RICOH
imagine. change.

Bezpečnostní řešení Ricoh

Chráníme váš byznys

Nedostatky v kybernetické bezpečnosti firem jsou největší hrozbou pro trvale úspěšné působení na trhu. Společnostem všech velikostí neustále hrozí, že se stanou cílem útoků narušujících jejich činnost, jako je neoprávněné získávání dat, cílené přetížení serverů nebo ransomware. Skutečné náklady těchto útoků se mohou vyšplhat do milionů. V roce 2017 zjistil institut Ponemon, že průměrné náklady na únik dat ve světě činí 3,62 milionu dolarů. V nadcházejících letech budou tyto náklady dále růst spolu s tím, jak nové zákonné směrnice (např. GDPR) s výrazně vyššími pokutami dopadnout na firmy, které dostatečně nezabezpečí své systémy a údaje. Aby se firma těmto pokutám vyhnula, musí prokázat, že je schopna údaje ochránit. K tomu je třeba holistický pohled na všechna zranitelná místa v celé firmě.

Zajistit kybernetickou bezpečnost je ještě složitější kvůli rozšiřování a digitalizaci moderních pracovišť a prudkému nárůstu objemu dat. Pracovní procesy často zahrnují několik zařízení, sítí a zeměpisných oblastí. Informace jsou nejvíce ohroženy při přesunech v rámci firmy. V každé fázi těchto přesunů je třeba je chránit. Vzhledem k souvisejícím bezpečnostním rizikům již moderní firmy nemohou existovat bez zabezpečených systémů pro správu dokumentů a informací. V posledních letech se navíc mnohonásobně rozšířily možnosti kancelářských tiskáren a multifunkčních zařízení. Nyní se z velké části podílejí na vstupech a výstupech dat, jejich přenosech a ukládání. To z nich dělá jedno z nejnebezpečnějších, a přitom často přehlížených, míst útoku na dnešním pracovišti.

Ačkoli nabídkou bezpečnostních funkcí se chlubí mnoho firem, společnost Ricoh bezpečná řešení a firemní služby vyvíjí již několik desetiletí. Například naše tiskárny již více než 20 let nabízejí funkce pro bezpečné přepsání pevného disku.

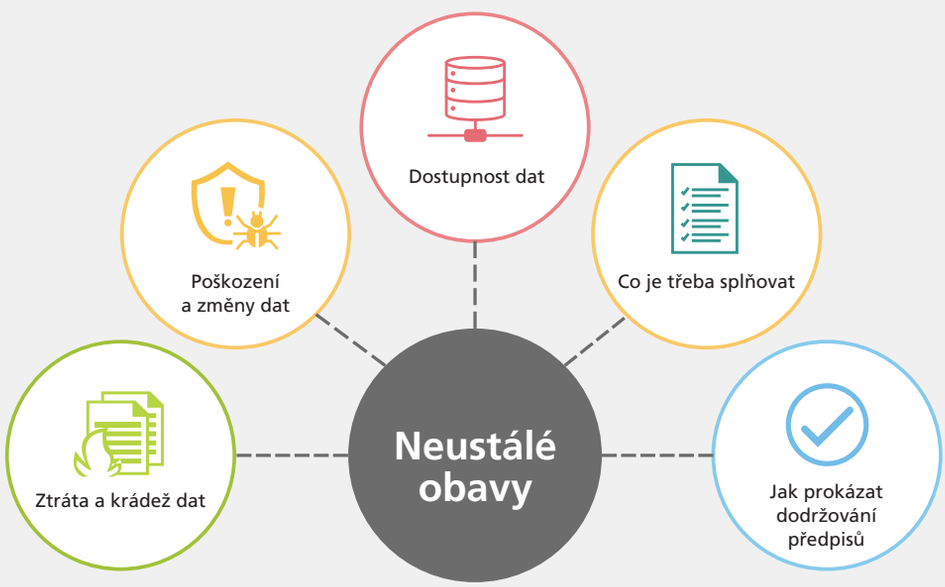
Bezpečnost je základem celého našeho portfolia pro digitální pracoviště. V současné době jsou v provozu více než 4 miliony našich kancelářských produktů. Každý z těchto produktů a všechny naše služby, které spolu s nimi dodáváme, obsahují zabudované bezpečnostní prvky. V mnoha našich zařízeních rovněž používáme vlastní operační systém Ricoh. Ten je významnou součástí našich bezpečnostních funkcí, protože představuje ochranu před hrozbami založenými na operačním systému. Ty se totiž zaměřují na rozšířenější operační systémy.

Společnost Ricoh nabízí konzistentní celosvětovou síť služeb a zákaznické podpory zajišťující účinné sdílení a uplatnění informací o bezpečnostních hrozbách. 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. Při vývoji produktů se neustále soustředíme na obchodní a bezpečnostní potřeby našich zákazníků, k čemuž nám pomáhá řada celosvětových inovačních programů založených na požadavcích zákazníků.

