzése, hogy azokat valós digitális bizonyítékként lehessen felhasználni jogi eljárásokban. Az adatok a „sima” digitális, IP-forgalomra vonatkozó információtól a rögzített VoIP alapú beszégetésekig terjedhetnek. A tevékenység felöleli a hálózati forgalmi adatok gyűjtését, elemzését, az anomáliák felderítését, az esetleges támadások eredetének keresését és az incidensek vizsgálatát.

Technikai gondok

A nyomozati munka ugyanazoknak az alapelveknek megfelelően halad, mint az IT-kriminalisztika általában: bizonyítékok azonosítása, rögzítése és elemzése, majd prezentálása (Fehérgallérosok nyomában – *IT-Security,* 2005/7.). Ezek már önmagukban problémás területek, de a vezetéknélküli technológiák egyedi sajátosságai jócskán bonyolítják a helyzetet.

A tapasztalható nehézségek javarészt a 802.11-es – a/b/g altípusok és a majdani „m” szabvány – hálózatok és a „megfoghatatlan” rádiófrekvenciás közeg természetéből adódnak.

Csatornák

Az interferencia elkerülése miatt a vezetéknélküli frekvenciaspektrum több csatornára oszlik, ezért olyan „multi-band” monitorozóeszközökre van szükség, amelyek a három mostani standard csatornafüggő modulációra egy időben képesek ráhangolódni. Az első gond az, hogy a detektálási lehetőségek nem mindig felelnek meg a vonatkozó rádiófrekvenciás előírásoknak. Másrészt több elérési pont figyelése esetén ezekkel sem lehetséges a teljes spektrum figyelése, hanem néhány ezredmásodpercenként folyamatosan ugrálni kell a csatornák között. Egy komolyabb vezetéknélküli rendszerben ezért a teljes forgalom figyeléséhez sok multi-band szenzoreszköz kell.

Minden elérési pontot monitorozni kell

Még egy „apróság”: a nemzetközi előírások meghatározzák az országok által használható csatornákat és az adó maximális energiaszintjét, de a támadók természetesen fittyet hánynak ezekre a regulákra, és erre az elemzőnek is fel kell készülnie.

A mobilkliensek és a roaming

Ami a felhasználóknak előny, az a kriminalisztika számára hátrányként jelentkezik: a kliensek a nagy térbeli kiterjedésű vezetéknélküli hálózatokban virtuálisan a jel megszakadása nélkül barangolhatnak. Ez a „roaming” technológia miatt lehetséges, ami azt jelenti, hogy kommunikáció közben nagyon gyorsan át lehet váltani az aktuális gyengülő jelű elérési pontról egy közelebbire. A nyomrögzítést nemcsak az nehezíti meg, hogy ilyenkor eszközök közötti váltás történik, hanem az is, hogy általában a csatorna is változik. Természetesen az alapgond az, hogy a hálózatot térben is le kell fedni a monitorozóeszközökkel – kézenfekvően az elérési pontok közelében.

Ha az összes elérési pontot a több csatorna figyeléséhez szükséges megfelelő számú érzékelővel „bedrótoztuk”, akkor már „csupán” az marad hátra, hogy ezeket a roamingos ugrások miatt összehangoltan működtessük. Ha pedig igazán pontosak akarunk lenni, és a figyelt eszköz helyzetét is rögzíteni akarjuk, akkor az egészet megfejelhetjük egy okos kis háromszögelő mechanizmussal.

Maga a forgalom

A vezetéknélküli forgalom alapvető jellemzője, hogy nem folyamatos, hanem csomagokban („keretekben”) zajlik, ezeknek pedig diszkrét méret-, illetve számossági (és sávszélességi) jellemzőik vannak.

Méretgond. A 802.11 technológiákban a méretet az MTU (Maximum Transmission Unit) írja le; bájtban kifejezett értéke 2304. Ezt a különféle titkosító mechanizmusok – WEP, WPA, WPA2 – jól megvariálják, ezért a tényleges csomagméret 2304–2324 bájt között alakul, és ezt érzékelni kell.

Számproblémák. Az adatcsomagok számába az zavar be, hogy a vezetékes hálózatoktól eltérően a megbízhatatlan rádiófrekvenciás technológia miatt a vezetéknélküli rendszerekben az adatcsomagok mellé beiktattak egy „control” és egy „management” csomagtípust is, amelyek mindegyike hatással van a tényleges forgalmazás mennyiségére, de szükségesek a pontos szinkronizálásokhoz és a megbízható adatforgalmazáshoz. Az értékes információ az adatcsomagokban van, de ezek összmérete a teljes forgalom volumenének – egy mobileszközön durván 200–300 megabájt óránként – mindössze 6–50 százaléka.

