RICOH
imagine. change.

Ricoh biztonsági megoldások

Segítünk megvédeni a vállalkozását

A kiberbiztonsági fenyegetések nagy veszélyt jelentenek a modern vállalatok túlélésére és sikerére. Mérettől függetlenül minden vállalat folyamatosan ki van téve a veszélynek, hogy olyan romboló hatású támadások áldozatává válik, mint például az adathalászat, a DDoS vagy a zsaroló programok. Ezeknek a támadásoknak a valós költségei csak milliókban fejezhetők ki. 2017-ben a Ponemon Institute megállapította, hogy az adatbiztonsági incidensek globális átlagköltsége 3,62 millió dollár volt. Ez a költség az elkövetkezendő években csak tovább fog növekedni, mivel az olyan szabályozások, mint a GDPR, súlyos bírságokkal fogják sújtani azokat a vállalatokat, amelyek nem képesek biztosítani rendszereik és adataik megfelelő védelmét. A súlyos büntetések elkerülése érdekében a vállalatoknak képesnek kell lenniük bizonyítani, hogy komolyan veszik az adatvédelmet. Ehhez a vállalat sérülékenységeit holisztikus megközelítéssel kell felderíteni.

A vállalatok kiberbiztonsági problémáit tovább bonyolítja a modern munkahelyek növekedése és digitalizálása, valamint az adatmennyiségek robbanásszerű növekedése is. A munkafolyamatok gyakran több eszközön, több hálózaton és több földrajzi területen zajlanak. Az adatok a vállalaton belüli átvitel során vannak kitéve a legnagyobb veszélynek. Éppen ezért, az adatátvitel minden szakaszában ügyelni kell a megfelelő védelemre. Figyelembe véve az ezzel járó biztonsági kockázatot, a modern vállalatok már nem működhetnek biztonságos dokumentum- és adatkezelő rendszerek nélkül. Ugyanakkor az irodai nyomtatók és multifunkciós eszközök tulajdonságainak száma az utóbbi években megtízszereződött. Ma már ezeken az eszközökön végzik az üzleti adatok bevitelének, kinyomtatásának, átvitelének és tárolásának jelentős részét. Ez teszi őket a munkahely egyik legveszélyesebb, mégis gyakran figyelmen kívül hagyott kockázati tényezőjévé.

Bár számos cég állítja, hogy biztonsági funkciókkal látja el az eszközeit, a Ricoh immár évtizedek óta fejleszti a biztonságos munkahelyi megoldásokat és szolgáltatásokat. Nyomtatóink például több mint 20 éve rendelkeznek biztonságos merevlemez-felülírási képességekkel.

Teljes digitális munkahelyi portfóliónk a biztonságra épül. Jelenleg több mint 4 millió irodai termékünk van használatban világszerte. Minden egyes készülékünk és az általunk telepített összes szolgáltatás beépített biztonsági funkciókkal rendelkezik. Számos készülékünkben pedig kizárólagosan Ricoh-alapú operációs rendszert alkalmazunk. Ez a biztonsági funkcióink egyik fő eleme, amely az operációs rendszerek szélesebb körét megcélzó támadások ellen véd azáltal, hogy a felhasználó kezébe adja az irányítást, és elszigeteli az eszközt a fenyegetésektől.

A Ricoh az egész világon egységes szolgáltatási és támogatási rendszert biztosít ügyfelei számára, amely garantálja a fenyegetésekkel kapcsolatos információk hatékony megosztását és a megfelelő intézkedéseket. Minden nyomtatónk rendelkezik az IEEE 2600 tanúsítvánnyal, a Ricoh pedig az IEEE Standards Association egyik vezető tagja és kulcsszereplője. A Ricoh emellett ISO 27001 tanúsítvánnyal is rendelkezik, és elkötelezte magát amellett, hogy a jövőben is megfeleljen ennek az információbiztonsági irányítási rendszernek. Termékfejlesztésünk során az ügyfelek üzleti igényeire és a biztonsági aggályaira összpontosítunk a globális és ügyfélközpontú innovációs programjainkon keresztül.

A bevált kiberbiztonsági gyakorlatok szigorú követelményeinek teljesítése érdekében a biztonsági funkciókat a Ricoh portfóliójának minden készülékébe és szolgáltatásába előre tervezett módon építjük be, soha nem utólagos kiegészítésként. Hisszük, hogy a sérülékenységek ilyen átfogó szemlélete a modern üzleti életben a túlélés elengedhetetlen feltétele.

BIZTONSÁGI KIHÍVÁSOK AZ ÜGYFELEKNÉL

TRENDEK: Az adatmennyiségek növekedésével a sebezhetőség, a támadások és a büntetések kockázata is emelkedik.

Digitális munkahelyek biztonságossá tétele és megerősítése

A Ricoh arra törekszik, hogy a világ minden pontján lehetővé tegye a biztonságosan végezhető digitális munkát. Ez a modern, digitális gazdaságban hozzáadott értéket jelent a hagyományos irodák keretein kívül is. A távolról is elérhető irodák és a távmunka nagy rugalmasságot és hatékonyabb munkavégzést jelentenek a mindennapi feladatok során. A vállalatok így jobban meg tudnak felelni ügyfeleik elvárásainak és a szolgáltatási követelményeknek.