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

ZABEZPEČENÍ ZÁKAZNÍKŮ

TRENDY: *Spolu s nárůstem objemu dat roste i výskyt zranitelných míst, útoků a finančních postihů.*



Zabezpečení a zdokonalení digitálních pracovišť

Ricoh se snaží umožnit a zabezpečit digitální práci všude, kde to lidé potřebují. V moderní digitální ekonomice to znamená dodávat vyšší hodnotu i v první linii mimo tradiční kanceláře. Vzdálené kanceláře a práce na dálku zvětšují flexibilitu a produktivitu firem v každodenním provozu. Mohou díky ní lépe naplňovat očekávání zákazníků a uspokojovat požadavky na služby.

Činnost na okraji sítě však představuje jedno z největších ohrožení bezpečnosti firmy. Je tedy třeba náležitě zabezpečit jak data vytvářená těmito pracovníky, tak vzdálená zařízení, pomocí nichž je pořizují. Zaměstnanci často pracují přes několik sítí a zeměpisných oblastí, což tento úkol dále komplikuje. Velmi důležité je také to, že podle různých předpisů, například GDPR, musí firmy prokazatelně zabezpečit data po celou dobu jejich existence. Jinak se vystavují riziku vážných postihů. Spolu s vývojem pracovišť a rozšiřováním digitálních pracovních procesů se komplikuje životní cyklus firemních dat. Pojďme se nyní podívat na jeho jednotlivé fáze.

Prvním krokem je vstup dat a zařízení na jejich pořizování. To je významná součást zabezpečení od firmy Ricoh. Poté je potřeba data přenést pomocí sítí a bezpečně uložit. V této fázi má zásadní význam ochrana neporušenosti dat. Systémy firmy Ricoh omezují přístup uživatelů k zařízením a síťovým funkcím tak, aby byla vyloučena nežádoucí manipulace s přenášenými nebo uloženými daty. Mezi tyto služby patří řízení přístupu, šifrování a ochrana proti kopírování. Říkáme tomu Řízené zpracování dat.

Uložené dokumenty však musí být snadno dostupné těm firemním pracovníkům, kteří je potřebují. Na této dostupnosti závisí možnost kdykoli podle potřeby informace účinně využívat. Analýza dat je základní součástí výkonného digitálního pracoviště. Účinně poskytuje přehled o všech aspektech činnosti firmy od prodeje až po lidské zdroje. Nástroje zabezpečené infrastruktury poskytují rychlý a bezpečný přístup bez ohledu na to, kde se uživatel nachází a jaké zařízení používá. Je nesmírně důležité, aby bezpečnostní protokoly neomezovaly inovace ani funkčnost a nevedly k tomu, že je budou zaměstnanci obcházet. Této fázi říkáme Uchování dat.

A konečně je tato data nutno umět bezpečně a prokazatelně zlikvidovat. Tento krok je velmi důležitý pro dodržování zákonných požadavků a omezení rizika odcizení nebo ztráty dat. K tomuto procesu ve skutečnosti dochází po celou dobu existence dokumentu, nejenom při jeho konečném smazání. Tisk jakéhokoli souboru zanechá jeho latentní obraz na pevném disku multifunkční tiskárny, který je třeba přepsat, aby nemohlo dojít k neoprávněnému přístupu k němu. Mezi služby smazání dat poskytované společností Ricoh patří čištění disku, vynulování paměti, mazání nevytištěných souborů a mazání při odhlášení. Hackerům brání v získání citlivých informací z dat, které po dokumentech zůstávají. Říkáme tomu Likvidace.

K účinnému zabezpečení pracovních dat po celou dobu tohoto životního cyklu firma Ricoh používá princip ochrany soukromí a zabezpečení zvaný „DDI" (angl. CIA): Důvěrnost, dostupnost a integrita. Těmito třemi zásadami se řídíme při návrhu našich produktů a řešení tak, aby splňovaly nezbytné standardy a předpisy. Takový přístup umožňuje inovace a růst na pracovišti a zároveň zachování účinnosti a bezpečnosti procesů.

PŘÍSTUP FIRMY RICOH K BEZPEČNOSTI

Stavíme na principech ochrany soukromí a zabezpečení DDI (CIA): Důvěrnost, Dostupnost a Integrita.

Bezpečnost je naší DNA. Všechny produkty a služby dodávané společností Ricoh obsahují zabudované bezpečnostní funkce.

Ricoh nabízí kompletní sadu bezpečnostních produktů a služeb, pomocí nichž můžete zabezpečit tvorbu dokumentů od počátku až do konce.

Nyní se podíváme postupně na všechny hlavní fáze: řízení, uchování dat,, likvidaci a podporu.

