Előházi János

MOBIL ESZKÖZÖK BIZTONSÁGI PROBLÉMÁI

Absztrakt

A mobil eszközök megjelenésük óta eltelt bő tíz évben hatalmas fejlődésen estek át. Ennek köszönhetően egyre több feladatot kapnak mind a magán-, de főleg az üzleti szférában. Elsősorban olyan feladatokat látnak el, melyek a kommunikáció és az elérhetőség köré csoportosulnak: vállalati erőforrásokhoz való hozzáférés, email kommunikáció, mobil-telekommunikáció, dokumentumok szerkesztése. Nagy tudásuk, kis méretük és a vezeték nélküli technológia használata miatt azonban számos veszélynek vannak kitéve, ugyanakkor a szerteágazó megoldások miatt (számos operációs rendszer, eszközönként egyedi frissítési lehetőségek stb.) nehézkes az ilyen eszközök egységes kezelése. A másik probléma, hogy a felhasználók a vállalati eszközöket magán célra is felhasználják, ezáltal a magán- és üzleti adatok keverednek.

A cikkben igyekszem összefoglalni a mobil eszközök felhasználási területeit, az adattípusokat, melyeket jellemzően tárolnak, biztonsági problémáikat, és megoldási lehetőségeket ezek csökkentésére.

In the last ten years since mobile devices appeared they went through an enormous development. As a result mobile devices play more and more important roles in our private and business life. Their tasks are strongly related to communication and availability: accessing business resources, email communication, mobile telecommunication, editing documents etc. Their ability, small size and wireless solutions however expose them to various risks, and at the same time because of their various structure (several operation system, individual upgrade methods etc.) makes it difficult to cerate a standard to manage these devices. Another huge problem is that users use their business related devices fro personal purposes as well, as a result personal and business data are stored on the same device.

In this article I will try to summarize the areas where mobile devices are used, the data types they manage, their security risks, and solutions to decrease the possibility of a successful attack against them and minimize data loss.

Kulcsszavak: *mobil eszközök, informatikai biztonság, vezeték nélküli adatátvitel, informatikai menedzsment*

Bevezetés

A mobil eszközök hatalmas fejlődésen estek át az elmúlt tíz évben, tudásuk szignifikánsan nőtt, áruk és méretük számottevően csökkent, a hatékony használatukhoz szükséges infrastruktúra pedig szinte mindenhol elérhető. Ennek köszönhetően mind az üzleti mind a magán szférában egyre fontosabb szerephez jutnak.

A mobil eszközöket négy csoportba kategorizálhatjuk méretük és tudásuk alapján.

- Okostelefonok;
- PDa-k;
- Tablet PC-k;
- Noteszgépek.

