

Je vaše podnikanie bezpečné?

Situácia, hrozby a riešenia v podnikaní:
Nepostrádateľné čítanie pre chytré firmy

Najväčšou hrozbou pre prežitie a úspech moderných firiem je kybernetická bezpečnosť.

Spoločnosti všetkých veľkostí sú neustále vystavené hrozbe rušivých útokov, ako je neoprávnené získavanie údajov, cielené preťaženie serverov alebo ransomware. Náklady na riešenie takýchto hrozieb sa šplhajú do miliónov eur. Záväzná nariadenia, ako je nariadenie GDPR, majú za cieľ čoraz viac postihovať spoločnosti bez vhodného zabezpečenia svojich systémov a údajov pokutami, ktoré môžu byť až likvidačné. Význam kybernetickej bezpečnosti firiem sa zvyšuje aj z dôvodu rozširovania a digitalizácie moderného pracoviska. Keďže pracovné postupy sú často rozdelené na viacero zariadení, sietí i lokalít, informácie je nutné počas ich presunu v rámci firmy chrániť.

Takisto sa v ostatných rokoch mnohonásobne rozšírili funkcie kancelárskych tlačiarní a multifunkčných zariadení. Spoliehame sa na ne pri zadávaní, získavaní, prenose a uchovávaní obchodných údajov. Práve preto sú jedným z potenciálne najzraniteľnejších miest dnešného pracoviska, hoci sa často prehliadajú.

Bezpečné systémy na správu dokumentov a údajov sú pre spoločnosti s prihliadnutím na tieto hrozby dôležitejšie než kedykoľvek predtým – a spoločnosti musia vedieť ich používanie preukázať.

60 %

Firmy v Európe a v USA, ktoré sa za posledný rok stretli s narušením bezpečnosti údajov vinou nezabezpečenej tlače*

*Štúdia Quocira Enterprise MPS, 2017. Skúmaná vzorka: 240 organizácií pôsobiach v rôznych odvetviach s celkovým počtom viac než 500 zamestnancov v Spojenom kráľovstve, Francúzsku, Nemecku a USA.

20mil. libier

Maximálna výška pokuty pre firmu, ktorá nedodržiava ustanovenia GDPR*

*Portál EÚ o nariadení GDPR, „Často kladené otázky o zavádzaní GDPR“ na stránkach www.eugdpr.org/gdpr-faqs (v angličtine).

Štyri hľadiská, na ktoré treba pamätať pri zabezpečovaní svojej firmy



Táto kombinácia bezpečnostných hrozieb a legislatívnych požiadaviek znamená, že hrozba finančných škôd a škôd na dobrom mene z kybernetických útokov nikdy nebola vyššia. Teraz je ten správny čas na investíciu do zabezpečenia vášho digitálneho pracoviska s partnerom, ktorému môžete dôverovať.



Dobrou správou je, že spoločnosť Ricoh už tieto otázky vyriešila za vás. Sme odborníkmi na porozumenie týmto hrozbám, pretože sa už celé desaťročia venujeme vývojom spôsobov, ako ich zmierniť. Každý výrobok a každé riešenie z celého nášho portfólia má zabudované najmodernejšie bezpečnostné opatrenia. Naše tlačiarne napríklad už viac než dvadsať rokov ponúkajú možnosť bezpečného prepisovania pevného disku. Bezpečnosť tvorí základ nášho portfólia riešení pre digitálne pracovisko.

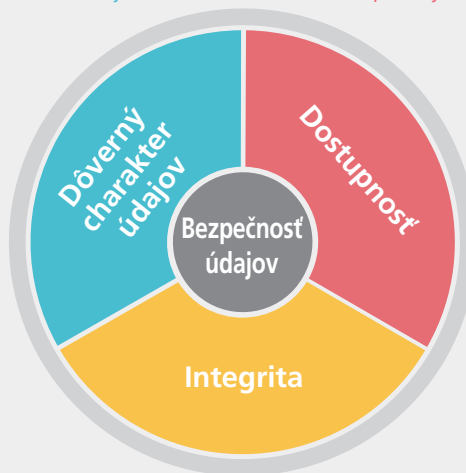
Spoločnosť Ricoh poskytuje zákazníkom konzistentnú štruktúru celosvetových služieb a podpory, ktorá zaisťuje efektívne zdieľanie informácií o aktuálnych hrozbách a reakciu na tieto hrozby. Osvedčenie IEEE 2600 je nielen základným prvkom všetkých našich tlačiarenských zariadení - spoločnosť Ricoh je tiež hlavným členom a kľúčovým autorom združenia IEEE Standards Association. Spoločnosť Ricoh je takisto držiteľom osvedčenia ISO 27001 a zaviazala sa trvalo dodržiavať požiadavky tohto systému na správu bezpečnosti informácií.

