RICOH
imagine. change.

Bezpečnostné riešenia od spoločnosti Ricoh

Chránime váš biznis

Nedostatky v kybernetickom zabezpečení spoločností sú najväčšou hrozbou pre trvalo úspešné pôsobenie na trhu. Spoločnosti všetkých veľkostí sú neustále vystavené hrozbe rušivých útokov, ako je neoprávnené získavanie údajov, cielené preťaženie serverov alebo ransomware. Tieto útoky dokážu spôsobiť škody za milióny. Podľa zistení organizácie Ponemon Institute z roku 2017 bola priemerná výška nákladov na porušenie bezpečnosti osobných údajov 3,62 milióna USD. A keďže štátne nariadenia, ako je nariadenie GDPR, majú za cieľ trestať spoločnosti bez vhodného zabezpečenia svojich systémov a údajov likvidačnými pokutami, táto suma len porastie. Aby sa spoločnosti vyhli týmto prísnym trestom, musia preukázať svoju schopnosť chrániť údaje.
To si vyžaduje celkový pohľad na slabé miesta naprieč celou firmou.

Význam kybernetickej bezpečnosti firiem sa zvyšuje aj z dôvodu rozširovania a digitalizácie moderných pracovísk, ako aj prudkého nárastu množstva údajov. Pracovné postupy sú často rozdelené na viacero zariadení, sietí i lokalít. Hrozba pre informácie je najvyššia, keď sa v rámci firmy prenášajú. Treba ich chrániť počas celej ich cesty. Vzhľadom na úroveň tejto bezpečnostnej hrozby už dnes moderné spoločnosti nemôžu fungovať bez riadne zabezpečených systémov na správu dokumentov a dát. Takisto sa v ostatných rokoch viacnásobne rozšírili funkcie kancelárskych tlačiarní a multifunkčných zariadení. Teraz sú do značnej miery zapojené do vstupov a výstupov dát, ich prenosu a ukladania. Práve preto sú jedným z najzraniteľnejších miest dnešného pracoviska, hoci sa často prehliadajú.

Hoci ponukou bezpečnostných funkcií sa chváli veľa firiem, spoločnosť Ricoh bezpečné riešenia a firemné služby vyvíja už niekoľko desaťročí. Naše tlačiarne napríklad už viac než dvadsať rokov ponúkajú možnosť bezpečného prepisovania pevného disku.

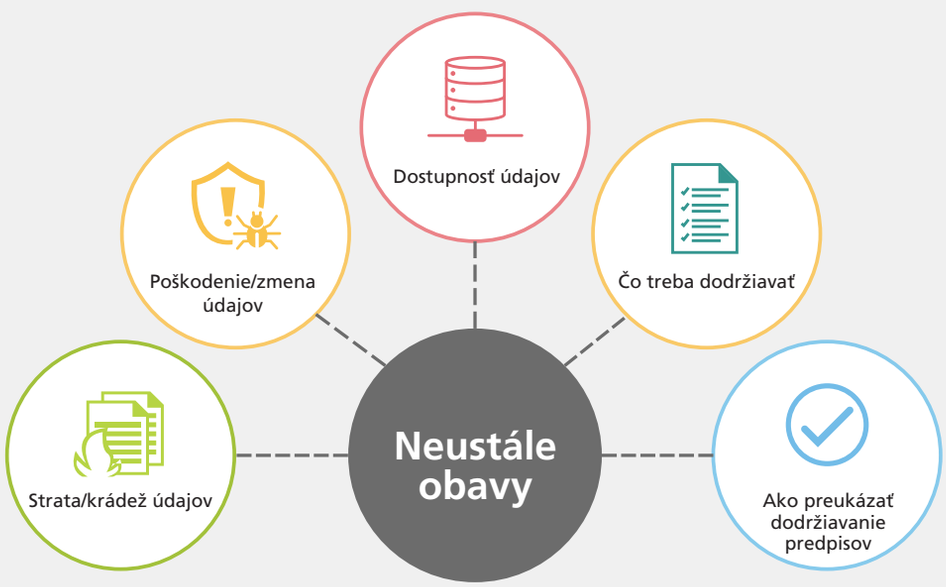
Bezpečnosť tvorí základ nášho portfólia riešení pre digitálne pracoviská. V súčasnosti máme v teréne viac než štyri milióny kancelárskych zariadení. Každý jeden z týchto produktov a každá jedna súvisiaca služba obsahuje zabudované bezpečnostné funkcie. Takisto v mnohých našich zariadeniach používame vlastný operačný systém Ricoh. Ide o hlavnú súčasť našich bezpečnostných obranných systémov, ktoré umožňujú dohľad nad hrozbami pre konkrétne bežne rozšírené operačné systémy i izoláciu od nich.

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 predným členom združenia IEEE Standards Association. Spoločnosť Ricoh je takisto držiteľom osvedčenia ISO 27001 a zaviazala sa trvalo dodržiavať požiadavky tohto systému na správu bezpečnosti informácií. Pri vývoji zariadení máme na pamäti obchodné potreby a bezpečnostné obavy našich zákazníkov vďaka sérii celosvetových programov inovácií zameraných na zákazníka.

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 pre úspech v modernom obchodnom prostredí.

BEZPEČNOSŤ ZÁKAZNÍKOV

TRENDY: Spolu so zvyšovaním objemov údajov sa rozširujú aj slabé miesta, útoky a finančné postihy.



