blancco

MINŐSÍTETT ADATTÖRLÉS

Az adattörlés kezelése a vállalatoknál:

automatizált folyamatok az optimális hatékonyságért

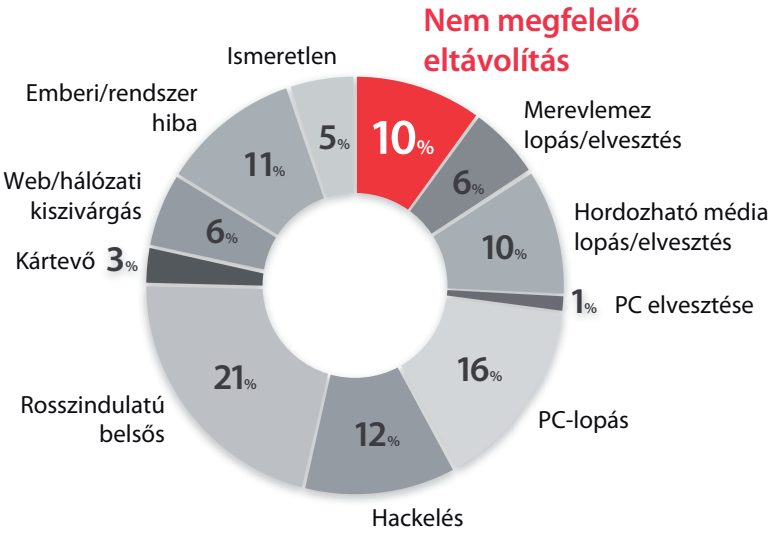
2013. március

Bevezetés

Az IT és számítógépes rendszerek működtetésével megbízott szakemberek egyre újabb kihívásokkal néznek szembe mindennapi munkájuk során: csökkenő humán erőforrás és szűkösebb költségvetés mellett kell megoldaniuk egy-egy vállalatnál vagy állami szervnél a legkritikusabb és egyben a legtöbb bizalmat igénylő működési feladatot.

Az IT tevékenység fontos részét képezi, hogy megbízható és már bizonyított adatvédelmi eljárásokat alkalmazzanak, különösen az adatokkal való visszaélések és a személyi adatok eltulajdonításának növekvő veszélye miatt. Kulcsfontosságú lépés meghatározni és beépíteni a tevékenységbe az IT eszközök adattörlési eljárásait, amelyek ütemezhetőek akkor is, ha a gépek újrafelhasználásra kerülnek, eladományozzák vagy végleg eltávolítják őket. Tehát olyan automatizált megoldás kell, amely felismeri a hardverek széles körét, az okostelefonoktól a high-end szerverekig, és amely intézi a naponta felmerülő, és egy-egy eszköz teljes életciklusát végigkísérő adattörlési feladatokat. Emellett képes követni és jelenteni, hogy mit töröltek és ki hajtotta azt végre.

Tartalomjegyzék



Esetenként:
Az incidensek száma százalékos értékben kifejezve a 2010. január és június közti időszakra vonatkoztatva.

Forrás: KPMG International, 2010. október

A nem megfelelően eltávolított IT eszközök által generált fenyegetések

Az adatok elvesztésének réme gyakorta az ellopott, elvesztett laptopokhoz, hordozható eszközökhöz kapcsolódik, ám a nem megfelelően leselejtezett IT eszközök ugyanolyan biztonsági fenyegetést jelentenek.
A KPMG International 2010-es jelentése[1] szerint az incidensek 10%-át okozzák a nem megfelelően eltávolított IT eszközökön maradt adatok. A saját vagy mások hírnevének rontása mellett az adott cégnek jelentős büntetéssel is szembe kell néznie, amit ez egyre szigorodó adatvédelmi szabályok miatt kell kifizetnie. A Kessler International 2009-es tanulmánya[2] szerint a merevlemezek kb. 40 százaléka, amely a használtcikk-piacra kerül, még mindig tartalmaz szenzitív adatokat.