ČTYŘI FÁZE ZABEZPEČENÍ DIGITÁLNÍHO PRACOVIŠTĚ

1 ŘÍZENÍ

Účinná kontrola dat je nezbytná k udržení jejich důvěrnosti a neporušenosti. Firemní informace jsou cenným majetkem a je třeba je chránit. Dnešní hardwarová zařízení jsou informačními terminály, které mohou fungovat jako zranitelné vstupní body k firemním informacím. Proto Ricoh k řízení a zabezpečení firemních dat používá celou řadu nástrojů pro autentizaci uživatelů a správu zařízení. Ty pracují s nastaveními na fyzických zařízeních, která povolují a omezují přístup pouze na určité funkce a data. Pro zajištění bezpečnosti dokumentů je také důležité omezit přístup zaměstnanců k informacím procházejícím multifunkčními tiskárnami ve firmě. Fáze řízení přístupu zahrnuje i ochranu zařízení proti škodlivému softwaru pomocí třístupňového přístupu firmy Ricoh k firmwaru zařízení.

Ochrana před nepovoleným kopírováním

Jako ochranu před pokusy o nepovolené kopírování nabízí Ricoh elegantní řešení, které zajišťuje bezpečnost papírových dokumentů. Funkce ochrany proti kopírování opatřuje dokumenty při tisku a kopírování neviditelnými vzory vytištěnými na pozadí. V případě kopírování nebo skenování takto vytištěného nebo zkopírovaného dokumentu bude tento vzor na kopii viditelný. Modul ochrany proti neoprávněnému kopírování umožňuje multifunkčním zařízením detekovat vložené vzory a v zájmu ochrany před únikem informací nahradit kopírovaný obraz šedou barvou. Tato funkce je užitečná při tisku důvěrných informací. Omezení kopírování důvěrných informací brání jejich únikům.

Důvěrný tisk

Dokument zaslaný z počítače může být v multifunkční tiskárně uložen na pevném disku. Funkce důvěrného tisku od společnosti Ricoh vyžaduje zadání hesla. Toto heslo je pak na multifunkční tiskárně nutno zadat před tiskem dokumentu. Protože dokument nelze vytisknout bez toho, aby jeho vlastník u zařízení fyzicky byl, zajišťuje tato funkce, že dokument zůstane pod kontrolou vlastníka.

Pokročilé zabezpečení získávání dat

Portfolio pokročilých řešení pro pořizování dat od společnosti Ricoh nabízí různé stupně šifrování a dešifrování na všech vrstvách zpracování a ve všech fázích pořizování. Správci mohou zajistit autentizaci přístupu k frontám zpracování pomocí přihlašování jednotlivých uživatelů nebo skupinových přihlašovacích údajů. Mezi další vrstvy zabezpečení patří Security Assertion Markup Language (SAML) pro rámec jednotného přihlašování (Single Sign On, SSO), ověřování totožnosti (Personal Identity Verification, PIV) a infrastruktura veřejného klíče (Public Key Infrastructure, PKI).

Vestavěná autentizace

Protokoly pro přístup k zařízení a ověřování identity v produktech Ricoh lze spravovat centrálně. Mezi dostupné metody patří identifikační karta, číslo PIN, síťové přihlášení, případně vícefaktorová kombinace těchto metod. Vícefaktorové ověřování posiluje bezpečnost, může však zpomalit práci vytížených uživatelů. Jednotné přihlašování (Single Sign On, SSO) tento problém zmírňuje tak, že uživatelům umožňuje používat jedno přihlášení k přístupu k celé řadě zařízení. V našich zařízeních je navíc předinstalován rychlý ověřovací software společnosti Ricoh na bázi karet, takže uživatelé mají k dispozici možnost rychlého přístupu k dokumentům. Použití čtečky / zapisovače NFC výrazně zjednodušuje přihlašování uživatelů a zároveň účinně zabezpečuje a řídí přístup k multifunkčním tiskárnám. Tento způsob přístupu navíc funguje spolu se stávajícím nastavením oprávnění, pomocí nějž zákazník omezuje přístup k funkcím multifunkčních tiskáren.

Streamline NX (SLNX)

Modul správy zařízení na platformě Streamline NX od společnosti Ricoh je software určený ke správě a monitorování zařízení v síti. Umožňuje správcům prohlížet a konfigurovat nastavení bezpečnosti zařízení pomocí předpřipravených šablon i vlastních parametrů. Mezi hlavní bezpečnostní nastavení patří povolování a zakazování protokolů, nastavení IP adres, hesla pro administrátory, e-mailové adresy pro zasílání upozornění, nastavení šifrování a další funkce. SLNX vás také může informovat, že některé zařízení nesplňuje vaše bezpečnostní zásady.