Zabezpečenie a zdokonalenie digitálnych pracovísk

Cieľom spoločnosti Ricoh je umožniť a zabezpečiť digitalizovanú prácu všade tam, kde to ľudia potrebujú. V modernej digitálnej ekonomike to znamená pridávať hodnotu nad rámec tradičných kancelárií aj v prvých líniách. Vzdialené kancelárie a práca na diaľku poskytujú spoločnostiam veľa flexibility a lepšiu produktivitu pri každodennej prevádzke. Pomáhajú spoločnostiam lepšie spĺňať očakávania zákazníkov a ich požiadavky na úroveň služieb.

Fungovanie na okraji siete však pre bezpečnosť firmy znamená jednu z najväčších hrozieb. Údaje, ktoré títo pracovníci vytvárajú, a vzdialené zariadenia, ktorými ich digitalizujú, treba riadne zabezpečiť. Celú úlohu ďalej komplikuje skutočnosť, že zamestnanci často pracujú naprieč jednotlivými sieťami a lokalitami. Je dôležité poznamenať, že v rámci štátnych nariadení, ako je nariadenie GDPR, sa od firiem vyžaduje, aby dokázali preukázať bezpečnosť údajov počas celého ich životného cyklu. V opačnom prípade im hrozia vážne postihy. Pracoviská sa vyvíjajú a čoraz viac využívajú digitálne pracovné postupy, čo postupne komplikuje životný cyklus obchodných údajov. Pozrime sa na to krok za krokom.

Prvým krokom je zadávanie údajov a zariadení, ktoré ich digitalizujú. Je to životne dôležitá zložka bezpečnostných obranných systémov spoločnosti Ricoh. Potom je potreba dáta preniesť pomocou sietí a bezpečne uložiť. V tejto fáze je nevyhnutné zachovanie integrity údajov. V rámci systémov Ricoh sa obmedzuje prístup používateľov k funkciám zariadení a sietí s cieľom zaistiť, aby sa s prenášanými aj uloženými údajmi nedalo manipulovať. Medzi tieto služby patrí dohľad nad prístupom, šifrovanie a ochrana pred kopírovaním. Hovoríme tomu Riadené spracovanie dát.

Dokumenty však musia byť po uložení tiež jednoducho prístupné pre tých ľudí v rámci spoločnosti, ktorí ich potrebujú. Na tejto dostupnosti závisí možnosť kedykoľvek podľa potreby informácie účinne využívať. Analýza údajov je životne dôležitou súčasťou výkonného digitálneho pracoviska. Ponúka účinný prehľad o všetkých prvkoch biznisu, od predaja po ľudské zdroje. Nástroje zabezpečenej infraštruktúry poskytujú rýchly bezpečný prístup bez ohľadu na umiestnenie používateľa alebo výber zariadenia. Je nevyhnutné, aby bezpečnostné protokoly nestáli v ceste inováciám ani funkčnosti, prípadne, aby sa nestretli s odporom zamestnancov. Túto fázu nazývame Uchovanie dát.

Údaje je napokon nutné likvidovať bezpečným spôsobom, ktorý možno preukázať. Tento krok je nevyhnutný pri dodržiavaní požiadaviek právnych predpisov a minimalizuje hrozbu následnej krádeže alebo straty dát. Tento postup je v skutočnosti aktívny počas celého životného cyklu dokumentu aj pri jeho konečnom odstránení. Tlač akéhokoľvek súboru zanecháva latentný obraz na pevnom disku multifunkčných zariadení, ktorý musí byť prepísaný, aby sa zabránilo neoprávnenému prístupu. Medzi služby spoločnosti Ricoh na likvidáciu údajov patrí čistenie pevného disku, vynulovanie pamäte, odstránenie nevytlačených súborov a odstránenie pri odhlásení, aby sa zabránilo hekerom v zostavovaní citlivých informácií z dát, ktoré dokument zanechá. Hovoríme tomu Likvidácia.

Spoločnosť Ricoh využíva na účinné zabezpečenie údajov používaných na pracovisku počas ich celého životného cyklu tzv. princípy DDI (angl. CIA) pre ochranu osobných údajov a bezpečnosť: Dôvernosť, dostupnosť a integrita. Pri zaisťovaní dodržiavania nevyhnutných noriem a predpisov u našich produktov a riešení sa riadime práve týmito princípmi. Tento prístup umožňuje inovácie a rast na pracovisku a zároveň zachováva postupy účinné a bezpečné.

PRÍSTUP SPOLOČNOSTI RICOH K BEZPEČNOSTI

Riadime sa troma princípmi ochrany osobných údajov a bezpečnosti podľa skratky DDI (CIA): dôverný charakter informácií, integrita and dostupnosť

Bezpečnosť máme v krvi. Súčasťou každého produktu a každej služby spoločnosti Ricoh sú vstavené bezpečnostné funkcie a schopnosti

Spoločnosť Ricoh ponúka úplný sortiment bezpečnostných produktov a služieb na zabezpečenie vytvárania dokumentov od začiatku do konca.

Teraz sa pozrieme na jednotlivé kľúčové fázy: riadenie, uchovanie dát, likvidáciu a podporu.