Az adattörlés szoftver alapú megközelítést kínál az összes szenzitív vagy bizalmas elektronikus információ felülírására és teljes eltüntetésére, amelyek az eltávolításra vagy újrafelhasználásra ítélt merevlemezeken vagy más digitális adathordozón találhatóak.

Ellentétben az alap fájltörlési parancsoktól, melyek csak a lemezszektorokhoz vezető direkt útvonalat távolítják el, és lehetővé teszik az adatok visszaállítását közönséges szoftveres eszközökkel, a minősített adattörlés esetén minden információ eltávolításra kerül, a lemez mégis működőképes marad. Erről, az adateltávolítás bizonyítékaként, törlési jelentés készül, részletes hardverspecifikációval.

AZ ADATVÉDELMI TECHNOLÓGIÁK ELŐNYEI ÉS HÁTRÁNYAI

Sokféle adatvédelmi és megsemmisítési technológia létezik, beleértve az eszközök fizikai megsemmisítését, demagnetizálást, lekódolást, újraformatálást és kevésbé átfogó szoftveres felülírási megközelítéseket is, de mindegyiknek megvan a hátulütője. Például a fizikai megsemmisítés és a demagnetizálás működésképtelenné teszi a meghajtót, meggátolva azt, hogy bármilyen értéket még kinyerhessen abból a vállalat az újraértékesítés vagy újrafelhasználás során, és jelentősen növeli a vállalat ökológiai lábnyomát is. Emellett a merevlemezek megsemmisítéséhez drága felszerelés szükséges, ezért a cégek gyakorta kiszervezik ezt a tevékenységet, ami ismét csak növeli az adatvesztés esélyét, például a szállítás során. Ráadásul sok esetben a fizikai megsemmisítéskor a töredezett digitális médiából még mindig lehetséges az adat-visszaállítás.

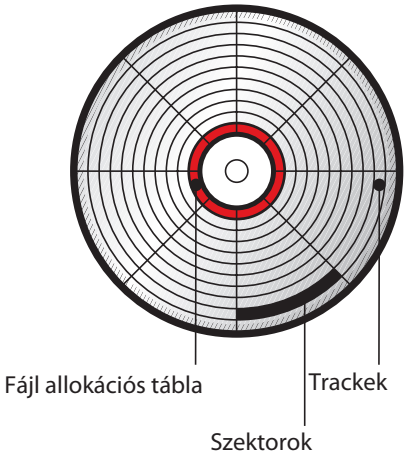
Más adatvédelmi eljárásoknak is vannak hátulütői. A szoftver alapú titkosítás bizonyos esetekben hatékony, ám meglehetősen időigényes, processzort lefoglaló művelet, továbbá nem teljesen biztonságos, ellenőrizhető módszer az adatok megvédésére, különösen inaktív eszközök esetében. Az aktív és inaktív rendszerek, amelyek titkosítást alkalmaznak, támadásoknak vannak kitéve, ha nem frissítik őket állandóan. Adatokat hagynak azoknak, akik képesek megtalálni a kulcsot, feltörni a titkosítást vagy kihasználni a folyamat végrehajtásának gyengeségeit.

A lemezek újraformázása ezalatt érintetlenül hagyja az adatokat, míg a kevésbé fejlett felülírási technológiák nem képesek elegendő felülírási mintát végrehajtani vagy nem kínálnak törlési jelentéseket, így nem tesznek eleget az előírásoknak. Például az ingyenes felülíró szoftverek nem adnak részletes, megvizsgálható jelentést, és így a szoftver hatékonysága nem ellenőrizhető. Ezek a szoftverek nem rendelkeznek a megfelelő tanúsítványokkal sem, melyek igazolják, hogy valóban azt és csak azt a funkciót hajtják végre, melyet állítanak magukról.

