Ricoh biztonsági megoldások

Biztonságban van a vállalkozása?

Üzleti tények, kockázatok és megoldások: alapvető tudnivalók az okos vállalkozásoknak

A kiberbiztonsági fenyegetések nagy veszélyt jelentenek a modern vállalatok túlélésére és sikerére.

Mérettől függetlenül, minden vállalat folyamatosan ki van téve annak a veszélynek, hogy olyan romboló hatású támadások áldozatává válik, mint például az adathalászat, a DDoS vagy a zsaroló programok,melyeknek költségei csak milliókban fejezhetők ki. Az olyan rendelkezések, mint a GDPR egyre súlyosabb bírságokkal fogják sújtani azokat a vállalatokat, amelyek nem képesek biztosítani rendszereik és adataik megfelelő védelmét. Eközben a modern munkahely bővülése és digitalizálása tovább növeli a kiberbiztonsági kihívásokat; ahogy a munkafolyamatok egyre több eszközön, hálózaton és földrajzi területen válnak elérhetővé, egyre fontosabbá válik a mindennapi munka során használt információk védelme.

Ugyanakkor, az irodai nyomtatók és multifunkciós készülékek lehetőségei az utóbbi években megtízszereződtek. 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.

Az egyre több kihívással szembenéző vállalkozásoknak minden eddiginél fontosabb, hogy integrált biztonsági megoldásokat alkalmazó dokumentum- és adatkezelési rendszerekkel rendelkezzenek, és ezt igazolni is tudják.

60%

Az Európában és az Egyesült Államokban működő vállalkozások közül az elmúlt év során ennyi jelentett be a nem biztonságos nyomtatás miatt bekövetkező illetéktelen adathozzáférést*

*A Quocirca Enterprise menedzselt nyomtatási szolgáltatásokról (MPS) szóló tanulmánya, 2017. Adatkészlet: az Egyesült Királyságban, Franciaországban, Németországban és az Egyesült Államokban tevékenykedő 240 olyan szervezet, amelyek 500-nál több munkavállalót foglalkoztatnak különféle iparágakban.

20 millió euró

A GDPR-nek nem megfelelő vállalatokra kiszabható maximális bírság*

*EU GDPR portál, „Gyakori kérdések a GDPR-ről” a www.eugdpr.org/gdpr-faqs.html címen.

RICOH
imagine. change.

Négy fontos szempont a vállalkozások biztonságához

Biztonságban vannak az adatai?

- Adattárolás
- Adatvesztés/-lopás veszélye
- Kibertámadások kockázata
- Illetéktelen módosítás/ adatsérülés kockázata
- Előre nem látható események

A valóság

Az adatok a vállalkozás legértékesebb eszközei. Könnyű a fejünket a homokba dugni és figyelmen kívül hagyni az olyan kockázatokat, mint az adatok eltulajdonítása, a számítógépes támadások vagy a természeti katasztrófák, de ha védtelenül maradunk, a következmények katasztrofálisak lehetnek.

A kockázatok

- Kibertámadás – A Ricoh havonta kb. 8 milliárd tűzfaltámadást ver vissza
- Az üzleti folytonosság elvesztése természeti katasztrófa következtében
- Adatlopás a szervezeten belül vagy kívül

Biztonságos a dokumentumkezelése?

- Dokumentum megosztása
- Dokumentumok megsemmisítése
- Eszközkezelés
- Biztonságos nyomtatás

A valóság

A dokumentumok mindennapi megosztása, tárolása és nyomtatása komoly biztonsági kockázatokat hordoz. Az egyszerű irodai nyomtatók jelentette kockázatot gyakran figyelmen kívül hagyják a biztonságos dokumentumkezelés kialakítása során.

A kockázatok

- Illetéktelen kezekbe kerülő bizalmas információk a nem biztonságos nyomtatás miatt
- Bizalmas információk kiszivárgása a dokumentumok/ eszközök nem megfelelően végzett megsemmisítése miatt
- Eszközök védelmének feltörése

Biztonságos a digitális munkahelye?

- Munkafolyamat menedzsment
- Mobil munkavégzés
- Biztonságos adatátvitel
- Informatikai infrastruktúra

A valóság

A rugalmas és mobil munkavégzés az előnyök mellett nagy kockázatokat is hordoz, hiszen kezelni kell a saját eszközökön végzett munka során megjelenő biztonsági réseket. Valóban biztonságos a nyilvános WiFi hálózat? Tényleg nem kerülhetnek illetéktelen kezekbe az eszközök?

