blancco

MINŐSÍTETT ADATTÖRLÉS

Legjobb gyakorlatok a minősített és megbízható adattörlési rendszer bevezetéséhez, valamint az adathordozók leselejtezéséhez

Szerző: Petrányi-Széll András

2013. július 5.

Tartalomjegyzék

1. Az adattörlés koncepciója és területei

Az adatok minősített törlésére az adatszivárgás megelőzése érdekében van szükség, mivel az operációs rendszerekbe épített törlési és formázási parancsok magukat az adatokat a legtöbb esetben érintetlenül hagyják, így pedig azok bármikor visszaállíthatóak.

A minősített, auditálható és rendszeres adattörlés célja az adatszivárgás megelőzése. A rendszertől elvárt alapvető követelmény annak biztosítása, hogy a leselejtezni kívánt adathordozókon, valamint a szervezeten belül tulajdonost váltó eszközökön a leselejtezéskor, illetve tulajdonosváltáskor ne maradjon semmilyen adat.

Az a trend, hogy az adathordozók fajtái folyamatosan szaporodnak, és a munkavállalók saját tulajdonban lévő eszközökre is felmásolhatnak vállalati adatokat, az adattörléssel kapcsolatban is új kihívást jelent. Fontos az adattörlést kiterjeszteni a PC-k mellett a mobileszközökre (okostelefonokra, tabletekre), valamint a flash adathordozókra (memóriakártyákra, USB kulcsokra) is.

Emellett fontos hangsúlyozni, hogy a kiválasztott adattörlési megoldást nem egy „end-of-life" intézkedésként érdemes bevezetni, hanem egy olyan módszertanként, mely az adathordozó teljes élettartama alatt biztosítja a szenzitív adatok megfelelő törlését, és ezzel csökkenti az adathordozó elvesztéséhez vagy tulajdonoscseréjéhez kapcsolódó adatvesztési kockázatokat.

Az adattörlési rendszer bevezetéséhez kapcsolódóan a jogi megfelelőség érdekében felül kell vizsgálni az adatkezelési szabályzatot, és abban külön ki kell térni az adattörlés kérdésére.

A minősített adattörlési rendszer bevezetése lehetővé teszi, hogy az eszközöket a lehető legteljesebb mértékben kihasználjuk, és a szervezeten belüli élettartamuk végén akár értékesítsük, akár jótékony célokra felajánljuk. A minősített adattörlés bevezetése tehát nem csupán magasabb szintre emeli a biztonságot, de költségmegtakarítást is eredményezhet, emellett pedig óvja a környezetet.

Nem működő megoldások az adattörlésben

A merevlemezek adattörlésére az alábbi rossz gyakorlatokat tartjuk nyilván:

Formázás

A formázás során az operációs rendszer az adatokhoz vezető útvonalakat törli, nem magukat az adatokat. Ezért az adatok fizikailag még ott maradnak az adathordozón, és egy egyszerűen kezelhető, ingyenes visszaállító szoftver segítségével a legtöbb esetben visszaállíthatóak.

Az operációs rendszer újratelepítése

Az operációs rendszer jellemzően csupán a merevlemez 1% és 10% közötti területét foglalja el, ezért csupán ekkora terület kerül felülírásra. A merevlemez többi területén tárolt adatok érintetlenül maradnak.

A merevlemez átfúrása vagy más nem hatékony fizikai megsemmisítése

A mai, több terabájtos merevlemezek adatsűrűsége igen magas, egy négyzetcentiméteren akár több tucat gigabájtnyi adat tárolható. Ezért az átfúrás nem csupán munkavédelmi kérdéseket vet fel, de az adattörlésre sem jelent megfelelő megoldást.

Ugyanez igaz a merevlemezek ledarálására, melynek során a darálókések közötti távolság szabja meg a fizikailag megmaradó részek nagyságát. A forgókéses darálók esetében ezenkívül előfordulhat, hogy egy merevlemezrész frontálisan csúszik be a kések közé, így pedig több centiméteres darabok maradhatnak érintetlenül.

Végül a következő tipikus probléma a fizikai megsemmisítés során, hogy a megsemmisítés jellemzően nem végezhető el a szervezeten belül, közvetlenül az adatgazda által, hanem külső vállalkozókra, harmadik személyekre van bízva. Így a szállítás és a megsemmisítés során a szervezet ezeknek a vállalkozóknak a megbízhatóságára van utalva.

Ugyanennek a problémának a másik oldala a megfelelő dokumentáció hiánya. A fizikai megsemmisítés során jellemzően nem marad felvétel a merevlemez sorozatszámáról, illetve a jegyzőkönyvek nem kerülnek digitális aláírásra és megfelelő tárolásra.

A megfelelő fizikai megsemmisítés ezzel szemben egyrészt külső szervezetek – például NATO – által minősített eszközökkel történik, másrészt olyan módon, melynek során a gép működésének köszönhetően egyértelműen dokumentálásra kerül a merevlemez sorozatszáma.

A megfelelő fizikai adatmegsemmisítés a merevlemezek esetében az adathordozó teljes megsemmisítésével történik. Ennek során olyan erős mágneses mezők hatásának tesszük ki a merevlemezt – például a Blancco Degausser segítségével –, hogy arról fizikailag eltűnik az adathordozó felület.

A minősített megsemmisítés alapelvei szerint minden esetben gondoskodni kell arról, hogy a megsemmisítés megfelelő fizikai eljárással, lehetőleg a szervezeten belül történjen meg az adatgazda vagy megbízható kezelőszemélyzet által, és jól dokumentálható, egyértelműen igazolható legyen.

Nem megfelelő szoftverrel végzett adattörlés

Az interneten számos adattörlést végző szoftver található. A legtöbb esetben ezek a szoftverek nincsenek minősítve külső szervezetek – például NATO – által, és az adattörlést nem megfelelően végzik el. A nem megfelelőségre példa az operációs rendszerből indított adattörlés, melynek során nem törlődnek azok a területek, melyeket az operációs rendszer saját maga számára fenntart.

Ugyanilyen problémát jelent, ha az adattörlést végző szoftver nem ismeri fel a hibás szektorokat, nincs felkészülve az úgynevezett remappelt szektorok kezelésére.

Végül érdemes hangsúlyozni, hogy az adattörlés egy olyan folyamat, mely nem csupán az adathordozó törléséből áll, hanem ehhez kapcsolódóan egyértelmű módon igazolja az adattörlést elvégző operátor kilétét, az adattörlés módszerét, az adattörlés sikerességét, a merevlemez vagy más adathordozó fizikai azonosítóit, majd mindezen adatokat visszakereshető, nem meghamisítható módon tárolja.

Az eszközök titkosítása vagy távoli törlése

A titkosításra használt algoritmusok feltörhetőek, a feltöréshez szükséges idő és az igényelt erőforrás azonban nagymértékben függ a titkosításra használt algoritmustól. A titkosított módon adatokat tartalmazó eszközöket azonban nem célszerű leselejtezni, méghozzá a következő okokból:

- A titkosításra használt módszer általában nem rendelkezik független minősítésekkel, így nem kizárható, hogy hátsó kaput tartalmaz.
- A titkosítás megfelelő erőforrás és motiváció birtokában esetlegesen feltörhető.
- A titkosított állományt általában jelszó védi, mely megfelelő ismeretek birtokában social engineering módszerekkel megfejthető.
- A titkosított állományt védő jelszó zsarolással, fenyegetéssel, erőszakkal megszerezhető.
- A titkosítás alkalmazásába hiba csúszhat (például nem megfelelő jelszó választása).
- A titkosítás önmagában nem nyújt auditálható, minősített riportokat.

Az eszközök távoli törlése, zárolása (lock down) ugyan nagymértékben növeli a biztonságot, de hatása szintén nem egyezik meg a minősített adattörlés hatásával, méghozzá a következő okokból:

- Az eszköz zárolására használt mechanizmus a legtöbb esetben könnyedén kijátszható (például Faraday-kalitka segítségével).
- Az eszköz zárolására, távoli törlésére használt mechanizmus hatása a formázáséhoz hasonló – a távoli törlés esetén az adatok nem teljes körűen kerülnek felülírásra, hanem az azokhoz vezető útvonal törlődik.
- A zárolás feloldására használt jelszó a social engineering módszerekkel, zsarolással, fenyegetéssel vagy erőszakkal megszerezhető.