A hálózat végpontjain végzett munka ugyanakkor a legnagyobb üzleti kockázatot is jelenti. A munkavállalók által létrehozott adatok, valamint az adatok rögzítéséhez használt távoli eszközök megfelelő védelmet igényelnek. Az alkalmazottak gyakran több hálózaton és földrajzi területen dolgoznak egyszerre, ami tovább bonyolítja a helyzetet. A GDPR-hez hasonló szabályozások előírják, hogy a vállalkozások bizonyíthatóan gondoskodjanak az adatok védelméről azok teljes élettartama során, különben súlyos büntetésekre számíthatnak. A munkahelyek fejlődésével és a digitális munkafolyamatok terjedésével az üzleti adatok életciklusa egyre bonyolultabbá válik. Vizsgáljuk meg ezt a kérdést lépésről lépésre.

Az első lépés az adatbevitelhez és az adatrögzítéshez használt eszköz, amely a Ricoh által kínált biztonság egyik alapvető eleme. Innen az adatokat hálózatokon keresztül kell elküldeni és biztonságosan tárolni. Ebben a szakaszban az adatok integritásának megőrzése döntő fontosságú. A Ricoh rendszerei korlátozzák a felhasználói hozzáférést az eszközökhöz és a hálózati funkciókhoz annak érdekében, hogy az adatokhoz ne lehessen illetéktelenül hozzáférni a küldés vagy a tárolás során. Ilyen funkció például a hozzáférés irányítása, a titkosítás és a másolásvédelem. Ezt mi Kontrollnak hívjuk.

A tárolt dokumentumoknak azonban könnyen hozzáférhetőnek is kell lenniük a vállalaton belül a jogosultak számára. Ettől a rendelkezésre állástól függ az információk hatékony lehívása és megjelenítése. Az adatelemzés a jól működő digitális munkahely létfontosságú eleme. Az elemzés lehetővé teszi a vállalat hatékony áttekintését, az értékesítési osztálytól kezdve a HR-ig. A jogosultságkezelő infrastruktúra eszközei gyors hozzáférést biztosítanak, függetlenül a felhasználó helyétől vagy az eszköztől. Alapvető fontosságú,

hogy a biztonsági protokollok ne akadályozzák az innovációt vagy a funkcionalitást, illetve ne váltsanak ki ellenállást a munkavállalókban. Ezt a biztonsági elemet Megőrzésnek hívjuk.

Végül az adatokat biztonságos, ellenőrizhető módon kell megsemmisíteni. Ez a lépés elengedhetetlen a szabályozási követelményeknek való megfeleléshez, és minimálisra csökkenti a későbbi adatlopás vagy adatvesztés kockázatát. Ez a folyamat valójában a dokumentum teljes élettartamára vonatkozik, nemcsak a végleges törlésére. A fájlok nyomtatásakor a multifunkciós nyomtatók (MFP-k) merevlemezén látens memóriakép marad, amelyet felül kell írni, hogy megakadályozzuk a jogosulatlan hozzáférést. A Ricoh adatmegsemmisítési szolgáltatásai közé tartozik a merevlemez adattisztítása, a memória kiürítése, a kinyomtatatlan fájlok törlése és a kijelentkezési törlés, amelyek megakadályozzák az érzékeny információk illetéktelenek általi összegyűjtését a dokumentum „digitális lábnyomai" alapján. Ez a fázis a Megsemmisítés.

A munkahelyi adatok hatékony, teljes életciklusra vonatkozó védelme érdekében a Ricoh az adatvédelemre és biztonságra vonatkozó úgynevezett „CIA" elveket alkalmazza: bizalmasság, rendelkezésre állás és integritás (Confidentiality, Availability, Integrity). Ezek a készülékeink és megoldásaink kialakításának vezérelvei, hogy minden előírásnak és szabványnak meg tudjunk felelni. Ez a megközelítés lehetővé teszi a munkahelyi innovációt és a növekedést, miközben hatékony és biztonságos folyamatokat biztosít.

A RICOH BIZTONSÁGRA VONATKOZÓ ELVEI

Az adatvédelemre és biztonságra vonatkozó „CIA" alapelveket követjük: bizalmasság, integritás és rendelkezésre állás

A biztonság a génjeinkben van. A Ricoh minden készüléke és szolgáltatása integrált biztonsági funkciókkal rendelkezik

A Ricoh minden igényt kielégítő biztonsági készülékeket és szolgáltatásokat kínál, amelyek a dokumentum teljes élettartama során gondoskodnak a megfelelő védelemről.

A következőkben részletesebben is megvizsgáljuk az egyes lépéseket: a kontrollt, a megőrzést, a megsemmisítést és a támogatást.

A DIGITÁLIS MUNKAHELYI BIZTONSÁG NÉGY SZAKASZA

1 KONTROLL

A hatékony kontroll alapvető fontosságú az adatok titkosságának és integritásának megőrzése szempontjából. Az üzleti információk nagyon értékesek, ezért védelemre szorulnak. A mai hardvereszközök olyan információs végpontok, amelyeken keresztül az üzleti adatok illetéktelen kezekbe kerülhetnek. A Ricoh ezért számos különféle felhasználói hitelesítő és eszközkezelő megoldást alkalmaz az üzleti adatok felügyelete és védelme érdekében. Ezek a fizikai eszközök beállításaira vonatkoznak, amelyek lehetővé teszik és korlátozzák bizonyos funkciók és adatok elérését. Az irodákban használt multifunkciós nyomtatókon áthaladó adatokhoz való felhasználói hozzáférés korlátozása a dokumentumok védelmének egyik alappillére. A kontroll emellett a kártevő szoftverek elleni védelmet is magában foglalja, amelyet a Ricoh háromrétegű módszerrel valósít meg az eszközök firmware-én.