A kockázatok

- Bizalmas vállalati információk elvesztése a rugalmas munkakörnyezet „gyenge láncszemei” miatt
- Illetéktelen hozzáférés az adatokhoz az átláthatatlan infrastruktúra és az eszközhasználat fölötti kontroll hiánya miatt

Megfelel az előírásoknak?

- Előírásoknak való megfelelés
- Megfelelés a GDPR (General Data Protection Regulation) előírásainak

A valóság

A meglévő szabályozási kötelezettségek mellé 2018 májusában kerül bevezetésre a GDPR. Vajon Ön készen áll rá, és tudja is igazolni a megfelelést?

A kockázatok

- Súlyos bírságok az előírásokat nem teljesítő vállalatok számára
- A vállalat hírnevének romlása

A biztonsági fenyegetések és a jogszabályi követelmények kombinációja következtében óriásira nőtt a kibertámadások miatt bekövetkező hírnévbeli és pénzügyi károk kockázata. Most jött el az ideje, hogy Ön is biztonságossá tegye digitális munkahelyét egy olyan partnerrel együttműködve, akire mindig számíthat.

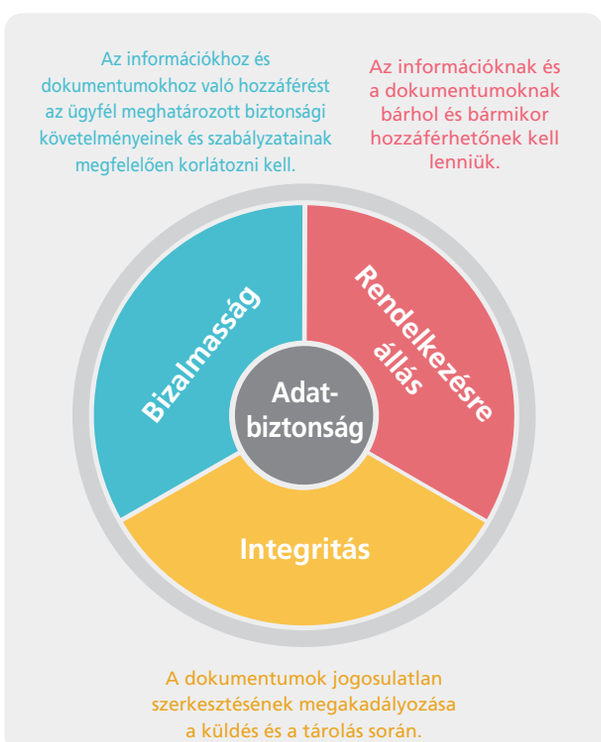
RICOH
imagine. change.

A jó hír, hogy a Ricoh már kidolgozta az Önnek megfelelő biztonsági megoldásokat. Szakértők vagyunk a biztonsági kockázatok kezelésében, hiszen évtizedek óta olyan eszközöket fejlesztünk, amelyek a legkorszerűbb, a teljes termékpalettánkba integrált biztonsági funkciók révén csökkentik a fenyegetettséget. Nyomtatóink például több mint 20 éve rendelkeznek biztonságos merevlemez-felülírási funkciókkal. Teljes digitális munkahelyi portfóliónk a biztonságra épül.

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 készülékünk 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.

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

Minden megoldásunkban az adatvédelemre és biztonságra vonatkozó „CIA" alapelveket követjük: bizalmasság, integritás és rendelkezésre állás.



RICOH
imagine. change.

Hogyan védi a Ricoh a digitális munkahelyet

Tisztában vagyunk azzal, milyen fontos a digitális munkahely biztonsága az üzleti adatok teljes – és rendkívül komplex – életciklusán keresztül. Mi négy kulcsfontosságú szinten valósítjuk meg a védelmi intézkedéseket. Ez a négy szint: a kontroll, a megőrzés, a megsemmisítés és a támogatás.

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. A vállalatunk ISO 27001 szabvány iránti elkötelezettsége és az összes készülékünkhöz megszerzett IEEE 2600 tanúsítvány azt jelenti, hogy a Ricoh mindig a lehető legjobb védelmi módszereket kínálja ügyfelei számára, a vállalat struktúrájától és növekedési stratégiájától függetlenül.

A technikai részletekre is kíváncsi? Töltse le a Ricoh biztonsági megoldásait részletesen tárgyaló jelentést: **Ricoh biztonsági megoldások**

Ha szeretné tudni, hogyan teheti biztonságosabbá és hatékonyabbá a vállalkozását a Ricoh segítségével, látogasson el a **www.ricoh.hu** címre, vagy vegye fel a kapcsolatot a Ricoh helyi képviselőjével.

Ricoh Hungary Kft.
2040 Budaörs
Puskás Tivadar út 14.

+36 23 806 800

www.ricoh.hu

RICOH
imagine. change.