Nem fér kétség hozzá, hogy napjaink legfontosabb értékei az adatok, melyeket óvni, védeni kell. Az információ megállíthatatlan, mégis meg kell találnunk azokat a lehetőségeket, melyek a személyes, vagy céges adatainkat bitonságosan kezelhetővé teszik.
Számtalan veszély fenyeget minket, az interneten keresztül érkező támadások száma évről évre növekszik, a vírusok terjedése, az adatlopások elszaporodása néha már megállíthatatlan folyamatnak tűnik, mégis mindössze csak azt kell felismernünk, hogy ezek a veszélyek minket is fenyegetnek, be kell látnunk, hogy akár egy ártalmatlannak tűnő levél megnyitása is visszafordíthatatlan pusztítást végezhet.
A megoldás most is a mi kezünkben van: odafigyelés és védekezés, természetesen a megfelelő eszközökkel. Ezért gondoltunk arra, hogy a hazai IT biztonság elismert cégével az ITBN díjas SafeSoft Kft.-vel (lásd cikkünk: Detektor Plusz 2012/1. 7. oldal) együttműködve a következő számainkban bővebb terjedelemben foglalkozunk a témával. (A szerk.)

Információ és adatvédelem
általános kérdések

SZEMÉLYES ÉS ÜZLETI ADATOK VÉDELMÉNEK JELENTŐSÉGE

Az információ minden korban érték volt, napjainkban azonban különösen megnőtt a jelentősége annak, hogy megbízható, friss információkkal rendelkezzünk üzleti partnereinkről, vagy azokról az emberekről akikkel valamilyen kapcsolatba kerülünk. Sajnos a megszerzett információkkal való visszaélés egyre elterjedtebb napjainkban. Rendkívül sok érdek fűződik személyes adataink és bizalmas üzleti információink megszerzéséhez

- Az üzleti adatok megszerzése (ipari kémkedés) versenyelőnyhöz juttatja a konkurenciát, szélsőséges esetben akár egy cég tönkremenetelét is jelenthetik a kiszivárgott üzleti információk.
- Személyes adataink megszerzésével feltérképezhetik fogyasztási szokásainkat, célzott reklámokat küldhetnek. Megtudhatják mikor merre járunk, mikor nem vagyunk otthon, információt szereznek egészségi állapotunkról, szokásainkról, kapcsolatainkról.

Az internetkorszak előtt ez a fajta veszély nem volt ilyen jelentős probléma, hiszen az információ megszerzése jóval körülményesebb volt. Adatainkat a hálózatba nem bekötött számítógépen, levelekben, iratokban őriztük, így kisebb esély volt ezek eltulajdonítására, hiszen ehhez fizikai hozzáférésre, esetleg betörésre volt szükség. A nem digitálisan tárolt információk sokszorosítása, másolása is sokkal nehezebb volt. Ezzel szemben, jelenleg számos módon kapcsolódunk az internethez: asztali gépekkel, laptopokkal, mobiltelefonokkal, táblagépekkel, hálózatba kötött szerverekkel, adatbázisokkal, amelyek folyamatos veszélyt jelenthetnek adatainkra. Külön figyelmet érdemelnek azon mobil eszközeink, melyeket magunknál tartunk, hiszen itt az elvesztés, ellopás veszélye is fennáll. Jó tudni, hogy a személyes adataink és bizalmas üzleti információink szinte mindegyike megtalálható valamilyen hálózatba kötött eszközön.

Az ügyeink egyre nagyobb százalékát intézzük hálózaton keresztül, gondoljunk csak a szolgáltatóknál történő on-line ügyintézésre, az elektronikus fizetésre, vagy akár a közösségi oldalakon elérhető és megosztott információkra, vagy az üzleti elektronikus levelezésre.

Az információáramlás rohanó világában, minden mindennel össze van kötve, ami egyfelől kényelmes, másfelől viszont rendkívüli módon megkönnyíti az információszerzést, adataink illetéktelen kezekbe kerülését.