Illetéktelen másolás elleni védelem

Az illetéktelen másolás megakadályozása érdekében a Ricoh elegáns megoldást kínál a nyomtatott dokumentumok védelméhez. A másolásvédelmi funkció a háttérbe illesztett speciális, láthatatlan mintákkal nyomtatja ki, vagy másolja le a dokumentumokat. Ha a kinyomtatott vagy lemásolt dokumentumot fénymásolják és/vagy beszkennelik, a másolatokon láthatóvá válnak a beillesztett minták. A másolásvédelmi modul lehetővé teszi az MFP számára a beillesztett minták felismerését és a fénymásolt kép szürke színnel való kitakarását az adatkiszivárgás megakadályozása érdekében. Ez a funkció különösen a bizalmas információk nyomtatásakor hasznos. A bizalmas információk másolásának korlátozása elősegíti az ilyen típusú adatok bizalmasságának megőrzését.

Zárolt nyomtatás

A számítógépről érkező dokumentumok az MFP merevlemez-meghajtóján tárolhatók. A Ricoh zárolt nyomtatás funkciójával a dokumentum küldésekor a felhasználó jelszót ad meg, amit nyomtatás előtt az MFP-n kell megadni. Mivel a dokumentum nem kerül kinyomtatásra, amíg a tulajdonos fizikailag az eszköznél nem tartózkodik, a zárolt nyomtatás garantálja, hogy a tulajdonos egy pillanatra se veszítse el a dokumentum fölötti kontrollt.

Továbbfejlesztett adatrögzítési biztonság

A Ricoh továbbfejlesztett adatbeviteli megoldásainak széles portfóliója különböző titkosítási és visszafejtési rétegeket kínál az adatrögzítési folyamat minden szakaszában. A rendszergazdák felhasználónként vagy csoportos hitelesítő adatok alapján is szabályozhatják a feldolgozási sorokhoz való hozzáférést. További biztonsági réteget jelent az SSO (egyszeri bejelentkezés) keretrendszerhez használt Security Assertion Markup Language (SAML), a személyazonosság ellenőrzése (PIV) és a nyilvános kulcsú infrastruktúrán (PKI) alapuló titkosítás.

Beágyazott hitelesítési módszerek

A Ricoh készülékeiben használt eszközhozzáférési és hitelesítési protokollok központilag kezelhetők. A rendelkezésre álló módszerek közé tartozik az azonosító kártya, a PIN-kód, a hálózati bejelentkezés vagy ezek kombinációja. A többtényezős hitelesítés nagyobb biztonságot jelent, ugyanakkor lassíthatja a munkát. Az egyszeri bejelentkezés (SSO) segít abban, hogy a felhasználók zökkenőmentesen férjenek hozzá több eszközhöz. Emellett a Ricoh Quick Authentication kártyaalapú hitelesítési szoftvert minden eszközünkön előre telepítettük, így a felhasználók ezzel a módszerrel is könnyen hozzáférhetnek a dokumentumaikhoz. Az NFC-olvasó/-író használata jelentősen leegyszerűsíti a felhasználó bejelentkezési folyamatát, miközben hatékonyan biztosítja az MFP-hez való hozzáférést. Ez a hozzáférési forma a létező MFP-jogosultságokkal együtt is működik, így az eszközfunkciókhoz való felhasználói hozzáférés az ügyfél által meghatározott módon korlátozható.

Streamline NX (SLNX)

A Ricoh Streamline NX platformjának eszközkezelő modulja a hálózatokon lévő eszközök kezelésére és felügyeletére szolgál. A szoftver lehetővé teszi a rendszergazdák számára, hogy előre konfigurált sablonok és egyedi paraméterek használatával tekintsék meg vagy konfigurálják az eszközök biztonsági beállításait. Az alapvető biztonsági opciók között megtalálható többek között a protokollok engedélyezése/letiltása, az IP-cím konfigurálása, a rendszergazdai felhasználónevek kezelése, a riasztásokhoz használt e-mail-címek megadása és a titkosítási beállítások kezelése. Az SLNX emellett arra is képes, hogy észlelje azokat a nyomtatókat, amelyek nem felelnek meg az ügyfél által megadott előírásoknak.

Az eszközök kártékony szoftverek elleni védelme

A Ricoh háromrétegű módszert alkalmaz az eszközök kártékony szoftverek elleni védelméhez. A Ricoh-eszközöket csak a Ricoh gépi kódjával vagy operációs rendszerével lehet működtetni. Másodszor, a rosszindulatú manipulációk megakadályozása érdekében a firmware-frissítéseket kizárólag a Ricoh gépi kódján lehet megírni és jóváhagyni. Végezetül, minden firmware-frissítéshez a Ricoh digitális aláírása szükséges. Ennek a háromlépéses módszernek köszönhetően a nem jóváhagyott firmware-t nem lehet betölteni a Ricoh eszközökön, így a kártékony programok, a kémprogramok és a vírusok hatékonyan kiküszöbölhetők.