Az első csoport az okos telefonok, melyek az alapvető GSM szolgáltatások mellett emeltszintű szolgáltatásokat is elérhetővé tesznek, mint pl. az email kezelés. A mai okos telefonok nagy része már 3G és HSDPA hálózatokhoz is képes csatlakozni, de az újabb eszközök támogatják a WiFi elérést is, csökkentve az adatkommunikációval járó költségeket. A második csoport a PDA-k csoportja, melyek többnyire Windows, Linux vagy Palm operációs rendszerek beágyazott verzióira épülnek. A mobiltelefonok és a PDA-k csoportjának van egy közös része, ugyanis számos PDA készülék alkalmas arra, hogy GSM vagy UMTS hálózatra is tudjon csatlakozni. Ezzel a megoldással csökkenthetjük az alkalmazott eszközök számát, és nő azok felhasználási rugalmassága, hiszen az általuk nyújtott szolgáltatások köre így meglehetősen széles, a hálózati elérés pedig kiszélesedik, hiszen a mobiltelefon hálózati lefedettsége jóval nagyobb, mint amit a vezeték nélküli Internet elérést biztosító hálózati csatlakozási pontok segítségével el lehet érni. A GPS megjelenése a mobil eszközökben is egyre gyakoribb. A legtöbb PDA készülék ma már tartalmaz GPS vevő egységet, és újabban az okostelefonokban is megjelenik ez a funkció. A harmadik csoport az úgy nevezett Tablet PC-k csoportja, melyek a PDA-któl méretükben és teljesítményben különböznek. A Tablet PC-k lényegükben a noteszgépekkel egyenértékű eszközök. Azoktól méretükben, tárolási kapacitásban és számítási képességekben különböznek. Léteznek az ebbe a csoportba tartozó eszközökből is olyanok melyek képesek mobiltelefonként is funkcionálni, de mivel méretük meghaladja a tenyérgépek méretét, ezért a bennük elhelyezett mobil-telekommunikációs egység igazán kényelmesen csak adatátvitelre használható. A negyedik csoportba tartoznak a noteszgépek, melyek teljes értékű számítógépként funkcionálnak. A modern notebookok mindegyike rendelkezik beépített WiFi elérési lehetőséggel, de egyes üzleti szféra számára kialakított modellek emellett 3G vagy HSDPA eszközöket is integrálnak. Ezek hiányában bővítőkártyák alkalmazásával ez a képesség is kialakítható. Az eszközök mérete és teljesítménye is ebben a megadott sorrendben nő, így egyre nehezebb mobil környezetben alkalmazni őket (pusztán a méretük miatt), viszont egyre több szolgáltatást képesek nyújtani. Mivel a nagyobb gépek az asztali gépekkel megegyező operációs rendszert futtatnak, azok menedzsmentje (mind operációs rendszer, mind felhasználó szinten) egyszerűsödik, hiszen az asztali gépek számára kialakított, már meglévő vállalati megoldások változtatás nélkül alkalmazhatóak rájuk.

Mobil eszközök jellemzői

Általánosságban elmondható, hogy egy mai modern mobil eszköz mérete jóval kisebb, tudásuk jóval nagyobb, minta pár évvel ezelőtt megjelent társaiké. A technológiai fejlődés a mobil szegmensben rohamos, így akár fél év elteltével olyan meghökkentő újítások jelennek meg, melyek nagyban kibővítik az ilyen eszközök felhasználhatóságát. A legtöbb modellben szerepel email és internet elérési szolgáltatás. A modernebb eszközök képesek UMTS hálózathoz kapcsolódni (esetleg rendelkeznek HSDPA eléréssel is), ezen felül rendelkezhetnek WiFi elérési lehetőséggel is. A Bluetooth alapú rádiós átvitel ma már szinte alapkövetelmény egy ilyen készüléktől.

Főleg a multimédiás elvárások miatt az eszközök tárolókapacitása jelentős mértékben megnőtt. A tíz évvel ezelőtti PDA-kra jellemző 16-32 Mbyte szabad terület helyett ma már a készülékek tárolókapacitása memóriakártyák segítségével több gigabájtig növelhető, és ezen a téren mind a tárolókapacitás, mind a sebesség és megbízhatóság nagy léptékben fejlődik. A

noteszgépek tárolókapacitása is sokat fejlődött a közelmúltban. A mágneses tárolóegységek teljesítményfelvétele csökkentésének köszönhetően, illetve a memória kártyákban felhasznált technológiát alkalmazó, merevlemezes háttértárat kiváltó egységeknek hála, illetve a mobil eszközökre optimalizált processzorok elterjedésének köszönhetően, a legtöbb noteszgép egy asztali számítógép tároló- és számítási kapacitásával rendelkezik.