Ochrana zařízení proti škodlivému softwaru

K ochraně svých zařízení proti škodlivému softwaru přistupuje společnost Ricoh na třech úrovních. Za prvé, se zařízeními Ricoh lze pracovat pouze pomocí strojového jazyka nebo operačního softwaru používaného výhradně firmou Ricoh. Za druhé, aby nebylo možno zlovolně upravovat software zařízení, musí být všechny aktualizace firmwaru napsány a schváleny pouze v tomto strojovém jazyku firmy Ricoh. A konečně, každá aktualizace musí být firmou Ricoh digitálně podepsána. Díky této trojfázové metodě nelze do zařízení Ricoh nahrát neschválený firmware. Škodlivý a špionážní software a viry jsou tedy v podstatě eliminovány.

Fyzické zabezpečení dokumentů

Osvědčené bezpečnostní metody nemusí být komplikované. V kancelářích je spousta práce a tištěné dokumenty představují značné bezpečnostní riziko jak kvůli možnosti krádeže, tak i nedbalosti zaměstnanců. Ricoh nabízí celou řadu rozšiřujících možností zabezpečení, které brání neoprávněnému přístupu k tištěným dokumentům. Například zamykatelné zásobníky brání odcizení speciálních tiskopisů, jako jsou formuláře na lékařské recepty ve zdravotnictví apod. Instalace deskových uzávěrů u všech kabelů pak zabrání možnosti narušování ze strany vlastních zaměstnanců. Díky řešení pro bezpečné tisk dokumentů (Print-to-me) lze dokumenty vytisknout pouze v přítomnosti vlastníka, takže nehrozí, že je získá někdo neoprávněný.

2 UCHOVÁNÍ DAT

Podle nových i stávajících zákonných požadavků musí firmy zajistit jak důvěrnost informací, tedy to, aby je nebylo možno ukrást ani nemohly uniknout, tak jejich neustálou integritu a neporušenost, tedy nemožnost jejich neoprávněných změn. Aby toho dosáhly, musí firmy omezit přístup k citlivým dokumentům, aby je nebylo možno neoprávněně upravovat ani falšovat. To dále funguje jako ochrana proti cíleným nebo náhodným hrozbám zevnitř firmy.

Využívání mobilních zařízení při práci ovšem jakýkoli scénář kybernetické bezpečnosti ještě více komplikuje. Je třeba zavést další bezpečnostní opatření, která umožní sdílení souborů z libovolného místa. Při přenosu po síti a mezi zařízeními musí být tyto soubory stejně bezpečné jako v úložišti. Silná šifrovací technologie může data účinně chránit a následovat je po celý jejich životní cyklus. To se přirozeně týká dokumentů, ale také hlavních bezpečnostních prvků, jako jsou hesla, nastavení maker a adresáře. Používá-li firma šifrování, budou mít hackeři problém získat užitečné informace i v případě, že už do firemní sítě proniknou. Zároveň šifrování chrání integritu dat v případě jejich úniku.

V mnoha oborech je velice důležitý provoz bez výpadků. Nepředvídatelné události, například přírodní katastrofy, tedy pro firmu představují přímé ohrožení. Zvláště zranitelné jsou v takových případech papírové dokumenty. Pomocí bezpečného cloudového úložiště digitalizovaných dokumentů lze zajistit nezbytnou odolnost vůči přírodním i lidmi způsobeným pohromám. Tato digitální data je nicméně nutno chránit pomocí příslušných bezpečnostních opatření.

Základní šifrování dat

Jako ochranu informací při jejich přesunech mezi zařízeními lze použít šifrování všech dat přenášených na pevný disk multifunkčních tiskáren Ricoh nebo na něm uložených. Vestavěné softwarové funkce podporují šifrování skenovaných a tištěných souborů typu end-to-end pomocí infrastruktury veřejného klíče (PKI). To chrání proti útokům typu „muž uprostřed" v prostředí zákaznikových informačních technologií.

Bezpečnost dále posiluje průběžné přepisování tiskových dat systémem bezpečného přepisu dat (Data Overwrite Security System, DOSS) firmy Ricoh. O něm se podrobněji zmíníme později v popisu likvidační fáze životního cyklu dat.

Ochrana systému BIOS a operačního systému

Multifunkční tiskárny Ricoh používají modul TPM (Trusted Platform Module), což je bezpečnostní modul pro zabezpečení hardwaru. TPM provádí šifrovací funkce a bezpečně ukládá kryptografická data. Ricoh do TPM ukládá kořenový šifrovací klíč, který chrání šifrovací klíč dat na pevném disku a digitální certifikát multifunkčního zařízení. Kromě toho tento modul správcům umožňuje provádět důvěryhodné spuštění, při němž je před spuštěním multifunkční tiskárny ověřena pravost firmwaru.

Ověřování firmwaru

Kořenový klíč a šifrovací funkce jsou vždy obsaženy v modulu TPM a nelze je změnit z míst za firewallem. Naše produkty díky tomu nelze zneužít ani je neoprávněně upravovat. To zajišťuje vysokou úroveň ověření firmwaru multifunkční tiskárny a identity zařízení a bezpečnost pevného disku. Jde o další dobrý příklad toho, že multifunkční tiskárny Ricoh jsou vytvářeny s důrazem na bezpečnostní zájmy našich zákazníků.

