Adatbiztonság

A WiFi-technológia elterjedésével a felhasználók közül egyre többen végzik munkájukat az irodán kívül, kávézókban, autóban, mobileszközöket használva. A technika azonban veszélyeket, az adathalászok számára pedig lehetőségeket rejt magában. De nemcsak a hálózati kapcsolat, a mobil eszközök hordozhatósága is veszélyes lehet az adatok biztonsága szempontjából. Egy kutatás szerint, Londonban hat hónap alatt mintegy 60 000 mobiltelefont és 4500 laptopot felejtettek a taxikban, egy cég pedig véletlenül egy olyan használt laptopot árverezett el az interneten, amely összes ügyfelük adatát tartalmazta. Miközben a vállalatok többsége egyre nagyobb figyelmet fordít az adatok és az informatikai rendszerek szoftverekkel való védelmére, a felmérések azt mutatják, hogy a mobileszközöket használó alkalmazottak nagyobb kockázatot jelentenek a vállalatok számára, mint a hackerek, az adathalászat, illetve a vírustámadások.

A WIFI-TECHNOLÓGIA VESZÉLYEIT KEVÉS FELHASZNÁLÓ ISMERI

Egy a Symantec által szervezett sajtóeseményen *Horváth Tamás,* a HuWiCo („Kábel Nélkül'" internetes Egyesület) tagja a WiFi előnyeiről és veszélyeiről tartott előadást. A technológia előnyei között kiemelte, hogy nagy sebességű kapcsolatot biztosít, így kényelmessé teszi az otthoni, illetve a mobil munkavégzést, valamint megoldást nyújthat azon cégek számára, amelyeknél az ügyfelek rendszeresen igényelnek internet-hozzáférést látogatásuk alkalmával.

A veszélyek között említette, hogy a felhasználók adataihoz WiFi-kapcsolaton keresztül könnyebben hozzáférnek az illetéktelen felhasználók, így a vezeték nélküli technológia alkalmazásakor kiemelten kell figyelni a megfelelő adatbiztonság biztosítására. Horváth Tamás arra is kitért, hogy miközben világszerte rohamosan terjednek a hotspotok, vagyis a WiFi-kapcsolatot biztosító pontok, Magyarországon ez a fejlődés lassabb, nem követi a nemzetközi trendeket. A kávézóüzemeltetők közül például sokan azért nem vezetik be a számukra egyébként nem nagy költséggel járó rendszert, mert attól félnek, az internetezők kevés fogyasztás mellett csak az asztalt foglalják..., hogy bár az újonnan vásárolt laptopok csaknem mindegyike képes már WiFi-kapcsolatra, ezt a felhasználók nagy része vagy nem tudja, hogy mit jelent, vagy ha igen, nincs tisztában a használatból eredő biztonsági kockázatokkal. A hordozható számítógépek legtöbbjén futó Windows operációs rendszer ugyanis elindulás után automatikusan vezeték nélküli hálózatok után kutat, méghozzá úgy, hogy az előzőleg használt WLAN hálózatok SSID-jét világgá kürtöli, ami így a támadó birtokába juthat, megkönnyítve ezzel a támadást a felhasználó számítógépe ellen. Az előadó arra is felhívta a figyelmet, hogy a nyilvános hotspotot használók a védtelen hálózat miatt jobban ki vannak téve a rossz szándékú embereknek, emiatt fokozott elővigyázatosság kell a nyilvános internetet használók részéről. Egy WiFi-kávézóban üldögélve például bármelyik másik felhasználó meg tudja állapítani, mi a kártya hardveres címe, amellyel a netre csatlakozunk, milyen gyártmányú a gépünk, illetve milyen ope-