A mobil eszközök hátrányos jellemzői közé tartozik a korlátozott számítási kapacitás, jellemzően pár száz megahertz és egy-két gigahertz között szerepel ezen eszközök órajele. Ez a számítási kapacitás-különbség a notebookokra egyre inkább nem jellemző. A teljesítmény növelése ugyanakkor a felvett energiaszükségletet is megnövelte, viszont az akkumulátorok mérete és súlya nem növelhető egy bizonyos mérték fölé, így manapság azt tapasztalhatjuk, hogy a pár éve még jellemzően egy feltöltéssel akár egy hetet is működő mobiltelefonok helyett akár minden nap töltenünk kell készülékünket. A notebookokban alkalmazott mobil processzoroknak köszönhetően viszont, azok rendelkezésre állási ideje lényegesen megnőtt. A pár éve jellemző egy-két óráig tartó működési idő, ma már a megfelelő működési mód kiválasztásával négy-öt órára is növelhető. A korlátozott energia mellett a másik hátránya a mobil megoldásoknak a sokféle operációs rendszer. A Tablet PC-ken és a notebookokon az asztali gépekkel megegyező operációs rendszerek futtathatók, de az ennél kisebb eszközök saját operációs rendszerrel és azokon belül is számos verzióval kerülnek a felhasználókhoz. Ez a sokszínűség megbonyolítja az ilyen eszközök központosított menedzsmentjét, ami egy vállalat szempontjából nagyon fontos, hiszen biztosítja a megfelelő szoftverfrissítések telepítését (pl.: operációs rendszerben felfedezett biztonsági rések javítását, illetve a vírusírtó és tűzfal alkalmazások frissítését). A biztonsági réseket tovább tágítja, hogy a legtöbb mobil eszközre nem is telepíthető vírusvédelem vagy tűzfal, pedig a vezeték nélküli kommunikáció miatt erre itt fokozottan szükség lenne.

A mobil eszközökön tárolt adatok típusát megvizsgálva kijelenthető, hogy szintén főleg a kommunikációs folyamatok köré csoportosíthatóak. Így főként kapcsolati információkat, illetve a kommunikációs folyamat eredményeként létrejövő dokumentumokat (pl.: SMS, MMS vagy e-mail) tárolunk el. A legtöbb vállalati információs rendszerek nagy része szintén böngészőn keresztül érhető el, így a használatuk során tárolt adatok is megjelennek az eszközökön. A legtöbb mai böngésző, a felhasználói kényelmet szem előtt tartva felkínálja, hogy a használat során begépelt felhasználói neveket és jelszavakat elmentik, hogy a legközelebbi használat során a felhasználónak ne legyen szüksége ezeket újból megadni. Léteznek olyan alkalmazások (pl.: Mozilla Firefox), ami lehetővé teszi az így eltárolt szenzitív információ titkosítását és védelmét egy úgynevezett mester-jelszó alkalmazásával. Ebben az esetben, ha a böngésző elindításakor nem adjuk meg a mester-jelszót, a böngésző nem képes dekódolni a tárolt felhasználói neveket és jelszavakat, így nem is ajánlja fel azok automatikus behelyettesítését a weblapokba. De a böngészők használata során számos más típusú adat is mentésre kerül, pl.: a különböző weboldalak által használt cookie objektumok, melyek segítségével képesek azonosítani a felhasználót, ha legközelebb az oldalra látogatnak. A legtöbb korszerű böngésző felajánlja azt a lehetőséget, hogy minden személyes adatot töröl a háttértárról, miután a felhasználó befejezte a program használatát.

Mobil eszközök fenyegetettségei

A mobil eszközök fenyegetettsége két ok köré csoportosítható. Egyik szempontból a készülékek mobil volta és kis méretük miatt könnyen elveszíthetőek vagy szándékosan eltulajdoníthatóak. A fenyegetettségek másik forrása a vezeték nélküli kommunikáció. A rádiós átvitel sajátossága, hogy nem egy zárt közegben halad, és emiatt nem csak a címzett képes fogadni az üzeneteket, hanem a hatósugárban bárki által vehető az eszköz sugárzása. Emiatt kifejezetten fontos, hogy megfelelő körültekintéssel használjuk a különböző vezeték