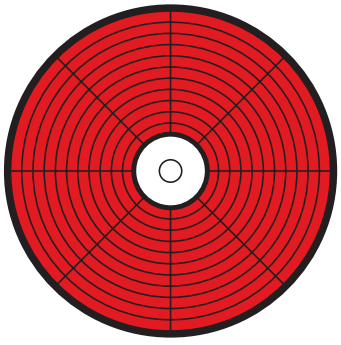
A fejlett, menedzselt adattörlés a védelem alapvető, első oszlopa, amikor érzékeny információkat tartalmazó eszközöktől akarunk megszabadulni. A cél a teljes adateltávolítás automatizálása és egy olyan technológia alkalmazása, amely az adattörlés eredményéről bizonyítékot kínál egy részletes jelentés formájában – a szervezetek csak így lehetnek biztosak afelől, hogy adataik teljesen védetté válnak.

A fejlett, menedzselt adattörlés a védelem alapvető, első oszlopa, amikor érzékeny információkat tartalmazó eszközöktől akarunk megszabadulni.

Törlési és formatálási módszer



Adattörlés



Megtisztított terület

Érintetlen terület

Folyamatos kihívások az adatbiztonsági menedzsmentben

Az IT szervezetek egyre növekvő kihívásokkal néznek szembe nap mint nap. A folyamatosan csökkenő költségvetés és a személyzeti korlátozások közepette egyre többet várnak el tőlük, a hálózatoknak pedig egy egyre képzettebb felhasználói bázis egyre növekvő forgalmának kell megfelelniük.

Egy 2011-es EMC/IDC Digital Universe tanulmány[3] szerint 2005-től 2010-ig a digitális adatok mindenfajta hálózaton áthaladásának mennyisége majdnem megtízszereződött, és nincs jele annak, hogy ez a forgalom csökkenne. 2010 és 2012 között a számok megduplázódtak, és 2015-re ismét kétszereződés várható.

FELTORNYOSULÓ SZABÁLYOK A VÁLLALKOZÁSOKKAL SZEMBEN

Számos szigorú iparspecifikus szabvány és rendelkezés jelent meg a világon, hogy csökkentsék a kockázatát a bizalmas adatok napvilágra kerülésének. Ilyen szabályok felbukkantak az egészségüggyel, pénzüggyel és hitel-információkkal kapcsolatban is. Ilyen regulák, amelyek kifejezetten igénylik az adatok törlését: Health Insurance Portability and Accountability Act (HIPAA), The Fair and Accurate Credit Transactions Act of 2003 (FACTA), Payment Card Industry Data Security Standard (PCI DSS), UK Data Protection Act 1998, illetve az EU adatvédelmi reformja szintén átfogó szabályozás.

Az adatok védelmére vonatkozó törvénykezési és szabályzási követelmények száma folyamatosan nő.

KEZDEMÉNYEZÉSEK AZ USA-BAN

A törvénykezési és szabályozási követelmények, amelyek körülveszik az adatvédelmet, sok más igény mellett jelentek meg a vállalkozások számára. 2012 februárjában Obama elnök kibocsátott egy keretmegállapodást a magánélet védelméről, amely innovációt sürgetett a globális digitális gazdaság területén is. Míg a jelentés a fogyasztók adatainak védelme érdekében készült, a digitális adatokkal kapcsolatos folyamatokat, problémákat és aggodalmakat is kiemelte.

A problémák kezelésére az Obama-adminisztráció bevezette a Consumer Privacy Bill of Rightsot (Fogyasztói adatok védelméről szóló törvény)[4]. Az új keretmegállapodás az adatvédelmi alapelvek egyértelmű szabályozóit nyújtja.

AZ EU ADATVÉDELMI DIREKTÍVÁJA

A közösségi oldalak, a felhő alapú számítások, a hely alapú szolgáltatások és az okos kártyák megjelenése mind ösztönző erőt jelentettek az EU adatvédelmi jogszabályainak frissítéséhez[5]. A frissítések egy kivonata jelenleg a tagállamoknál van felülvizsgálat és jóváhagyás céljából, a feltehető kibocsátásuk 2013 júniusában várható.