Fizikai dokumentumbiztonság

A legjobb biztonsági gyakorlatok nem mindig bonyolultak. Az irodákban mindig nagy a nyüzsgés, és a kinyomtatott dokumentumok komoly üzleti kockázatot jelentenek mind a lopás, mind a munkavállalói gondatlanság tekintetében. A Ricoh számos kiegészítő fizikai védelmi lehetőséget kínál a nyomtatott dokumentumokhoz való jogosulatlan hozzáférés megakadályozására. A papíradagoló lezárásával megakadályozható, hogy az érzékeny dokumentumok, például az orvosi vények sablonjai illetéktelen kezekbe kerüljenek. A kábelcsatlakozók vakdugós lezárásával pedig megelőzhető a vállalaton belüli illetéktelen hozzáférés. A biztonságos dokumentumkiadási megoldás (Print-to-me) biztosítja, hogy a dokumentumok kinyomtatására csak a tulajdonos jelenlétében kerülhessen sor, így a nyomtatványokat biztosan nem felejtik majd a nyomtatóban.

2 MEGŐRZÉS

Az új és meglévő jogi előírásoknak megfelelően a vállalkozásoknak biztosítaniuk kell az információk bizalmasságát, hogy megakadályozzák azok ellopását vagy kiszivárgását, valamint az adatok integritását, hogy ne lehessen őket illetéktelenül módosítani. Ezért fontos, hogy a vállalkozások korlátozzák az érzékeny dokumentumokhoz való hozzáférést. Ezzel megakadályozható a jogosulatlan módosítás és a hamisítás. A hozzáférés korlátozása védelmet nyújt a vállalaton belüli célzott vagy alkalmi fenyegetések ellen is.

A mobil munkavégzés minden kiberbiztonsági helyzetet még összetettebbé tesz. Kiegészítő védelmi intézkedésekre van szükség, hogy a fájlmegosztás bárhonnan biztonságosan használható legyen. Ezeknek a fájloknak ugyanolyan biztonságban kell lenniük a hálózaton és az eszközökön történő tranzakciók során, mint a tároláskor. Az erős titkosítási technológia képes hatékonyan nyomon követni és megvédeni az adatokat azok teljes életciklusa során. Ez egyrészt vonatkozik a dokumentumokra, de más fontos biztonsági elemekre is kiterjed, például a tárolt jelszavakra, a makróbeállításokra és a címjegyzékekre. A hálózatra esetleg bejutó támadóknak a titkosított adatokkal sokkal nehezebb dolguk van, ha használható információt szeretnének kinyerni, hiszen a titkosítás ilyenkor is megőrzi az adatok integritását.

A folyamatos rendelkezésre állás számos iparágban nélkülözhetetlen. Az olyan előre nem látható események, mint a természeti katasztrófák közvetlen üzleti kockázatot jelentenek. A papír alapú dokumentumok ilyen esetben különösen nagy veszélynek vannak kitéve. A biztonságos, felhő alapú digitalizált dokumentumtár erős védelmet nyújt a természeti és ember által okozott katasztrófákkal szemben. Ugyanakkor, a digitális adatok megőrzése érdekében megfelelő biztonsági intézkedéseket kell hozni.

Elengedhetetlen adattitkosítás

Az eszközökön áthaladó adatok védelme érdekében a Ricoh MFP-kre merevlemezére küldött vagy ott tárolt bármely adathoz engedélyezhető a titkosítás. A beépített szoftveropciók garantálják a végponttól végpontig terjedő titkosítást a beolvasott és kinyomtatott fájlokhoz a felhasználó PKI-kulcsa révén. Ez védelmet nyújt az úgynevezett „közbeékelődéses" támadásokkal szemben az ügyfél informatikai környezetében.

A biztonság növelése érdekében a Ricoh Adatfelülírási Biztonság Rendszere (DOSS) folyamatosan felül is írja a nyomtatási adatokat, amit részletesebben később, az adat-életciklus „Megsemmisítés" szakaszában tárgyalunk.

A BIOS és az operációs rendszer védelme

A Ricoh multifunkciós nyomtatók egy úgynevezett megbízható platform modult (Trusted Platform Modul – TPM) alkalmaznak, amely egy szabotázs-biztos hardveres biztonsági modul. A TPM kriptográfiai funkciókat végez, és biztonságosan tárolja a titkosítási adatokat. A Ricoh a TPM segítségével tárolja a gyökér titkosítási kulcsát, amely a merevlemez adattitkosítási kulcsát és az MFP-k digitális tanúsítványát védi. Ezen kívül lehetővé teszi a rendszergazdák számára, hogy biztonságos rendszerindítást végezzenek az MFP-firmware hitelességének ellenőrzésével.

Firmware-ellenőrzés

A gyökér kulcsa és a titkosítási funkciók mindig a TPM-ben találhatók, és nem módosíthatók a tűzfalon kívülről, ami segít megakadályozni a készülékeinkkel való visszaélést vagy a rosszindulatú manipulációt. Ez az eljárás biztosítja az MFP-firmware, az eszközidentitás és merevlemez-biztonság magas szintű ellenőrzését. Ez újabb jó példa arra, hogy a Ricoh MFP eszközeiben az ügyfelek biztonsága mindig kiemelt szerepet kap.

Jelszókezelés

A Ricoh eszközök több rendszergazdai felhasználóval is konfigurálhatók, különböző szerepkörökkel és eltérő jelszavakkal. Ezeknek a felhasználóknak a jelszavai távolról, webes adminisztrációs eszközökkel is beállíthatók, és rendszeresen ellenőrizhetők. Ez lehetővé teszi a feladatok elkülönítését, ami számos üzleti szabályzatban fontos szempont.

Felhasználói hozzáférés korlátozása

A Ricoh felhasználó-kezelő eszköze lehetővé teszi a rendszergazdák számára a felhasználói hozzáférési jogosultságok korlátozását. A rendszergazda például adott felhasználókra korlátozhatja az MFP regisztrált címjegyzékének elérését. Ezzel megakadályozható a személyes adatokhoz és az irodai eszközökön tárolt nyilvántartásokhoz való jogosulatlan hozzáférés.