ŠTYRI FÁZY ZABEZPEČENIA DIGITÁLNEHO PRACOVISKA

1 DOHĽAD

Účinný dohľad na údajmi je nevyhnutný na zachovanie ich dôverného charakteru a integrity. Obchodné informácie sú primárnym aktívom, ktoré treba chrániť. Súčasné hardvérové zariadenia sú informačnými terminálmi, ktoré môžu predstavovať zraniteľné brány k obchodným informáciám. Spoločnosť Ricoh preto využíva množstvo nástrojov na overovanie používateľov a správu zariadení s cieľom zabezpečovať obchodné informácie a dohliadať nad nimi. Týkajú sa nastavení fyzických zariadení, ktoré umožňujú či obmedzujú prístup k určitým funkciám a údajom. Obmedzenie prístupu zamestnancov k informáciám prechádzajúcim akýmkoľvek multifunkčným zariadením v kancelárii predstavuje nevyhnutný a overený krok na zachovanie bezpečnosti dokumentov. Fáza dohľadu tiež zahŕňa ochranu zariadení pred škodlivým softvérom prostredníctvom trojstupňového prístupu spoločnosti Ricoh k firmvéru na zariadeniach.

Dohľad nad neoprávneným vytváraním kópií

Aby sa zabránilo pokusom o neoprávnené vytváranie kópií, spoločnosť Ricoh ponúka elegantné riešenia, ktoré zaisťujú bezpečnosť tlačených dokumentov. Funkcia ochrany proti kopírovaniu vytlačí alebo skopíruje dokumenty so špeciálnymi neviditeľnými vzormi vloženými na pozadí. Pokiaľ sa tlačené alebo kopírované dokumenty kopírujú alebo skenujú, tieto vložené vzory sa na kópiách objavia. Modul ochrany proti neoprávnenému kopírovaniu umožňuje multifunkčnému zariadeniu odhaliť tieto vložené vzory a nahradiť kopírovaný obrázok šedou farbou, a tak zabrániť úniku informácií. Táto funkcia je užitočná pri tlači informácií dôvernej povahy. Obmedzenie duplikovania dôverných informácií predchádza takémuto druhu úniku informácií.

Dôverná tlač

Dokument z počítača možno uložiť na pevnom disku multifunkčného zariadenia. Pomocou funkcie dôvernej tlače môže používateľ pred odoslaním dokumentu zadať heslo, ktoré je treba pred tlačou opäť zadať na multifunkčnom zariadení. Keďže dokument sa nevytlačí pred tým, než sa jeho majiteľ bude nachádzať pri zariadení, dôverná tlač zaisťuje dohľad majiteľa nad týmto dokumentom.

Pokročilé zabezpečenie získavania dát

Portfólio pokročilých riešení pre bezpečnú digitalizáciu dát spoločnosti Ricoh ponúka rôzne vrstvy šifrovania a dešifrovania vo všetkých vrstvách spracovania počas jednotlivých fáz digitalizácie. Správcovia môžu povoliť prístup k frontám procesov podľa prihlasovacích údajov jednotlivých používateľov alebo podľa poverení skupiny. Medzi ďalšie vrstvy zabezpečenia patrí Security Assertion Markup Language (SAML) pre rámec jednotného prihlásenia (SSO), šifrovanie osobnej identity (PIV) a šifrovanie verejnej kľúčovej infraštruktúry (PKI).

Vstavaná autentizácia

Protokoly prístupu k zariadeniam a overenia totožnosti vo všetkých produktoch Ricoh možno spravovať centralizovane. Medzi dostupné spôsoby patrí preukaz totožnosti, PIN, prihlasovacie údaje do siete alebo viacfaktorová kombinácia týchto spôsobov. Viacfaktorové overovanie zvyšuje bezpečnosť, môže však spomaliť zaneprázdnených používateľov. Jednotné prihlásenie (SSO) tento problém odstraňuje, keďže používateľom umožňuje bezproblémový prístup k viacerým zariadeniam. Okrem toho je na našich zariadeniach vopred nainštalovaný softvér spoločnosti Ricoh na rýchle overenie pomocou kariet, ktorý umožňuje používateľom jednoduchý prístup k dokumentom. Použitie čítačky/zapisovača NFC výrazne zjednodušuje proces prihlasovania používateľa, pričom účinne zabezpečuje prístup k multifunkčnému zariadeniu a poskytuje nad ním dohľad. Tento druh prístupu funguje aj v spojení s existujúcimi povoleniami multifunkčného zariadenia, ktoré obmedzujú prístup používateľa na tie funkcie zariadenia, ktoré určil zákazník.

Streamline NX (SLNX)

Modul správcu zariadení v rámci platformy Streamline NX spoločnosti Ricoh je softvérom spoločnosti Ricoh na správu a monitorovanie zariadení v sieti. Tento softvér umožňuje správcom zobraziť alebo nakonfigurovať nastavenia zabezpečenia pre zariadenia pomocou predpripravených šablón a vlastných parametrov. Medzi kľúčové nastavenia zabezpečenia patrí zapnutie/vypnutie protokolov, nastavenie IP adresy, heslá správcovských používateľov, e-mailové adresy pre upozornenia, nastavenia šifrovania a ďalšie. Modul SLNX takisto umožňuje upozorniť na všetky zariadenia, ktoré nespĺňajú vaše požiadavky bezpečnostných zásad.