nélküli átviteli lehetőségeket. E két veszélyforrásból származó károk csökkenthetőek lennének, ha hasonlóan az asztali rendszerekhez, központosított rendszerkarbantartás és felhasználó-jogosultság menedzsment lenne megvalósítható. Sajnos a PDA és okostelefon készülékeken futó sokféle operációs rendszer ezt nem teszi lehetővé, így a vírustámadásokból, kommunikációs támadásokból és a szoftverhibákból származó problémáknak a készülékek legtöbb esetben, teljes mértékben ki vannak téve, annál is inkább, mert a beágyazott operációs rendszerek nagy részére sem megfelelő védettséget nyújtó tűzfal, sem vírusvédelem nem létezik (bár vannak ez irányú törekvések).

A mai mobil eszközök alapvető szolgáltatása a Bluetooth vezeték nélküli átvitel. A Bluetooth lehetővé teszi, hogy a készüléket vezetékek segítsége nélkül kihangosítóval, fülhallgatóval kössük össze, vagy más kommunikációs eszköz számára a készülék maga, mint modem működjön, de felhasználható két eszköz közötti tetszőleges típusú adat átvitelére is. A Bluetooth szabvány bizonyítottan ellenáll a támadásoknak, ám azonban a szabvány implementálása során programozói hibák vagy „spórolások” (mint például számláló alkalmazása véletlenszám generátor helyett) számos támadásnak tették ki a technológiát. Ezek közül a legfontosabbak a Bluesnarfing, Bluebugging, Bluejacking és DoS (Denial of Service) támadások. A Bluesnarfing támadás főként 2003-2004 között volt jellemző. Az újabb verziók már kivédték ezt a támadási módszert. A támadás csak akkor működött, ha a készülék Bluetooth rádió adója felfedezhető módban működött. A támadó hozzáfért az eszközön tárolt információkhoz. A Bluebugging arra adott lehetőséget a támadónak, hogy Bluetooth utasításokat hajtson végre a felhasználó tudta nélkül a készüléken. Így a készülék által implementált bármely Bluetooth parancsot (pl.: fájl küldés) végrehajthatott úgy, hogy a felhasználó nem vette észre, hogy készülékét támadás érte. A legfőbb veszélye, hogy tetszőleges hívásparancsok is kiadhatóak a készüléknek anélkül, hogy a felhasználó észrevenné, így a készüléken átfolyó hívások lehallgathatóak. A Bluejacking az előbbi támadási módszerekhez képest ártalmatlan. Kihasználva, hogy az un. névjegyküldés során a Bluetooth eszközök nem teszik kötelezővé a párosítást, névjegy helyett tetszőleges szöveges üzenetet lehetett küldeni más Bluetooth eszközökre. A DoS támadás a készülék energiaellátása ellen irányult; mivel a Bluetooth adás-vétel jóval több energiát emészt fel, mintha a készülék csak készenlétben állna, folyamatos párosítás kéréssel, melyek sikertelenül záródtak, egy idő után a támadott készülék energiaellátása elfogy, és szolgáltatásai nem vehetőek igénybe, amíg újból fel nem töltik. [4]

