blancco

MINŐSÍTETT ADATTÖRLÉS

Adattörlési stratégiák az üzleti életben

Mobil eszközök a vállalkozásban

2013. február

Bevezetés

A modern mobileszközök mára nélkülözhetetlen eszközzé váltak a munkahelyeken is: egy nemrég az USA-ban és Európában készült felmérés szerint a vállalatok 77%-a biztosít okostelefonokat az alkalmazottainak[1].

A mobillal ellátott alkalmazottak korábban a végrehajtók, értékesítők és marketingesek közül kerültek ki leginkább, de a „hozd a saját készüléked" forradalma újrarajzolta az üzleti élet képét, több lehetőséget adva még több és különböző területen dolgozó embernek. 2013 végére a munkahelyeken használt okostelefonok fele a munkavállalók birtokában lesz az IDC előrejelzése szerint[2]. A Gartner szerint 2016-ra a munkaerő kétharmada birtokolni fog egy okostelefont[3].

E mobileszközök nagy része tartalmazhat érzékeny vállalati, ügyfél- vagy alkalmazotti adatokat, azonban a cégek jelentős hányada nem ügyel az adatbiztonságra. A fenyegetettséget ugyanis nem csupán a kártevők, az adathalászat és kémprogramok jelentik, a használt eszközök helytelen kezelése sokkal nagyobb biztonsági kockázattal jár.

Olyan szigorú szabályokat kell tehát a vállalatoknak bevezetniük, amelyek biztosítják, hogy a mobileszközökön tárolt érzékeny adatok ne kerüljenek illetéktelen kezekbe a selejtezés, megsemmisítés vagy újrafeldolgozás során. A biztonságos adattörlés során igazolni lehet az adatok tényleges eltávolítását. A közelmúltban készült felmérések szerint azonban a szervezetek 71%-a nem rendelkezik szabályozással arra nézve, hogy a BYOD (Bring your own device) eszközökön tárolt adatokat hogyan kell kezelni[4].

Tartalomjegyzék

Miért fontos a mobileszközök biztonságos törlése?

KIS ESZKÖZÖK, NAGY KOCKÁZAT

A mobileszközök kis méretük ellenére az információk valóságos tárházai. Néhány okostelefon és tablet akár 60 gigabájtnyi adatot is képes tárolni, köztük egyre inkább céges e-maileket, ügyféladatokat, jelszavakat és más érzékeny információt is, amelyek könnyen illetéktelen kezekbe kerülhetnek, ha megfelelő törlés nélkül szabadulnak meg a készülékektől.

Az emberek 99%-a használja mobilját üzleti célokra. 77%-uk használta a telefonokat az üzletfelek nevének és címének tárolására, 23%-uk tárolta az ügyfelek adatait és 17%-uk töltött le céges információkat, dokumentumok és spredsheeteket – mutatta ki már 2009-ben egy tanulmány[5]. Egy másik tanulmány pedig már 2008-ban kimutatta, hogy a használt okostelefonok sokszor tartalmaznak érzékeny adatokat[6], a mostani tanulmányok pedig ezt már 60% és 99% közé becsülik (7,8).

Riasztó adat, hogy egy brit felmérésben a válaszadók 81%-a azt állította, hogy eladás előtt minden adatot törölt a mobiljáról, és tízből hatan meg voltak győződve róla, hogy az információk így tényleg el is tűntek a telefonjukról.[9] A legtöbben elmondták, hogy manuálisan törölték adataikat, így persze a „törölt" adatok visszaállíthatóak maradtak.

SZABÁLYOZÁSI AGGODALMAK

Miközben az Egyesült Államokban már az orvosok 80%-a használ[10] speciális, okostelefonon futó alkalmazásokat a mindennapi munkájának elősegítésére és a betegadatok kezelésére, az adatvesztéssel egy szervezet nem csupán a jó hírnevét teszi kockára, de sokszor súlyos büntetéssel is szembe kell néznie.

Európában 2013 júniusában várható az adatvédelemre vonatkozó szabályok felülvizsgálatának befejezése, illetve az új szabályok kibocsátása. Ezek már követelményeket fogalmaznak meg az online adatok törlésére és átlátható folyamatok használatára a személyes adatokkal dolgozó cégek számára, továbbá bátorítást is tartalmaznak jóváhagyott eszközök és folyamatok alkalmazására.
Az új szabályozás szankciókat is kilátásba helyez, kisebb vétségek esetén 250 000 eurótól az éves globális forgalom 0,5%-áig, súlyosabb vétség esetén 1 millió eurótól a forgalom 2%-áig terjedő büntetésekkel lehet számolni.

