



Je vaše firma bezpečná?

Realita, rizika a řešení v podnikovém světě:
Nepostradatelné čtení pro chytré firmy

Nedostatky v kybernetické bezpečnosti jsou největší hrozbou pro přežití a úspěch moderních firem.

Společnostem všech velikostí hrozí, že se stanou obětí rušivých útoků, například phishingu, DDoS a ransomwaru. Škody způsobené takovými útoky se mohou pohybovat v milionech. Závazné směrnice, například GDPR, se stále důrazněji snaží postihovat firmy potenciálně likvidačními pokutami v případě, že své systémy a data náležitě nezabezpečí. Náročnost kybernetického prostředí navíc zvětšuje neustálé rozšiřování a digitalizace moderního pracoviště. Pracovní postupy zahrnují stále více různých zařízení, sítí a zeměpisných oblastí a informace je při přesunech ve firmě nutno neustále chránit.

V posledních letech se navíc mnohonásobně rozšířily možnosti kancelářských tiskáren a multifunkčních zařízení. Spoléháme se na ně při zadávání, získávání, přenosu a uchovávání dat. To z nich dělá potenciálně jedno z nejnebezpečnějších, a přitom často přehlížených, míst útoku na dnešním pracovišti.

Tváří v tvář těmto obtížím nyní firmy musí klást větší důkaz než kdykoli dříve na zabezpečení dokumentů a systémů pro správu dat. A navíc to musí být schopny prokázat.

60 %

Firmy v Evropě a USA, v nichž loni došlo k úniku dat vinou nezabezpečeného tisku*

*Studie Quocira Enterprise MPS Study, 2017. Zkoumaný vzorek: 240 organizací s 500 a více zaměstnanci z různých oborů z Velké Británie, Francie, Německa a USA.

20 mil. liber

Maximální potenciální pokuta za porušení GDPR firmou*

*Portál EU o GDPR, „Často kladené otázky o zavádění GDPR“ na adrese www.eugdpr.org/gdpr-faqs.html.

Čtyři otázky o zabezpečení vaší firmy



Vzhledem k této kombinaci bezpečnostních hrozeb a legislativních požadavků je nyní riziko narušení dobré pověsti a vzniku finančních ztrát větší než kdykoli dříve. Je tedy ta pravá chvíle investovat do zabezpečení digitálního pracoviště ve spolupráci s partnerem, kterému můžete věřit.



Dobrou zprávou je, že Ricoh již na bezpečnost myslí. Jsme v porozumění těmto rizikům experti, protože jsme strávili celá desetiletí hledáním způsobů, jak je zmírnit. Výsledkem jsou moderní bezpečnostní opatření zabudovaná do všech našich produktů a řešení. Například naše tiskárny již více než 20 let nabízejí funkce pro bezpečné přepsání pevného disku. Bezpečnost je základem celého našeho portfolia pro digitální pracoviště.

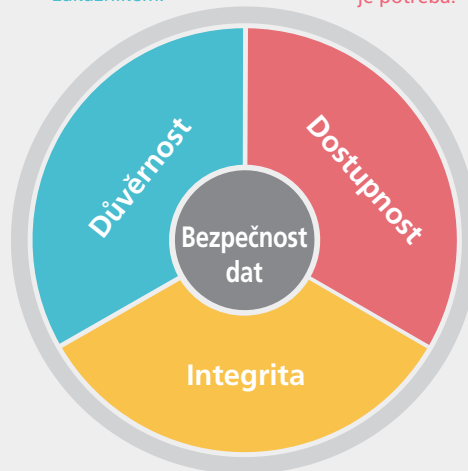
Ricoh zajišťuje konzistentní celosvětové služby a zákaznickou podporu. Díky ní jsou informace o hrozbách účinně sdíleny a využívány. Nejenom, že jsou naše tisková zařízení standardně certifikována podle normy IEEE 2600, ale Ricoh je také předním členem a významným autorem standardů v rámci Standardizační asociace IEEE. Kromě toho má společnost Ricoh certifikaci ISO 27001 a zavázala se tento systém správy bezpečnosti informací dodržovat.

Abychom splnili náročné požadavky na účinné, průkazné a osvědčené metody kybernetické bezpečnosti, je zabezpečení součástí všech našich produktů a služeb již od fáze návrhu - nikdy jen jako doplněk. Věříme, že tento holistický pohled na zranitelná místa je nezbytný pro přežití moderních firem.

Všechny aspekty našeho přístupu k zabezpečení jsou založeny na našich principech ochrany soukromí a bezpečnosti DID (angl. „CIA“): Důvěrnost, Integrita a Dostupnost.

Přístup k informacím a dokumentům musí být omezen podle bezpečnostních požadavků a zásad určených zákazníkem.