Kelemen László

ESEMÉNYNAPTÁR

Időpont	Megnevezés	Helyszín	Web	Részvételi díj	Leírás
Február 27–március 1.	EuroCIS 2007	Düsseldorfi Vásárváros, Németország	*www.eurocis.com*	Napijegy 20 euró	Európa egyik legnagyobb, a kereskedelmi alkalmazásoknak szentelt távközlési, informatikai és biztonságtechnikai bemutatója, amelyre 200 kiállítót és mintegy ötezer döntéshozó látogatót várnak.
Március 14–15.	SecureWorld Expo	Boston, Egyesült Államok	*www.secureworldexpo.com/events/index.php?id=240*	195 dollár	A konferencia témái: biztonságtechnológia, IT-biztonság, a fizikai és a digitális biztonság konvergenciája, kockázatkezelés, vállalati biztonság.
Március 15–21.	CeBIT	Hannover, Németország	*www.cebit.de*	Napijegy 38 euró	A számítástechnikai és telekommunikációs szakkiállítás főbb témái: üzleti folyamatok; kommunikáció; digitális eszközök és rendszerek; bank és finanszírozás; államigazgatás.
Március 19–23.	Cybercrime Summit 2007	Atlanta, Egyesült Államok	*www.southeastcybercrimesummit.com/*	249 dollár	A korábban Southeast Cyber Crime Summit névre hallgató konferencián ismertetik az információbiztonság legújabb trendjeit, kitérnek az egyes bűnözési technikákra is.
Március 27.	IDC IT Security Roadshow 2007	Budapest	*www.idchungary.hu*	Költségvetési szervek, média: ingyenes; vállalati szféra 19 000 forint+ áfa; IT-vállalatok, tanácsadó cégek: 65 000 forint + áfa	A konferencia témái: a hálózatok védelme a belső és külső fenyegetésekkel szemben; adat- és hálózatvédelmi szabályok bevezetése; megelőző biztonság és behatolásérzékelés, hackertechnikák és észlelésük; a hagyományos és webes alkalmazások biztonsága, a mobil- és vezetéknélküli hálózatok biztonsága; titkosítási eszközök és kihívások, személyazonosság-lopás és -kezelés.

OKTATÁS, TANFOLYAMOK

Tanfolyam címe	Leírás	Időpont	Időtartam	Részvételi díj	Webcím	Helyszín
ISO 27001:2005 vezetőauditor-tanfolyam	A tanfolyam célkitűzései: megismertetni az ISO 27001, BS 7799–2, ISO 17799 és ISO 19011 szabványok célját, tartalmát és kapcsolataikat; elsajátíttatni az auditáláshoz szükséges elméleti és gyakorlati ismereteket; értelmezni az ISO 27001 követelményeit egy audit összefüggéseiben; teljesíteni a nemzetközi vezető auditori regisztráció képzési követelményeit.	Március 5.	4 nap	310 000 forint + áfa	*www.training.hu.sgs.com*	Budapest, Sirály u. 4.
Bevezetés a McAfee vírusvédelmi rendszerek hatékony üzemeltetésébe	A tanfolyamon ismertetik napjaink (és a közeljövő) vírusait, a VirusScan Enterprise 8.0i jellemzőit (On-Access Scan, On-Demand Scan, Email Scan, Buffer Overflow protection, Access protection, Unwanted Programs), majd végigveszik, hogyan kezeljünk egy vállalati védelmi rendszert központilag – a gyakorlatban bemutatják a McAfee ePolicy Orhestratort.	Március 7.	1 nap	21 000 forint + áfa	*www.piksys.hu*	Budapest, Boráros tér 7.
DRP – IT-katasztrófaelhárítás: elmélet és gyakorlat	Katasztrófának nevezünk minden olyan eseményt, amelynél adat vagy információ vész el, vagy valamilyen elektronikus szolgáltatás nem lesz elérhető (például leáll a levelezés). Az elsődleges cél, hogy ezektől a váratlan eseményektől védjük meg a céget, megfelelő akciótervekkel egészítve ki a meglévő IT-eszközöket, hogy a váratlan események által okozott károkat közel nullára csökkentsük. A tanfolyam témái: A katasztrófaelhárítási terv szükségessége; A fenyegetések azonosítása; A szolgáltatások kiesésének hatáselemzése; A katasztrófaelhárítás tervezésének megvalósítása; A katasztrófaelhárítási terv tartalma.	Március 12.	3 nap	139 000 forint + áfa	*www.net-academia.net*	Budapest, Andrássy út 62.