Az Európai Hálózat és Információ Biztonsági Ügynökség (ENISA) szintén felismerte, hogy a legnagyobb kockázatot az információ biztonságára nézve a megfelelő adattörlés nélkül eltávolított okostelefonok jelentik, ezek az eszközök mégsem alanyai azoknak a törlési eljárásoknak, amelyek meg vannak szabva merevlemezek esetében[11].
Ez különösen annak az elemzői előrejelzésnek a fényében zavaró, amely szerint 100 millió mobiltelefon kerül újrahasznosításra évente[12].

A kockázatok csökkentése

A vállalatoknak szükségük van egy biztonságos eljárásra a mobileszközök külső és belső memóriájában tárolt adatok eltávolításához, mielőtt újrafelhasználják, újrahasznosítják vagy megsemmisítik őket. Az eszközök fizikai megsemmisítése nem elégséges, hiszen a töredezett digitális médiából is kinyerhetők az adatok, nem beszélve arról, hogy ez eljárás a környezetre is veszélyes lehet.

Sok felhasználó azt gondolja, hogy ha az okostelefonokat visszaállítják a gyári beállításokra, az megsemmisíti az adatokat a belső memóriában is, de a legtöbb esetben az adat ott tovább létezik. Bár egy kezdő nehéznek találhatja az adatok visszaállítását, egy képzett hacker vagy számítógépes szakértő könnyen megoldhatja ezt.

A szoftveres adateltávolítás azonban teljesen felülírja az eszköz memóriáját. Néhány gyártói alkalmazás használja ugyan ezt a technikát, de ezek az alkalmazások nem generálnak ellenőrizhető riportot, mely tartalmazza az eszköz sorozatszámát és más hardveres részleteket, amelyek igazolják, hogy az adat eltűnt, pedig mindez szükséges az eszköz kockázatmentes újraértékesítéséhez vagy újrafelhasználásához. Mindezek mellett ezek az alkalmazások csak bizonyos eszközök operációs rendszereivel működnek együtt, és csak manuálisan végrehajthatóak.

FEJLETT ADATTÖRLÉS

A nemzetközileg elismert tesztelő ügynökségek (pl. TÜV SÜD) által jóváhagyott, fejlett adattörlés speciális felülíró szoftverrel valósul meg számos biztonsági, technikai és hatékonysági előnnyel. Nem csupán eltávolítja az összes adatot a mobileszközről, de részletes jelentést is szolgáltat bizonyítékként.

A hamisításbiztos és ellenőrizhető jelentés alapvető része a szabályos teljesítésnek és a törvény által előírt vizsgálatoknak. Enélkül egy üzleti vállalkozás nem lenne képes adatai biztonságát megőrizni. Az adattörlési megoldásoknak átfogó törlési jelentéseket kell generálniuk, hogy az átvizsgálási folyamatokat, az auditorokat elláthassák a kritikus információkkal, mint a hardver állapota, a fontos szériaszámok és eszközcímkék, a szoftverrészletek a licencek megállapításához, valamint az, hogy milyen törlési módszert alkalmaztak és ki hajtotta végre a törlést.

A RUGALMAS, AUTOMATIZÁLT FOLYAMATOK NÖVELIK A PRODUKTIVITÁST

A fejlett adattörlő szoftver lehetővé teszi az operátorok számára, hogy automatizálják és végrehajtsák ugyanazokat a törlési folyamatokat számos mobileszköz esetében egy normál munkaállomásról. A törlő szoftver szintén automatikusan küldi a törlési jelentéseket a központi konzolnak.

A hatékonysága mellett a fejtett adattörlő szoftver detektálhatja és egyidejűleg törölheti az adatokat különböző típusú mobileszközökről és tablet platformokról, mert közvetlenül kommunikál az operációs rendszerükkel. Ezek az eszközök széles skálán mozoghatnak: iOS, Nokia Symbian, Android, Windows Mobile és BlackBerry.