Szinte minden modern PDA, notebook vagy egyes mobiltelefonok képesek rá, hogy WiFi hálózatokhoz csatlakozzanak. A WiFi ma már igen elterjedt vezeték nélküli adatátviteli módszer, és kezdeti gyengeségeire hamar kifejlesztettek javításokat. A WiFi alkalmazásával járó legnagyobb veszély, hogy a felhasználó egy megszokott felületet (Internet) ér el rádiós kommunikáció segítségével, és megfeledkezik róla, hogy a vezetékes összeköttetés nyújtotta biztonság, rádiós hálózatokon nem létezik: ott az adást minden résztvevő veheti. A WiFi eszközök kezdetektől kínálnak titkosítási eljárásokat, mellyel a rádiós kommunikáció védhető. A kezdetben kidolgozott WEP (Wired Equivalent Privacy) titkosítási eljárás sem a 64, sem pedig 128 bites titkosítási kulccsal nem nyújtott elegendő védelmet, a mai számítógépek számítási kapacitása mellett a kulcs úgynevezett brute force (nyers erő) alkalmazásával is perceken belül feltörhető, és a további kommunikáció megfejthető. Ez a támadási forma azt jelenti, hogy az összes lehetséges kombinációt kipróbálva is rövid időn belül megfejthető a kommunikáció titkosításához alkalmazott kulcs. [1] A később kidolgozott WPA vagy WPA2 (Wi-Fi Protected Access) a vevő és az adó közötti megosztott információra (jelszó) épül, és a titkosítási kulcsokat dinamikusan változtatja. Az így kidolgozott védelem már megfelelő szintű érzékeny adatok átvitelére is rádiós hálózaton. [2][3] A vezeték nélküli hálózatok gyenge pontja még az úgynevezett Access Point, vagyis az a router, ami elérhetővé teszi a

hálózatot a rádiós eszközök számára is. Ezek a routerek gyakran böngésző alkalmazásával állíthatóak be, hogy ez a folyamat minél egyszerűbben elvégezhető legyen, és ne legyen szükséges speciális célszoftvert telepíteni a művelet elvégzéséhez. Az alapértelmezett adminisztrációs jelszó és felhasználói név megváltoztatása nélkül, a támadónak elég a gyártók által definiált alapértelmezett beállításokat ismernie, és kedvére konfigurálhatja a hálózatunkat, elérve azt is, hogy minden kérés saját eszközein keresztül zajlódjon le, így azokat akár módosítva a klasszikus man-in-the-middle támadást is könnyen megvalósíthatja. Kevésbé súlyos esetben csak a hálózat erőforrásait használhatja jogosulatlanul. A man-in-the-middle támadás lényege, hogy a közé a két fél közé, mely között a kommunikáció eredetileg lefolyt volna, egy harmadik fél ékelődik, és a kommunikáló felek számára a partnert személyesíti meg. Kevésbé súlyos esetben, csak a kommunikáció megfigyelésére képes, viszont súlyosabb esetben a kommunikáció tartalmát is módosíthatja anélkül, hogy a felek ezt észrevennék.

A mobil eszközök támadhatóak fizikai eltulajdonítás útján is. Így a bennük tárolt adatok megfelelő előzetes védelem nélkül, a támadó számára teljesen hozzáférhetőek. A támadó felhasználhatja az így szerzett eszközt arra is, hogy magát az eredeti tulajdonosnak kiadva a hálózaton jogosulatlanul férjen hozzá a hálózat erőforrásaihoz. Amennyiben az eszközön tárolt adatokról nem készítettek biztonsági másolatot, úgy azok elvesztése is problémát okoz. A megfelelő védelem az ilyen támadások ellen: a három alapvető hozzáférés-szabályozás közül (biometriai, tudás alapú, birtok alapú) legalább kettőt alkalmazni kell. Ezzel meggátolható, hogy egy támadó használni tudja a készüléket. Viszont nem akadályozható meg, hogy a háttértárolón elhelyezkedő adatokhoz szabadon hozzáférjen, ezért szükség van a tárolt adatok erős hardveres titkosítására. A hardveres titkosítás előnye, hogy alkalmazás-független. A titkosítási folyamat a tárolóeszközön belül zajlik le. Ezek az eszközök sok esetben el vannak látva olyan védelemmel is, ami érzékeli, hogyha fizikailag akarják megkerülni a hardveres védelmet, és ha van rá mód, az adatokat tönkre teszik. A szoftveres megoldások sok esetben elegendő védelmet biztosítanak, ha a titkosítási algoritmus elég erős, és az alkalmazott kulcs megfelelő az adott felhasználáshoz. Ezek alkalmazása mellett a támadó számára lehetetlen vagy nehéz az eszközökön tárolt adatokhoz való hozzáférés. A fizikai eltulajdonításból vagy elvesztésből eredő legnagyobb kár azonban az elveszett adatok pótlása. Mivel a modern eszközök tárolókapacitása igen nagy, a felhasználó nincsen rákényszerítve arra, hogy csak a legszükségesebb adatokat tárolja a mobil eszközön, és a pillanatnyilag nem szükséges információkat máshol tárolja. Emiatt hajlandó elfelejtkezni a rendszeres biztonsági mentések fontosságáról, és sokkal nagyobb mennyiségű adat veszik el egy ilyen esetben, mint ami egyszerűen pótolható lenne.