A szabályszegések esetén szankciókat is kilátásba helyez az új regula, 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. A felhő alapú szolgáltatásokat nyújtó cégeknek összhangban kell működniük a törvénnyel, ha a feldolgozott adatok EU-állampolgárokat is érintenek, függetlenül attól, hogy a szervereik az EU-ban találhatók-e vagy sem.

TELJESEN ÁTLÁTHATÓ TÖRLÉSI ELJÁRÁS

A sikeres törlés egymagában nem elegendő, részletes, átlátható bizonyíték szükséges a törlésről, hogy a szabályzóknak és törvényi követelményeknek is megfeleljen a művelet. Az átfogó vizsgálatok fontos dokumentumokat szolgáltatnak az eszközök életciklusáról.

A felhő alapú szolgáltatásokat nyújtó cégeknek összhangba kell működniük a törvénnyel, ha a feldolgozott adatok EU-állampolgárokat is érintenek, függetlenül attól, hogy a szervereik az EU-ban találhatók-e vagy sem.

HOZD A SAJÁT ESZKÖZÖD!

A szervezeteknek a „Bring Your Own Device – Hozd a saját eszközöd!" (BYOD)-höz társított kihívásokkal is szembe kell nézniük. A Juniper Research jelentése szerint több mint 150 millió, az alkalmazottak tulajdonát képező eszközt használnak ma a munkahelyeken. Az okostelefonok száma a vállalkozásokban 2014-re elérheti a 350 milliót is[7].

A mobileszközök kis méreteik ellenére rengeteg információt képesek tárolni: e-maileket, vásárlói adatokat, jelszavakat és más érzékeny információt. Egy 2009-es felmérés kimutatta, hogy az emberek 99%-a üzleti célból is használja a telefonját. 77%-uk az üzletfelek nevét és címét is tárolja a telefonján, 23%-uk vásárlói adatokat is tárol, és 17%-uk töltött le rájuk dokumentumokat, táblázatokat[8].

Nemcsak a kártevők, az adathalászok és a kémprogramok veszélyeztetik az adatainkat, a mobileszközök (okostelefonok, tabletek) helytelen leselejtezése sokkal nagyobb biztonsági problémát okozhat. Az Európai Hálózati és Információs Biztonsági Ügynökség (ENISA) megállapítása szerint az információbiztonságra nézve a legnagyobb veszélyt az jelenti, hogy az okostelefonokat teljes adattörlés nélkül helyezik használaton kívül[9]. Ez különösen annak fényében aggasztó, hogy az elemzők becslése szerint évente több mint 100 millió mobiltelefont hasznosítanak újra[10].

A legtöbb esetben a „gyári beállítások visszaállítása" parancs nem elegendő az adatok biztonságba helyezéséhez, mert ekkor az adatok még mindig visszaállíthatók széles körben hozzáférhető eszközök segítségével.

A mobileszközökkel kapcsolatos biztonsági irányelvek és a jogszabályi követelmények betartásához, és az adatok megvédéséhez be kell vezetni a fejlett törlési technológiával folytatott adattörlési menedzsmentet.

A törlés kezelésének fontossága az eszközök teljes életciklusában

A fogyasztók és alkalmazottak nagyban függnek a személyes és üzleti információk biztonságától. Ha hiba csúszik az információ hatékony törlésébe, az nemcsak egy márkáról vagy cégről alkotott képet rombolhat le, de a részvények árfolyamának eséséhez, vásárlók és üzleti partnerek elvesztéséhez és negatív sajtómegjelenésekhez is vezethet. Egy óvatlanul kidobott, bizalmas adatot tartalmazó merevlemez könnyen eredményezhet „személyiséglopást" vagy rossz fényben tüntethet fel egy szervezetet a nyilvánosság előtt, és költséges pereskedéshez is vezethet. Hatással lehet az alkalmazottak fluktuációjára, a mindennapi üzleti ügyletekre és a belső információs biztonságra is.

