DATA ERASURE CASE STUDY

Az SSD-k biztonságos törlése akadályozza meg az adatok kiszivárgását

A csendes-óceáni és japán menedzserek 85 százaléka úgy véli, hogy a vállalat kitett egy belső támadásnak.

Egy átlagos adatszivárgás 274 millió japán jen (837 millió forint) kárt okoz.

Egy ellopott adat átlagosan 13 788 japán jen (42 ezer forint) kárt jelent a szervezetnek.

Az internetre csatlakoztatott eszközök (IoT, vagyis Internet of Things) elterjedésével a Samsung Japán is ellátta alkalmazottjait okoseszközökkel, melyek lehetővé teszik, hogy irodán kívül is hatékonyan dolgozzanak. A vállalat számára ez azt jelenti, hogy a munkatársaknak minden eszközük megvan arra, hogy optimális hatékonysággal és produktivitással dolgozhassanak. Másfelől viszont új veszélyek is keletkeznek: ezeken az eszközökön megjelennek a vállalati adatok, így megnőtt az adatszivárgás kockázata, amely pénzügyi és reputációs veszteséget okoz. Újrahasznosítás előtt az eszközöket megfelelően kell fertőtleníteni, hogy a vállalati adatok biztonságban maradjanak.

Samsung Japán

A Samsung Japán a Samsung Electronics félvezetőrészlegének helyi értékesítője, a vállalat félvezető-komponensek – memória, rendszer LSI, TFT-LCD és organikus EL termékek – értékesítésére szakosodott.

> **Mivel a teljes adattörlési folyamat automatizált, csökkentettük a kézi munkához kapcsolódó emberi hibákat, a felszabaduló erőforrásokat pedig egyéb dokumentumok készítésére és házon belüli auditokra fordítottuk. Becslésem szerint az adattörlések jelenlegi menedzselése a korábbi munkaórák egyhatodát igényli, tehát sikerült növelnünk a hatékonyságot.**
>
> **Hiroki Uno, Business Innovation Partner, Samsung Japán**

Kihívás

A high-tech félvezetőgyártó Samsung Japán SSD-vel ellátott saját márkás okoseszközöket (okostelefon, táblagép és PC) biztosított alkalmazottjainak. Ezek az eszközök gyakran olyan bizalmas adatokat tartalmaztak, mint titkosított technológiai leírások, valamint az ügyfelekre vonatkozó információk. A vállalatnak szüksége volt egy biztonságos és hatékony megoldásra a belső SSD-meghajtók teljes fertőtlenítésére. A korábbi adatfertőtlenítési folyamat során a törlés után az alkalmazottak manuálisan nyitották fel az eszközöket, és jegyezték le azok sorozatszámát, hogy auditálható módon történjen az adatfertőtlenítés. Ez a folyamat rengeteg emberi munkát és időt igényelt.

Megoldás

Annak érdekében, hogy a vállalatnál egy sor IT-eszköz – legyen az asztali számítógép, laptop, táblagép vagy okostelefon – SDD-meghajtójáról biztonságosan töröljék az adatokat, egy holisztikus adattörlési menedzsment megközelítést vezettek be.

A **Blancco Driver Eraser** megoldás segítségével a vállalat gyorsan és hatékonyan egyszerre több SSD-t töröl, különböző eszközökön egyidejűleg – anélkül, hogy a folyamat kárt okozna, vagy zavarná az operációs rendszert. A Samsung Japánnak egy hatékony módszerre volt szüksége a törlés tanúsítására is. A **Blancco Management Console** megoldással az összes adattörlési licenc egy helyről menedzselhető, ahogy a felhasználókat is erről a felületről lehet létrehozni vagy módosítani.
A tevékenységek felügyelete is központosított, ahogy a hamisítás ellen védett és auditálható törlési jegyzőkönyvek is innen kezelhetők.

A Blanccóról

A Blancco Technology Group megoldásai de facto szabványt jelentenek az adattörlés és mobileszközök diagnosztikájának területén. A **Blancco Drive Eraser** egy abszolút védelmi vonal a költséges adatszivárgások és a hatósági auditok ellen, a 100 százalékban megváltoztathatatlan, minősített adattörlési jegyzőkönyveinek segítségével. Minősített adattörlési megoldásainkat a világ 18 kormányzati testülete tesztelte, minősítette, elfogadta és javasolta. Nincs még egy olyan biztonsági vállalat, mely ezt a magas szintű megfelelőséget biztosítaná partnereinek a kormányzati ügynökségek, hatóságok és független tesztelőlaboratóriumok elvárásaival szemben.