Mobil eszközök védelme

Mivel a legtöbb mobil eszközön a felhasználó menedzsment nem vagy csak nehézkesen oldható meg, ezért nagyon fontos a felhasználók oktatása, abból a célból, hogy megismerjék, milyen veszélynek vannak kitéve, ha mobil eszközt használnak illetve, hogy betartsák a cég által megkövetelt felhasználói előírásokat (mivel azok szoftveresen nem tartathatóak be). Ilyen például a rendszeres adatmentés, vagy nem engedélyezett programok telepítésének mellőzése, de a megfelelő biztonságú protokollok kizárólagos alkalmazása is idetartozik. Nagyon fontos a felhasználók felelősségének tisztázása, és egy olyan szabályrendszer megalkotása és betarttatása, mely nem nehezíti meg a munkavégzést számottevően, de megelőzi a legelterjedtebb fenyegetések bekövetkeztét. Fontos a felhasználók motiválása, hogy elfogadják, hogy a kényelmes munkavégzést érintő többlet adminisztráció és odafigyelés az ő érdekük.

Nagyon fontos az eszközökhöz való megfelelő szintű hozzáférés szabályozása valamilyen felhasználó-azonosítási módszerrel (birtok-, tudás alapú, biometriai). Ezáltal illetéktelen fél nem veheti igénybe az eszköz szolgáltatásait. A hozzáférés-szabályozáson túl létfontosságú az adatok titkosítása. Ma már számos szoftveres és hardveres megoldás létezik, ami a mobil eszközök tároló-elemein elhelyezkedő adatokat megfelelő szintű titkosítással látja el, lehetetlenné téve az eszközt megszerző számára, hogy a tárolt információhoz hozzáférjen. Fontos, hogy az eszköz eltulajdonításakor vagy elvesztésekor keletkezett információveszteség minimalizálása érdekében az eszközön tárolt adatokról megfelelő gyakorisággal biztonsági mentés készüljön. Manapság egyre több okostelefonra és PDA-ra készítenek a gyártók vírusvédő programokat. Ilyen terméket kínál például a Symantec cég, mely évtizedek óta jelen van a vírusvédelmi piacon, ami nem csak beágyazott Windows operációs rendszeren, de számos okostelefonra jellemző Symbian rendszeren is elérhető. [5] [6] Főleg beágyazott Windows alapú eszközökre léteznek már tűzfal programok is, vagy komplett VPN (Virtual Private Network) megoldást nyújtó rendszerek is. Ilyen programcsomagot kínál a Bluefire Technologies cég. [7] [8]