Világpolgárok a selyemúton

Határokon átívelő virtuális tranzakciók nyomában: Ellenőrzőpontok a cybertérben.

Amikor bekapcsoljuk a számítógépünket és csatlakozunk az internetre, ritkán tudatosul bennünk, hogy székünkben ülve rendszeresen elhagyjuk az ország határait, és világpolgárként, kontinenseken át utazgatunk. Levelezésünket egy nagy amerikai cég szerverein tároljuk, fotóinkat egy másikén. Online pénzügyeinket szintén amerikai cégre bízzuk, honlapunkat viszont egy ismeretlen ország jól hangzó doménje alá jegyezzük be. A nyaralást pedig már régen nem utazási irodán keresztül intézzük, hanem közvetlenül a spanyol, indiai vagy akár perui hotel honlapján foglaljuk le és fizetjük ki. Ilyenkor a saját szobánkban ülve talán nem is tűnik fel, hogy nem Magyarországon vagyunk, és nem a magyar törvények érvényesek ránk. És hiába érezzük magunkat világpolgárnak, ezt a fogalmat a jog nem ismeri.

Fel van adva a lecke

Azt, hogy egy határokon átívelő virtuális tranzakcióra mely ország törvényei vonatkoznak, még jogászok számára sem egyszerű eldönteni. A vásárló természetesnek veheti, hogy például egy légitársaság magyar nyelvű honlapján vásárolt repülőjeggyel kapcsolatban a hazai fogyasztóvédelmi előírások vonatkoznak rá. Csakhogy hamar kiderülhet: a légitársaságnak nincs is magyarországi képviselete, és igazából egy Kajmán-szigeteken bejegyzett vállalat. Akkor – gondolhatjuk – a szervereknek otthont adó ország törvényei az érvényesek. Igen ám, de könnyen kiderülhet, hogy a szerverek egy távoli, egzotikus királyság légkondicionált termében duruzsolnak, ahol nemhogy fogyasztóvédelem, de még parlament sincs. A történet tovább bonyolódik, amikor kiderül, a jegyet igazából egy virtuális légitársaságtól vettük, amelyiknek semmije sincs 77 nyelvű honlapján kívül; és csupán más társaságok szolgáltatásait közvetíti a saját márkanevén.

Nem egyszerű tehát világpolgárnak lenni – az esetek túlnyomó többségében azonban nem szokott problémánk lenni. Sőt, általában az interneten a dolgok könnyebben, gyorsabban, jobban kitalálva működnek, mint a valóságban. Ahhoz azonban, hogy ez így legyen, a szolgáltatásokat nyújtó vállalatoknál hadosztálynyi jogász dolgozik három műszakban.

Késésben a jog

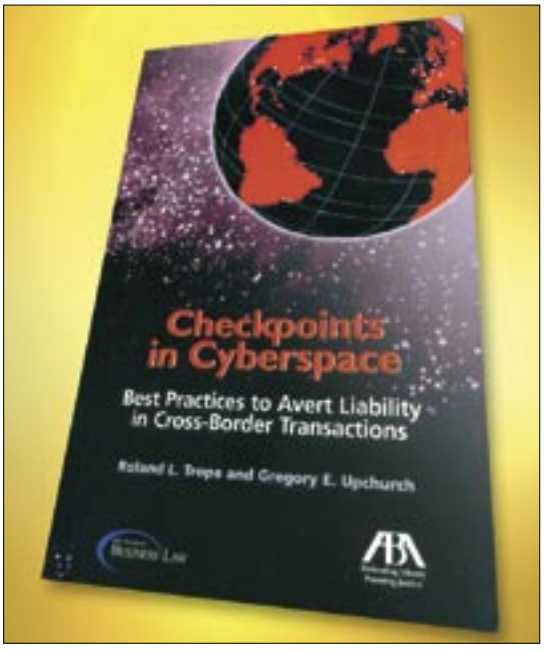
Talán érdemes is kimondanunk: a jog kiábrándító és lehangoló mértékben le van maradva a valóság, pontosabban a virtuális valóság mögött. Ez a tény nem is akkor aggasztó igazán, amikor magánemberként, fogyasztóként csatlakozunk az internetre, hanem akkor, amikor kis hazai vállalkozásként szeretnénk globálisan értékesíteni termékeinket és szolgáltatásainkat. Az „Ellenőrzőpontok a cybertérben” című könyv szerzői az internetet az egykori selyemúthoz hasonlítják, amely magába szívta a kereskedelmet Európa és Ázsia között. Bár az út számtalan országon haladt keresztül, amelyekben a vallás, a kultúra és a törvények alapvetően különböztek, mégis, a közös cél, a kereskedelem érdekében egyik ország sem erőltette ezeket különösebben.