Felhasználó kizárása funkció

Ha a bejelentkezési folyamat során többször egymás után hibás jelszót adnak meg, a Ricoh MFP képes megállapítani, hogy jelszófeltörési kísérletről van-e szó. Ez aktiválja a kizárási funkciót, amely blokkolja a szóban forgó felhasználói nevet. A blokkolt felhasználói névvel még akkor sem lehet belépni, ha a megfelelő jelszót adják meg hozzá. A kizárás csak bizonyos idő elteltével, illetve rendszergazdai beavatkozással oldható fel, ami hatékonyan távol tartja a potenciális támadókat.

3 MEGSEMMISÍTÉS

A biztonságos adatmegsemmisítés az átfogó kiberbiztonsági védelem alapvető része. Könnyen beleeshetünk abba a csapdába, hogy a felelősségünket megszűntnek véljük, miután az adatok elhagyták a vállalatot. Azonban számos előírás értelmében az adatmegsemmisítésnek mindenre kiterjedő folyamatnak kell lennie, amely kizárja a későbbi lopás vagy visszaélés kockázatát. Amíg ez nem igazolható hitelt érdemlő módon, addig a vállalat adatokért való felelőssége nem szűnik meg.

Az életciklusuk végén visszaküldött irodai eszközök gyakran fel nem ismert kockázatot jelentenek üzleti adatok biztonsága szempontjából. A Ricoh tanúsított és nyomon követhető szolgáltatást kínál az életciklusuk végén járó nyomtatókon tárolt adatok törlésére. Ez magában foglalja az olyan, gyakran figyelmen kívül hagyott elemeket is, mint a mentett hálózati beállítások, a felhasználói adatok, a merevlemez-adatok vagy akár az eszközön maradt matricák. Ennek elmulasztása esetén jelentősen megnő a kockázata a bizalmas vállalati és személyes adatok illetéktelen kezekbe kerülésének. Ugyanakkor a jogszabályoknak való megfelelés érdekében ezt a folyamatot már az eszköz élettartama során is rendszeresen el kell végezni. Ezzel biztosítható, hogy a vállalatok mindig magas szintű kontrollt gyakoroljanak a felelősségi körükbe tartozó adatok fölött.

Kép felülírása: Adatfelülírási biztonsági rendszer (DOSS)

Az MFP eszközök merevlemezei a dokumentumadatokról látens lemezképet tárolnak memóriájukban, hogy hatékonyabbá tegyék a munkafolyamatok feldolgozását. A Ricoh által fejlesztett Adatfelülírási biztonsági rendszer biztosítja az ilyen lemezképek folyamatos felülírását a következő feladat megkezdése előtt. Ha bárki ártó szándékkal férne hozzá a merevlemezhez, akkor sem lenne képes kinyerni a korábbi feladatokból visszamaradt adatok „lábnyomát". A Ricoh büszke arra, hogy immár több mint 20 éve kínálja ezt a jól bevált biztonsági funkciót.

Adattisztítás az eszköz élettartamának végén

A Ricoh az MFP-k és nyomtatók élettartamának végén igénybe vehető teljes körű adattisztítási szolgáltatást kínál, amellyel az eszközök összes memóriamodulja és lemeze helyreállíthatatlan módon, véglegesen törölhető az iparágban elfogadott biztonsági megoldásokkal. A Ricoh informatikai szolgáltatásai között megtalálható a mindenre kiterjedő ártalmatlanítás is, amelynek része a többszintű minősített adattörlés.

Merevlemezek cseréje és eltávolítható tárolók

A Ricoh olyan merevlemez-ártalmatlanítási szolgáltatást is kínál, amely lehetővé teszi az ügyfelek számára, hogy megtartsák a merevlemezüket, amelyet egy új, üres merevlemezzel helyettesítünk, amikor a bérelt készüléket visszaadják. Így a vállalatok teljes körű és bizonyítható kontrollt gyakorolhatnak adataik fölött.

4 TÁMOGATÁS

A vállalatok növekedésével egyre nagyobb az eszközök és hálózatok közötti kapcsolatok száma is. A vállalatoknak olyan stratégiákra van szükségük, amelyek biztosítják, hogy az infrastruktúra növekedése ne járjon biztonsági kockázatokkal. Ismerniük kell rendszereik gyenge pontjait, és megfelelő intézkedésekkel kell védekezniük a célzott és az alkalmi támadások ellen.

Az üzleti infrastruktúra elemzéséhez és a sebezhetőségek azonosításához gyakran tapasztalt IT-biztonsági szakértőre van szükség. Sok vállalkozás nem engedheti meg magának a számítógépes biztonsági környezet kezelését belső informatikai személyzetet alkalmazva. A magas költségek és a nehezen megoldható hiányosságok miatt sok vállalkozás tehetetlenül néz szembe a kihívásokkal.

A Ricoh informatikai támogató szolgáltatása informatikai beszerzési és konfigurációs szolgáltatásokat, valamint távfelügyeleti, ügyfélszolgálati és átállás menedzsment szolgáltatásokat kínál a kiberbiztonság javítása érdekében. A kiberbiztonság megteremtéséhez az üzleti kockázatok teljes körű megértésére van szükség. A Ricoh Security Incident Response Team (SIRT) biztosítja, hogy a fenyegetettséggel kapcsolatos létfontosságú információk a világ minden táján eljussanak az ügyfelekhez, és hatékonyan összehangolja a szükséges válaszlépéseket.