Ochrana zariadení pre škodlivým softvérom

Prístup spoločnosti Ricoh k ochrane svojich zariadení pre škodlivým softvérom je trojstupňový. Zariadenia Ricoh v prvom rade možno prevádzkovať len s použitím programovacieho jazyka alebo operačného systému, ktorý využíva len spoločnosť Ricoh. Aby sa zabránilo škodlivej manipulácii so softvérom zariadenia, musia byť všetky aktualizácie firmvéru v druhom rade napísané a schválené výhradne v programovacom jazyku Ricoh. A napokon musí spoločnosť Ricoh každú aktualizáciu firmvéru digitálne podpísať. Pomocou tejto trojstupňovej metódy nemožno na zariadenia Ricoh načítať neschválený firmvér, takže škodlivý softvér, spyware a vírusy sú účinne eliminované.

Bezpečnosť fyzických dokumentov

Overená prax v oblasti bezpečnosti nemusí byť vždy zložitá. V kanceláriách je vždy ruch a tlačená dokumentácia predstavuje výraznú obchodnú hrozbu, či už ide o krádež alebo nedbalosť zamestnancov. Spoločnosť Ricoh ponúka niekoľko doplňujúcich možností zabezpečenia na predchádzanie neoprávnenému prístupu k tlačeným dokumentom. Zamykanie zásobníkov napríklad predchádza krádeži špeciálnych papierových tlačív, ako sú šablóny na predpis liekov v prostredí zdravotnej starostlivosti a pod.. Montáž výplňových dosiek pre všetky káble tiež zabraňuje možnosti narušenia od vnútorných hrozieb. Bezpečná tlač dokumentu (tzv. Print2Me) zabezpečuje, že dokumenty sa vytlačia len vtedy, keď je prítomný ich vlastník, aby sa eliminovalo riziko pozabudnutia.

2 UCHOVANIE DÁT

Firmy musia v súlade s požiadavkami nových i aktuálnych právnych predpisov zaistiť dôverný charakter informácií, aby nemohlo dôjsť k ich krádeži ani úniku, i trvalú integritu, aby ich nebolo možné zmeniť. Na dosiahnutie týchto cieľov musia spoločnosti obmedziť prístup k dokumentom citlivej povahy. Predchádza sa tak neoprávnenej úprave a falšovaniu. Tiež pôsobí ako ochrana pred cielenými alebo príležitostnými hrozbami v rámci spoločnosti.

Mobilná práca komplikuje každý variant kybernetickej hrozby. Na prispôsobenie zdieľania súborov z akéhokoľvek miesta je nutné zaviesť ďalšie bezpečnostné opatrenia. Tieto súbory musia byť zabezpečené počas prenosu sieťami a zariadeniami i počas ich uchovávania. Výkonná šifrovacia technológia dokáže účinné sledovať a chrániť údaje naprieč celým ich životným cyklom. Týka sa to nielen samotných dokumentov, ale aj ďalších zásadných bezpečnostných prvkov, ako sú uložené heslá, nastavenia makier a adresáre. Vďaka zavedenému šifrovaniu sa hekerom možno podarí získať prístup k vašej sieti, už však budú len ťažko extrahovať akékoľvek zmysluplné informácie, čo zaručí ich integritu aj v prípade narušenia.

Pre mnoho odvetví je prvoradé vyhýbať sa prestojom. Nepredvídateľné okolnosti, ako sú živelné pohromy, teda predstavujú priamu obchodnú hrozbu. V takejto situácii sú mimoriadne zraniteľné najmä papierové dokumenty. Používanie bezpečného úložiska na báze cloudovej technológie pre digitalizované dokumenty prináša nutnú odolnosť voči pohromám spôsobeným živlami i človekom. Na zachovanie týchto digitálnych údajov je však nutné prijať vhodné bezpečnostné opatrenia.

Šifrovanie dôležitých údajov

Ak chcete ochrániť informácie pohybujúce sa naprieč zariadeniami, je možné využívať šifrovanie pre všetky údaje, ktoré prechádzajú alebo sa nachádzajú na pevnom disku multifunkčného zariadenia Ricoh. Vstavané softvérové možnosti poskytujú úplné šifrovanie pre súbory na tlač a skenovanie prostredníctvom kľúča verejnej kľúčovej infraštruktúry používateľa (PKI). Údaje sú tak chránené pred útokmi „prostredníkov" v rámci IT prostredia zákazníka.

Pre zvýšenú bezpečnosť sú takisto údaje určené na tlač neustále prepisované pomocou bezpečnostného systému prepisovania údajov (DOSS) spoločnosti Ricoh, o ktorom si povieme viac neskôr v časti o fáze zničenia v životnom cykle údajov.

Ochrana BIOS a operačného systému

Multifunkčné tlačiarne Ricoh používajú modul TPM (Trusted Platform Module), čo je bezpečnostný modul pre zabezpečenie hardvéru. Modul TPM vykonáva kryptografické funkcie a bezpečne ukladá kryptografické údaje. Spoločnosť Ricoh používa modul TPM na ukladanie šifrovacieho kľúča, ktorý chráni šifrovací kľúč údajov pevného disku a digitálne osvedčenie multifunkčných zariadení. Umožňuje tiež správcom vykonať operáciu dôveryhodného spúšťania, pričom overí pravosť firmvéru multifunkčného zariadenia skôr, ako mu umožní prevádzku.

Overenie firmvéru

Kľúč a kryptografické funkcie sú vždy obsiahnuté v module TPM a nemôžu byť zmenené z vonkajšej strany brány firewall, čo zabraňuje zneužitiu alebo škodlivému zásahu do našich produktov. Tento postup umožňuje vysokú úroveň overenia firmvéru multifunkčného zariadenia, totožnosti zariadenia, ako aj zabezpečenie pevného disku. Ide o ďalší dobrý príklad toho, ako sú multifunkčné zariadenia spoločnosti Ricoh navrhnuté s bezpečnostnými záujmami zákazníkov ako prioritou.