Ezenkívül amikor egy eszköz gazdát cserél, akkor a merevlemezén maradt alkalmazások vagy szoftverek licencelési problémákat vethetnek fel. Egy szerver áthelyezése egy másik osztályra vagy részlegre ugyanígy sértheti a szoftverlicencet, és könnyen jelentős büntetéseket vonhat maga után a kereskedő részéről.

Adattörlési stratégia alkalmazásával lehetségessé válik az újraértékesítés vagy adományozás anélkül, hogy aggódni kellene az eszközökön lévő érzékeny adatok miatt. A fizikai megsemmisítés is egyre járhatóbb útnak látszik, ha adattörléssel kombinálják. Így magasabb fokú biztonság érhető el, mert ez akkor is biztosítja az adatok védelmét, ha a fizikai megsemmisítési folyamat sikertelen, vagy a technológiai fejlődés valamely módon lehetővé teszi az adatok kinyerését az eszközök darabjaiból.

Az adattörlés azonban nem csak az életciklus végén fontos, hanem szükséges lehet egy eszköz működésének korai fázisaiban is, amikor bizonyos ideiglenesen elhelyezett bizalmas adatokra már nincs szükség. A fejlett adattörlési eszközökkel egy-egy fájl vagy könyvtár is célba vehető a még aktív rendszereken. Ez a célzott törlési folyamat ideális az olyan ideiglenes, bizalmas adatok eltávolítására, mint a hitelkártya-, az ügyfél-információk vagy levédett hivatali dokumentumok, ezáltal a napi adatmegsemmisítés könnyed gyakorlattá válik.

Sok vállalkozás használ költséges és komplex adatközpont-konfigurációkat, melyeket különféle asztali gépekről és laptopokról működtetnek, így a törlésnek potenciális hatása lehet az üzleti funkciókra. A szerverek vagy tárolóegységek, amelyek kritikus alkalmazásokat futtatnak, nem kapcsolhatók le vagy távolíthatóak el költséges és időrabló procedúrák nélkül, hogy aztán ismét online üzemmódba kapcsolják őket. Ezért elengedhetetlen egy fejlett törlési eszköz, amellyel megcélozhatók speciális adatok, logikai egységek vagy tárolók az aktív rendszereken.

A HELYBEN TÖRTÉNŐ TÖRLÉS FONTOSSÁGA

A helyben történő adattörlés a legbiztonságosabb opció, mert így az érzékeny információ nem hagyja el a vállalkozást, vagy ha szükséges, már az adott irodát sem.
Az IT Eszközkezelők Nemzetközi Szövetsége (IAITAM)[11] kombinált megközelítést javasol követendő gyakorlatként: helyszíni törlést a külső – az eltávolítást és a törlést újra elvégző félhez történő szállítás előtt. Azok a vállalatok, melyek nem gondoskodnak megfelelően az adattörlés kezeléséről, sok esetben súlyos büntetésekkel néznek szembe[12].

Az adattörlés azonban nem csak az életciklus végén fontos, hanem szükséges lehet egy eszköz működésének korai fázisaiban is, amikor bizonyos ideiglenesen elhelyezett bizalmas adatokra már nincs szükség.