Követelmények az adattörléssel szemben

Az adattörlésre alkalmazott megoldással kapcsolatban megfogalmazott követelmények:

a) Annak érdekében, hogy az adattörlések követhetőek és ellenőrizhetőek legyenek, az egyes törlésekről kiállított jegyzőkönyveket visszakereshető módon szükséges tárolni.
b) Azért, hogy a jegyzőkönyveket ne lehessen meghamisítani vagy utólag módosítani, a jegyzőkönyveket elektronikus aláírással érdemes lepecsételni.
c) Annak érdekében, hogy az adattörlések megbízható módon történjenek meg, kizárólag olyan minősített adattörlési megoldást lehet használni, mely a legszigorúbb biztonsági előírásoknak is megfelel, és melynek forráskódját független, megbízható szervezetek tanúsították.
d) A mechanikai hibával rendelkező merevlemezek leselejtezhetőségének érdekében ezeket a merevlemezeket meg kell semmisíteni. A megsemmisítésről kiállított jegyzőkönyvet ugyanabban a rendszerben, visszakereshető módon célszerű tárolni, mint a törlésről kiállított jegyzőkönyveket. A meghamisítás elkerülése érdekében a megsemmisítéséről is egyértelmű bizonyítékot kell tárolni.
e) A törlésre alkalmazott szoftveres megoldásnak a merevelemezek törlése mellett támogatnia érdemes az okostelefonok törlését, a flash meghajtók és memóriakártyák törlését, a fájlok törlését, valamint a logikai meghajtók törlését.
f) A törlésre alkalmazott szoftveres megoldásnak több minősített algoritmust érdemes támogatnia.
g) A törlésre alkalmazott megoldásnak képes kell lennie arra, hogy a törölt adathordozóra vonatkozó azonosítási adatokat a törlési jegyzőkönyvben rögzítse.
h) A törlésre alkalmazott megoldásnak képesnek kell lennie a vállalati környezetek támogatására, különös tekintettel a szoftver disztribúciójának elősegítésére a hálózatban lévő kliensekre.

Az adattörlési rendszer előnyös tulajdonságai

Az adattörlésre alkalmazott megoldás elbírálása szempontjából előnyt jelentő tulajdonságok:

Minősítések

a) NATO-minősítés.
b) Common Criteria minősítés.
c) Egyéb minősítések, különös tekintettel a TÜV-SÜD és a CESG minősítésekre.

Menedzsment

a) MSI telepítőcsomagok támogatása.
b) Törlési jegyzőkönyvek központosított kezelése és a hálózaton keresztül történő begyűjtése.
c) Külső adatbázisok (SQL, MySQL, Oracle, LDAP) támogatása.
d) Jogosultságok támogatása.
e) Active Directory támogatás.
f) Törlési jegyzőkönyvek importálása és exportálása.
g) Integráció lehetősége külső eszköz-nyilvántartási (asset management) rendszerrel.
h) Törölt adathordozók hardverösszetevőinek átfogó jegyzőkönyvezése.
i) Törlési jegyzőkönyvek visszakereshetőségének biztosítása, a jegyzőkönyvek szűrése az adattörlést végző személy nevére.

Egyéb műszaki összetevők

a) Hibás szektorok érzékelése.
b) Átirányított szektorok felderítése és törlése.
c) RAID konfiguráció lebontása.
d) IDE, ATA, SATA, SCSI, SAS, FC lemezek támogatása.
e) HMG Infosec Standard No: 5 algoritmus és más törlési algoritmusok támogatása.
f) Licencmenedzsment támogatása.
g) A hálózatba nem kötött kliensek törlésének támogatása on-site adattörlési megoldásokkal.
h) Távoli adattörlés elvégzésének lehetősége.
i) Lehetőség az adattörlés folyamatának nyomon követésére.

2. Kezelendő problémák és tipikus forgatókönyvek

Az alábbiakban sorra vesszük, hogy milyen esetekben van szükség az adathordozó fertőtlenítésére.

Leselejtezés

Az adathordozók megbízható fertőtlenítésére van szükség olyankor, amikor azok elhagyják a szervezetet, mivel leselejtezésre, elajándékozásra vagy értékesítésre kerülnek.

Ebben a pontban a működő merevlemezek fertőtlenítésével foglalkozunk, a nem működő, meghibásodott merevlemezek törlésével kapcsolatban lásd a később leírtakat.

Az adatszivárgás szempontjából veszélyt jelentő eszközök veszélyességi szempontból sorba rendezve a következőek:

– Szervermerevlemezek
– PC- és notebookmerevlemezek
– Okostelefonok és az azokban található memóriakártyák
– USB kulcsok és más flash adathordozók

Szervermerevlemezek törlése

Egy szervermerevlemez leselejtezésére sor kerülhet, ha magát a szervert selejtezik le, ha a merevlemezt selejtezik le vagy a merevlemez meghibásodik.

Emellett sor kerülhet fájlok vagy logikai meghajtók törlésére olyankor, ha a szerveren tárolt adatokat, adatbázisokat más tárolóhelyre mozgatják át. Egy példa erre a recovery site (visszaállítási szerver) próbája, melynek során a másodlagos, tartalék szerverre kerülnek az üzleti adatok. Ezeket az adatokat a mentési próba után törölni szükséges.

A szerver leselejtezése során biztosítani kell, hogy a leselejtezett eszközön semmilyen üzleti adat ne maradjon. Ennek érdekében minden szervermerevlemezt fertőtleníteni kell minősített adattörlési megoldások segítségével.

A fertőtlenítés a következő módokon történhet:
– Helyben, a szerverről indítva (USB kulcs vagy CD meghajtó segítségével).
– Távolról indítva (PXE boot vagy korábban telepített kliens segítségével).
– A szerver elszállításával és törlésével a vállalat informatikai munkatársai által üzemeltetett fertőtlenítő laboratóriumban.
– A merevlemezek kiszerelésével, majd azok törlésével a vállalat informatikai munkatársai által üzemeltetett fertőtlenítő laboratóriumban.
– A szerver elszállításával harmadik félhez, mely szolgáltatásként törli a szerveren tárolt adatokat.

A fertőtlenítés – azaz a minősített adattörlés – nem lehetséges olyankor, amikor a merevlemez valamilyen mechanikai vagy elektronikai oknak köszönhetően működésképtelen. Ez azonban nem jelenti azt, hogy a merevlemezen nem maradnak adatok.

Éppen ezért kiemelten fontos, hogy a meghibásodott szervermerevlemezeket degausser segítségével megsemmisítsük, a megsemmisítésről pedig jegyzőkönyv készüljön. A garanciális időszakban meghibásodott merevlemezek által okozott költségkiesés ellen a szervezet úgy tud védekezni, ha olyan szerződést köt a beszállítóival, mely lehetővé teszi, hogy a meghibásodott merevlemezeket ne kelljen a szállítónak visszajuttatni.

Megjegyzés: A minősített adattörlés a merevlemezek módszeres, meghatározott algoritmusok szerinti felülírását jelenti. A minősített adattörlés olyan törlési eljárás, mely után semmilyen módszerrel nem állíthatóak vissza az adatok a merevlemezekről, maguk a merevlemezek azonban használhatóak maradnak. A minősített adattörlés éppen ezért jól dokumentált, és a merevlemezek nagyságától függően akár több órát is igénybe vevő folyamat.

PC- és notebookmerevlemezek törlése

A PC és a notebookok törlésére sor kerülhet, ha az eszköz leselejtezésre kerül, ha a szervezeten belül gazdát vált vagy meghibásodik.

Fontos, hogy a PC-k és notebookok fertőtlenítését ne csupán akkor végezzük el, amikor az eszköz élettartama véget ér, hanem olyankor is, amikor a szervezeten belül gazdát cserél. (A minősített fájltörlésekkel pedig tovább növelhetjük a biztonságot.)

A fertőtlenítés a következő módokon történhet:
– Helyben, a PC-ről vagy notebookról indítva (USB kulcs vagy CD meghajtó segítségével).
– Távolról indítva (PXE boot vagy korábban telepített kliens segítségével).
– Az eszköz elszállításával és törlésével a vállalat informatikai munkatársai által üzemeltetett fertőtlenítő laboratóriumban.
– A merevlemezek kiszerelésével, majd azok törlésével a vállalat informatikai munkatársai által üzemeltetett fertőtlenítő laboratóriumban.

A meghibásodott merevlemezeket a meghibásodott szervermerevlemezekhez hasonlóan meg kell semmisíteni.

Fontos, hogy hibásnak kell tekinteni azt a merevlemezt is, melyen a minősített adattörlés közben túlságosan sok hibás szektort talál a törlést végző szoftver. Egyes kémprogramok képesek arra, hogy a lemezen hibásnak látszó szektorokat hozzanak létre, és azokban adatokat rejtsenek el. A minősített adattörlési rendszernek ezért a túlságosan sok hibás szektor esetében javasolnia kell a merevlemez megsemmisítését.

Mivel a legnagyobb adatszivárgási kockázattal azok a merevlemezek járnak, melyek elhagyják a szervezetet, fontos, hogy a leselejtezett merevlemezeket mindenképpen töröljük.