Správa hesiel

Zariadenia Ricoh možno nakonfigurovať s viacerými používateľmi ako správcami, z ktorých každý môže mať na zariadeniach rôzne úlohy a odlišné heslá. Heslá pre týchto používateľov možno nakonfigurovať na diaľku pomocou webových správcovských nástrojov a pravidelne overovať. Umožňuje to „oddelenie povinností," čo je požiadavka, ktorú určuje mnoho nariadení o obchodnej činnosti.

Obmedzenie prístupu používateľov

Nástroj na správu používateľov spoločnosti Ricoh umožňuje správcom systému obmedziť prístupové práva používateľov. Správca môže napríklad nastaviť práva tak, aby umožnil vybraným používateľom prístup k registrovanému adresáru multifunkčného zariadenia. Zabraňuje sa tak neoprávnenému prístupu k osobným údajom a záznamom uloženým v kancelárskych zariadeniach.

Zablokovanie prístupu používateľov

Pokiaľ budú v priebehu prihlasovacieho procesu opakovane zadané nesprávne heslá, multifunkčné zariadenie Ricoh môže posúdiť, či sa niekto pokúša o zistenie hesla. Spustí sa tak funkcia zablokovania, ktorá zabráni prístupu zo strany daného používateľa. Zablokované používateľské meno nemožno overiť ani vtedy, ak sa skombinuje so správnym heslom. Zablokovanie možno ukončiť až po uplynutí určitého času alebo zo strany správcu, čo marí pokusy nádejných hekerov.

3 LIKVIDÁCIA

Bezpečná likvidácia údajov tvorí základnú súčasť všetkej komplexnej ochrany pred kybernetickými útokmi. Je ľahké nadobudnúť dojem, že obchodná zodpovednosť za údaje sa končí, keď organizáciu opustia. Mnoho nariadení však určuje, že likvidácia údajov musí byť komplexný proces odstraňujúci všetko riziko následnej krádeže alebo zneužitia. Kým to nedokážete preukázať, povinnosti firmy v súvislosti s údajmi naďalej trvajú.

Reklamované či opravované kancelárske zariadenia a zariadenia na konci životnosti predstavujú hrozbu pre obchodné informácie, na ktorú sa často zabúda. Spoločnosť Ricoh ponúka osvedčenú a auditovateľnú službu na odstraňovanie údajov z týchto zariadení na konci životnosti. Súčasťou je bežne prehliadaný materiál, ako sú uložené nastavenia siete, používateľské údaje, údaje o pevnom disku alebo dokonca aj nálepky, ktoré zostali nalepené na zariadení. Pokiaľ sa spoločnosti týmito hľadiskami nezaoberajú, existuje značné riziko sprístupnenia dôverných informácií o spoločnosti a jej zamestnancoch. Aby ste však trvalo dodržiavali požiadavky právnych predpisov, tento postup by sa mal neustále diať aj počas životnosti zariadenia. Tak zaručíte, aby vaša spoločnosť mala najvyššiu možnú úroveň dohľadu nad údajmi, za ktoré zodpovedá.

Prepisovanie obrazov: Bezpečnostný systém prepisovania údajov (DOSS)

Pevné disky multifunkčných zariadení účinne fungujú tak, že ukladajú latentné obrázky dokumentu do svojej pamäte pre spracovanie úloh. Bezpečnostné riešenie prepisovania údajov od spoločnosti Ricoh zaisťuje ich prepísanie pred začiatkom ďalšej úlohy. Ak by sa teda ktokoľvek pokúšal o prístup k pevnému disku so škodlivým úmyslom, nemal by prístup k „odtlačku" akýchkoľvek údajov, ktoré na ňom zostali po predchádzajúcich úlohách. V spoločnosti Ricoh sme hrdí na to, že toto overené bezpečnostné opatrenie môžeme ponúkať už viac než 20 rokov.

Služba čistenia na konci životnosti

Spoločnosť Ricoh ponúka službu Úplné čistenie údajov, službu pre multifunkčné zariadenia a tlačiarne na konci životnosti, ktoré majú všetky pamäťové moduly a ukladacie miesto na disku zariadenia vymazané bez možnosti obnovy pomocou bezpečnostných riešení osvedčených v rámci odvetvia. IT služby spoločnosti Ricoh ponúkajú aj komplexnú službu likvidácie zariadení vrátane niekoľkých úrovní osvedčených služieb na vymazávanie údajov.

Výmena pevného disku a vymeniteľného úložiska

Spoločnosť Ricoh takisto ponúka službu likvidácie pevného disku, ktorá zákazníkom umožňuje ponechať si svoj pevný disk a pri vrátení vybavenia na konci prenájmu ho nahradiť novým a prázdnym. To zaručuje úplný a preukázateľný dohľad spoločnosti nad prostredím svojich údajov.

4 PODPORA

Ako firmy rastú, nevyhnutne rastie aj počet prepojení medzi jednotlivými zariadeniami a sieťami. Tieto firmy potrebujú stratégie na zaistenie toho, aby rast infraštruktúry nepredstavoval bezpečnostnú hrozbu. Musia si byť vedomé slabých stránok svojho systému, aby podnikli kroky na predchádzanie cielených a príležitostných útokov.