Mondhatni, ez ma is így van. Elvileg például üzletek működtetéséhez minden fejlett országban szükség van valamiféle végzettségre. Mégis, egy online áruházon ezt a szabályt egyelőre egy országnak sem jutott eszébe számon kérni. A versenyképesség, a gazdasági növekedés fontosabb célnak minősül. Vannak szabályok, amelyeket viszont számon kérnek. Méghozzá minden országban másként. A megfelelő jogászok azonban sok esetben megfizethetetlenül drágák egy hazai vállalat számára.

Technológiát Iránba?

Szerencsére itt van nekünk *Roland L. Trope* és *Gregory E. Upchurch* kötete, ami igazából nem más, mint esettanulmányok hosszú sora, iparágakon és kontinenseken át. Hogyan adjunk el technológiai terméket Iránba? Mire figyeljünk, ha Japánnal kereskedünk online? Mi a helyzet az áfával, ha külföldre adunk el különböző virtuális szolgáltatásokat? Melyik ország törvényeit kell alapul venni egy esetleges peres eljárásban? Rengeteg egyszerű és összetettebb kérdésre ad választ a könyv, s ezek megválaszolása egy kezdő ügyvédnek is biztos megélhetést nyújtana néhány évre.

Sós Éva



KÖNYV-JELZŐ

Szerző: Roland L. Trope és Gregory E. Upchurch
Cím: Checkpoints in Cyberspace
Best Practices to Avert Liability in Cross-Border Transactions
Kiadó: American Bar Association
Ár: 72 dollár
Terjedelem: 496 oldal

Evangelizáció az oktatásban

Elméleti ismeretek mellett gyakorlati képzést és piacképes tudást ad a speciális kollégium.

Mostanra érett be egy olyan know-how, amelyet kár lenne veszni hagyni – mondja az ELTE és a Kancellár.hu közös kezdeményezésének hátteréről *Papp Péter,* a Kancellár.hu ügyvezetője. Álláspontja szerint az iparban dolgozók feladata az evangelizáció is. Azt szeretnék, hogy minél több hallgató ismerkedjen meg az IT-biztonság gyakorlati oldalával. Ha jól képzett, kész szakemberek állnak munkába – az eladói és a vevői oldalon egyaránt –, akkor lehet arra számítani, hogy megértik egymás nyelvét.

A vállalat alkalmazottainak fele az ELTE programozó matematikus szakán végzett, ugyanakkor azt tapasztalták, hogy a képzés során nem foglalkoztak kellő mértékben az információbiztonsággal. „Arra a következtetésre jutottunk – mondja Papp Péter –, hogy szükség van egy olyan tantárgyra, amelynek keretében piacképes tudást szerezhetnek a hallgatók. Természetesen pusztán a speciális kollégium elvégzésétől senki sem válik profi szakemberré, de a képzés anyaga biztos alapot nyújt, ahonnan autodidakta módon professzionális szintre lehet eljutni."

Gyakorlatorientált képzés

Tematika

A Kancellár.hu immár öt éve rendszeresen tart háromnapos információbiztonsági kurzusokat információbiztonsági vezetőknek. Az ELTE-n most indított információbiztonsági speciális kollégium ennek bővített változata. Az új tantárgyat azok vehetik fel, akik letették a szoftverszigorlatot. A hallgatóknak a félév végeztével vizsgán kell számot adniuk tudásukról. Ha ezen megfelelnek, kreditpontot kapnak.

A speciális kollégium heti két óra előadásból áll. Ezeket jórészt a Kancellár.hu szakemberei tartják, de az oktatók között van *Kovács Attila,* az ELTE Informatikai Karának docense is. A vizsgáztatást ugyancsak közösen végzik.