Minősített adatokat tartalmazó eszközök selejtezése

A minősített adatokat tartalmazó eszközök leselejtezésére egyes szervezetek szigorúbb szabályozást írnak elő, és a merevlemez minősített adattörlése – fertőtlenítése – után annak megsemmisítését írják elő.

Amennyiben minősített adatokat tartalmazó adathordozókat kívánunk megsemmisíteni, a következő szempontokat kell figyelembe vennünk:

– Az adathordozó megsemmisítése lehetőleg kizárólag a szoftveres adattörlés – fertőtlenítés – után történjen meg. A minősített adattörlés ugyanis az adathordozó közvetlen operátora, az adatgazda által is elvégezhető. Emellett a minősített adattörlés során az adathordozó sorozatszáma, mint egyedi azonosító érték, közvetlenül kinyerhető, és a digitálisan lepecsételt jegyzőkönyvben tárolható. A megsemmisítést ezzel szemben jellemzően más személy végzi, mint az adathordozón tárolt minősített adat gazdája. Fontos ezért, hogy már ehhez a személyhez is a fertőtlenített adathordozó kerüljön.

– Az adathordozó megsemmisítése lehetőleg a szervezeten belül történjen meg. Amennyiben lehetséges, olyan eszközt kell alkalmazni az adathordozó megsemmisítésére, mely irodai használatra lett tervezve. Így csökkenthető az adathordozó szállítási terhe, az adathordozó megsemmisítése pedig az adatgazdához a legközelebb vihető.

– A megsemmisítésről ugyanolyan jegyzőkönyv készüljön, mint az adathordozók fertőtlenítéséről. A jegyzőkönyv minél egyértelműbben tárolja az adathordozó közvetlen azonosítóit, és lehetőleg ugyanabban a rendszerben – könnyen visszakereshető módon – kerüljön tárolásra, mint a fertőtlenítésekről kiállított jegyzőkönyvek.

Meghibásodott eszközök kezelése

A meghibásodott merevlemezeken az esetek 99%-ában visszaállítható módon rajta vannak még az adatok. A meghibásodás oka jellemzően mechanikai vagy elektronikai hiba, mely a merevlemezekben az adatok tárolásáért felelős mágneses területeket nem érinti.

Éppen ezért fontos, hogy a meghibásodott, és ezért minősített adattörlési eljárással nem fertőtleníthető adathordozók ne hagyják el a szervezetet, hanem kerüljenek megsemmisítésre a fentiekben leírt irányelvek szerint, melyek az adathordozók szervezeten belüli, az adatgazda által végzett és jól dokumentált megsemmisítését javasolják.

A megsemmisítést megbízható külső szervezetek által minősített eszközökkel kell elvégezni, az egyszerű átfúrás vagy kalapácsozás nem csupán munkavédelmi kérdéseket vet fel, de nem garantálja a módszeres megsemmisítést és nem kínálja a megbízható dokumentálás előnyeit sem. A fizikai károsodást szenvedett adathordozókról az esetek jelentős részében helyreállíthatóak az adatok, ezért a módszeres megsemmisítés során olyan eljárást kell választani, mely technológiájának köszönhetően garantálja az adathordozó megbízható megsemmisítését.

A garanciális időszakban meghibásodott merevlemezek által okozott költségkiesés ellen a szervezet úgy tud védekezni, ha olyan szerződést köt a beszállítóival, mely lehetővé teszi, hogy a meghibásodott merevlemezeket ne kelljen a szállítónak visszajuttatni.

Gazdaváltás a szervezeten belül

Az adathordozók a szervezeten belül is gazdát válthatnak, ilyenkor pedig sokszor nem azonos jogosultsági szintű munkatárshoz kerülnek. Példa lehet erre egy vezető leselejtezett notebookja vagy okostelefonja, vagy akár egy kölcsönadott USB kulcs.

A gazdaváltás egyes eseteit nem a minősített adattörlési rendszer keretein, hanem más adatkezelési szabályzatokon belül lehet kezelni. Erre példa az USB kulcsok személyhez kötése, sorszámaik feljegyzése.

A gazdaváltásnak a minősített adattörlés körébe tartozó eseteiben a fertőtlenítést ugyanúgy kell kezelnünk, mint ha leselejtezésről beszélnénk. A gazdát váltó adathordozót fertőtleníteni kell, a fertőtlenítést pedig jegyzőkönyvezni szükséges.

A megfelelő nyilvántartási rendszer lehetővé teszi, hogy az eszköz életútját kövessük a szervezeten belül, és figyelemmel kísérjük, hogy a gazdaváltáskor sor került-e a fertőtlenítésre.

A felhőben tárolt adatok kezelése

A minősített adattörlés tárgya alapesetben egy fizikai adathordozó: merevlemez, USB kulcs, memóriakártya, mobiltelefon, SSD disk.

Bizonyos esetekben azonban fontos, hogy minősített módon töröljünk logikai meghajtókat (LUN-okat) a felhőben tárolt adatok közül.

Az alábbi esetekben kiemelten fontos a felhőből történő adattörlés:

- A felhőben tárolt adatokat egy másik szerverparkba helyezzük át – ilyenkor fontos gondoskodni arról, hogy az eredeti helyükről megbízható módon töröljük az adatokat.
- Az adatközpontban adattárolásra megbízást adó megrendelő el kívánja vinni az adatokat az adatközpontból – ilyenkor megbízható adattörlési eljárásra van szükség, valamint jegyzőkönyvre, mely igazolja, hogy a szolgáltató törölte az adatait.
- Mentési próba során az adatokat az eredeti tárolóhelyükön kívüli helyre is bemásoljuk – ebben az esetben gondoskodni kell arról, hogy a mentési próba után az adatok másolata ne maradjon a másolati helyen.
- A felhőben működő adathordozók leselejtezésre kerülnek – ebben az esetben egyrészt törölhetjük a logikai egységeket, másrészt fertőtleníthetjük a merevlemezeket mint fizikai adathordozókat.

A logikai egységek (LUN-ok) törlése során a logikai egységek kerülnek fertőtlenítésre és felülírásra, nem pedig a fizikai merevlemezek. Ezért a logikai egységek törlését nem end-of-life intézkedésként kell bevezetni, azaz nem olyankor kell elvégezni, amikor a merevlemezeket leselejtezik, hanem kiemelten a fenti esetekben. Emellett fontos a merevlemezek – a fizikai adathordozók – törléséről is gondoskodni, amikor azok elhagyják a szervezetet vagy a szervezeten belül gazdát váltanak.

Bizonyos esetekben – például virtuális szalagkönyvtárak (virtual tape library) esetében – szükség van arra, hogy eldöntsük, hogy a logikai egységeket szeretnénk törölni vagy a merevlemezeket. Amennyiben nincs lehetőség arra, hogy a logikai meghajtókat (LUN-okat) megszólítsuk és töröljük, kizárólag a fizikai merevlemezeket tudjuk törölni, úgy, hogy azokat kivesszük a tárolóból. Ez megbízható megoldást jelent az adatok törlésére, azonban minden fizikai merevlemez fertőtlenítését el kell végezni.

Fájlok törlése

A fizikai adathordozók törlése mellett a biztonság növelése érdekében – újabb védelmi rétegként – bevezethetjük a szenzitív fájlok rendszeres, minősített törlését.

A fájltörlés hátteréről tudni kell, hogy amikor az operációs rendszer segítségével a lomtárba mozgatunk egy fájlt, majd onnan is töröljük, a fájl valójában nem törlődik a merevlemezről.

A fájlról az operációs rendszer ugyanis árnyékmásolatokat (shadow copy) és előző verziókat (previous versions) tárol, melyeket ugyanúgy szükséges felülírni, mint az eredeti fájl helyét.

A minősített fájltörlés során ezért egy fájl összes létező másolata felülírásra kerül az adathordozón. Ez ugyan pluszidőt vesz igénybe, azonban garantálja, hogy az adott fájl véglegesen törlődik az adathordozóról.

A fájlok minősített törlése során a célunk, hogy tovább növeljük az adatbiztonságot. A minősített fájltörlés folyamata – az adathordozók teljes törléséhez hasonlóan – jó szándékot és felelősségteljes magatartást vélelmez az adatgazda részéről, és nem garantálja, hogy a rosszindulatú vagy felelőtlen operátor is megfelelően végzi el az adattörlést.

A fájlok törlése olyan alkalmazás segítségével történik a számítógépeken, mely helyettesíti az operációs rendszerbe épített adattörlési parancsot, és így lehetőséget ad az eszköz tulajdonosának a megbízható fájltörlésre.

A fájltörlési rendszer bevezetését érdemes megfontolni a mobilkliensek esetében, valamint azokban az esetekben, amikor a szervezet kötelessége valamilyen fájl vagy adatbázis teljes törlését elvégezni, miután az annak kezelésére való joga megszűnt.