Bezpečnosť je základným kameňom, nie len doplnkom každého produktu a služby z portfólia spoločnosti Ricoh. Spĺňame tak náročné požiadavky na overenú, účinnú a preukázateľnú prax v oblasti kybernetickej bezpečnosti. Veríme, že tento celkový pohľad na slabé miesta je nevyhnutný na prežitie v modernom obchodnom prostredí.

Každé hľadisko nášho prístupu k bezpečnosti sa riadi tromi princípmi ochrany osobných údajov a bezpečnosti podľa skratky DID (angl. „CIA“): Dôverný charakter údajov, Integrita a Dostupnosť.

Pristup k informáciám a dokumentom musí byť obmedzený v súlade s bezpečnostnými požiadavkami a zásadami určenými zákazníkom.

Pristup k informáciám a dokumentom kedykoľvek a odkiaľkoľvek podľa potreby.



Zabránenie neoprávnenej úprave dokumentov počas prenosu i počas uloženia.

RICOH
imagine. change.

Ako spoločnosť Ricoh zabezpečuje digitálne pracovisko

Rozumieme potrebe zabezpečenia vášho digitálneho pracoviska počas celého a komplexného životného cyklu obchodných údajov. Dosahujeme to zavádzaním bezpečnostných opatrení naprieč štyrmi základnými fázami: Kontrola, uchovanie, likvidácia a podpora.



Moderné digitálne pracovisko musí byť rovnako dynamické ako kybernetické hrozby, ktorým čelí, a rovnako flexibilné ako pracovné postupy v jeho rámci. Preto si myslíme, že kybernetická bezpečnosť by mala fungovať bezproblémovo naprieč celou technológiou, ktorú si naši zákazníci zvolili na lepší dohľad nad svojim pracoviskom. Dodržiavanie predpisov normy ISO 27001 naprieč celou našou organizáciou, ako aj osvedčenie IEEE 2600 pre všetky naše produkty znamená, že so spoločnosťou Ricoh sú vám k dispozícii overené postupy dohľadu nad vašim biznisom - bez ohľadu na to, ako sa ho rozhodnete štruktúrovať a rozvíjať.

Máte záujem o technické podrobnosti? Viac informácií o bezpečnostných kapacitách spoločnosti Ricoh nájdete v našom reporte, ktorého úplné znenie si môžete prevziať tu: **Bezpečnostné riešenia od spoločnosti Ricoh**

Viac informácií o tom, ako vám spoločnosť Ricoh môže pomôcť zabezpečiť a podporiť vašu spoločnosť, nájdete na stránkach ricoh.sk, prípadne sa obráťte na jej miestneho obchodného zástupcu.



RICOH Slovakia s.r.o.
Polus Tower II, Vajnorská 100/B
831 04 Bratislava



+421 850 003 005



www.ricoh.sk

RICOH
imagine. change.

Fakty a čísla uvedené v tomto prospekte sa vzťahujú na konkrétne obchodné prípady. Odlišné okolnosti môžu priniesť odlišné výsledky. Všetky názvy spoločností, značiek, produktov a služieb sú majetkom a registrovanými ochrannými známkami ich príslušných vlastníkov. Copyright © 2017 Ricoh Europe PLC. Všetky práva vyhradené. Tento prospekt, jeho obsah a formu nie je možné modifikovať, upravovať, čiastočne ani úplne kopírovať, ani začleňovať do iných dokumentov bez predchádzajúceho písomného súhlasu spoločnosti Ricoh Europe PLC.