Egyelőre az ilyen eszközök vírusfenyegetettsége nem számottevő, de a megelőzés ebben az esetben is fontos, ezért ezek telepítése és rendszeres frissítése elengedhetetlen a biztonságos működés szempontjából. Figyelembe véve a mobil eszközök terjedési ütemét feltételezhető, hogy akár hónapokon belül elterjednek azok a vírusok, melyek célzottan ezeket az eszközöket támadják meg. Sokszor az eszköz operációs rendszerének hibáit kihasználva képesek a támadók sikeres támadást végrehajtani. Ma már az összes gyártó elérhetővé teszi Internetes honlapján az általa gyártott eszközök szoftverfrissítéseit, így a szervizt mellőzve, a felhasználó maga végezheti el a frissítést, időt spórolva meg. Egyre elterjedtebb az úgynevezett over-the-air frissítési megoldás is, amelynek során a mobil eszköz maga tölti le az operációs rendszer frissítéseit az Internetről, és a telepítéshez nincsen szükség asztali számítógépre. Az ilyen készülékek többnyire külön menüpontot szentelnek ennek a funkciónak, így a felhasználó egyszerűen tudja alkalmazni. A hátránya ennek a megoldásnak, hogy jelenleg a mobil hálózatokon elérhető adatátvitel ára nagyságrendekkel nagyobb a hagyományos Internet (WiFi, ADSL vagy egyéb megoldás) költségeinél. A mobil eszközök operációs rendszereinek frissítése sok esetben azt vonja maga után, hogy a készülék saját memóriája teljesen törlődik, és azok az adatok, amelyek nem külső tároló egységen (pl.: memória kártya, vagy számítógépre lementett biztonsági mentések) helyezkednek el, a frissítés után többé nem elérhetőek. Az ezzel járó bonyolultságot sokan inkább nem vállalják fel, holott az operációs rendszer naprakészen tartása a legalapvetőbb megoldás a biztonságos működés megteremtéséhez.

Összefoglalás

Elmondható hogy ezen eszközök használata során a legtöbb dolog a felhasználóra van bízva, ezért ebben az esetben a felhasználó a kiemelten gyenge láncszem. Elengedhetetlen a megfelelő oktatás és felhasználói fegyelem kialakítása, hogy a jövőbeli károk minél alacsonyabb szinten tarthatóak legyenek. A heterogén eszközrendszer karbantartása központilag nagyon nehézkes, illetve nem valósítható meg az asztali gépeknél jól bevált felhasználó menedzsment sem. A sokféle eszköz mindegyike egyedi karbantartási megoldást igényel. A legtöbb esetben a legegyszerűbb megoldás, ha az eszköz frissítése és folyamatos mentése is a felhasználóra van bízva.

Az eszközök karbantartása és frissítése mellett nagyon fontos a kommunikációs csatornák körültekintő alkalmazása. Fontos a Bluetooth kapcsolatok minimalizálása és a WiFi elérés megfelelő szintű titkosítása. Fontos, hogy a felhasználó tisztában legyen vele, hogy ha nem megfelelő titkosítású WiFi hálózathoz kapcsolódik, milyen információt ne közöljön a

hálózaton, hogy a fontos adatok védettek maradjanak. Emiatt elengedhetetlen, hogy a felhasználó ne csak használni tudja ezeket a technológiákat, de tisztában legyen vele (bizonyos mértékig), miként működnek, milyen veszélyei vannak, és milyen kompromisszumok árán érdemes őket használni.

Összességében megállapítható, hogy a mobil eszközök tudásuk megnövekedése miatt a mindennapi munkát kényelmesebbé teszik, és megrövidítik a válaszra való várakozás idejét, felgyorsítva ezzel a munkavégzést. Egyre alacsonyabb áruk pedig jelentősen elősegíti elterjedésüket. A mobil eszközök kiemelten fontos szerepet játszanak abban, hogy a sürgős információ minél hamarabb eljusson (akár munkaidőn kívül is) a címzetthez. Tudatos alkalmazásuk során több hasznot termelnek, mint amennyi kárt okozhatnak.

Felhasznált irodalom

[1] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

[2] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[3] http://en.wikipedia.org/wiki/IEEE_802.11i

[4] http://www.gcn.com/print/24_20/36437-1.html

[5] http://www.symantec.com/about/news/release/article.jsp?prid=20060130_01

[6] http://www.coolest-gadgets.com/20070523/anti-virus-protection-for-windows-mobile-norton-mobile-security/

[7] http://www.bluefiresecurity.com/products/mss/

[8] http://www.bluefiresecurity.com/products/vpn/