Például ha egy alkalmazott notebookon dolgozik otthonról, és biztonságos VPN kapcsolaton keresztül belép a vállalat hálózatába, ahonnan egy dokumentumot átmásol a saját gépére azért, hogy azon dolgozzon, majd a kész dokumentumot visszatölti a vállalat hálózatába, a lokális példányt pedig hagyományos módszerekkel törli a gépéről – ilyenkor a helyi példány még ott fog maradni a notebook merevlemezén. Ha a notebook elveszik, fennáll az adatszivárgás veszélye.

A minősített fájltörlés bevezetése abban segít, hogy az érzékeny adatok – szerződések, fotók, adatbázisok és más dokumentumok – biztosan eltűnjenek arról a számítógépről, melyen szerkesztették őket. Ezáltal a minősített fájltörlés növeli a biztonságot, és segít a szerződéses vagy törvényi kötelezettségeknek való megfelelésben.

Ennek során a kezelőt arra kell kioktatni, hogy a hagyományos lomtár helyett a minősített adattörlési megoldás asztalra kihelyezett saját lomtár ikonját használja, és ebbe dobja bele a megsemmisíteni kívánt fájlokat. Előnyt jelent, ha a fájltörlési rendszer képes ugyanabban a rendszerben tárolni a törlésekről kiállított jegyzőkönyveket, mint amelyben az adathordozók törléseiről szóló jegyzőkönyvek tárolódnak.

A fájltörlés segítségével megbízható módon törölhetőek például azok az adatbázisok és fájlok, melyek kezelésére nézve a szervezetnek csak ideiglenes jogosultsága áll fenn.

Fontos, hogy a minősített fájltörlési rendszer bevezetése nem nyújt védelmet az ellen, hogy a fájlokról a rosszindulatú kezelő tetszőleges másolatot készíthessen – mint ahogy az adathordozók minősített törlése sem garantálja, hogy az adathordozókon tárolt adatokról a törlés előtt nem készült másolat.
Ez nem is a rendszer célja.

A minősített fájltörlési rendszerek bevezetése a szervezet önvédelmi mechanizmusai közé tartozik, célja, hogy a szervezet magasabb szintre tudja emelni saját biztonságát. Olyan, mint egy zár az ajtón, melyet, ha nyitva hagyunk, akkor nem nyújt védelmet. A minősített adattörlési rendszer a védelmen túl azonban riportolhatóvá és auditálhatóvá teszi az adattörlés folyamatát, a kiállított jegyzőkönyvekhez pedig felelősséget kapcsol – hasonlóan ahhoz, ahogy egy beléptető rendszer képes regisztrálni az épületen belüli mozgásokat és a beléptetést végző személyek kilétét.

A minősített fájltörlés elvégezhető számítógépeken, notebookokon és szervereken is.

A proaktív minősített fájltörlés emellett jellemzően szervereken történik, és olyan adatállományok kerülnek előre meghatározott ütemezés szerinti törlésre, melyek érzékeny adatokat tartalmaznak. Példa lehet erre egy logfájl vagy egy adatbázis, mely a szerveren tárolódik, azonban tárolásának célja csak meghatározott ideig áll fenn, ezután gondoskodni kell a törléséről.

3. A kezdő projekt fókusza

Amikor egy szervezet a minősített adattörlés bevezetése mellett dönt, a következő szempontokat érdemes megfontolnia.

Tipikus esetben a szervezetben nincs megfelelően nyilvántartva, hogy milyen adathordozón milyen adat található, ezért a kezelt adatok irányából megközelíteni az adattörlési rendszer bevezetését tipikusan túlságosan sok energiát igénybe vevő folyamat.

Emellett egy merevlemez törlésének költsége – főként az adatvesztés kockázatához mérten – nagyon alacsony, a licencelés módozatától függően tipikusan a néhány száztól a pár ezer forintig terjed.

Mivel a legnagyobb adatvesztési kockázatot ezek jelentik, a kezdő projekt fókuszába azon **működőképes** asztali számítógépek, notebookok és a szerverek merevlemezeinek törlését érdemes bevonni, melyek **véglegesen** elhagyják a szervezetet.

A merevlemezeket – azok fontossága és tartalma szempontjából – megkülönböztetjük egymástól, és a minősített adatokat tartalmazó merevlemezekre szigorúbb adattörlési szabályokat léptetünk életbe.

A fertőtlenítés esetei

Az első célként tehát azt érdemes kitűzni, hogy a szervezetet ne hagyja el véglegesen úgy működő merevlemez, hogy előtte nem kerül fertőtlenítésre. A fertőtlenítés módja ebben az esetben a teljes adattörlés.

Minden merevlemezt – beleértve az asztali munkaállomásokat, a notebookokat és a szervereket is – fertőtleníteni kell, akár önállóan, akár gépbe szerelve hagyja el a szervezetet.

A nyilvántartás módja

El kell dönteni, hogy az adattörlések nyilvántartására milyen rendszert alkalmazunk.

– Amennyiben az adattörlések száma néhány év tekintetében nem haladja meg a százas nagyságrendet, elegendő lehet a törlési jegyzőkönyvek kinyomtatása és papír alapon való tárolása.

– Amennyiben a minősített adattörlési rendszer szolgáltatója ingyenes felhő alapú nyilvántartási lehetőséget biztosít az adattörlésekhez, a jegyzőkönyveket ide is feltölthetjük. Ebben az esetben kizárólag a törlési riportok kerülnek a felhőben való tárolásra, maguk az adatok nem. A felhő alapú tárolás megfelelő megoldás lehet a kis- és középvállalatok számára.

– Amennyiben az adattörlések száma éves szinten több százas nagyságrendet ér el, érdemes saját központi elektronikus nyilvántartást bevezetnünk, mely lehetővé teszi a jegyzőkönyvek könnyű visszakereshetőségét, és a szervezeten belül tárolja az adatokat.

Az adatkezelési szabályzat

A minősített adattörlési rendszer bevezetése mellett felül kell vizsgálnunk a szervezet adatkezelési szabályzatát. A szabályzatnak ki kell térnie az adattörlés eseteire is.

Szabályoznunk kell, hogy az adattörléseket kicsoda, milyen jogosultsági szinttel rendelkező személy végzi el. Ehhez kapcsolódóan meg kell határoznunk a minősített adathordozók körét, és rendelkeznünk kell ezek adattörlési módjáról. Például elképzelhető az a forgatókönyv, hogy a szervezet minden merevlemezét a leselejtezés előtt az informatikai részlegen felállított adattörlési laboratóriumban törlik az informatikus munkatársak, a szervezet vezetőjének, főosztályvezetőinek számítógépeit azonban helyben, a vezetők irodájában törli az informatikai osztály kiemelten minősített munkatársa – így ezek a merevlemezek már az informatikai részlegre sem kerülhetnek el fertőtlenítés nélkül.

Mivel az adattörlés költsége jellemzően alacsony, már a kezdetekben érdemes úgy rendelkezni, hogy valamilyen módszerrel minden egyes merevlemez, mely elhagyja a szervezetet, fertőtlenítésre kerüljön.

Az adattörlések lehetséges módozatai

A minősített adattörlés több módon történhet:

- A számítógép (adathordozó) helyben történő törlésével USB kulcsról vagy CD-lemezről indítva.
- A merevlemez kiszerelésével és későbbi csatlakoztatásával az adattörlést elvégző eszközhöz.
- A számítógép beszállításával a vállalat kijelölt központi informatikai osztályára, ahol az adattörlést elvégzik.
- A hálózaton keresztül, távoli adattörlés segítségével.
- Összetett módszertan bevezetésével.

Helyben történő törlés

A fenti módszerek közül a legkönnyebben a számítógép helyben történő törlése valósítható meg. A módszer alkalmazása során az informatikai osztály munkatársa kimegy a számítógéphez, törli a számítógépet, majd a törlési jegyzőkönyvet elektronikus formában lementi USB kulcsra, valamint kinyomtatja a helyszínen. A kiállított, aláírt törlési jegyzőkönyv feljogosíthatja a felelős személyt arra, hogy engedélyezze, hogy a számítógép elhagyja a szervezetet.

Amíg az informatikus munkatárs nem törli a számítógépet, és nem állítja ki a törlési jegyzőkönyvet, addig az eszköz nem hagyhatja el a szervezetet.

A helyben törlés előnye, hogy azonnal, akár 24 órán belül bevezethető intézkedést jelent. Ha a vállalat elhatározza a minősített adattörlések bevezetését, az informatikus rövid oktatást követően egy lemezképfájllal, egy bootolható USB kulccsal és CD-lemezzel felszerelkezve indulhat a helyszínre, hogy a törlést elvégezze.

