Kiss Gergely
MTI Sajtóadatbank

Az Internet és a biztonság

Őszintén, reklám nélkül az Internetről

Sok szó esik manapság az Internet nagyszerűségéről, előnyeiről. Az igazsághoz tartozik azonban az árnyoldal is, s annak legsötétebb pontja: az Internet-bűnözés. Az alábbiakban vázlatos áttekintést kaphatunk az intellektuális bűnözés e sajátos, modern műfajáról, és az ellene való védekezés lehetőségéről.

Az Internet vitathatatlan előnye, hogy segítségével könnyen és gyorsan juthatunk a világ bármely részén közreadott információhoz, feltéve, hogy a kívánt információt egy szolgáltató hozzáférhetővé teszi a felhasználók számára. Egy hálózatra kapcsolódó felhasználói munkaállomásról az összes szolgáltatói szerver elérhető.

Ez viszont azt is jelenti, hogy a szolgáltató gépe az összes, immár több tízmillió felhasználó számára nyitottá válik. Mindez addig nem okoz problémákat, amíg a hozzáférhetővé tett gép vagy gépek nincsenek összekapcsolva a cég vagy intézmény belső hálózatával. Ebben az esetben a kívülről bejelentkező felhasználók valóban csak a hozzáférhetővé tett információkhoz – egyetlen szerver anyagához – juthatnak hozzá. Mihelyst azonban az Internetre kapcsolódó szerver és a belső hálózat gépei között összeköttetést teremtünk, önkéntelenül is megadjuk a lehetőséget arra, hogy a felhasználó minden olyan információhoz hozzáférjen, amelyet valamilyen okból (állami, szolgálati, üzleti érdekeket szem előtt tartva) nem kívánunk közkinccsé tenni. Belső hálózatunk már egy állandó Internet-elérhetőséggel rendelkező gép rákapcsolásával is sebezhetővé válhat.

Az Internet elérhetőségének és szolgáltatásainak exponenciális növekedése, a felhasználói tábor radikális bővülése nem csak pozitív szándékokat hozhat felszínre. E globális virtuális társadalomnak is megvan a maga „alvilága", amely illegális úton próbál információhoz jutni – lehetőleg ingyen, vagy mások költségére, és lehetőleg korlátozott hozzáférésű, tehát nem nyilvános információkhoz.

Az elmúlt hetekben Budapesten két olyan fórum is foglalkozott az Internet és a biztonság kérdésével, amely tekintélyes számú szakmai érdeklődőt vonzott: az egyiket az ICON Kft. szervezte 1996. április 30-án *Biztonságos Internet* címmel, a másikat a Magyar Adatbázisforgalmazók Szövetsége rendezte meg 1996. május 8-án egy klubnap keretében *Digitális aláírás* elnevezéssel. A jelen összefoglaló nagyrészt a két fórumon elhangzottakra és írásos anyagokra támaszkodik.

Miért van szükség a védelemre?

Ha áttekintjük, hogy egy szolgáltatónak milyen szempontokat kell figyelembe vennie hálózata megvédéséhez, elsősorban azt a kérdést kell megvizsgálnunk, hogy *kitől kell megvédeni a hálózatot.*

Az egyszerűbb eset: ha a támadás kívülről jön

A jelenleg kb. 94 millió terminálos felhasználói táborból mindig lesznek olyanok, akik illetéktelen módon akarnak információhoz jutni, vagy ennél rosszabb eset, amikor szándékos károkozás a céljuk. A *Data Communications* 1996 áprilisában tett közzé egy felmérést, amely szerint „minden ötödik Internetre kapcsolt céghez betörtek".

Mivel az Internet nyílt hálózat, rengeteg belépési pontot kínál, s a támadó könnyen elrejtőzhet. Igen egyszerű dolog névtelenségbe burkolózva garázdálkodni az Interneten.

Az Egyesült Államokban alakult ki az az osztályozási mód, ahogyan a *kívülről behatolókat* csoportosítják:

Hacker – nem rosszindulatú illegális behatoló, nem károkozás a célja, nem követ el illegális tevékenységet, de adatokhoz, információkhoz, programokhoz szeretne hozzájutni, s meglehetősen szabadon kezeli a copyright kérdését.