Na rozbor podnikovej infraštruktúry a určenie týchto slabých miest sa často vyžaduje špecializovaná odbornosť v oblasti bezpečnosti IT. Mnoho firiem jednoducho nemá možnosť zamestnávať vlastných IT pracovníkov s nevyhnutnými znalosťami na správu svojho kybernetického bezpečnostného prostredia. Náklady a nedostatky tohto prístupu často nútia tieto spoločnosti do nebezpečnej nečinnosti.

Služba podpory IT spoločnosti Ricoh ponúka služby obstarávania a konfigurácie IT, ako aj funkcie vzdialeného monitorovania, servisného stola a riadenia prechodu, ktoré ďalej podporujú proces kybernetickej bezpečnosti. Kybernetická bezpečnosť závisí od celkového porozumenia obchodným hrozbám. Tím odozvy na bezpečnostné incidenty (SIRT) spoločnosti Ricoh zaisťuje zdieľanie životne dôležitých informácií so zákazníkmi po celom svete a okamžitú koordináciu účinnej odozvy.

Posúdenie bezpečnosti infraštruktúry

Funkcia správcu zariadení v rámci platformy Streamline NX (SLNX) spoločnosti Ricoh je navrhnutá tak, aby vykonávala neoceniteľnú funkciu auditu bezpečnostných zásad. Platforma SLNX poskytuje funkciu, ktorá manažérom IT umožňuje nastaviť zariadenia na základe firemných zásad, distribuovať tieto nastavenia a analyzovať nastavenia pomocou vizualizovaného prehľadu. Služba SLNX takisto môže manažment upozorniť, pokiaľ určité zariadenie nespĺňa firemné zásady.

Optimalizácia bezpečnosti tlače

Spoločnosť Ricoh ponúka komplexnú službu optimalizácie bezpečnosti tlače (PSO) spolu s odbornými a riadenými konzultačnými službami s cieľom určiť bezpečnostné nedostatky súvisiace s jednotlivými zariadeniami. Ide o webový nástroj s grafickým sprievodcom, ktorý poskytuje prehľad o aktuálnom stave a umožňuje spoločnosti Ricoh ponúkať odporúčania produktov s cieľom znížiť hrozbu.

Tím odozvy na bezpečnostné incidenty (PSIRT)

Aktívnu odozvu spoločnosti Ricoh na nové hrozby a vývoj účinných protiopatrení spravuje tím odozvy na bezpečnostné incidenty produktov spoločnosti Ricoh (PSIRT). Ide o program, ktorý spoločnosť Ricoh používa na zaistenie toho, aby bol celý balík produktov (hardvér aj softvér) neustále aktualizovaný a chránený proti novým identifikovaným hrozbám a zraniteľným miestam. To nám pomáha udržovať konzistentne vysokú úroveň služieb na celosvetovej škále a minimalizovať dosah problémov produktov Ricoh so zraniteľnosťou.

Podporná dokumentácia

Príprava a vzdelávanie je kľúčovým prvkom všetkých systémov kybernetickej bezpečnosti. Zákazníkovi treba poskytnúť zálohovú dokumentáciu, používateľské príručky, bezpečnostné biele knihy i školenia. Rovnako ako pri mnohých prvkoch kybernetického bezpečnostného prostredia je i tu preukázateľné dodržiavanie predpisov nevyhnutné, a táto dokumentácia zohráva kľúčovú úlohu pri zabezpečovaní základov podnikov.

AKO VÁM MÔŽE SPOLOČNOSŤ RICOH POMÔCŤ?

Jedinečná pozícia spoločnosti Ricoh na zabezpečenie špičkových bezpečnostných riešení v celom prostredí IT a tlače je čiastočne daná trvalým porozumením meniacich sa podmienok na trhu a zodpovedajúcim vývojom našej stratégie. Naše riešenia sú navrhnuté tak, aby chránili všetky informácie počas celého ich životného cyklu a úzko sa dotýkali štyroch oblastí bezpečnosti údajov, ktorým sme sa venovali v tejto správe.

Máme k dispozícii špecializovaných odborníkov, ktorí zodpovedajú za analýzu potrieb trhu vrátane požiadaviek špecifických pre dané odvetvie, pre +ktoré je možné pripraviť nové riešenia alebo prispôsobiť súčasné riešenia.

Takisto je pre nás prioritou vývoj našich interných kapacít na navrhovanie a uvádzanie bezpečnostných riešení. V rámci našej organizácie pre rozvoj služieb sme s týmto cieľom vytvorili špecializované tímy, ktoré sa zameriavajú na vývoj nových služieb pre štátne orgány, riadenie rizík, dodržiavanie predpisov aj kybernetických bezpečnostných služieb.