A módszer hátránya, hogy az informatikusoknak a helyszínre kell menniük az adattörlés elvégzéséhez. Ezért ez a módszer jellemzően ott alkalmazható jól, ahol a számítógépek egy épületen belül helyezkednek el. Emellett, ha a törlésre munkaidőben kerül sor, akkor számolni kell azzal, hogy a fertőtlenítés, valamint a gép újratelepítésének ideje alatt a gép kiesik a munkavégzésből.

A helyben történő adattörlés ugyanakkor a legbiztonságosabb módszerek közé tartozik, mivel a gépnek nem kell a hálózatra kötve lennie, sem a gép, sem a merevlemez nem kerül szállításra, melynek során extra kockázatnak van kitéve, és végül a merevlemez törlése az adatgazda jelenlétében végezhető el, az adatgazda pedig azonnal kézhez veheti és hitelesítheti a törlési riportot.

Merevlemez kiszerelése és törlése a központban

A merevlemezek kiszerelése a számítógépekből kizárólag akkor javasolt, ha a merevlemezek – például technológiaváltás miatt – önállóan kerülnek leselejtezésre. Ebben az esetben a merevlemez kiszerelése és az informatikai osztályon történő fertőtlenítése biztosítja, hogy az adott számítógép a lehető legkevesebb időre essen ki a hasznos munkavégzésből, illetve, hogy ne kelljen éjszakai műszakban elvégezni a törlését. Ellenkező esetben, ha a merevlemez a számítógéppel együtt hagyja el a szervezetet, a lemez kiszerelése a legtöbbször olyan pluszmunkát jelent, melyet érdemes elkerülni.

Amennyiben nagy tömegben kell merevlemezeket önállóan leselejtezni, javasolt olyan eszköz használata, mely egyszerre több merevlemezt tud törölni. Ilyen a Blancco Erasure Module (8 merevlemez egyidejű törlése) vagy a Blancco Erasure Cube (4 merevlemez egyidejű törlése). Ezzel a módszerrel az adattörlés ideje a töredékére csökkenthető.

A technológiaváltás projektjét tervezhetjük szakaszosra, felmérve, hogy egy kezelő hány gépet tud naponta újratelepíteni. Ebben az esetben az üzemeltetést végző a helyszínen egy adott számú merevlemezt kicserél az új generációs lemezre, majd a régi merevlemezeket a központba viszi, ahol azok azonnal törlésre kerülnek.

Amennyiben a csere nem szakaszosan történik, hanem egyszerre nagyobb tömegű, még adatokat tartalmazó merevlemez halmozódik fel a központban, akkor gondoskodni kell azok biztonságos raktározásáról és kezeléséről, ami jellemzően összetett feladatot jelent a szervezet számára.

A számítógép beszállítása központi törlésre

A számítógép központi törlése az egy telephelyes cégek esetében jelent működőképes megoldást, több telephely esetében a szállítás biztonsági kérdéseket vet fel.

Ebben az esetben a számítógép működési helyéről az üzemeltetésért felelős kezelő az adattörlés kialakított helyére szállítja a számítógépeket.

Amennyiben az adattörlés helye hálózatosan van kialakítva, az egyszerre törölhető számítógépek száma gyakorlatilag nem korlátozott.

A megoldás előnye, hogy ebben az esetben a számítógépek fizikai karbantartása, valamint műszaki állapotának felmérése is elvégezhető.

A Blancco Erasure Client beépített hardvertesztjeinek segítségével feljegyezhető a perifériák – billentyűzet, képernyő, egér stb. – állapota, tesztelhető a CPU, a memória és az alaplap. Ez természetesen növeli a gépekkel végzendő munka mennyiségét, ugyanakkor lehetővé teszi a számítógépek állapotának részletes feljegyzését.

Távoli adattörlés indítása a hálózaton keresztül

Az adattörlések távoli indítása jelenti a leggazdaságosabb, leghatékonyabb módszert az adattörlések kezelésére.

Ebben az esetben lehetőségünk van a klienseket a hálózatról bootolni PXE boot vagy a Blancco Erasure klienst disztribútálni a hálózaton MSI telepítőcsomagok segítségével. Mindkét módszerrel hatékonyan törölhető egyszerre nagyobb mennyiségű kliens – akár egyetlen éjszaka alatt megoldható a teljes vállalat összes számítógépének helyben történő törlése.

A törölt kliensek a fertőtlenítés után biztonságosan eltávolíthatóak a hálózatból.

A hálózaton keresztüli törlés nem csupán a nagy tömegű adattörlést teszi lehetővé, hanem azt is, hogy az eseti adattörléseket rugalmasan, gyors reakcióidővel lehessen elvégezni.

Összetett módszertan alkalmazása

A fentiekben ismertetett adattörlési eljárások a legtöbb esetben keverten, egymással párhuzamosan élő gyakorlatként kerülnek alkalmazásra, például:

- A kutató és fejlesztő munkatársak régi számítógépeit helyben, az adatgazda jelenlétében törli az üzemeltetésért felelős munkatárs, így az adatok semmilyen módon nem hagyják el a k+f laboratóriumot, még rövid időre sem.
- A legfontosabb vezetők számítógépeit szintén helyben, az adatgazda jelenlétében, vagy hálózatról, szintén az adatgazda jelenlétében törölhetjük, így az ezekben található merevlemezek sem kerülnek kiszerelésre, szállításra és tárolásra.
- Az értékesítés vagy elajándékozás céljából leselejtezésre kerülő, nem minősített adatokat tartalmazó számítógépeket egyszerűen kivehetjük a hálózatból, és megfelelően biztosított szállítás mellett a vállalat fertőtlenítő laboratóriumába (informatikai osztályára) szállíthatjuk, ahol helyileg kialakított hálózaton keresztül történik meg egyszerre több tucat számítógép törlése, emellett egyidejűleg sor kerül a hardverelemek átfogó tesztelésére és állapotának felmérésére.
- Egyedi merevlemez upgrade (például SSD-re való csere) esetén a korábbi, minősített adatokat nem tartalmazó merevlemezt helyben kiszerelhetjük a számítógépből, a törlését pedig elvégezhetjük a központban. Így biztosítható, hogy a gép a lehető legrövidebb időre esik ki a hasznos munkavégzésből, illetve, hogy nem kell éjszakai munkavégzést előírni az üzemeltetést végző munkatársak számára.
- Amennyiben nem jelent döntési szempontot, hogy az adott számítógép néhány órára, a fertőtlenítés idejére kiesik az aktív munkavégzésből, vagy a fertőtlenítés könnyen ütemezhető éjszakára vagy hétvégére, az adattörlést indíthatjuk a hálózaton keresztül is. Igaz ez akkor is, ha úgy kerül sor tömeges merevlemez-leselejtezésre, hogy az egyéb hardverelemek állapotát nem szükséges átfogó módon felmérni.

Összefoglalás

Összefoglalva a fentieket, az adattörlési rendszer bevezetésének első körében azt az esetet kívántuk lefedni, amikor a még működőképes merevlemezek véglegesen elhagyják a szervezetet. Célunk az volt, hogy az adatvesztés szempontjából legnagyobb kockázatot jelentő esetet kezeljük, és ezt a célunkat elértük.

Felállítottuk a központi nyilvántartó rendszerünket, melyben immár visszakövethető módon tárolódnak a digitálisan aláírt jegyzőkönyvek azokról a merevlemezekről, melyek véglegesen elhagyták a szervezetet.

Mostantól nem hagyhatja el a szervezetet véglegesen olyan működőképes merevlemez, mely nem került fertőtlenítésre.

Az adattörlési jegyzőkönyvek emellett egyértelműen személyhez köthetőek, azokhoz felelősségi körök rendelhetőek.

Az adatvesztés kockázatát tovább mérsékeltük azzal, hogy a minősített adatokat tartalmazó merevlemezekre szigorúbb adattörlési szabályokat léptettünk életbe, melyek azoknak a helyben történő törlését írják elő, adott esetben az adatgazda jelenléte mellett. Ezzel csökkentettük a szállítás, a kezelés és a raktározás közben fennálló adatvesztési kockázatokat.

Nagyot léptünk előre a jogi megfelelőség érdekében is, mivel adatkezelési szabályzatunkat kiegészítettük adattörlési szabályzatunkkal. Ezzel csökkentettük mind a cég vezetőinek, mind munkatársainak potenciális felelősségre vonhatóságát.

Ebben az első körben viszont nem foglalkoztunk még azzal az esettel, amikor működésképtelen merevlemez hagyja el a szervezetet, és nem foglalkoztunk azzal, ha egy merevlemez ideiglenesen, például szerviz céljából hagyja el a szervezetet. Nem kezeltük az USB kulcsok és egyéb adattárolók törlését, nem foglalkoztunk a fájltörlésekkel, valamint az adatközpontok logikai egységeinek fertőtlenítésével sem. Ezekkel az adattörlési rendszer bevezetésének következő lépcsőiben fogunk foglalkozni.