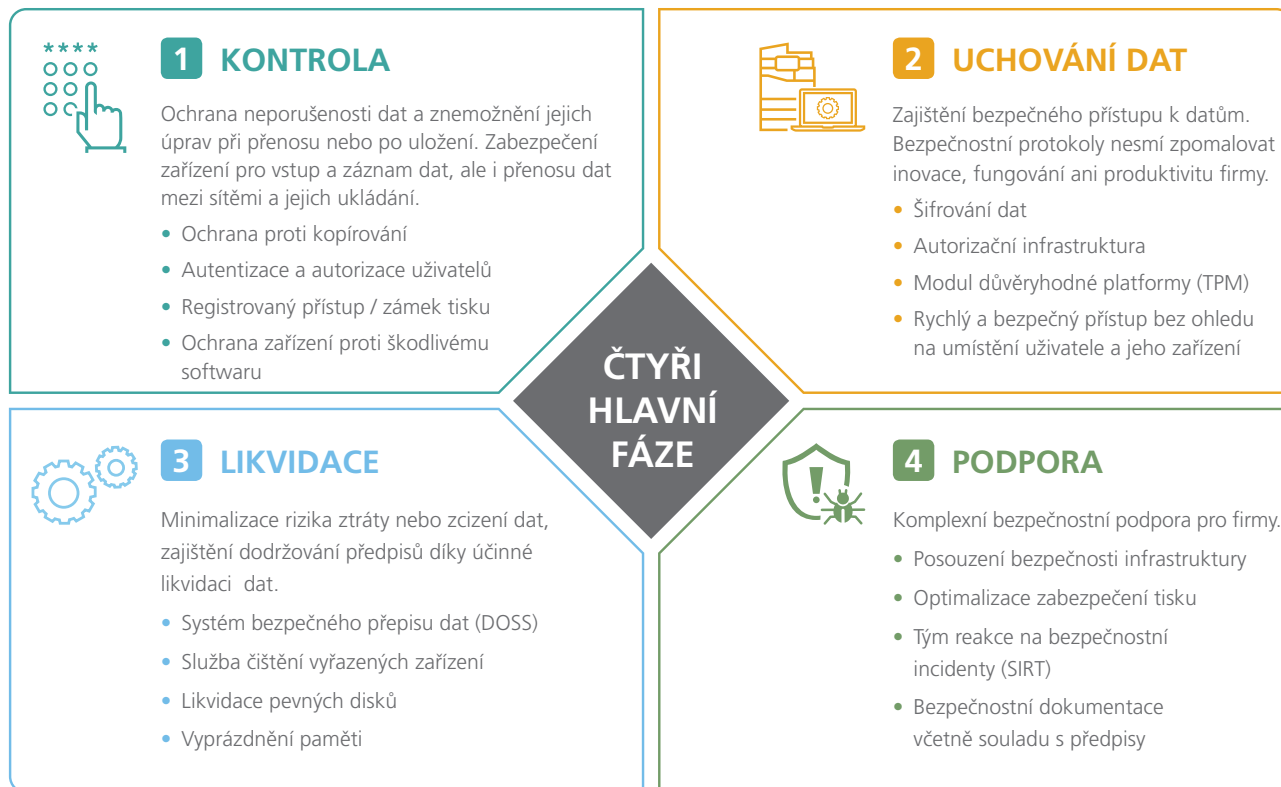
Přístup k informacím a dokumentům odkudkoli a kdykoli je potřeba.



Ochrana před neoprávněným kopírováním dokumentu při jeho přenosu a uložení.

Jak Ricoh zabezpečuje digitální pracoviště

Uvědomujeme si, jak důležité je zabezpečit vaše digitální pracoviště po celou dobu složitého životního cyklu firemních dat. Dosahujeme toho pomocí bezpečnostních opatření zaváděných ve čtyřech kriticky důležitých fázích: Kontrola, uchování dat, likvidace a podpora.



Moderní digitální pracoviště musí být stejně dynamické jako kybernetické hrozby, kterým čelí, a stejně flexibilní jako pracovní postupy na něm používané. Proto věříme, že by kybernetická bezpečnost měla fungovat bezešvým způsobem na veškerých technologiích, které se zákazníci rozhodnou na svém pracovišti používat. Díky tomu, že celá naše organizace dodržuje normu ISO 27001 a naše produkty mají certifikaci IEEE 2600, si můžete být jisti, že ať se svoji firmu rozhodnete strukturovat a rozvíjet jakkoli, budete díky společnosti Ricoh stále používat osvědčené bezpečnostní postupy.

Zajímají vás technické informace? Pro další popis bezpečnostních funkcí společnosti Ricoh lze stáhnout celý report:

Bezpečnostní řešení Ricoh

Chcete-li zjistit, jak může Ricoh pomoci se zabezpečením a podporou vaší firmy, navštivte náš web na adrese ricoh.cz nebo kontaktujte svého místního zástupce Ricoh.



RICOH Czech Republic s.r.o.
Jihlavská 1558/21
140 00 Praha 4



+420 841 116 117



www.ricoh.cz

RICOH
imagine. change.

Údaje a hodnoty uvedené v tomto prospektu se vztahují na konkrétní obchodní případy. V jiných situacích se výsledky mohou lišit. Všechny názvy společností, značek, produktů a služeb jsou majetkem a registrovanými ochrannými známkami svých příslušných vlastníků. Copyright © 2017 Ricoh Europe PLC. Všechna práva vyhrazena. Tento prospekt, jeho obsah a rozvržení je zakázáno upravovat nebo přizpůsobovat, kopírovat z části nebo vcelku nebo začleňovat do jiných dokumentů bez předchozího písemného svolení společnosti Ricoh Europe PLC.