Overovanie a autorizácia používateľa

- Dôverná tlač
- Vložený softvér pre overovanie ako základná súčasť
- Overovanie/obmedzenie prístupu používateľov
- Jednotné prihlásenie
- Viacero správcov s rozdielnymi úlohami
- Ochrana heslom pre dokumenty PDF (heslo pre skenované dokumenty)
- Ochrana proti neoprávnenému kopírovaniu
- Dohľad nad prístupom založený na rozsahu IP
- Bezpečná správa zariadení a tlače
- PKI (verejná kľúčová infraštruktúra) / podpora čipových kariet
- Bezpečná tlač (print2me / dôverná tlač)

Ochrana zariadení pre škodlivým softvérom

- Servery
- Menej náchylné na poškodenie škodlivým softvérom
- SOP - posilnená verzia systému Android
- Operačný systém (riadiaci programovací jazyk) multifunkčných zariadení, ktorý využíva len spoločnosť Ricoh
- Trojstupňový prístup - digitálny podpis, preberanie pomocou nástroja Ricoh, musí byť napísané v špecifickom riadiacom jazyku

Likvidácia pevných diskov

- Likvidácia pevných diskov, prepisovanie obrázkov,
- Úplné čistenie údajov
- Služby na konci životnosti: likvidácia údajov v pamäťových moduloch, uchovávanie

Správa zariadení

- Nastavenie kvót/obmedzenie účtov
- DMNX - jednoduchá tabuľa bezpečnostného auditu, správa hesiel, monitorovanie, upozornenia

Ochrana BIOS a operačného systému

- Bezpečné spúšťanie pomocou modulu dôveryhodnej platformy (TPM)

Prepisovanie obrazov a vymeniteľných pamäťových médií

- Bezpečnostný systém prepisovania disku (DOSS)
- Vymeniteľný pevný disk

Šifrovanie údajov

- Šifrovanie pevného disku prostredníctvom modulu TPM
- Šifrovacie kľúče prostredníctvom modulu TPM
- Úplné šifrovanie súborov na tlač a skenovanie pomocou kľúča PKI
- Pevný disk osvedčený podľa noriem FIPS (Federal Information Processing Standards)
- Úplné šifrovanie pre tlač
- Úplné šifrovanie pre skenovanie

Aktualizácie firmvéru a správa hesiel

- Vzdialený audit hesiel
- Zablokovanie prístupu používateľov
- Overenie firmvéru prostredníctvom modulu TPM

Dodržiavanie priemyselných noriem

- Osvedčenie ISO 27001
- Osvedčenie IEEE 2600.2 pre vybrané produkty
- Osvedčenie ISO 15408 pre vybrané produkty
- Bezpečnostná dokumentácia a školenia

VIACSTUPŇOVÝ PRÍSTUP SPOLOČNOSTI RICOH K BEZPEČNOSTI ZARIADENÍ

Niet pochýb o tom, že úloha poskytovateľa multifunkčných zariadení sa vyvinula ďaleko nad transakčné, jednorozmerné poskytovanie hardvéru až k skutočnému spravovaniu údajov. Funkcie multifunkčných zariadení dnes zahŕňajú digitalizáciu informácií z viackanálových vstupov, klasifikáciu digitalizovaných údajov a integráciu pracovných postupov, ako aj ich bezpečné a zabezpečené uchovávanie a analýzu. V tejto komplexnej sieti prísnych viacúrovňových pravidiel a požiadaviek na uchovávanie - spolu s vnútornými a vonkajšími hrozbami, ktoré ohrozujú záznamy zo straty, zničenia alebo manipulácie - používame viacstupňový prístup k bezpečnosti zariadení, aby sme zabezpečili, že vaše multifunkčné zariadenie a systémy, ktoré spája, poskytujú tú najlepšiu možnú ochranu.

1. Zariadenie

Srdcom všetkých modelov spoločnosti Ricoh je samotné zariadenie. Pri ich návrhu, výrobe a zavádzaniu je bezpečnosť základnou požiadavkou. Operačný systém, ktorý využíva len spoločnosť Ricoh, nezdieľa slabé miesta, ktoré sa vyskytujú v mnohých komerčných operačných systémoch, a naše zariadenia sú štandardne osvedčené podľa normy IEEE2600.2. Šifrovanie pevného disku a jeho bezpečné prepisovanie zaručuje zachovanie dôverného charakteru spracovávaných údajov.

2. Chytrý ovládací panel (SOP) poskytuje používateľské rozhranie

Podobne ako MFP, aj chytrý ovládací panel obsahuje operačný systém, ktorý využíva len spoločnosť Ricoh. Neinštalujú sa žiadne zbytočné komponenty a prístup k hlavnému adresáru nie je možný. Spoločnosť Ricoh tvrdo pracovala na tom, aby zaistila, že bezpečnosť zariadení sa so zavedením panelu SOP neoslabí.

