

Quentyn Taylor, a Canon Europe információbiztonsági igazgatója

Vegye kezébe dokumentumai biztonságát!

[Az amerikai CBS televíziós csatorna egy közelmúltbeli vizsgálatában](#) "rávilágított" arra a tényre, hogy a multifunkciós nyomtatók olyan merevlemezeket tartalmaznak, amelyek tárolják az adatokat, ezért ezek az eszközök digitális időzített bombák.

Mára már az egyszerű irodai másolók is intelligens, hálózatra csatlakozó eszközzé fejlődtek, melyek egyre kifinomultabb módon igyekeznek megfelelni a felhasználók széles körű igényeinek. Ezek az eszközök olyan számítógép-kiszolgálók, melyek központi szolgáltatásként kínálják a nyomtatási funkciót, ezért a dokumentumkezelési feladataikhoz és az adatok tárolásához, merevlemezeket használnak. Az olyan kiegészítő funkciók, mint az e-mail, a nyomtatás, a másolás, a faxolás és a beolvasás fokozzák ugyan a [termelékenységét](#), de az adattovábbítás következtében biztonsági fenyegetést jelentenek. A vállalatok ismerik [multifunkciós nyomtatóik](#) képességeit és a potenciálisan érzékeny adatok mennyiségét, azonban valóban mindent megtesznek-e annak érdekében, hogy ezek ne kerüljenek illetéktelen kezekbe?

Hogyan segíthetnek ebben a gyártók, mint például a [Canon](#)?

Ne becsüld alá az ellenséget!

A vállalatok többnyire tisztában vannak az olyan külső fenyegetésekben rejlő veszélyekkel mint a vírusok vagy a hackertámadások, így ezek ellen általában megfelelő védelemmel rendelkeznek. Míg a szervezetek tűzfalak és más biztonsági megoldások segítségével kiemelten kezelik és folyamatosan fejlesztik a hálózati biztonság területeit, a kevésbé nyilvánvaló fenyegetéseket sokszor alábecsülik. Egy felügyelet nélküli nyomtató biztonsági szempontból pontosan olyan kockázatot jelent, mint egy felügyelet nélkül hagyott számítógép, hiszen az egyes üzleti osztályok rengeteg bizalmas vagy személyes információt küldenek át egy nyomtatón. Az illetéktelen kezekbe kerülő információk nem ritkán súlyos pénzügyi vagy jogi problémát okozhatnak egy szervezetnek, és akár a vállalatról a közvéleményben kialakult képet is veszélyeztethetik.

Az egyre nagyobb mennyiségű elektronikus adat munkahelyi tárolása egyre érzékenyebbé teszi a szervezeteket a biztonsági fenyegetésekkel szemben. A tartalomdigitalizálás és az elektronikus munkafolyamatok azonban olyan trendek melyek elősegítik az innovációt és növelik a hatékonyságot, így elterjedésük a közeljövőben várhatóan nem fog lelassulni.

Kié a felelősség? Az emberi tényező

Az informatikai osztályoknak az informatikai infrastruktúra biztonsága mellett felelősséget kell vállalniuk a [dokumentumok biztonságáért](#) is. Mivel az adatbiztonság prioritást élvez az üzleti életben a hálózatbiztonság az informatikai vezetők felügyelete alá tartozik, ám a nyomtatást érintő beszerzéseket gyakran más részlegek

vagy pénzügyi osztályok felügyelik. Ennek fő oka, hogy a beszerzési döntések általában az áron és nem a biztonságon alapulnak, ugyanakkor a multifunkciós nyomtatók is megfelelő biztonsági intézkedéseket igényelnének. Az informatikai személyzetén túl a bizalmas információkat használata vagy továbbítása esetén azonban az alkalmazottaknak is különösen ébernek kell lenniük. A Canon úgy véli, hogy a bizalom fontos, amikor az alkalmazottak vállalati információkhoz férnek hozzá, de a felügyelet még fontosabb.

A dokumentumkezelési folyamatok során a vállalatok számtalan megoldást alkalmazhatnak az információk kiszivárgásának korlátozására, ezért a megfelelő technológiát biztosító forgalmazóknak kiemelt szerepük van. A Canon például teljes körű dokumentum-, és hardverbiztonsági portfoliót kínál – többek között az adattitkosítást, a biztonságos adattörlést, a nyomtató merevlemezének eltávolítását és a hozzáférés-kezelést illetően is –, mely a dokumentum életciklusának minden szakaszában biztosítja az ügyfelek érzékeny adatainak védelmét. Megfelelő biztonsági intézkedések mellett így a kockázat is jelentős mértékben csökkenthető, azonban mindig az adott vállalat méret-, és biztonsági igényeihez illeszkedő, személyre szabott megoldásra van szükség.

Újrahasznosítás és leselejtezés

Az adatbiztonsági intézkedéseknek azonban a szervezetben mozgó dokumentumok védelmén túl ki kell terjedniük egy sokkal fontosabb területre: az újraértékesítés és leselejtezés során alkalmazott adatbiztonsági feladatokra is. A vállalatoknak vajon van válaszuk arra, mi történik ilyenkor a multifunkciós nyomtatóik merevlemezével? A bizalmas információk kezelése során ugyanis ez jelenti a legnagyobb kockázatot.

Általában senki nem fektet pénzt egy épület biztonsági rendszerébe úgy, hogy aztán éjszakára nyitva hagyja az ajtót. Egy számítógépet sem ajándékozunk csak úgy el vagy dobunk ki, miután nem használjuk többet. A legtöbb szervezet rendelkezik olyan irányelvekkel, amelyek biztosítják az adatok biztonságos törlését a forgalomból kivont számítógépek merevlemezeiről, ám a nyomtatók merevlemezén tárolt információkat csak a nyomtató élettartama során védik.

A Canon szerint az ügyfelek a megfelelő segítséggel jól kezelhetik ezt a problémát is.

A Canon szigorú irányelvekkel rendelkezik, amelyek csökkentik annak kockázatát, hogy a vásárló merevlemezén található adatok – az eszköz élettartama végén vagy a kölcsönzési idő lejártával – illetéktelen kezekbe kerüljenek. A Canon irányelvei biztosítják a merevlemezekben szereplő információk végleges törlését, vagy a merevlemez fizikai eltávolítását. A védelem ilyen magas szintű biztosításának érdekében a szervezeteknek mindig érdemes meggyőződniük arról, hogy újraértékesítés vagy újrahasznosítás esetén a merevlemezén tárolt összes adatot törölték.

Biztonsági keretrendszer

A szervezeteknél kiemelten fontos, hogy a jogosultsággal rendelkező alkalmazottak időben hozzájussanak az információkhoz, ám emellett feltétlenül szükség van egy olyan biztonsági keretrendszerre, amely kizárja, hogy illetéktelen személyek is hozzáférjenek a bizalmas adatokhoz. A gyártók felelőssége, hogy megfelelő biztonsági intézkedésekkel a multifunkciós eszközök minden szolgáltatása esetén biztosítsák az adatvédelmet.