Infrastruktúra-biztonsági értékelés

A Ricoh Streamline NX (SLNX) eszközkezelő funkciója felbecsülhetetlen biztonsági szabályzat-auditot tesz lehetővé. Az SLNX olyan funkciókat biztosít, amelyek lehetővé teszik az informatikai szakemberek számára, hogy a vállalati szabályzat alapján állítsák be az eszközöket, csoportosan telepítsék a kívánt konfigurációkat és vizuális jelentés formájában elemezzék a beállításokat. Az SLNX arra is képes, hogy figyelmeztesse a vezetőséget, ha egy eszköz nem felel meg a vállalati irányelveknek.

A nyomtatási biztonság optimalizálása

A Ricoh teljes körű nyomtatási biztonságot optimalizáló (PSO) szolgáltatást nyújt professzionális és koordinált tanácsadással az eszközök biztonsági hiányosságainak azonosítására. Web alapú, grafikus telepítővel rendelkező eszköz, amely segít áttekinteni a jelenlegi állapotot, továbbá lehetővé teszi a Ricoh számára, hogy ajánlatokat tegyen a kockázatok csökkentése érdekében.

Termékbiztonsági incidensekre reagáló csapat (PSIRT)

A Ricoh aktív reagálását új fenyegetések esetén, valamint a hatékony ellenintézkedések kifejlesztését a Ricoh termékbiztonsági incidensekre reagáló csapata (PSIRT) irányítja. Ez a Ricoh-program biztosítja, hogy teljes termékcsomagunk (hardver és szoftver) folyamatosan frissített állapotban legyen, és megfelelő védelemben részesüljön az újonnan azonosított fenyegetésekkel és sebezhetőségekkel szemben. Így globális szinten is képesek vagyunk fenntartani szolgáltatásaink egységesen magas színvonalát, ezen felül minimálisra csökkentjük a sebezhetőségi problémák Ricoh termékekre gyakorolt hatását.

Támogató dokumentáció

Az előkészítés és a képzés minden kiberbiztonsági rendszer kulcsfontosságú eleme. Az ügyfél számára biztosítani kell a biztonsági mentések dokumentációját, a felhasználói kézikönyveket, a megfelelő biztonsági tanulmányokat és a képzéseket. A kiberbiztonsági környezet számos eleméhez hasonlóan az igazolható megfelelés döntő jelentőségű, és ez a dokumentáció kulcsszerepet játszik a vállalat működésében.

HOGYAN SEGÍTHET A RICOH?

A Ricoh az iparágban vezető biztonsági megoldásokat biztosít a teljes informatikai és nyomtatási környezethez, mely részben a piaci körülményekben bekövetkező változások alapos megértésének és a fejlesztéseknek köszönhető. Megoldásainkat úgy tervezzük, hogy az adatok teljes életciklusa során védelmet nyújtsanak az információk számára, és maximális mértékben lefedjék az említett négy adatbiztonsági területet.

Szakértőink elemzik a piaci igényeket, beleértve azokat az iparági követelményeket is, amelyekhez új megoldásokat lehet létrehozni, illetve a már meglévők testre szabhatók.

Elkötelezettek vagyunk amellett is, hogy fejlesszük a belső lehetőségeinket, és biztonságorientált megoldásokat nyújthassunk.
Ennek érdekében olyan dedikált csapatokat hoztunk létre a szolgáltatásfejlesztési részlegünkben, amelyek kifejezetten az új szabályozási, kockázatkezelési, megfelelési, valamint kiberbiztonsági szolgáltatások fejlesztésére összpontosítanak.

Felhasználói hitelesítés és jogosultságok

- Zárolt nyomtatás
- Alapkiépítésben elérhető beágyazott szoftver a hitelesítéshez
- Felhasználói hitelesítés / hozzáférés korlátozása
- Egyszeri bejelentkezés
- Több rendszergazda szerep
- Jelszavas PDF-védelem (jelszó a beolvasott dokumentumhoz)
- Jogosulatlan másolás elleni védelem
- IP-tartomány szerinti hozzáférés-vezérlés
- Biztonságos eszköz- és nyomtatáskezelés
- PKI (nyilvános kulcsú infrastruktúra) / okos kártya támogatása
- Biztonságos nyomtatás (print2me / zárolt nyomtatás)

Az eszközök kártékony szoftverek elleni védelme

- Szerverek
- Kártékony szoftverekre nem vagy kevésbé érzékeny
- SOP – az Android fokozott biztonságú verziója
- Az operációs rendszer csak Ricoh által alkalmazott verziója (gépvezérlő nyelv) az MFP eszközökhöz
- 3 rétegű megközelítés – digitális aláírás, Ricoh eszközön keresztüli letöltés, speciális vezérlési nyelv használata

Merevlemezek ártalmatlanítása

- Merevlemez-ártalmatlanítás, kép felülírása
- Teljes adattisztítási szolgáltatás
- Az eszköz élettartama végén nyújtott szolgáltatás: adatok megsemmisítése a memóriamodulokban és tárolókon

Eszközkezelés

- Kvótabeállítás / fiók korlátozása
- DMNX – központi biztonságkezelés, jelszókezelés, megfigyelés és riasztás