Cracker – tevékenysége komoly műszaki problémákat is okozhat, illegálisnak minősül, károkozásra is hajlamos (beavatkozik egyes rendszerek működésébe, átprogramoz, megbénít, blokkol). Ha nincs is mindig konkrét célja, azért teszi meg, amit tesz, mert képes rá. „Nem ott törnek be, ahol

akarnak, hanem ott, ahol biztonsági lyukakat találnak."

Phreak – ún. telefonvonal-betyár, aki a távközlési vonalakat ingyen vagy más számlájára használja.

Az egyéni behatolók mellett komoly veszélyforrást jelentenek a szervezeteket képviselő behatolók. Itt elsősorban a szervezett alvilág és a nemzetközi hírszerzéssel foglalkozó csoportok tevékenysége említendő meg: mind eszközeikben, mind céljaikban gyakorlatilag egyformák, az ipari kémkedéstől a katonai felderítésig széles a skála.

A kívülről jövő behatoló tevékenységének következtében az illetéktelen használat okoz könnyen számszerűsíthető kárt. Nyilvántartási adatokat, számlákat módosíthatnak és törölhetnek, vállalati titkok kerülhetnek nyilvánosságra, s ha a sikeres betörés ténye nyilvánosságra kerül, ez a vállalati jó hírnév elvesztését is jelentheti, ami pl. egy bank esetében katasztrofális hatású lehet.

A leggyakoribb módszerek: az operációs rendszerek és a programhibák kihasználása, a konfigurálási hibák és hiányosságok okozta „lyukak" felderítése, a protokollhibák kiaknázása, valamint a belső biztonsági rendszer hiányosságainak kihasználása.

A bonyolultabb eset: ha a támadás belülről jön

A kívülről jövő behatolás mellett egyáltalán nem elhanyagolhatók azok az esetek, amikor a támadás belülről, a cég munkatársától jön. Az *American Bar Association* felmérése szerint a számítógéppel elkövetett bűncselekmények 78%-ában az elkövető a kárvallott intézmény alkalmazottja volt.

Az *USA Kereskedelmi Minisztériuma* által elvégzett felmérés már 1983-ban a következő eredményt hozta: „Az alkalmazottak 40%-a feltétlenül becsületes, 30%-a bizonyos körülmények között (zsarolás, megvesztegetés) képes bűntett elkövetésére, 30%-a pedig rendszeresen keresi annak lehetőségét, hogy illegális előnyökhöz jusson", vagyis az alkalmazottak közel egyharmada lop a vállalatától.

A *Népszabadság* tette közzé az alábbi hírt: „Pécsett egy 28 éves férfi modemen keresztül betört volt munkahelyére, és az ottani számítógépből próbált adatokat szerezni, feltehetőleg jelenlegi munkahelye, egy rivális cég számára. Egyelőre nem tudható, milyen adatokat szerzett, és mire használta azokat, ám így is felelősségre vonható számítógépes csalásért, amiért akár 2–8 év börtön is kaphat."

Olyan eset is előfordult már, hogy a munkaadót vonták felelősségre az alkalmazott által a vállalati hálózaton keresztül elkövetett illegális cselekményért, mert pl. a konkurenciára vonatkozó adatokat igyekezett az Internet-kapcsolat segítségével megszerezni.

Lehetőségek a védekezésre

A legkézenfekvőbb, ha nem is mindig célszerű megoldás, hogy a cég elzárja belső hálózatát, adatbázisát a külső kapcsolattól, így az Internettől is. Ebben az esetben az Internet-kapcsolat külön hálózat kiépítését igényli. Ez a megoldás sem jelent azonban védelmet a belülről jövő támadással szemben.

Ha a belső hálózat kerül összeköttetésbe az Internettel, 100%-os biztonsági megoldás nem létezik, annak ellenére, hogy már kifejlesztettek olyan eszközöket és módszereket, amelyek a belső hálózat védhetőségét növelik meg. Két alapelv figyelembevétele különösen indokolt:

- ki kell zárni a jogosulatlan (külső és belső) hozzáférés lehetőségét minden ismert támadható ponton,
- folyamatos elektronikus megfigyelés és elemzés alatt kell tartani a hálózati forgalom alakulását, hogy a gyanús tevékenységet azonnal ki lehessen szűrni.

A legtöbb cég akkor követ el tipikus hibát, amikor előbb köti össze belső hálózatát az Internettel, és csak később, egy esetleges behatolás után („post mortem") határozza el a biztonsági rendszer kiépítését.