A szervezetek rengeteg, az adatbiztonságot veszélyeztető fenyegetéssel néznek szembe, ezért az érzékeny és tulajdonosi üzleti információk védelme érdekében szigorú szabályozást javasolt bevezetni a mobileszközökre vonatkozóan[13]. Az is fontos, hogy ez a szabályozás összetett forgatókönyveket, eljárásokat is tartalmazzon[14], emellett pedig lényeges, hogy a kiválasztott adattörlési technológia a mobileszközökre vonatkozó szabályozás részeként kerüljön alkalmazásra.

Ha egy szervezet okostelefont vagy tabletet értékesíteni, adományozni akar, vagy csupán egy másik munkatársnak szeretné kiadni, a fejlett adattörlés során el kell távolítania az információkat az eszközről, mielőtt az elhagyja a cég területét[15]. A törlő szoftvert kezelheti a cég belső IT személyzete is, de a vállalat megbízhat egy a mobileszközök újrahasznosításával foglalkozó céget, amely jóváhagyott adattörlést végezhet a helyszínen, vagy amelyik támogatja a mobileszközök biztonságos szállítását a saját telephelyére a törlés céljából. Az IT személyzet vagy az eszközkezelő párosíthatja a sorszámozott törlési jelentést a raktárkészlettel, hogy audit esetén bizonyíthassák, hogy minden adatot töröltek.

FELÜLÍRÁSI KÖVETELMÉNYEK PLATFORMONKÉNT:

Apple iOS: az iPhone, iPod és iPad eszközök titkosítottak, ezért nem szükséges felülírni az összes felhasználói adatot tartalmazó területet. Azonban a titkosítási kulcsot felül kell írni, hogy a felhasználói adat később visszaállíthatatlanná váljon.

Android: szükséges a felhasználói adatokat tartalmazó területeket felülírni. Egy egyszerű gyári visszaállítás és/vagy újraformázás nem biztonságos, és az adatok meglehetősen könnyen visszaállíthatóak.

BlackBerry: szükséges az IT szabályok, külső alkalmazások eltávolítása és a felhasználói adatokat tartalmazó területeket felülírása.

Nokia Symbian: szükséges a felhasználói adatokat tartalmazó területeket felülírni. A gyári visszaállítás nem elégséges.

Windows Mobile: szükséges a felhasználói adatokat tartalmazó területeket felülírni. A gyári visszaállítás nem elégséges.

SAJÁT TULAJDONÚ ESZKÖZÖK SZABÁLYOZÁSA

Egyre több saját tulajdonú eszközt használnak a munkahelyen a munkavállalók. A Gartner szerint 2014-re a cégek 90%-a támogatni fogja a vállalati alkalmazások használatát privát eszközökön[16]. Ezáltal az alkalmazottak nem csupán produktívabbak lesznek, de csökkenhet a vállalat mobileszköz-támogatásra fordított költsége is. Azonban ezek az előnyök biztonsági kockázattal járnak, különösen, ha nem alkották meg a megfelelő szabályokat.

A szabályozásnak magában kell foglalnia az eszköz szériaszám alapján történő munkahelyi regisztrációját az IT személyzetnél, amely ezután nyomon tudja követni az eszköz állapotát, amikor az vállalati adatokhoz fér hozzá.

A szabályozás részeként szükség van egy lemondó nyilatkozatra az alkalmazottaktól, akik vállalják, hogy mielőtt egy új mobilkészülékre váltanának, leadják jelenlegi készüléküket az adattörlés végrehajtására. A törlés azután történik meg, miután az információkat letöltötték a készülékről és átvitték a következő készülékre.

A mobileszközökkel kapcsolatos szabályozás szerint az alkalmazott felelős minden a céggel kapcsolatos információ kiszivárgásáért a privát mobileszközéről, amíg a törlési jelentés nem jut el az IT személyzetig.

Az alkalmazott éppen ezért köteles minden tőle telhetőt megtenni az eszköz védelmére, így például képernyőjelszót használni, és azonnal jelenteni az eszköz eltűnését.

Összefoglalás

A gyors, erőteljes törlési eljárás növeli a mobileszközök biztonságát. Tekintet nélkül az eszköz tulajdonosára, a mobileszközökkel kapcsolatos vállalati biztonságpolitika részeként nyomon kell követni a felhasználókat és eszközeiket, amelyek hozzáférhetnek a céges adatokhoz. Egyik legfontosabb aspektusa ennek a szabályozásnak az okostelefonok és táblagépek leselejtezése, újrafelhasználása vagy újraértékesítése előtti adattörlési eljárás, amely létfontosságú megelőző intézkedés az adatok elvesztésének, bírságok vagy más negatív hatások elkerülése érdekében.