4. A fókusz kibővítésének lépései

A merevlemezek törlésének kiterjesztése

Működőképes merevlemez ideiglenesen elhagyja a szervezetet

Amikor a merevlemez szerviz céljából hagyja el a szervezetet, fontos észben tartani, hogy a teljes adattörlés az operációs rendszert is törli az eszközről. Ezért a következő lehetőségeink vannak annak biztosítására, hogy a merevlemez ne tartalmazzon érzékeny adatokat.

Egyszerű megoldás, ha a notebookot vagy PC-t úgy adjuk szervizbe, hogy a merevlemezt kiszereljük belőle, és a gyári rendszert egy másik merevlemezre töltjük vissza előzetesen elkészített lemezképfájlból. A megoldás alkalmazásához szükséges, hogy a még használatba nem vett számítógépekről olyan lemezkép készüljön, melyet ilyenkor telepíteni tudunk a gépre.

Nem jelent jó megoldást az, ha lementjük az érzékeny adatokat a számítógépről, majd fertőtlenítés – teljes adattörlés – nélkül töltjük vissza ugyanarra a merevlemezre az eredeti lemezképet. Ilyenkor nem a teljes merevlemez kerül módszeres felülírásra, csupán az operációs rendszer által elfoglalt, tipikusan 5–10 százaléknyi tárterület, a merevlemez többi részéről pedig visszaállíthatóak az adatok.

Ehelyett vagy az eredeti merevlemezt kell fertőtleníteni teljes adattörlés segítségével, majd erre visszaállítani a lemezképet, vagy pedig helyettesítő lemezt kell használni.

A helyettesítő lemez használata azoknál a szervezeteknél célszerű, ahol többtucatnyi azonos hardverkomponenseket tartalmazó számítógépekből álló géppark üzemel. Ilyenkor a beszerzett nagyszámú gép egyikéről készítünk egy lemezképet az eredeti gyári állapotnak megfelelően, majd magát a fizikai merevlemezt raktározzuk. Egy számítógép meghibásodása esetén a gépet ezzel a helyettesítő lemezzel adjuk szervizbe, a szerviz idejére pedig biztosítjuk a meghibásodott gépből kiszerelt merevlemez biztonságos őrzését.

A helyettesítő lemez alkalmazása olyan esetekben is lehetséges, amikor a minősített adattörlést valamilyen hardverkomponens (például a képernyő) meghibásodása megnehezíti.

Egy másik, de nem túl szerencsés megoldás, ha a gépet úgy adjuk szervizbe, hogy minősített fájltörlés segítségével töröljük a szenzitív adatokat. Ez kizárólag abban az esetben jelent megoldást, ha a gépen egyébként is minden egyes szenzitív adatokat tartalmazó fájl minősített fájltörlés segítségével kerül törlésre. A minősített fájltörlés azonban nem töröl olyan adatokat, mint a böngészők által tárolt jelszavak.

A harmadik megoldás az, ha a merevlemezt minősített adattörlés segítségével teljes mértékben fertőtlenítjük, majd – ha ez egyáltalán szükséges – visszaállítjuk rá az eredeti lemezképet és így adjuk szervizbe. A minősített adattörlés előtt – ha ez lehetséges és szükség is van rá – lemezképet készíthetünk a merevlemez tartalmáról, hogy a felhasználó beállításai könnyen visszaállíthatóak legyenek a szerviz után.

A helyettesítő merevlemez alkalmazásához képest ez a megoldás növeli az átfutás idejét a minősített adattörléshez, a lemezkép előállításához és visszaállításához szükséges idővel. További hátránya, hogy bizonyos hardverkomponensek (például a képernyő) meghibásodása estében a lemezképek készítése nehézségekbe ütközik, előnye viszont, hogy nem kell megbontani hozzá a gép burkolatát.

Nem működőképes merevlemez hagyja el a szervezetet

A működésképtelennek tűnő merevlemezek a legtöbb esetben pusztán valamilyen mechanikai vagy elektronikai hiba miatt nem működnek, a mágneses adathordozó felület néhány ritka kivételtől eltekintve nem sérül meg, arról az adatok a hiba javítása után visszaállíthatóak.

Éppen ezért fokozottan veszélyes a pillanatnyilag működésképtelen merevlemezek egyszerű leselejtezése vagy a gyártónak való visszaadása.

A feladatunk ebben az esetben, hogy a beszállítóinkkal olyan szerződést kössünk, mely lehetővé teszi, hogy a garanciális időn belüli meghibásodás esetén ne kelljen visszaadnunk a merevlemezt.

A mechanikai vagy elektronikai hiba miatt működésképtelen merevlemezeket ezután degausser segítségével meg kell semmisítenünk. A Németországban, magas minőségű alkatrészekből gyártott Blancco Degausser nagy erejű mágneses mezők segítségével teljesen megsemmisíti a merevlemezek mágneses adathordozó felületét, ezért a NATO minősítési rendszerében a legmagasabb, COSMIC TOP SECRET (CTS) minősítést kapta meg. Ilyen minősítést más merevlemez-megsemmisítő rendszer eddig nem nyert el.

A degausser alkalmazása természetesen anyagi terhet jelent a szervezet számára, azonban szinte az egyedüli biztos módszer a működésképtelen merevlemezek megsemmisítésére.

Más módszerek – például krematórium alkalmazása – nem minősítettek, nem vizsgáltak. A megsemmisítés eredményéről nem készül egyértelmű bizonyító erővel bíró okirat, ezért a működésbe hiba csúszhat (a kemence nem működik, de erről a szerkezet nem ad visszajelzést). Más módszerek (például az átfúrás) az adathordozó felületek nagyobb részeit érintetlenül hagyhatják, ezért nem megbízhatóak.

Amennyiben a megsemmisítésre házon kívül kerül sor, a megsemmisítendő adathordozókat szállítani és ennek során biztosítani kell. A szállítást és a megsemmisítést bérmunkában végző vállalkozást minősíteni szükséges, részükről felelősségbiztosítást kell igénybe venni. A szállítás és a megsemmisítés bérmunkába történő kiadása mindig növeli annak lehetőségét, hogy a külső vállalkozóhoz beépített ügynök szerzi meg az adatokat.

Ezenkívül problémát jelent, hogy a megsemmisítésre használt fizikai módszerek (elégetés, bezúzás) nem integrálhatóak egy központi nyilvántartó rendszerbe, mely visszakereshetően tárolja a megsemmisítésről készült jegyzőkönyveket.

A megbízhatóan működő degausser szerkezetek ezzel ellentétben magukba zárják a merevlemezt, lefotózzák annak sorozatszámát, melyet követően a megsemmisítés folyamata nem szakítható meg. A megsemmisítésről ezután jegyzőkönyvet állítanak ki, mely tartalmazza a merevlemez egyedi azonosítóit.

Amennyiben a vállalat több száz számítógéppel rendelkezik, javasolt egy degausser önálló beszerzése, és a központi telephelyen történő elhelyezése. Így biztosítható, hogy a merevlemez ne hagyja el a szervezetet, a megsemmisítésen pedig akár az adatgazda is részt vehessen. Ebben az esetben csupán a központ és a telephelyek közötti szállítást kell megbízható módon – zárható, lepecsételt adathordozók, megbízható szállító segítségével – megoldani.

Amennyiben a vállalat kevesebb számítógéppel rendelkezik vagy egy degausser beszerzése túlságosan nagy anyagi terhet jelent számára, a degaussert bérelheti. Ebben az esetben a működésképtelen merevlemezeket időlegesen raktározni szükséges, majd ha elegendő mennyiségű felgyűlt belőlük, sor kerülhet az eszköz bérlésére.

Ha a vállalat számára még a degausser bérlése is túlságosan nagy terhet jelent, olyan vállalkozót vehet igénybe, mely rendelkezik megbízható degausserrel, és bérmunkában megsemmisíti a merevlemezeket a számára. Ebben az esetben javasolt, hogy a megsemmisítésen a vállalat képviselője vegyen részt, és a megsemmisítésére olyan degausser segítségével kerüljön sor, mely egyrészt megfelelően minősített, másrészt feljegyzi a megsemmisített adathordozó egyedi azonosítóját, majd a megsemmisítésről jegyzőkönyvet állít ki.

Szervezeten belüli gazdacsere kezelése

Amikor egy eszköz a szervezeten belül gazdát cserél, a jogosultság szempontjából jellemzően azonos szinten marad vagy lefelé vándorol. Lefelé vándorlás során például előfordulhat, hogy az igazgató korábban használt notebookját megkapja annak titkárnője. Könnyen belátható, hogy ez adatszivárgási kockázatot jelent a szervezet számára.