A BIOS és az operációs rendszer védelme

- Biztonságos rendszerindítás a megbízható platform modul (TPM) használatával

Kép felülírása és eltávolítható adathordozók

- Adatfelülírási biztonsági rendszer (DOSS)
- Eltávolítható merevlemez

Adattitkosítás

- Merevlemez-titkosítás TPM-en keresztül
- Titkosítási kulcsok TPM-en keresztül
- Nyomtatási és szkennelési fájlok végponttól végpontig történő titkosítása PKI kulcs használatával
- FIPS-tanúsítvánnyal rendelkező merevlemez (Federal Information Processing Standards)
- Végponttól végpontig terjedő titkosítás a nyomtatáshoz
- Végponttól végpontig terjedő titkosítás a szkenneléshez

Firmware-frissítések és jelszókezelés

- Távoli jelszóellenőrzés
- Felhasználó kizárási funkció
- Firmware-ellenőrzés TPM-en keresztül

Megfelelés az iparági szabványoknak

- ISO 27001 tanúsítvány
- IEEE 2600.2 tanúsítvány adott termékekhez
- ISO 15408 tanúsítvány adott termékekhez
- Biztonsági dokumentáció és képzés

A RICOH TÖBBSZINTŰ ESZKÖZBIZTONSÁGI MEGKÖZELÍTÉSE

Kétségtelen, hogy a multifunkciós készülékek gyártójának szerepe ma már messze túlmutat a hardvereszközök szállításán, és az adatkezelés területét is lefedi. Az MFP-k funkciói között a többcsatornás bemenetekről történő adatgyűjtés, a rögzített adatok osztályozása, a munkafolyamat-integráció, valamint a biztonságos tárolás és analitika egyaránt megtalálható. A szigorú, több jogi keretrendszert is lefedő szabályok és az adatmegőrzési követelmények útvesztőjében – amelyet a belső és külső, adatvesztéssel, adatmegsemmisítéssel vagy illetéktelen manipulációval fenyegető kockázatok tesznek még átláthatatlanabbá – többszintű megközelítést alkalmazunk az eszközbiztonság terén annak biztosítása érdekében, hogy az MFP és a hozzá kapcsolódó rendszerek a lehető leghatékonyabb védelmet nyújtsák a felhasználóknak.

1. Az eszköz

Minden Ricoh modell középpontjában az eszköz áll. Az eszközöket a biztonsági követelmények maximális szem előtt tartásával tervezzük, gyártjuk és valósítjuk meg. A kizárólag csak a Ricoh által használt operációs rendszer nem osztozik azokon a sebezhetőségeken, amelyek számos kereskedelmi forgalomban kapható operációs rendszerben jelen vannak, és készülékeink az IEEE2600.2 szabvány szerinti tanúsítvánnyal rendelkeznek. A merevlemez-titkosítás és a képfelülírási funkció garantálja a feldolgozott adatok titkosságának megőrzését.

2. Felhasználói felület okos kezelőpanellel (SOP)

Az MFP-hez hasonlóan az SOP is a Ricoh exkluzív operációs rendszerét használja. Nem telepítünk felesleges összetevőket, és a gyökérszintű hozzáférés nem lehetséges. A Ricoh mindent megtett annak érdekében, hogy az okos kezelőpanel használata ne veszélyeztesse az eszköz biztonságát.

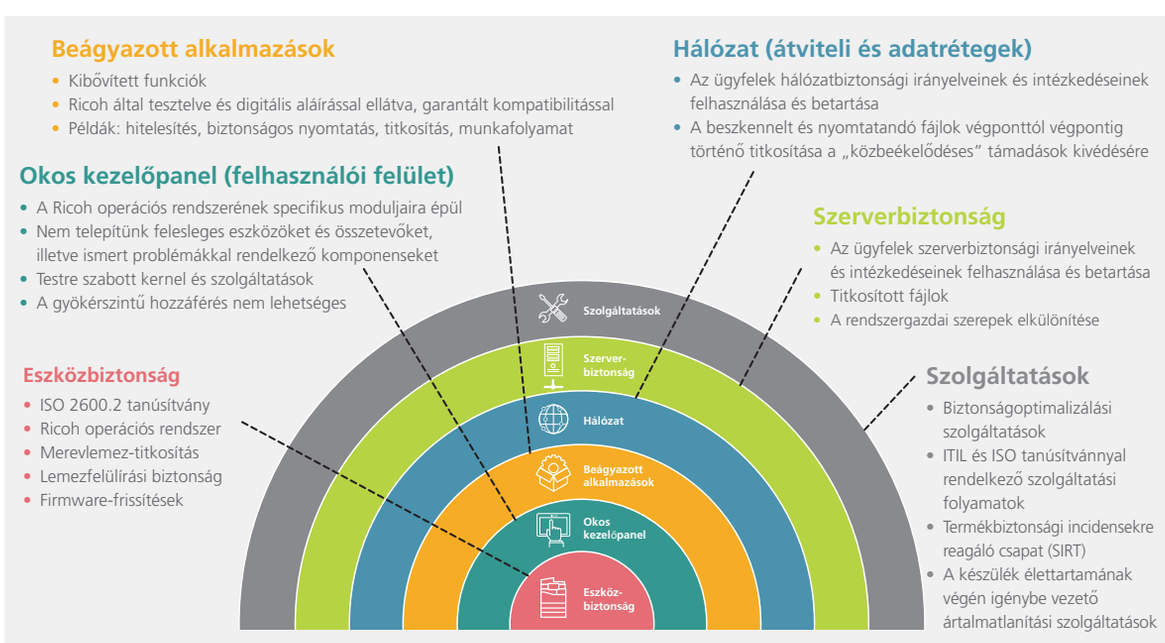
3. Okos alkalmazások

Az okos kezelőpanel felületébe beágyazható alkalmazások további – többek között munkafolyamattal és adatrögzítéssel kapcsolatos – funkciókat nyújtanak a felhasználó számára. Egyes alkalmazások alapvető biztonsági funkciókat biztosítanak. Ezek közé tartozik a biztonságos nyomtatás, a kártyás hozzáférés és a titkosítás. Az alkalmazásokat a Ricoh vagy a Ricoh Developer Program tagjai fejlesztik, és a kezelőpanelen futtatott minden alkalmazás számára kötelező a Ricoh kompatibilitási tesztjén való megfelelés és a digitális aláírás.