Správa hesel

Na zařízeních Ricoh lze nastavit několik správců, přičemž každý z nich může mít jiné role a vlastní heslo. Hesla těchto uživatelů lze vzdáleně nastavovat pomocí webových správcovských nástrojů. Lze je také pravidelně kontrolovat. To umožňuje „oddělení pravomocí", což je požadavek přítomný v mnoha předpisech platných pro firmy.

Omezení přístupu uživatelů

Nástroj pro správu uživatelů od firmy Ricoh správcům systému umožňuje omezit přístupová práva uživatelů. Správce například může nastavit oprávnění, kterým poskytne vybraným uživatelům přístup k registrovanému adresáři multifunkční tiskárny. Tím zamezí neoprávněnému přístupu k osobním údajům a záznamům uloženým na kancelářských zařízeních.

Funkce uzamčení uživatele

V případě opakovaného zadání chybných přihlašovacích hesel může multifunkční tiskárna Ricoh posoudit, zda se někdo snaží heslo prolomit. To aktivuje funkci uzamčení, která příslušné uživatelské jméno zablokuje. Zablokované uživatelské jméno nelze použít k přihlášení, ani pokud je později použito se správným heslem. Uzamčení lze zrušit až po uplynutí určitého času, případně ho může zrušit správce. To v podstatě zabraňuje pokusům o prolomení hesla.

3 LIKVIDACE

Bezpečná likvidace dat je základní součástí každého komplexního kybernetického zabezpečení. Je snadné podlehnout mylnému přesvědčení, že zodpovědnost firmy končí v okamžiku, kdy data opustí její prostory. Mnoho předpisů však stanoví, že likvidace dat musí být komplexní proces, který zamezí veškerým rizikům jejich následné krádeže nebo zneužití. Dokud to nelze dokázat, závazky firmy ohledně příslušných dat stále trvají.

Vyřazená a vrácená kancelářská zařízení představují pro obchodní informace hrozbu, kterou si mnozí neuvědomují. Ricoh nabízí certifikovanou a průkaznou službu odstraňování dat z těchto vyřazených tiskáren. Zahrnuje to zapomenuté materiály, jako jsou uložená síťová nastavení, údaje o uživatelích, data na pevném disku a dokonce nálepky ponechané na zařízení. Pokud je firma neodstraní, hrozí značné riziko prozrazení důvěrných firemních a osobních údajů. Ale aby bylo vyhověno předpisům, měl by tento proces probíhat průběžně i během životnosti zařízení. To firmám zajišťuje maximální míru kontroly nad údaji, za které jsou zodpovědné.

Přepsání obrazu: Systém bezpečného přepisu dat (DOSS)

Pevné disky multifunkčních tiskáren slouží k ukládání obrazů dat obsažených v dokumentech pro účely zpracování tiskových úloh. Bezpečné řešení přepisu dat od společnosti Ricoh zajišťuje, že jsou tato data vždy před zahájením další úlohy přepsána. Díky tomu v případě, že by někdo přistupoval k pevnému disku neoprávněně, nezíská přístup k „otisku" žádných dat pozůstalých z předchozích úloh. Ve společnosti Ricoh jsme hrdí na fakt, že tuto osvědčenou bezpečnostní funkci nabízíme již více než 20 let.

Služba čištění vyřazených zařízení

Ricoh nabízí službu úplného odstranění dat, což je služba pro vyřazená multifunkční zařízení a tiskárny. Jejich paměťové moduly a disková úložiště jsou neobnovitelně smazána pomocí certifikovaných bezpečnostních řešení. Služby firmy Ricoh v oblasti IT zahrnují i komplexní likvidaci zařízení včetně certifikovaného mazání dat na několika úrovních.

Výměna pevného disku a vyjímatelného úložiště

Ricoh nabízí i službu likvidace pevného disku, díky níž si zákazníci udrží o svém pevném disku přehled - a po jeho vrácení na konci pronájmu jej nahradí novým prázdným pevným diskem. To firmám zaručuje úplnou a prokazatelnou kontrolu nad jejich datovým prostředím.

4 PODPORA

Spolu s rozvojem firem nevyhnutelně roste i počet spojení mezi zařízeními a sítěmi. Firmy potřebují strategie, které zajistí, že takový růst infrastruktury nebude bezpečnostním rizikem. Musí si uvědomovat slabá místa svého systému a podniknout preventivní kroky, které zabrání cíleným i náhodným útokům.

Často jsou k analyzování firemní infrastruktury a odhalení těchto zranitelných míst potřeba specializované znalosti z oboru bezpečnosti IT. Udržování vlastních pracovníků IT s nezbytnými znalostmi, kteří by se starali o kybernetickou bezpečnost, nepřipadá pro mnoho firem v úvahu. Náklady a neekonomičnost takového přístupu tyto firmy často nutí k nebezpečné nečinnosti.

