

Kényes adatok biztonsága az okostelefonokon

Ha a 2010-re vagy különösen a 2011-re szóló IT jóslatokat visszamenőleg megnézzük, jól látható, hogy a mobilitás, a mobil eszközök szignifikáns előretörését jósolják, és ezzel együtt az okostelefonok, netbookok, tabletek biztonsága is terítékre kerül. Itt egyaránt található kockázatok az egyszerű felhasználók szempontjából, de a vállalati felhasználásnak is feladja a leckét mindez.

Mielőtt belevágunk a közepébe, egy link erejéig megemlíthetjük a múltat is, amikor még alig voltak mobilos kártevők, támadások, és ha meg is jelent nagy ritkán egy-egy Bluetoothon keresztül terjedő Symbian platformos vírus, ezek széleskörű elterjedést vagy jelentős károkozást nem tudtak felmutatni. Akit ez a hőskor behatóbban is érdekel, elolvashatja a *Vírusok Varázslatos Világa* cikksorozat 10. részét.
<http://antivirus.blog.hu/media/image/pdf/vvva.pdf>

Ha a fogalmakat akarjuk tisztázni, akkor az is érdekes kérdés, hogy mitől okos egy okostelefon. Erre többféle válasz is lehetséges, az egyik legfrappánsabb az, hogy segítségével az interneten levelezhetünk, közösségi oldalakat érhetünk el, illetve weboldalakat böngészhetünk.

És mit kell tudni mindehhez egy okostelefon tulajdonosnak? Nyilvánvalóan a megbízható programok, szolgáltatók, letöltések tudatos és körültekintő kiválasztásával gyengíthetjük némileg kitértségünket, ám minden ellen nincs orvosság, csak a tőlünk elvárható legnagyobb gondossággal járhatunk el. Már az eszköz kiválasztásánál is figyelembe kell(ene) venni, mire akarjuk majd használni. Ha fontos céges adatok hatékony védelme, távoli vállalati levelezés és szerverelérés, elvesztés esetén távoli törlés, vagy blokkolás a cél, akkor ennek megfelelő okostelefont kell, például titkosított partíción üzemelő, például BlackBerry-ben kell gondolkodni. A mostani céges telefon helyzet kicsit hasonlít ahhoz, mikor kicsit viccesen a nyolcvanas években a Commodore64 volt a vállalati adatfeldolgozó computer. Vannak persze törekvések arra, hogy az újabb okostelefonok már nyújtsanak üzleti telefonokra jellemző flotta és adatvédelmi funkciókat is, de a magánembereknek, vagy átlagfelhasználóknak más a szempontja, mint egy nagyvállalatnak.

Adatok, jelszavak, értékeink

Ezekután nézzük meg, mi lehet kényes adat egy okostelefonon. A címjegyzékünk, hívásaink listája, küldött és fogadott SMS-eink, illetve az adattárolási lehetőségek miatt bármi, amit oda feltöltünk, begépelünk. Ez lehet első körben például egy szöveges állomány, amiben a jelszavainkat és PIN kódjainkat tároljuk. Ám a sornak még nincs vége, hiszen aki internetezik is az okostelefonnal (hiszen részint ezért van), az a levelezését és a netezés közbeni jelszavait, accountjait, személyes adatait is erre bízta. A készülék, az adatok kétféle veszélyben lehetnek, mi elvesztjük őket és/vagy azok pluszban még illetéktelen kezekbe is kerülnek. Ebből külön külön mindkettő kellemetlen lehet, de a kettő együttesen különösen nemkívánatos.