4. Hálózat és szerverek

Függetlenül attól, hogy ki kezeli az informatikai infrastruktúrát, a Ricoh garantálja, hogy termékei és szolgáltatásai megfeleljenek az informatikai és hálózati biztonsági házirendeknek. A nyomtatott és szkennelt fájlok végponttól végpontig terjedő titkosítása, a szerverek adatainak titkosítása és a rendszergazdai feladatok elkülönítése olyan módszerek, amelyek védelmet nyújtanak a „közbeékelődéses" vagy a „belső" támadásokkal szemben.

Teljes termékpalettánkat átfogó biztonsági szolgáltatások jellemzik. Ez magában foglalja a tanácsadást és a menedzselt szolgáltatásokat is, amelyek megkönnyítik ügyfeleink számára a dokumentum- és információbiztonság felügyeletét, optimalizálását és kezelését. Ezen felül, a termékek élettartama végén igénybe vehető szolgáltatást is nyújtunk, amelyek biztosítják a memóriában és merevlemezeken található adatok visszaállíthatatlan törlését az eszközök ártalmatlanítása előtt.



HOGYAN VÉDI A RICOH A DIGITÁLIS MUNKAHELYET

Ügyfeleinknek különféle biztonsági aggályai vannak, de mindegyikre igaz, hogy az adatmennyiségek növekedésével a sebezhetőségek, a támadások és büntetések kockázata is emelkedik. Az adatok titkosságának és biztonságának megőrzése, valamint a támadásoktól való védelme folyamatos erőfeszítéseket kíván. A Ricoh például havonta kb. 8 milliárd tűzfaltámadást ver vissza. Több tízezer globális, országos és iparági adatkezelési szabályzat létezik, a vállalatoknak igazolniuk kellaz ezeknek való megfelelést. Érthető módon minden vállalkozás – mérettől függetlenül – olyan partnert keres, akiben megbízhat, hiszen csak így tudhatja biztonságban a teljes digitális munkahelyet lefedő eszközparkot.

A Ricoh számos megoldást fejlesztett ki a vállalatokat fenyegető különféle kockázatok csökkentése érdekében. Mivel az információbiztonsági kockázatok elképesztő ütemben változnak, a Ricoh az ügyfelek visszajelzéseire épülő programok keretében fejleszti és biztosítja szolgáltatásait.

Ügyféltanácsadói csapataink alapvető stratégiai fókuszcsoportokként működnek. Az innen származó visszajelzéseket használjuk fel, hogy jobban megértsük az ügyfelek üzleti tevékenységét alakító trendeket, ösztönzőket és prioritásokat. Technológiai tanácsadói konferenciáink keretében közvetlenül a fő döntéshozóktól szerezzük be a legfontosabb információkat. A Ricoh mérnöki és K+F csapata ezeket a konferenciákat használja arra, hogy értékes felhasználói visszajelzéseket kérjenek az ötletekről, koncepciókról és prototípusokról. Végezetül, a Ricoh az egyéni ügyfelekkel is együttműködik, hogy új és fejlett biztonsági funkciókat dolgozzon ki a vertikális és általános piaci ügyfelek számára. Ez az ügyfélközpontú megközelítés segít a termékfejlesztési terveink alakításában, ügyfeleinknek pedig segít maximálisan kihasználni a globális szolgáltatási és támogatási hálózat minden előnyét.

A modern digitális munkahelynek dinamikusság szempontjából a számítógépes fenyegetések állandóan változó környezetéhez, rugalmasság szempontjából pedig a gyakorlati munkafolyamatokhoz kell igazodnia. Mi abban hiszünk, hogy a kiberbiztonsági megoldásoknak zökkenőmentesen kell működniük minden olyan technológiai eszközön és szolgáltatásban, amelyet ügyfeleink a munkájuk során használnak. Az ISO 27001 szabvány iránti, teljes vállalatunkra vonatkozó elkötelezettségünk, az összes termékünkhöz megszerzett IEEE 2600 tanúsítvány, valamint a kizárólag a Ricoh által használt operációs rendszer azt jelenti, hogy ügyfeleinknek mindig bevált biztonsági gyakorlatokra alapuló védelmi módszereket kínálunk, a vállalat struktúrájától és növekedési stratégiájától függetlenül.

A biztonsági fenyegetések, a jogszabályi követelmények és az összetett iparági szabványok kombinációja következtében óriásira nőtt a kibertámadások miatt bekövetkező hírnévbeli és pénzügyi károk kockázata. Itt az ideje, hogy megbízható partnert válasszon, aki képes biztosítani vállalata legsebezhetőbb eszközeinek védelmét, hogy Önnek csak az üzleti sikerre kelljen koncentrálnia.

RICOH
imagine. change.

www.ricoh.hu