A tervek szerint az információbiztonsági kurzus beépülhet az egyik oktatási modulba. „A hagyományos képzésben az utolsó két év modul-rendszerű – avat be a részletekbe Kovács Attila. – A különböző szakirányokból tömböket képeztünk, amelyek közül a hallgatóknak négyet kell elvégezniük. Az egyik ilyen egység a szoftvertechnológia – ide kerülhet be az új tantárgy. Jelenleg 30 fős kerettel terveztük a speciális kollégiumot, ám ha a modulképzés része lesz, ez a szám 30–40 fővel növekedhet."

Három fő témával foglakozik a tantárgy:

- technológia: a korszerű cég működési folyamatai s azok vetületei az információbiztonságban;
- jogi háttér: a vállalatműködés jogi keretei, vagyis az a jogi környezet, amelyben az IT-biztonsági kritériumokat alkalmazni kell;
- szabványok: a szakterület hazai és nemzetközi szabványainak bemutatása.

Gyakorlatközpontúan

Korábban az egyetemen inkább elméleti jellegű anyagot tanítottak. Bemutatták a különböző protokollok elméleti matematikai hátterét, arról azonban nem szóltak, hogy milyen szabványok épülnek rájuk, azokhoz milyen jogrendszer kapcsolódik, s mindez hogyan épül be a technológiába. A speciális kollégium ezzel szemben gyakorlati példákon keresztül ismerteti a tananyagot: azokat a szabványokat, dokumentumformátumokat, szabályzatokat mutatják be, amelyeket a Kancellár.hu munkatársai mindennapi munkájukban használnak.

Matula Zsolt

BIZTONSÁG A BME-N

Nem hiányzik az IT-biztonság a BME oktatott tantárgyai közül sem. Minden informatikus hallgatónak – évfolyamonként 350 főnek – kötelező 7. félévi tárgya az adatbiztonság. Emellett évről évre mintegy 40 hallgató jelentkezik a BME Villamosmérnöki és Informatikai Karán a műszaki informatikai szakon az infokommunikációs rendszerek biztonsági szakirányára. Ez utóbbi keretében, a 7–9. félévben a következő öt speciális tárgyat oktatják, különböző laboratóriumi gyakorlatok kíséretében:

- a számítógépes biztonságtechnológia;
- a hálózatbiztonsági protokollok;
- a hibatűrő hálózati architektúrák és modellezésük;
- az infokommunikációs szolgáltatások biztonsága;
- a biztonságos elektronikus kereskedelem alapjai.

A terület gazdája a BME-n a híradástechnikai tanszék, ezen belül az adatbiztonság tantárgyért *Vajda István* egyetemi tanár a felelős, míg az infokommunikációs rendszerek biztonsága című szakirányon folyó oktatást *Buttyán Levente* egyetemi docens irányítja. Mindketten a Crysys Adatbiztonsági Laboratóriumhoz tartoznak.

A kétszintű képzés keretében MSc-szinten a szakirány folytatását is tervezik, a jelenlegihez hasonló tartalommal. „Igyekszünk széles spektrumot lefedni. Az a célunk, hogy mindenki megtalálja az őt érdeklő témát – beszél a tananyagról Buttyán Levente. – Szakirányunk keretében elsősorban elméletet oktatunk ugyan, de mindvégig ügyelünk az alkalmazhatóságra. A laboratóriumi gyakorlatok során gyakorlati jellegű tudást szerezhetnek a hallgatók."

Az elmélyülést az egyes területeken önálló laborok segítik. Mivel ezek általában tanszéki kutatási projektekhez kapcsolódnak, a hallgatók egyszersmind ilyen irányú tapasztalatokat is szerezhetnek.

IT-SECURITY

Mit olvas a szakértő?

Célirányosan szűrve és rendszerezve.

Gál Tamás

Aktív rendszerüzemeltetői, illetve rendszermérnöki minőségében sem engedheti meg magának azt a luxust *Gál Tamás*, hogy tájékozatlan, vagy elavult tudású legyen.

Mindez fokozottan igaz az IT-biztonságra, különösen azért, mert speciális szakterületéhez (amelynek MVP-szakértője) tartoznak a Microsoft vállalati tűzfal- és egyéb biztonsági kiszolgáló termékei.

A hírforrások típusát tekintve nála már átvették a vezetést a blogok és az RSS-hírcsatornák, amelyeket naponta többször is átnéz. Több Microsoft-termékcsapat és -szakember blogját is kiemelkedőnek tartja; a TechNet- és az MSDN-oldalakról elérhető rengeteg feed közül az egyik legfontosabbnak a Security Bulletinst ítéli. Több jelentősebb cég vagy szervezet hírei mellett a biztonsággal kapcsolatos területeken aktív MVP-kollégák webnaplói is remek olvasmányok.