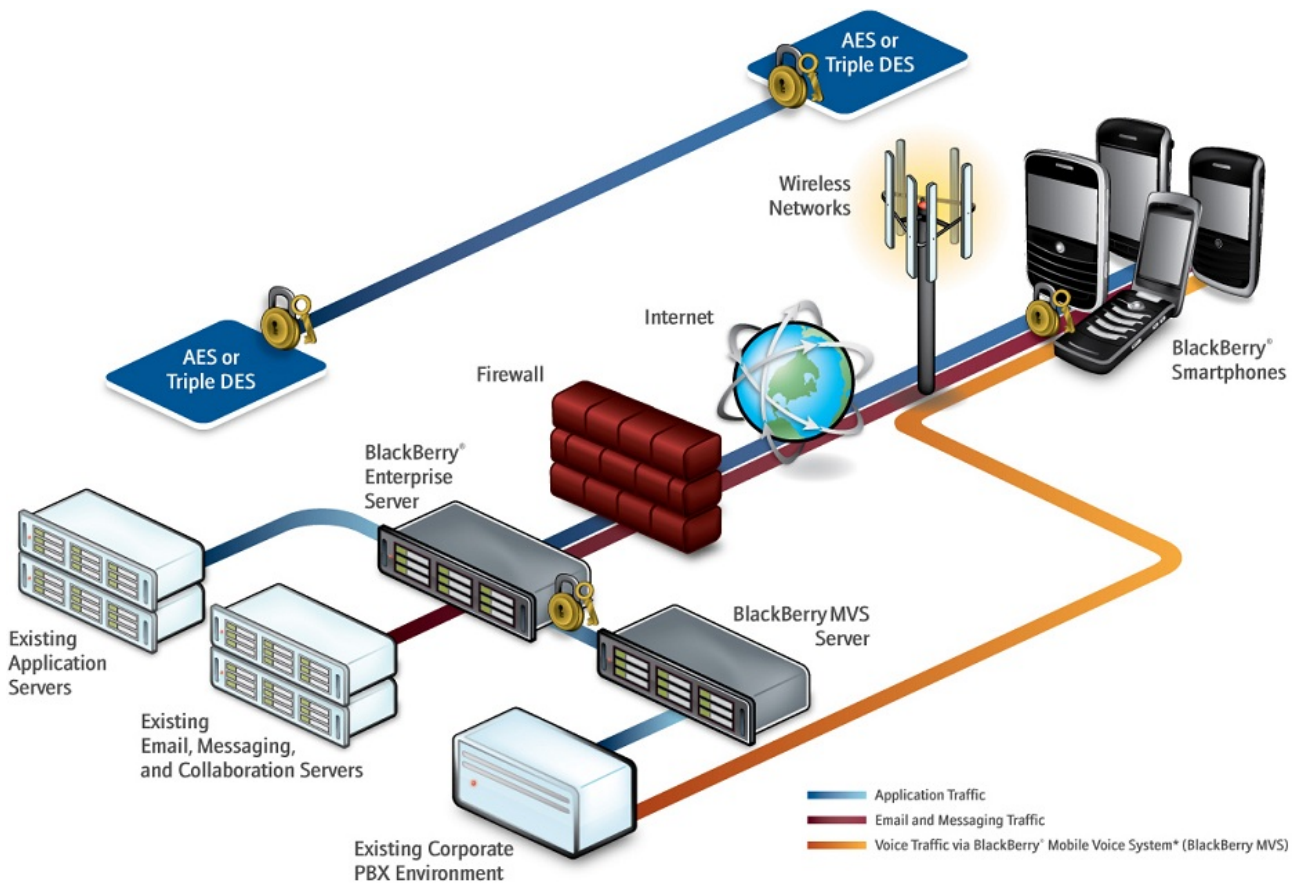
Védeők hadrafogása

Ezek után nézzük, milyen lehetőségeink lesznek, ha rendelkezünk egy okostelefonos internetbiztonsági csomaggal. Általában ezekben olyan menüpontokkal találkozhatunk, mint vírus, spamszűrő, lopásgátló funkciók, jelszavas védelem, biztonsági audit. A Security Audit menüpont segít feltérképezni az "adatvagyonunkat", ezek a tárolt adatok, számok, telepített applikációk és a kritikus beállítások állapota: szabad memória mérete, bekapcsolt Bluetooth, GPS és GSM beállítások, csatlakoztatott memóriakártya, USB eszköz, és hasonlók. Lefuttatása után egy riportban összefoglalja azokat a gyenge pontokat, ahol változtatás szükséges. De mindenféle incidens nélkül is hasznos lehet ez, például a nem használt Bluetooth kikapcsolása hasznos nem csak a biztonságunk miatt, hanem az akkumulátor idővel való takarékos gazdálkodáshoz is.

Ezek elvégzése után már olyan funkciókat tudhatunk a tarsolyunkban, mint a minden fájl, mappa, alkalmazás és memóriakártya folyamatos vírusellenőrzése, fekete és fehérlistázni lehet a bejövő hívásokat, és persze blokkolni a tiltott vagy ismeretlen számokat. Netezés közben is hatékonyan megvédhet a kártevőktől, kártékony linkektől. Ha esetleg ellopnák a telefonunkat, SIM kártya csere esetén lezár a készülék, és a korábban megadott értesítési számokra titokban riasztást küld SMS-ben, de ugyancsak hasznos az úgynevezett Remote Wipe, azaz távoli törlési lehetőség is, ezzel lehet ugyanis letakarítani minden adatunkat az ellopott, ismeretlen helyen levő telefonunkról. Ha minderről gondoskodtunk, akkor elmondhatjuk, tettünk valamit az okostelefonunk biztonsága érdekében.

Következő cikkünkben pedig majd arról lesz szó, mik a veszélyek, pontosan milyen információkat tudhatnak meg rólunk az okostelefonunkon keresztül.

Csizmazia István, IT biztonsági szakértő
Sicontact Kft., a NOD32 vírus magyarországi képviselője
antivirus.blog.hu



Ha megbízható, titkosított kapcsolaton keresztül nagyvállalati felhasználásról van szó, akkor a Blackberry lehet az egyik jó választás, Obama elnök is ilyet használ.



A vírusvédelem is lényeges, azonban egy okostelefon esetében a lopásgátló, és távoli törlési, értesítési lehetőségek kiemelten fontosak



Nem kell szakértőnek lenni ahhoz, hogy hatékony védelmünk legyen: a Security Audit segít feltérképezni okostelefonunk gyenge pontjait.