Služba podpory IT poskytovaná firmou Ricoh zahrnuje dodávku a konfiguraci IT, ale i vzdálené monitorování, servisní středisko a správu procesu změny, které dále podporují proces kybernetické bezpečnosti. Ta závisí na holistickém pochopení rizik hrozících firmám. Tým reakce na bezpečnostní incidenty (SIRT) firmy Ricoh zajišťuje sdílení důležitých informací o hrozbách se zákazníky po celém světě a umožňuje okamžitou koordinaci účinných reakcí.

Posouzení bezpečnosti infrastruktury

Funkce správy zařízení Streamline NX (SLNX) firmy Ricoh slouží k provádění nezbytného auditu bezpečnostních zásad. SLNX správcům IT umožňuje nastavovat zařízení podle firemních zásad, tato nastavení distribuovat a analyzovat pomocí grafických přehledů. SLNX také upozorní management, pokud nějaké zařízení firemní zásady nesplňuje.

Optimalizace zabezpečení tisku

Ricoh nabízí komplexní službu optimalizace zabezpečení tisku (PSO) spolu s profesionálními a spravovanými konzultačními službami, které odhalí mezery v zabezpečení zařízení. Jde o webový nástroj s grafickým průvodcem, který umožňuje prohlížet současný stav a umožňuje firmě Ricoh doporučit takové produkty, které existující rizika omezí.

Tým reakce na bezpečnostní incidenty (PSIRT)

Aktivní reakce firmy Ricoh na nové hrozby a vývoj účinných protiopatření jsou řízeny jejím týmem reakce na bezpečnostní incidenty související s produkty (PSIRT). Jde o program, pomocí nějž Ricoh zajišťuje, aby celá naše nabídka produktů (hardware i software) byla průběžně aktualizovaná a chráněná proti nově objeveným hrozbám a zranitelným místům. To nám pomáhá trvale udržovat vysokou úroveň služeb v celosvětovém měřítku a minimalizovat dopad zranitelných míst na produkty Ricoh.

Podpůrná dokumentace

Příprava a instruktáž je zásadní součástí každého systému kybernetické bezpečnosti. Zákazník by měl obdržet záložní dokumentaci, uživatelské příručky, bezpečnostní dokumenty a školení. Stejně jako u mnoha jiných součástí prostředí kybernetické bezpečnosti je i zde nezbytné prokazatelným způsobem splnit zákonné požadavky a tato dokumentace hraje klíčovou roli při ochraně firmy proti ztrátám.

JAK MŮŽE RICOH POMOCI?

Jedinečná pozice společnosti Ricoh při dodávkách špičkových řešení v celém oboru IT a tisku je z části založena na dobrém přehledu o měnících se podmínkách na trhu a na odpovídajícím směřování naší činnosti. Naše řešení jsou navržena tak, aby chránila veškeré informace v průběhu celého jejich životního cyklu a důsledně se držela čtyř aspektů datové bezpečnosti zmiňovaných v této zprávě.

V naší společnosti pracují specializovaní experti, kteří mají za úkol analyzovat potřeby trhu včetně požadavků specifických pro určitý obor. Podle toho pak lze vytvářet nová řešení nebo upravovat řešení stávající.

Kromě toho se své možnosti vytvářet a instalovat řešení zaměřená na bezpečnost snažíme neustále rozvíjet. Proto jsme v rámci naší organizace poskytující služby zřídili specializované týmy, které se soustředí na vývoj nových služeb pro státní správu, management rizik, dodržování předpisů i kybernetickou bezpečnost.

Ověření a autorizace uživatele

- *Důvěrný tisk*
- *Standardní vestavěný software pro ověřování*
- *Ověřování uživatelů a omezení přístupu*
- *Jednotné přihlašování*
- *Více administrátorů s různými rolemi*
- *Ochrana souborů PDF heslem (hesla pro skenované dokumenty)*
- *Ochrana před neoprávněným kopírováním*
- *Kontrola přístupu podle rozsahu IP adres*
- *Bezpečná správa zařízení a tisku*
- *Podpora PKI (infrastruktura veřejného klíče) a karet SmartCard*
- *Bezpečný tisk (print2me / důvěrný tisk)*

Ochrana zařízení proti škodlivému softwaru

- *Servery*
- *Odolné či méně náchylné vůči malwaru*
- *SOP - odolnější verze Androidu*
- *Vlastní operační systém multifunkčních tiskáren (jazyk řízení přístrojů) od firmy Ricoh*
- *Přístup o třech úrovních - digitální podpis, stažení pomocí nástroje Ricoh a použití specifického řídicího jazyku*

Likvidace pevných disků

- *Likvidace pevných disků a přepsání obrazu*
- *Služba úplného odstranění dat*
- *Služba pro vyřazená zařízení: likvidace dat v paměťových modulech a úložištích*