Hasznos és „leülős" forrás a hírlevél is, akár belső vagy publikus Microsoft-hírlevelekről van szó, akár egyéb forrásból érkezőkről (Windows IT Pro, Shavlik, MCP-Mag, egyebek). A nagy és ismert biztonsági portálokat manapság már szintén csak a feed-olvasóból figyeli, mivel szinte mind rendelkezik RSS-csatornával, és csak extrém hosszú cikkek esetén kényelmesebb a böngésző.

Magyarul értelemszerűen jóval kevesebb forrás közül válogathat, de a magyar Microsoft TechNet-oldala, a NetAcademia Tudástára vagy a Technetklub levelezőlistái azért nem maradhatnak ki a felsorolásból.

Schopp Attila

A LEGJOBB FORRÁSOK

Hírforrás	URL	Jellemzők
Blogok, RSS		
Steve Riley on Security	*http://blogs.technet.com/steriley*	A biztonsági „mágus" blogja
Thomas Shinder Blog	*http://blogs.isaserver.org/shinder*	Az ismert ISA-MVP blogja
ISA Server Product Team Blog	*http://blogs.technet.com/isablog/default.aspx*	Az ISA-fejlesztőcsapat blogja
Security Bulletins	*http://www.microsoft.com/technet/security/current.aspx*	Információk, letöltés, RSS
F-Secure News	*http://www.f-secure.com/weblog*	Érdekes blog, vírusokról és egyéb kártevőkről
CERT Advisory	*http://www.cert.org*	Sérülékenységek, tudásbázis, RSS
Portálok/fórumok		
TechNet Security Center	*http://www.microsoft.com/technet/security/default.mspx*	Minden, ami Microsoft és biztonság
ISA Server Resource Site	*http://www.isaserver.org*	A legjobb ISA Server-portál
TechNet Forums	*http://forums.microsoft.com*	Érdekes kérdések és hasznos válaszok lelőhelye
Hírlevelek		
Windows IT Pro	*http://www.windowsitpro.com/email*	IT Pro-hírlevelek rengeteg témakörben
MCP Magazine	*http://mcpmag.com*	Heti hírlevelek szintén több IT Pro-területen

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*

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:
Harsányi Erika – *eharsanyi@vogelburda.hu,* tel.: 888-3452
Németh Krisztina – *knemeth@vogelburda.hu,* tel.: 888-3468
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

TERJESZTÉS
Terjesztett példányszám: 8000–10 000
Terjesztési osztály: 1426 Budapest, Pf. 300/39

Ügyfélszolgálat és bolt: Budapest VI., Teréz körút 47. (Nyugati pu.-nál) Hétfő–péntek: 9–20 óráig, szombat-vasárnap: 9–15 óráig

Nyomda: Pauker Nyomdaipari Kft.
1047 Budapest, Baross u. 11–15.
Felelős vezető: Vértes Gábor ügyvezető igazgató

IT-BUSINESS TODAY

goes mobile ...

Az IT-BUSINESS TODAY SMS küldésével WAP rendszerben már mobiltelefonon is elérhető, így számítógép segítsége nélkül is elérhetővé válnak a legfontosabb ICT-piaccal kapcsolatos hírek, történések, események.

Próbálja ki most!

Küldje el az ITBTODAY szót SMS-ben a +36 30 285 5441 számra és kövesse az instrukciókat!

WAP cím: **wap.it-business.hu**

Név:	**Gábor**
Életkor:	**31 év**
	(20 éve számítógépekkel foglalkozik)
Jármű:	**Bickli**
Végzettség:	**Programozó matematikus**
Képzések:	**5 országban, 16 tanfolyam.**
Tanulás:	**Napi 2 órát tanul.**
Szenvedélye:	**A munkája**

Különös ismertető:

Magyarország 8 bankigazgatójának ad információbiztonsági tanácsot.

Gábor egyike a kancellár.hu 25 szakértőjének!

kancellár.hu

az informatikai biztonság szakértője

Magyarország vezető információbiztonsági cége.

Duna Tower 1138 Budapest, Népfürdő u. 22. telefon: +36 1 2704tel fax: +36 1 2704fax e: info@kancellar.hu w: kancellar.hu