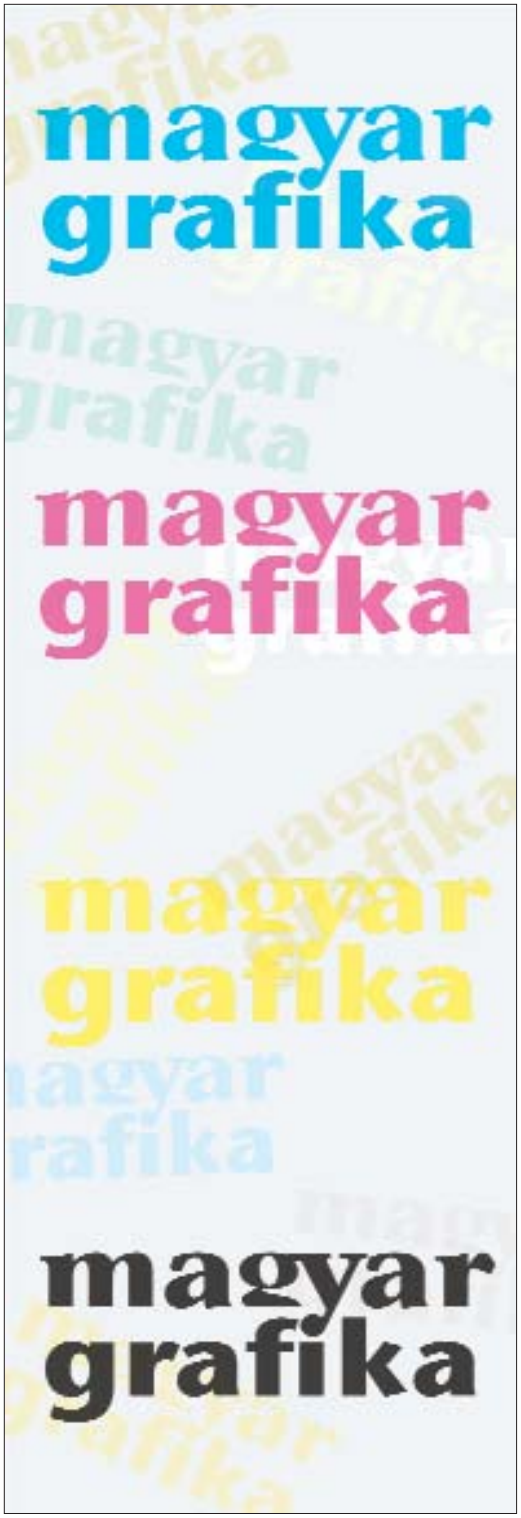
rációs rendszert használunk. Ez még nem számít bűncselekménynek, azonban ha valaki azt is megvizsgálja, milyen nyitott portok találhatók a gépünkön, illetve megpróbál hozzáférni az adatainkhoz, az már illegálisnak tekinthető. Mivel a WiFi-kártya mindig a legerősebb jelhez kapcsolódik, tudtán kívül az is bűncselekményt követhet el, akinek számítógépe az otthoni internetezés közben a szomszéd erősebb jelet kibocsátó WiFi-kapcsolatához csatlakozik. Megfelelő védelemmel azonban a WiFi-kapcsolat is biztonságosan működik.

A MOBILESZKÖZÖK NAGYOBB KÁRT JELENTHETNEK, MINT A VÍRUSOK

A Symantec megbízásából, a mobileszközök használatáról készült kutatás eredményeit *Bartha Hedvig,* a Symantec PR menedzsere ismertette.

Az Economist Intelligence Unit által lefolytatott felmérésből az derül ki, hogy a biztonsággal kapcsolatos kételyek jelentik messze a legnagyobb akadályt a mobil számítástechnika előnyeinek céges környezetben történő kihasználásával szemben. A kutatás komoly hiányosságokat mutatott ki a cégek mobileszközökre vonatkozó jelenlegi védelmi rendelkezéseiben. Bár a cégek jelentős részét érte már anyagi veszteség a mobileszközökkel kapcsolatos védelem hibái miatt, csak kis részük tanulmányozta a kézi számítógépekkel, okostelefonokkal és más mobileszközökkel kapcsolatos veszélyeket. A kutatás szerint, a cégek közel egyharmadánál nincs a mobilbiztonsággal kapcsolatos külön óvintézkedés.

A megkérdezett cégek kevesebb mint fele használ a mobileszközök védelmére külön védelmi szoftvert, és sok cégnél hiányzik a mobilbizton-



ságot szolgáló, tervszerű stratégia. A cégek nem kevesebb mint 78 százaléka vagy esetileg foglalkozik az új típusú eszközök védelmi követelményeivel, vagy megpróbálja az eszközöket a meglevő hálózatvédelmi szabályozásba besorolni. Teszik ezt annak ellenére, hogy a legtöbb vezető érzi, hogy a mobilhálózatok számos veszélyforrással szemben (például a vírustámadásokkal, a hackerek általi veszélyeztetéssel vagy a kényes információk felfedésével, illetve kiszivárgásával) sebezhetőbbek, mint a helyhez kötöttek.

Az informatikai védelemnél hajlamosak vagyunk arra, hogy a tizenéves „kódtörő" rémképe lebegjen a szemünk előtt. A mobilvilágban azonban az alkalmazotti gondatlanság legalább annyira káros lehet, mint a vírusok és a neten garázdálkodó bűnözők. Számos alkalmazott használ olyan eszközt, amelyen minimum a cég kényes adatait tartalmazó e-mailek találhatók. Ezek az eszközök sűrűn elkallódnak. A felmérés szerint valószínűbb, hogy az elveszett vagy ellopott eszközök okoznak anyagi veszteséget, mint a céget kívülről érő támadások.