Správa zařízení

- *Nastavování kvót a limitů účtů*
- *DMNX - společný panel pro kontrolu zabezpečení, správu hesel, monitorování a upozornění*

Ochrana systému BIOS a operačního systému

- *Bezpečné spouštění pomocí modulu Trusted Platform Module (TPM)*

Přepsání obrazu a výměnných úložných médií

- *Systém bezpečného přepisu disku (DOSS)*
- *Výměnný pevný disk*

Šifrování dat

- *Šifrování pevného disku pomocí TPM*
- *Šifrovací klíče chráněné pomocí TPM*
- *End-to-end šifrování tištěných a skenovaných souborů pomocí klíče PKI*
- *Pevné disky s certifikací FIPS (Federal Information Processing Standards)*
- *End-to-end šifrování tisku*
- *End-to-end šifrování při skenování*

Aktualizace firmwaru a správa hesel

- *Vzdálený audit hesel*
- *Funkce uzamčení uživatele*
- *Ověření firmwaru pomocí TPM*

Soulad s oborovými předpisy

- *Certifikace ISO 27001*
- *Certifikace IEEE 2600.2 u vybraných produktů*
- *Certifikace ISO 15408 u vybraných produktů*
- *Dokumentace a školení v oboru zabezpečení*

NĚKOLIKASTUPŇOVÝ PŘÍSTUP FIRMY RICOH K ZABEZPEČENÍ ZAŘÍZENÍ

Není pochyb o tom, že úloha dodavatele multifunkčních zařízení je nyní mnohem víc než jednosměrnou transakcí spočívající v dodání hardwaru a zahrnuje i skutečnou správu dat. Multifunkční tiskárny jsou nyní schopny přijímat informace z různých vstupních kanálů, třídit pořízená data a integrovat je do pracovních procesů a bezpečně je ukládat a analyzovat. K tomu je třeba připočíst složitý systém předpisů a požadavků na uchovávání dat, ale i vnější a vnitřní hrozby, které mohou vést ke ztrátě, zničení nebo neoprávněným úpravám dat. K zabezpečení zařízení proto přistupujeme na několika úrovních. Vaše multifunkční tiskárna a systémy, k nimž je připojena, vám díky tomu zajistí nejlepší možnou ochranu.

1. Zařízení

Srdcem všech modelů Ricoh je zařízení. Při jejich návrhu, výrobě i nasazení je bezpečnost jedním z hlavních požadavků. Operační systém používaný pouze firmou Ricoh nesdílí zranitelná místa přítomná v mnoha komerčních operačních systémech. Naše zařízení jsou standardně certifikována podle normy IEEE2600.2. Šifrování pevného disku a bezpečné přepisování disku zajišťují důvěrnost zpracovávaných dat.

2. Chytrý ovládací panel (SOP) funguje jako uživatelské rozhraní

Podobně jako multifunkční tiskárna používá i SOP operační systém firmy Ricoh. Nejsou v něm nainstalovány žádné zbytečné komponenty a kořenový přístup není možný. Firma Ricoh se důsledně postarala o to, aby zavedení chytrého provozního panelu neoslabilo bezpečnost zařízení.