Ezért a szervezeten belüli gazdaváltás esetén úgy kell kezelnünk a merevlemezt és a többi adathordozó médiumot (lásd később), mintha elhagyná a szervezetet, és ennek értelmében teljes fertőtlenítést kell végrehajtanunk.

Kiemeljük, hogy a szervezeten belüli gazdaváltás esetén végrehajtott teljes fertőtlenítés segít megelőzni a munkajogi pereket, mivel biztosítja, hogy az eszközt leadó munkavállaló magánéletéhez kapcsolódó dokumentumok nem kerülnek máshoz.

Ideális esetben az eszköznyilvántartásban egy adathordozó csak akkor rendelhető az új gazdájához, ha az adathordozó fertőtlenítéséről kiállított jegyzőkönyv egyértelműen igazolja, hogy a teljes adattörlés megtörtént.

Szervezeten belüli technológiaváltás kezelése

Néhány esetben technológiaváltás vagy szerepkörváltás miatt is szükség lehet az adathordozó minősített törlésére. Ilyen eset lehet például, ha egy számítógépen korábban kutató-fejlesztő munka történt, de most általános internetezés céljára lesz használva.

Ezeket az eseteket érdemes a gazdaváltáshoz hasonlóan kezelni.

Kompromittálódott adathordozók kezelése

Előfordulhat, hogy nem szándékosan a szervezet merevlemezére olyan információ – például szabadalom vagy szoftver – kerül, melynek kezelésére nincs jogosultsága. Az operációs rendszer újratelepítése vagy a merevlemez formázása nem jelent egyértelmű megoldást a jogosultság nélküli tartalom kezelésének megszüntetésére.

Ezekben az esetekben is teljes adattörlésre, fertőtlenítésre van szükség.

Ugyanez igaz a vírusfertőzés eseteire is. A vírusirtó szoftver által elvégzett vírusirtás megoldást jelent a fertőzés azonnali kockázatainak elkerülésére, és lehetővé teszi az adatmentést, de nem garantálja azt, hogy a kártevőnek egyetlen működő komponense sem marad a gépen. A veszélyhez kapcsolódó kockázat szintje ugyan ebben az esetben alacsony, mégis, amennyiben olyan számítógép válik vírusfertőzés áldozatává, melyen minősített adatokat kezelünk, szükség lehet a merevlemezek teljes fertőtlenítésére.

További lépések a biztonság növelése érdekében

Notebookok védelme fájltörlés bevezetésével

A szervezeten kívül mozgó adathordozók extra kockázattal járnak. Például egy alkalmazott titkosított VPN kapcsolaton keresztül bejelentkezik a vállalat hálózatába, letölt onnan a notebookjára egy dokumentumot, megszerkeszti és visszatölti a vállalat szerverére.

Ezután a dokumentumot hagyományos törléssel az operációs rendszer lomtárába helyezi, majd a lomtárat kiürítve törli.

Ilyen esetben a fájl a legtöbb esetben visszaállítható a merevlemezről, mivel az operációs rendszer árnyékmásolatokat (shadow copy) és előző verziókat (previous versions) tárol a fájlról. Ezért, ha a notebook elveszik, vélelmezhető, hogy a nem megfelelően törölt fájlokkal kapcsolatban fennáll az adatszivárgás kockázata.

A megoldás a kockázat kezelésére a minősített fájltörlés bevezetése. Ennek során olyan alkalmazást telepítünk a notebookokra, mely az operációs rendszer által tárolt összes másolatot észleli, törlés esetén pedig ezek helyét minősített algoritmusok segítségével felülírja.

A fájlok törléséről szóló riportokat a minősített adattörléseket nyilvántartó központi rendszerünkben érdemes tárolni.

Számítógépek védelme fájltörlés bevezetésével

A fájltörlés bevezetése a szervezeten belül lévő számítógépeken az illetéktelen hozzáférésből származó kockázatokat képes csökkenteni.

Amikor egy adatgazda nincs jelen, a számítógépéhez mások – például a takarítószemélyzet – is hozzáférhetnek. A számítógépek ugyan jelszóval vannak védve, de a jelszavakat sokszor különböző social engineering technikákkal megszerzik a hackerek, akik így hozzáférnek a helyi számítógépeken tárolt fájlokhoz. A minősített fájltörlés kiterjesztése az asztali számítógépekre csökkenti ezt a kockázatot.

USB eszközök és memóriakártyák törlése

A biztonság növelése érdekében a következő lehetőségünk a minősített adattörlés kiterjesztése a hordozható adathordozókra.

Ehhez kapcsolódóan a következőket érdemes tudnunk a flash adathordozók törlésének hátteréről:

- A merevlemezekhez hasonlóan a flash adathordozók törlése hagyományos törléssel vagy formázással nem biztonságos, mivel a fájlok könnyen helyreállíthatóak a formázás után is.
- Egyes kártevők, például a Vörös Október névre keresztelt malware képesek arra, hogy az USB kulcsokról törölt fájlokat a háttérben visszaállítsák, és elküldjék a kártevők készítőinek.
- Az USB kulcsok és a memóriakártyák „hajlamosak arra”, hogy észrevétlenül elhagyják a szervezetet vagy gazdát váltsanak.

A fenti okokból kifolyólag könnyen belátható, hogy a minősített adattörlés fontos eleme az USB kulcsokra vonatkozó vállalati előírásoknak, ugyanakkor azt is érdemes hangsúlyozni, hogy önmagában nem kezeli teljes körűen a cserélhető adathordozókhoz kapcsolódó kockázatokat.

A minősített adattörlés mellett a legtöbb esetben szükség lehet a vállalati számítógépek USB portjainak letiltására vagy a hozzáférés szabályozására.

Emellett érdemes a cserélhető adathordozókra másolt állományokat fájlszéf (például G Data Fájlszéf) segítségével titkosítani, így az adathordozó elvesztése esetén a károk mértéke csökkenthető (mivel egy laikus megtaláló nem fogja feltörni a titkosított fájlokat).

Az USB eszközökre és memóriakártyákra vonatkozó minősített adattörlésre nézve a következő intézkedések bevezetését érdemes megfontolni:

- Amennyiben egy USB eszközön vagy memóriakártyán személyes adatokat tartalmazó vagy minősített ügyiratok kerülnek tárolásra, akkor az USB eszközt vagy memóriakártyát fertőtleníteni kell, amint a tárolás célja megszűnik.
- Amennyiben egy USB eszköz vagy memóriakártya a szervezeten kívül járt, és ott adatokat másoltak rá, az adatok lemásolása után, miután megszűnt az adatok tárolásának célja, a szervezeten belüli használatba vétele előtt először fertőtleníteni szükséges.
- Amennyiben egy USB eszköz vagy memóriakártya abból a célból hagyja el a szervezetet, hogy a szervezeten kívül adatokat másoljanak rá, fertőtleníteni kell, mielőtt elhagyja a szervezetet.

Néhány példa a tárolt adatok jellegére és a törlésre:

- Egy flash adathordozóra szerződést másolnak, mely személyes adatokat is tartalmaz. Az adathordozót fertőtleníteni szükséges a lehető legrövidebb időn belül, amint a tárolás célja megszűnt.
- Egy fényképezőgéppel felvételek készülnek egy baleset helyszínén. Az adathordozót fertőtleníteni szükséges, amint a felvételek biztonságosan mentésre kerültek a szervezeten belüli szerverre.

Mivel a flash adattárolók fertőtlenítése a merevlemezek fertőtlenítéséhez hasonlóan teljes felülírással történik, a szervezetnél érdemes olyan méretű eszközöket használni, melyek kapacitása nem túl nagy a tárolni kívánt adatokhoz képest. Ez jelentősen megkönnyíti a flash adattárolók fertőtlenítését.

Néhány mintaadat az USB kulcsok fertőtlenítésének időigényéhez:

2 GB méretű USB kulcs egyszeres felülírással (HMG Infosec Standard 5, Baseline) fertőtlenítve – 6 perc (USB2.0)

4 GB méretű USB kulcs egyszeres felülírással (HMG Infosec Standard 5, Baseline) fertőtlenítve – 12 perc (USB2.0)

8 GB méretű USB kulcs egyszeres felülírással (HMG Infosec Standard 5, Baseline) fertőtlenítve – 30 perc (USB2.0)

2 GB méretű USB kulcs négyszeres felülírással (U. S. Department of Defense Sanitizing) fertőtlenítve – 20-25 perc (USB2.0)

4 GB méretű USB kulcs négyszeres felülírással (U. S. Department of Defense Sanitizing) fertőtlenítve – 45-50 perc (USB2.0)

8 GB méretű USB kulcs négyszeres felülírással (U. S. Department of Defense Sanitizing) fertőtlenítve – 2 óra (USB2.0)

Megjegyzés: Az USB kulcsok és az egyéb flash adathordozók törlési sebessége függ az adathordozó típusától és a számítógép paramétereitől is, melynek segítségével a törlést elvégezzük.