A felmérés azt mutatja, hogy a legtöbb vállalatvezető csak nagy vonalakban van tisztában a mobileszközök használatának biztonsági problémáival. Az ázsiai-csendes-óceáni térség felsőbb vezetői – állításuk szerint – a legtájékozottabbak a mobil számítástechnikához kapcsolódó veszélyekről: 37 százalékuk „teljesen tisztában van a veszélyekkel". Európa a második 30 százalékkal, míg Észak-Amerikában csak 25 százalék vélekedik így. Bár a többség nagyjából tisztában van a mobil munkavégzés lehetséges kockázatával és az előnyökkel, a felmérésből úgy tűnik, hogy általában csak a hordozható számítógépekre gondolnak. Ebből az következik, hogy a megkérdezett cégek többségénél még nem is foglalkoztak a többi mobileszköz biztonsági jelentőségével. A vállalatvezetésnek a mobilveszélyekről kialakult torz képe aláássa az alkalmazottak magatartásának megváltoztatására és a mobileszközökön tárolt adatok hathatósabb védelmét szolgáló, szigorúbb védelmi szabályok létrehozására irányuló kísérletek hatásosságát.

A cégek nyilván nem tilthatják meg az alkalmazottaknak a mobileszközök használatát, de azt biztonságossá kell tenniük. Egyes cégeknél meglehetősen merev szabályozást vezettek be, amit a központi informatikai részleg felügyel. Máshol úgy vélik, hogy több felelősséget kell áthárítani a végfelhasználóra, persze az informatikai részleg eszközeinek és támogatásának segítségével. Bármelyik utat választják a cégek, gondoskodniuk kell arról, hogy a védelmi intézkedések összeegyeztethetőek legyenek a mobilalkalmazottak munkamódszereivel. Ha nem így tesznek, elveszíthetik azokat az előnyöket, amelyek a mobiltechnikába történő beruházás fő mozdítórugói voltak.

MI KELL AHHOZ, HOGY AZ ADATOK MOBILOK ÉS VÉDETTEK LEGYENEK?

- A felsőbb vezetésnek prioritásként kell kezelnie a mobilbiztonságot. A vállalatvezetőknek jólértesültnek kell lenniük a megjelenő veszélyforrásokról, és a védelmi eljárások betartásával jó példával kell elöljárniuk.
- A cégeknek ki kell használniuk a hálózat megfigyelésére szolgáló eszközöket, hogy tudják, ki vagy mi fér hozzá a hálózathoz. Gondoskodniuk kell arról, hogy valamennyi eszközön rendszeresen frissítsék a szoftvereket, és meg kell győződniük arról, hogy a szerverek a hálózatra kapcsolódni kívánó felhasználóknak mind a jogosultságát, mind a vírusvédelmét ellenőrizni tudják.
- A felhasználókat ki kell oktatni mind a technikai, mind a fizikai jellegű gyakorlati óvintézkedésekre, mielőtt rájuk ruházzák a felelősséget. A felhasználóknak – ha ügyfelek adatait viszik magukkal – tudniuk kell például a titoktartási törvények vonatkozásairól.
- Azt is biztosítani kell, hogy a felhasználók tudják, mi a teendő, ha ellopják tőlük az eszközt (például értesíteniük kell az informatikai részleget, hogy távolról törölhessék a kényes adatokat).
- Az úton levő hordozható számítógépek eredményesen megvédhetők saját (letölthető) tűzfallal és VPN-en keresztül felépített kapcsolattal.
- Tanulmányozni kell a felhasználók magatartását, és a tapasztalatok alapján olyan szabályokat

kell alkotni, amelyek a maximális biztonság mellett a legnagyobb rugalmasságot és termelékenységet eredményezik.

- Bár a biztonságot többnyire gondatlanságból sértik meg az alkalmazottak, az értékes adatok szándékos ellopása vagy kiszivárogtatása sem ritka. Az átfogó mobilbiztonsági szabályzatnak az iPoddal, USB-tárolóval vagy fényképezőgépes mobiltelefonnal történő információlopással is foglalkoznia kell.

A Volvo Trucks-nál például nem csupán a járművek hatékony közlekedése áll az élen vezetőinek gondolataiban. A világ egyik legnagyobb, 130 országban működő nehéztehergépkocsi-gyártója állandóan úton levő dolgozóinak hozzá kell férniük a cég adataihoz. Mint sok észak-európai cég, a Volvo Trucks is korán belekezdett a mobiladat-kezelésbe, de az aránylag kiforrott használat nem vezetett laza magatartáshoz. A cég valójában imponálóan szigorúan ellenőrzi a felhasználókat. „Nagyon szigorúak vagyunk a tekintetben, hogy miként kapcsolódnak a felhasználók a cég hálózatához" – mondta Björn Sand, a Volvo Trucks informatikai igazgatója. Szavai szerint, a cég „intenzíven" használja a mobiladatokat.

Symantec
A Symantec világelső a magánszemélyek és vállalatok információinak védelmében, hozzáférhetőségének és épségének biztosításában. A kaliforniai Cupertinóban lévő vállalat működése a világ több mint 40 országára terjed ki. További információ a www.symantec.hu címen található.