A biztonságos informatikai rendszer építőkövei (biztonsági rendszerfejlesztési szempontok)

Kockázatelemzés: értékek, veszélyek, és a bekövetkezési esély felmérése; baj esetén mekkora a veszteség, mennyit érdemes az ésszerű védekezésre költeni.

A biztonsági politika kialakítása: ki használhatja a rendszert, mit jelent a rendeltetésszerű használat, ki rendelkezik a használati joggal; a rendszeradminisztrátorok jogai és kötelességei, a felhasználók jogai és kötelességei; hogyan kezeljük a titkos információkat.

A biztonsági eljárások kidolgozása és gyakorlati megvalósítása: az illetékesség megbízható azonosítása (strong authentication); titkosítási eljárások alkalmazása, „tűzfal" (firewall) használata; mentési és helyreállítási tervek kidolgozása, a felhasználói tevékenység figyelése, felkészülés a rendkívüli esetekre.

Vállalati CERT: ún. „Computer Emergency Response Team" (számítástechnikai vészhelyzet csoport) létrehozása, amely olyan szakértőkből áll, akik a biztonsági rendszert kialakítják, fejlesztik,

üzemeltetik, a rendkívüli helyzetek megelőzéséért és elhárításáért felelősek.

Rendszeres felülvizsgálat: a biztonság rendszeres ellenőrzést kíván, amely folyamatos alkalmazkodást is jelent a változó biztonsági követelményekhez (dinamikus biztonság).

A tűzfal, a titkosítás és az azonosítás

A biztonsági rendszer kialakítása a felügyelet és az üzemeltetés mellett megfelelő *műszaki hátteret is* igényel. A *tűzfal* olyan munkaállomás, amely hardver- és szoftverelemek alkalmazásával a jelenleg elérhető legteljesebb körű védelmet ígéri. Jellemzői:

- egyetlen csatlakozási pont az Internet világhálózatához, minden adatforgalom csak ezen a ponton keresztül bonyolódhat;
- kívülről, a külső felhasználó részéről csak ez a gép látható, a belső hálózat struktúrája rejtett marad;
- a betörésgyanús tevékenység észlelhetővé válik;
- a szolgáltatások központilag konfigurálhatók és letilthatók.

Általánosságban tehát megállapítható, hogy a tűzfal alkalmazása jelentősen csökkenti a kívülről jövő illetéktelen behatolás esélyét. A legtökéletesebb tűzfal sem lehet azonban elég biztonságos titkosítás és szigorú azonosítási eljárások nélkül.

A *titkosítás*nak azért van nagy szerepe, mert az Internet kétirányú adatforgalmat tesz lehetővé: míg a kívülről jövő adatforgalom és tevékenység jól monitorozható, addig a belső hálózatról kifelé küldött adatokat nincs ami megvédje. A küldött adatcsomagok, e-mail üzenetek csak speciális módszerekkel foghatók el, illetve speciális módszerekkel reprodukálható a tartalmuk. (Nem véletlen, hogy minden Internet-könyv felhívja a felhasználó figyelmét, hogy ne küldjön hitelkártyaszámokat a hálózaton keresztül.) A kimenő információkat tehát mindenképpen titkosítani kell. Sokféle kezdeményezés létezik ennek megvalósítására, azonban még nincs általánosan elfogadott megoldás (ipari szabvány). A szoftvercégek és kormányzatok is párhuzamosan dolgoznak rajta.

A *szigorú azonosítási eljárás*nak egyre fontosabb szerepe van, mert az egyszerű user/password védelem manapság gyakran kevésnek bizonyul. Számítógépes jelszófeltörő programokkal egyheti futtatással a jelszavak 25%-a volt feltörhető (Egyesült Államok). Megoldások léteznek az eszközös azonosításra, valamint a lokális és a központi azonosításra is.

A legfontosabb biztonsági kérdések

- *Védelem a külső behatolás ellen (tűzfal, hálózati forgalom monitorozása),*
- *védelem a belső behatolás ellen (jogosultságok definiálása, hálózati forgalom monitorozása, szigorú azonosítás),*
- *biztonságos informatikai rendszer kiépítése (először részletes rendszerfejlesztési elemzés készítése, a fizikai megvalósítás csak a kockázati tényezők ismeretében kivitelezhető),*
- *alapos felkészülés a behatolási tevékenység által okozott helyzet megelőzésére és elhárítására (CERT),*
- *a kimenő információk titkosítása (algoritmusok, kulcsok alkalmazása).*

Beérkezett: 1996. VI. 11-én.