Cégünk a SafeSoft Kft. azzal a céllal alakult 2004-ben, hogy megbízható biztonsági szoftver és hardvermegoldásokat kínáljon a piac számára. Üzleti politikánk kizárja a végfelhasználók felé történő értékesítésből származó esetleges félreértéseket, mivel ügyfeleink viszonteladók és rendszerintegrátorok közül kerülnek ki.
Termékpalettánkkal igyekszünk a minőség mellett a lehető legnagyobb mértékben lefedni az IT biztonság területét, biztosítva egy teljes körű szoftveres és hardveres megoldást a titkosítástól a digitális aláíráson át a tűzfalakig.
Termékeinkkel a terület legnagyobb és legmegbízhatóbb gyártóit képviseljük – esetenként kizárólagosan – Magyarország, Horvátország és Románia területén. Hosszú évek óta jó kapcsolatot ápolunk az, Athena, Avira, Barracuda Networks, CenterTools, HID, Lieberman Software, Omnikey, Precise Biometrics, Ruckus Wireless, SafeNet, Safetica, WatchGuard cégekkel; termékeinkhez jól képzett munkatársaink magas színvonalú terméktámogatást is nyújtanak.

Bán István, SafeSoft ügyvezető igazgató

A LEGFONTOSABB FENYEGETÉSEK ÉS AZ ELLENÜK VALÓ VÉDEKEZÉS

■ *Felhasználói azonosítók, jelszavak védelme*

Sajnos legtöbbször nincs szükség semmilyen különleges hacker módszerre, a felhasználók gondatlansága, oda nem figyelése önmagában is megteszi a magáét. Jellemző példák a bankkártyára ragasztott PIN kód, kiskutyánk neve mint jelszó, bankkártya számának közzététele a Facebook-on.

Védekezésül válasszunk valamilyen bonyolult jelszót, lehetőleg ne a születési dátumunkat, vagy a kedvenc háziállatunk nevét adjuk meg. Fontos, hogy ne használjuk mindenütt ugyanazt a jelszót.

Vállalati hálózat elérése esetén ajánlatos kétfaktoros anonosítást alkalmazni, ahol a jelszó mellett még valamilyen egyéb azonosító is szükséges, például smart kártya, One Time Password token, sms stb...

■ *Vírusok*

Talán a leginkább ismert fenyegetés, amely elsősorban a Windows valamely verzióját futtató számítógépeket érinti. Régebben a vírusok inkább romboltak, ma már egyre gyakoribbak azok a kártevők, amelyek csendben, meglapulva személyes adataink ellopására, vagy gépünk zombivá tételére szakosodtak. A megbízható vírusvédelmi szoftver, manapság elengedhetetlen minden számítógépen.

■ *Hálózatvédelem*

Általában a személyi számítógépeket beépített szoftveres tűzfal védi, de a teljes biztonság érdekében otthon is érdemes beruházni egy megfelelő célhardverbe. A szerverek, vállalati hálózatok védelmére UTM (Universal Threat Management) eszközöket javasolt bevezetni, melyek átfogó védelmet nyújtanak.

■ *Wifi*

Otthoni hálózatban is fontos a maximális biztonságra törekedni (megfelelő kódolás, a Wifi azonosító elrejtése, mac address kontroll stb...). Vállalati hálózatban központilag menedzselhető eszközök telepítése, központi authentikáció, illegális (rogue) access pointok kiszűrése is elengedhetetlen.

■ *Adathordozók védelme*

Lehet szó akár laptopokról, merevlemezekről, pendrive-okról, a jelszavas védelem nem elegendő. Amennyiben a merevlemez nincs titkosítva, a rajta levő információ rendkívül könnyen kinyerhető. Fokozottan igaz ez a magunknál tartott pendrive-okra és memóriakártyákra. Mindez megelőzhető, ha megfelelő titkosítást alkalmazunk.

■ *E-mailek védelme*

Kommunikációnk (üzleti és magán) jelentős részét e-mailben bonyolítjuk. Talán kevesen gondolják végig, hogy amikor meggondolatlanul közzéteszik e-mail címüket web lapokon, levelezési listákon, akkor a részükre érkező kéretlen reklámlevelek (SPAM) számát is exponenciálisan növelik. Vállalati hálózatokban elengedhetetlen egy központi spam szűrő telepítése, hiszen a levélszemét rengeteg időt és energiát emészt fel.

Amikor legszemélyesebb gondolatainkat, adatainkat osztjuk meg barátainkkal e-mailben, érdemes belegondolni abba, hogy a titkosítatlan e-mail biztonság szempontjából egyenértékű a postai nyílt levelezőlappal.

Vállalati környezetben a bizalmas üzleti információk kiszivárogtatásának leggyakoribb eszköze az e-mail, ezért a spamszűrő mellett mindenképpen javasolt valamilyen adatszivárgás elleni (Data Loss Prevention) megoldás bevezetése is.

Nagy Gábor