Mivel a Blancco minősített törlési eljárása automatikusan generál részletes törlési jelentést, többféle mobilplatformot támogat és több eszköz törlését is képes egy időben elvégezni, megfelelő választás azon vállalatoknak, amelyek biztonságban akarják tudni adataikat. A technológiai szabványokhoz és tanúsítványokhoz vagy jóváhagyásokhoz igazodva ez a szoftver garantálja, hogy semmilyen adat nem maradt az eszközökön a törlés után.

Hivatkozások

1 IDC, "IDC Benchmark Study Examines Enterprise Mobile Device Policies," 04 June 2012, http://www.idc.com/getdoc.jsp?containerId=prUS23519412

2 Blackberry, "Employee-owned Smartphones: Seize the Opportunity," White paper

3 TechCrunch.com, "Gartner: 1.2 Billion Smartphones, Tablets To Be Bought Worldwide In 2013; 821 Million This Year: 70% Of Total Device Sales," 6 November 2012, http://techcrunch.com/2012/11/06/gartner-1-2-billion-smartphonestablets-to-be-bought-worldwide-in-2013-821-million-this-year-70-of-total-device-sales/

4 KnowBe4 – ITIC, "KnowBe4 and ITIC Latest Study Reveal Companies Lack Security for 'BYOD'," 04 September 2012, http://www.prweb.com/releases/2012/9/prweb9858074.htm

5 Government Technology, "4.2 Million Cell Phone Users Leave Sensitive Data Unprotected," 19 March 2009, http://www.govtech.com/security/42-Million-Cell-Phone.html

6 Businessweek, "The Recycled Cell-Phone Trap," 3 November 2008, http://www.businessweek.com/technology/content/nov2008/tc2008113_981236.htm

7 PC World, "Your Old Smartphone's Data Can Come Back to Haunt You," 10 July 2011, http://www.pcworld.com/article/235276/your_old_smartphones_data_can_come_back_to_haunt_you.html

8 Dark Reading, "Old Smartphones Leave Tons Of Data For Digital Dumpster Divers," 15 December 2011, http://www.darkreading.com/mobile-security/167901113/security/news/232300628/old-smartphonesleavetons-of-data-for-digital-dumpster-divers.html

9 CPPGroup plc, "Second Hand Mobiles Contain Personal Data," 22 March 2011, http://www.prnewswire.com/news-releases/second-hand-mobiles-contain-personal-data-118434314.html

10 Healthcare Technology Online, "Bracing For Healthcare's Mobile Explosion," 6 January 2012, http://www.healthcaretechnologyonline.com/article.mvc/Bracing-For-Healthcares-Mobile-Explosion-0001?sectionCode=Welcome&templateCode=EnhancedStandard&user=2431702&source=nl:32854\

11 ENISA, http://www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks/top-ten-smartphone-risks?searchterm=Top+Ten+Smartphone+

12 ABI Research, "Recycled Handset Shipments to Exceed 100 Million Units in 2012, 20 December 2007, http://www.abiresearch.com/press/1015-Recycled+Handset+Shipments+to+Exceed+100+Million+Units+in+2012"

13 CIO, "Managing Mobile Devices: 10 Lessons Learned, via Forrester," 22 September 2011, http://www.cio.com/article/690281/Managing_Mobile_Devices_10_Lessons_Learned_via_Forrester

14 Government Security News, "The Urgent Need for Mobile Device Security Policies," 14 November 2011, http://www.gsnmagazine.com/article/24983/urgent_need_mobile_device_security_policies

15 International Association of Information Technology Asset Managers (IAITAM)

16 Gartner, "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond," 2010, http://www.gartner.com/it/page.jsp?id=1480514

blancco

MINŐSÍTETT ADATTÖRLÉS

További információ a Blancco termékeiről: http://torles.hu

A Blancco termékek kizárólagos magyarországi disztribútora a V-Detect Antivírus Kft.

V-DETECT ANTIVÍRUS KFT.

www.v-detect.hu