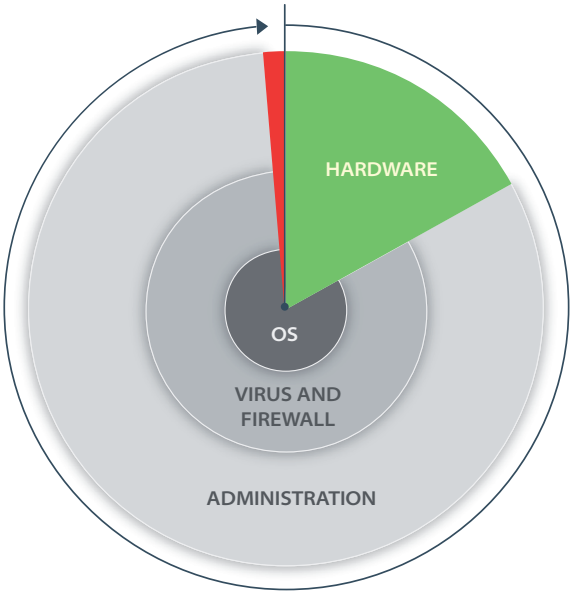
Az elismert, folyamatorientált adattörlési megoldás előnye

A nemzetközileg elismert „Common Criteria” tanúsítvány igazolja, hogy az adattörlő szoftver szigorú, független tesztelési folyamaton ment át, és képes véglegesen eltávolítani az adatokat a merevlemezekről és egyéb tárolóeszközökről. Szintén igazolja, hogy a szoftver eleget tesz a szabványoknak, amelyeket az International Standards Organization (ISO-IEC 15408) lefektetett.

A folyamatorientált, centrálisan kezelt automatizált adattörlési megoldás növelheti a termelékenységet és a hatékonyságot is. E folyamatok lecsökkentik az emberi hibázás lehetőségét a központosított megfigyeléssel és vizsgálattal, a minimális manuális adatbevitellel, a részletes törlési jelentésekkel és a hálózat alapú jelentéstovábbítással, amely elősegíti az előírt átvizsgálási folyamatokat.

A folyamatorientált, centrálisan kezelt automatizált adattörlési megoldás növelheti a termelékenységet és a hatékonyságot is.

Az adattörlés és jelentés mellett ez a folyamat hardvertesztek sorozatát is végrehajtja automatikusan vagy manuális módon, így biztosítva a szükséges információt az újrafelhasználáshoz vagy az IT eszközök ismételt piacra dobásához. Egy ilyen adattörlési megoldással lehetséges kevesebb idő alatt több eszközt is a folyamatba bevonni, főként a hagyományos eltávolítási módszerekhez vagy a kevésbé fejlett és erőteljes törlési eszközökhöz képest. A megoldás hozzáigazítható egyes szervezetek speciális igényeihez és hardveres vagy hálózati környezetéhez.



Az adattörlés kezelésének ára

A FOLYAMAT

Az automatikus adattörlés átfogó és centralizált online menedzsment jellegű megközelítése lefedi a folyamat összes állomását, a bootolástól az adatbázisba történő jelentésküldésen keresztül a tanúsítvány elkészítéséig és a számítógép kikapcsolásáig. A kezelési felület teszi lehetővé a távolról történő ellenőrzést a törlés felett, állapotfigyeléssel, teljes automatizációval, minimális felhasználói beavatkozással, teljes körű adattörlési jelentésekkel és statisztikával. Ezek a lehetőségek 25-30 százalékkal növelik a hatékonyságot más módszerekkel szemben. Például a fejlett törlési eljárással az IT személyzet képes végrehajtani szerverenként kétszáznál is több merevlemez egyidejű törlését. Ráadásul képesek távolról irányítani különféle IT eszközök törlését azonos időben.

A központosításból és automatizálásból nyert hatékonyság hozzájárul az ilyen szoftverbe történő alacsony beruházási költséghez is. Figyelembe véve a kockázatot és a lehetséges büntetéseket az adatvesztés miatt, az adattörlési eljárás ára minimális, ha a teljes eszközköltséghez hasonlítjuk, ami magában foglalja a hardvert, szoftvert, tűzfalat és vírusvédelmet.