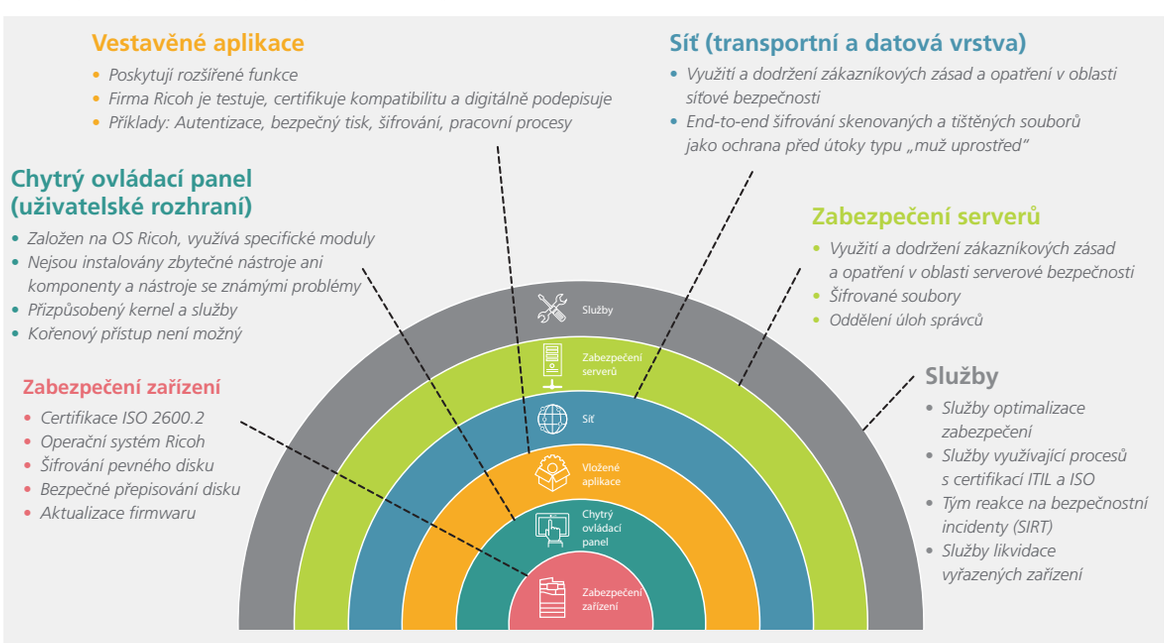
3. Chytré aplikace

Lze je zabudovat do SOP, což uživateli poskytne další funkce včetně pracovních procesů a pořizování dat. Některé aplikace obsahují základní bezpečnostní funkce. Patří mezi ně možnost bezpečného tisku, přístup pomocí karet a šifrování. Aplikace vyvíjí firma Ricoh nebo členové Programu pro vývojáře Ricoh. Před spuštěním v SOP musí všechny aplikace projít testováním kompatibility ve firmě Ricoh a být digitálně podepsány.

4. Síť a servery

Bez ohledu na to, kdo infrastrukturu IT spravuje, se společnost Ricoh stará o to, aby naše produkty a služby vyhovovaly vašim bezpečnostním zásadám pro IT a sítě. End-to-end šifrování tištěných a skenovaných souborů, šifrování dat na serverech a oddělení povinností správců chrání proti hrozbám zevnitř firmy a útokům typu „muž uprostřed".

Celá naše nabídka je doplněna komplexní řadou služeb v oblasti zabezpečení. Patří mezi ně konzultace a spravované služby, které zákazníkům pomáhají sledovat, optimalizovat a spravovat bezpečnost dokumentů a informací. Nabízíme také řadu služeb pro zařízení na konci životnosti, které zajistí důkladně vyčištění pamětí RAM a pevných disků vyřazených zákaznických zařízení.



JAK RICOH CHRÁNÍ DIGITÁLNÍ PRACOVIŠTĚ

Naši zákazníci mají celou řadu významných potřeb v oblasti bezpečnosti. Všechny je podtrhuje známá pravda, že spolu s nárůstem objemu dat roste i počet zranitelných míst, útoků a zákonných pokut. Udržení důvěrnosti, bezpečnosti a neporušenosti dat je neustálý boj. Ve firmě Ricoh například odrážíme měsíčně asi 8 miliard útoků na firewall. Existují desítky tisíc světových, národních i oborových regulací a předpisů vztahujících se na data. Firmy musí být neustále schopny prokázat, že je všechny splňují. Je pochopitelné, že organizace všech velikostí hledají partnera, kterému mohou věřit. Takového, který jim pomůže udržet bezpečnost v rámci portfolia pokrývajícího celé digitální pracoviště.

Společnost Ricoh vyvinula celou řadu řešení mírnících různá rizika, kterým firmy čelí. Situace v oblasti hrozeb pro informační bezpečnost se neuvěřitelně rychle mění. Společnost Ricoh využívá při dalším vývoji a poskytování služeb informací zjištěných v rámci svých programů „Hlas zákazníka".

Naše zákaznické poradní sbory fungují jako důležité strategické zájmové skupiny. Díky nim získáváme lepší informace o trendech, významných hnacích silách a prioritách, které utvářejí podobu obchodních aktivit našich zákazníků. Na našich technologických informačních konferencích se lze dozvědět důležité informace od klíčových osobností. Technické, výzkumné a vývojové týmy společnosti Ricoh na těchto konferencích získávají cennou zpětnou vazbu od zákazníků ohledně nápadů, koncepcí a prototypů.

A konečně, firma Ricoh spolupracuje s jednotlivými zákazníky na vývoji nových a rozšířených bezpečnostních funkcí pro zákazníky na specializovaných i obecných trzích. Tento přístup založený na zákaznících nám pomáhá ověřovat správnost našeho směřování při vývoji produktů. A naši zákazníci díky němu mohou lépe využívat celosvětové sítě podpory a služeb.

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. V celé naší organizaci dodržujeme normu ISO 27001, naše produkty mají certifikaci IEEE 2600 a používají operační systém specifický pro firmy Ricoh. To znamená, že ať se svoji firmu rozhodnete strukturovat a rozvíjet jakkoli, budete stále používat osvědčené bezpečnostní postupy.

Vzhledem k aktuální kombinaci bezpečnostních hrozeb, legislativních požadavků a složitých oborových standardů je nyní riziko poškození pověsti a finančních ztrát způsobených kybernetickými útoky větší, než kdykoli dříve. Přišel tedy čas spolupracovat s důvěryhodným partnerem, který vám pomůže zabezpečit nejzranitelnější firemní aktiva a chránit vaši budoucnost.

RICOH
imagine. change.

www.ricoh.cz