Adattörlés a felhőben

Bizonyos esetekben szükség van arra, hogy az adatközpontban vagy szerverek logikai meghajtóin töröljünk adatokat.
Ez a Blancco LUN segítségével lehetséges.

Ilyen eset lehet például, ha szolgáltatóként adatközpontunkban tároljuk ügyfelünk adatait, de az ügyfél úgy dönt, hogy nem kívánja a továbbiakban igénybe venni a szolgáltatásunkat. Ebben az esetben hiteles jegyzőkönyvvel kell igazolnunk, hogy az adatokat megfelelő, minősített módszerrel töröltük.

Egy másik példa a recovery site tesztje: az adatok menthetőségét, a mentési eljárást tesztelve másolat készül az eredeti fájlokról. A mentési próba befejeztével biztosítanunk kell, hogy az ideiglenes másolat nem marad meg.

Szerverek proaktív fájltörlése

A szerverek esetében lehetőségünk van arra, hogy olyan szkripteket hozzunk létre, melyek segítségével a megadott fájlok vagy mappák előre meghatározott ütemezés szerint minősített módon törölhetőek.

Ez lehetőséget ad annak biztosítására, hogy ne tároljunk tovább olyan adatokat és adatbázisokat a szervereken, melyek kezeléséhez már nincs jogosultságunk.

Példa lehet erre egy internetes weboldal, melyen a vásárló megkezdi a regisztrációt, de a folyamat végén nem végzi el a szerződés megkötését. Így nem jön létre a szervezet és a vásárló között szerződés, még akkor sem, ha a vásárló saját maga kezdte el megadni személyes adatait. Amennyiben ezeket az adatokat a vásárló kényelme érdekében ideiglenesen tároljuk, erre egyrészt ki kell térnünk az adatkezelési szabályzatban, másrészt a kikötött idő után ezeket az adatokat törölnünk szükséges.

Egy másik példa az üzlethelyiségekben elhelyezett kamerás felvételek tárolása a szerveren – ezeket a felvételeket a kezelésükre engedélyezett idő után törölnünk kell.

Munkaállomások proaktív fájltörlése

A munkaállomások esetében is lehetőségünk van a proaktív fájltörlésre szkriptek segítségével. Meghatározható például, hogy a gép kikapcsolása előtt a Windows lomtár tartalma kerüljön felülírásra, vagy proaktív törlés alá vonhatóak mappák és fájlok.

5. Nem a minősített adattörlés körébe tartozó kérdések

Data Leak Prevention

A minősített adattörlés elsősorban nem adatokat, hanem adathordozókat véd, és biztosítja, hogy ne kerüljenek ki a szervezetből adatokat tartalmazó adathordozók.

A Data Leak Prevention (DLP), azaz az adatszivárgást megelőző rendszerek ezzel szemben adatokat, nem pedig adathordozókat védenek. Az internetes kijáratokon figyelve biztosítják például azt, hogy egy adott karaktersorozatot tartalmazó dokumentum ne hagyja el a szervezetet.

A Data Leak Prevention rendszerek ugyanakkor nem figyelik – hiszen nem is ez a dolguk –, hogy a leselejtezett adathordozókon milyen adatok maradnak.

Törlés vészhelyzetben

A minősített adattörlés az adathordozó teljes fertőtlenítésével jár, ami jellemzően hosszabb időt, tipikusan néhány órát vesz igénybe. Ez az időigény a fertőtlenítésre használt módszer jellegéből adódik, és nem rövidíthető le.

A merevlemezek fizikai megsemmisítése ezzel szemben néhány perces folyamat a Blancco Degausser segítségével, a megsemmisítéshez azonban a merevlemezt ki kell szerelni, majd be kell helyezni a degausserbe. A degausser ugyanakkor egyidejűleg egy merevlemezt képes befogadni.

A minősített adattörlés tehát semmiképpen, a minősített megsemmisítés pedig erős korlátokkal tekinthető vészhelyzeti intézkedésnek. Ugyanez igaz a távoli törlésekre is. Távoli törlést el tudunk indítani egy számítógépen vagy notebookon, de ez jellemzően órákat vesz igénybe, és egy külső személy által bármikor megszakítható (akár egyszerű áramtalanítással). A minősített adattörlés módszertana ezért mindig feltételezi, hogy mi kontrolláljuk az eszközt.

A vészhelyzetben alkalmazható eljárások a minősített adattörléssel szemben képesek arra, hogy nagyon egyszerű módon, néhány pillanat alatt zárolják vagy formázzák az eszközöket.

A zárolás ugyanakkor jellemzően valamilyen titkosítás segítségével történik, és a szükséges jelszó birtokában vagy nyers számítási erő alkalmazásával feloldható. A zárolt adathordozón – zárolva és titkosított módon – ott van minden adat. Ha a zárolt eszköz tehát egy kellő számítási erővel bíró szervezet kezébe kerül, a zárolás feltörésére van esély. Emellett meg kell jegyezni, hogy a zárolásra a szervezetek jellemzően olyan módszereket használnak, melyek forráskódját külső szervezet nem hitelesítette. Ezek a módszerek ezért elméletileg tartalmazhatnak olyan beépített hátsó kapukat, melyeket a gyártójuk önös érdekből vagy biztonsági okokból helyezett el bennük.

Beépült ügynök elleni védelem

A minősített adattörlés a legtöbb esetben nem nyújt védelmet a beépült ellenséges ügynök ténykedése ellen. A teljes fertőtlenítés és a fájltörlés értelme az önvédelem. Ezek a módszerek lehetőséget adnak a szervezetek számára arra, hogy teljes biztonsággal leselejtezzék és értékesítsék régi adathordozóikat.

A valódi minősítésekkel rendelkező adattörlési megoldásokat számos szervezet szakértői tették már próbára. A Blancco által fertőtlenített adathordozókról a NATO, az FBI, az Egyesült Államok Hadseregének szakemberei, valamint a világ számos más katonai és rendőri szervezete próbált már adatokat visszaállítani – mind sikertelenül. Nem véletlen, hogy a Blancco a világ legtöbb minősítéssel rendelkező adattörlési megoldása, és az sem, hogy a Blancco szoftvereit használja az Európai Unió Bizottsága és a NATO maga is.

A minősített adattörlés tehát teljes biztonsággal lehetővé teszi az adathordozók leselejtezését, és megelőzi az összes adatvédelmi incidens több mint 10%-át. Azonban, ahogyan ezt a fentiekben hangsúlyoztuk, nem nyújt védelmet a szándékos adatszivárogtatás ellen, így például egy beépült ügynök a saját USB kulcsára annyi másolatot csinál a védett dokumentumainkról, amennyit csak az USB tároló kapacitása lehetővé teszi, és amennyit mi megengedünk neki. Ellene más módszerekkel kell védekeznünk.

A minősített adattörlés azonban képes megelőzni azokat a szándékos adatszivárogtatásokat, melyek során a beépült ügynök egy leselejtezett adathordozóról szerezné meg az adatokat – például a megsemmisítésre való szállítás közben.

blancco
MINŐSÍTETT ADATTÖRLÉS

A Blanccóról

A Blancco a világ vezető gyártója a menedzselt, megbízható és minősített adattörlés területén. A nemzetbiztonsági szervezetek, a rendőrség, a pénzügyi szolgáltatók és a számítógép újrahasznosításával foglalkozó szervezetek első számú választása.

1997-ben alapított vállalatunk a legtöbb szakmai minősítéssel rendelkező hardveres és szoftveres adattörlési megoldásokat kínálja a világon. A Blancco menedzselhető adattörlési rendszerével nem csupán az adathordozók száz százalékos fertőtlenítése oldható meg, de kezelhető a teljes adattörlés folyamata is, beleértve az adattörlések visszakövethetővé és auditálhatóvá tételét.

Finn központú cégünk 14 saját irodát tart fent Európában, Észak- és Dél-Amerikában, Ázsiában és Ausztráliában. Szoftvereink és hardveres megoldásaink segítségével ügyfeleink mindennap több tízezer számítógépről törlik az adatokat.

A Blancco magyarországi képviseletét a V-Detect Antivírus Kft. látja el, a disztribúcióért pedig a Kvazar Micro CEE Kft. felel.

VDA Kizárólagos magyarországi képviselő a V-Detect Antivírus Kft.
www.v-detect.hu

KVAZAR-Micro MINDIG LÉPÉSELŐNYBEN Magyarországi disztribútor a Kvazar-Micro CEE Kft.
hwsw@kvazar-micro.hu

További információ: http://torles.hu