Az adattörlési megoldás zökkenőmentes integrálása a meglévő IT infrastruktúrába alapvető fontosságú mind működési, mind gazdasági szempontból. Ezáltal lehetővé válik az együttműködés más IT eszközkezelő rendszerekkel, illetve az adatok egyszerű importja és exportja, valamint a webes szolgáltatási felületek használata.

Konklúzió

Az adatbiztonsági és az adatvédelmi szabályok előírásai, az adatok kiszivárgásának állandó kockázata és az adatvesztéshez kapcsolódó magas költségek indokolttá teszik az érzékeny információ teljes és biztonságos eltávolítását.

Mivel a szervezetek IT eszközei egyre több és több bizalmas adatot fognak tárolni a jövőben, elengedhetetlen egy átfogó adattörlési eljárás bevezetése. Az adatokat teljesen meg kell semmisíteni, mielőtt az IT eszközöket kivonják, újra felhasználják, újrahasznosítják vagy eladományozzák. A vállalatoknak sok esetben meg kell felelniük a növekvő számú kormányzati és iparági szabványoknak és szabályozóknak is.

A Blancco egy fejlett és centralizált adattörlési megoldást kínál a felhasználóknak. Gyors, automatizált és biztonságos eszközt ahhoz, hogy időt és pénzt takarítsanak meg, miközben biztosítják az érzékeny adatok védelmét.

A modern adattörlés szoftver alapú megközelítést alkalmaz az adatok felülírásához és az összes elektronikus információ megsemmisítéséhez a merevlemezen vagy más digitális médián, oly módon, hogy a lemezek működőképesek maradnak. A fejlett törlési eszközök képesek megcélozni adott bizalmas adatokat is egy aktív rendszerben. Emiatt az adattörlési szoftver nem csak egy, az életciklus végén szükséges beszerzési döntés, hanem az eszközök használatba vételének kezdetétől figyelembe kell venni szükségességét.

A Blancco egy fejlett és centralizált adattörlési megoldást kínál a felhasználóknak. Gyors, automatizált és biztonságos eszközt ahhoz, hogy időt és pénzt takarítsanak meg, miközben biztosítják az érzékeny adatok védelmét. Az automatizált adattörlési lehetőségek révén az IT részlegek a leggyorsabb és a leginkább személyre szabott megközelítéshez jutnak hozzá egy kifinomult és felgyorsított törlési, jelentési és átvizsgálási folyamat képében.

További információ:
http://törlés.hu

Hivatkozások

1 KPMG International, "Data Loss Barometer –Insights into Lost and Stolen Information in 2010," Issue 3, 2010

2 Kessler International, "Is Your Confidential Information Being Sold on eBay?", February 2009, http://www.investigation.com/press/press75.htm

3 IDC, sponsored by EMC Corporation, "Extracting Value from Chaos," June 2011, http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

4 Obama Administration, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

5 European Commission, January 2012, http://ec.europa.eu/justice/data-protection/index_en.htm

6 MaaSters Blog, "Enterprise Mobility Update: 350 Million BYOD Smartphones by 2014," August 2012, http://www.maas360.com/maasters/blog/businessintelligence/ enterprise-mobility-350-million-byodsmartphones-2014/

7 Juniper Research, August 2012, http://www.juniperresearch.com/viewpressrelease.php?pr=330

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

9 ENISA, "Smartphones: Information Security Risks, Opportunities and Recommendations for Users," December 2010, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks/top-ten-smartphone-risks

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

11 http://www.iaitam.org/

12 Dark Reading, "$1.5M Fine Marks A New Era In HITECH Enforcement," March 2012, http://www.darkreading.com/database-security/167901020/security/vulnerabilities/232700031/1-5m-fine-marks-a-new-era-in-hitech-enforcement.html

blancco

MINŐSÍTETT ADATTÖRLÉS

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

A Blancco termékek képviseletét Magyarországon a V-Detect Antivírus Kft. látja el.

V-DETECT ANTIVÍRUS KFT.

www.v-detect.hu