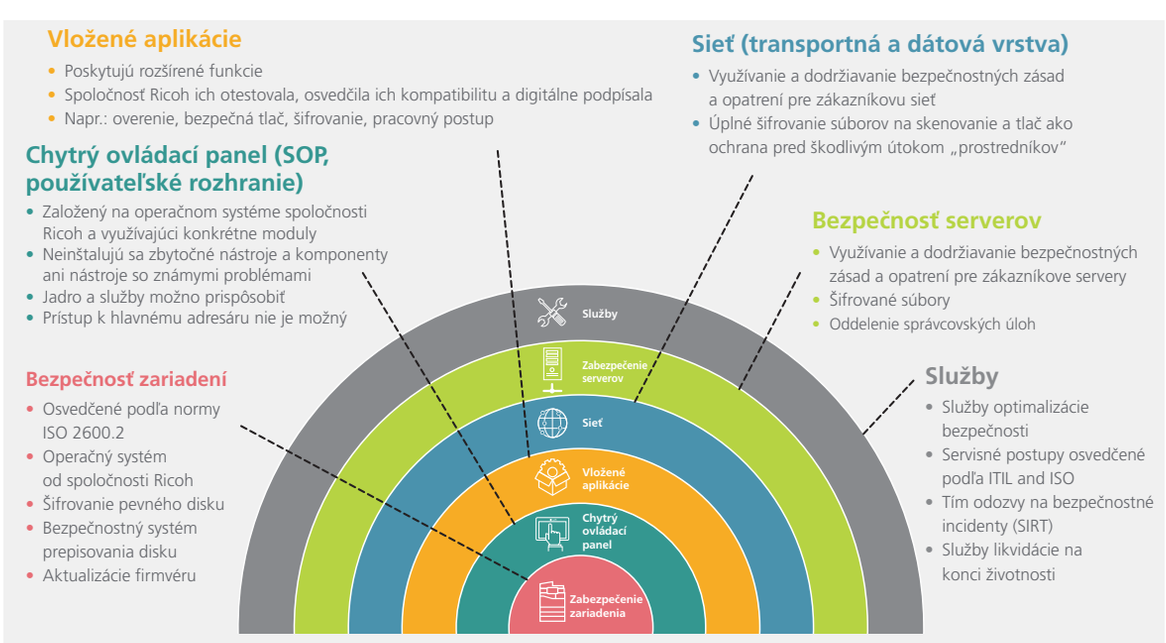
3. Chytré aplikácie

Tieto aplikácie možno vložiť do panelu SOP, aby používateľom poskytli ďalšie funkcie vrátane pracovných postupov a digitalizácie údajov. Niektoré aplikácie poskytujú základné bezpečnostné funkcie. Ide napríklad o možnosti bezpečnej tlače, prístup kartami a šifrovanie. Tieto aplikácie vyvíja spoločnosť Ricoh alebo členovia vývojárskeho programu Ricoh, a všetky musia pred použitím v paneli SOP prejsť testovaním kompatibility SOP a byť digitálne podpísané.

4. Siete a servery

Spoločnosť Ricoh zaručuje, že jej produkty a služby vyhovujú vašim zásadám bezpečnosti IT a sietí bez ohľadu na to, kto vám spravuje infraštruktúru IT. Úplné šifrovanie súborov na tlač a skenovanie, šifrovanie údajov na serveroch či oddelenie správcovských povinností sú spôsoby, ako sa chrániť pred škodlivým útokom zvnútra alebo od „prostredníkov."

Celý náš sortiment zahŕňa komplexnú škálu bezpečnostných služieb. Patria sem poradenské a správcovské služby, ktoré pomáhajú zákazníkom monitorovať, optimalizovať a spravovať bezpečnosť svojich dokumentov a informácií. Takisto máme pre zákazníkov k dispozícii škálu služieb na konci životnosti zariadení, ktoré zaistia vyčistenie pamäte RAM a pevného disku pred ich likvidáciou.



AKO SPOLOČNOSŤ RICOH CHRÁNI DIGITÁLNE PRACOVISKO

Naši zákazníci čelia niekoľkým kľúčovým bezpečnostným problémom, ktoré sú podložené skutočnosťou, že spolu so zvyšovaním objemov údajov sa rozširujú aj slabé miesta, útoky a postihy. Zachovanie dôvernej a bezpečnej povahy údajov, ako aj ich ochrana pred manipuláciou je neustály boj. V spoločnosti Ricoh napríklad odrážame približne 8 miliárd útokov na brány firewall mesačne. Jestvujú desiatky tisíc celosvetových, vnútroštátnych a priemyselných nariadení o ochrane údajov a firmy musia byť schopné nepretržite preukazovať dodržiavanie každého z nich. Je pochopiteľné, že organizácie všetkých veľkostí hľadajú partnera, ktorému môžu dôverovať - partnera, ktorý im pomôže udržať si bezpečnosť v rámci portfólia, ktoré pokrýva celé digitálne pracovisko.

Spoločnosť Ricoh vyvinula širokú škálu riešení na zmiernenie rôznych hrozieb, ktorým podniky čelia. Vzhľadom na to, že povaha bezpečnostných hrozieb sa vyvíja neuveriteľne rýchlo, spoločnosť Ricoh pri ďalšom rozvoji a dodávaní služieb čerpá z ohlasov zákazníkov.

Naše zákaznícke poradenské rady fungujú ako kľúčové strategické skupiny. Využívame ich na lepšie pochopenie trendov, katalyzátorov a priorít, ktoré formujú firmy našich zákazníkov. Naše technologické poradenské konferencie poskytujú dôležité poznatky od kľúčových rozhodovacích orgánov. Technické oddelenie a oddelenie výskumu a vývoja využíva tieto konferencie na získanie hodnotnej odozvy zákazníkov k nápadom, konceptom a prototypom. Spoločnosť Ricoh takisto spolupracuje s jednotlivými zákazníkmi pri vývoji nových a rozšírených bezpečnostných funkcií pre zákazníkov na vertikálnom i všeobecnom trhu. Tento prístup založený na zákazníkoch, ktorý nám pomáha overovať plány našich produktov, pomáha našim zákazníkom využívať celosvetovú sieť služieb a podpory.

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 svojím pracoviskom. Dodržiavanie predpisov normy ISO 27001 naprieč celou našou organizáciou, ako aj osvedčenie IEEE 2600 pre všetky naše produkty spolu s ich jedinečným operačným systémom od spoločnosti Ricoh znamená, že overené postupy dohľadu nad vaším biznisom sú vám k dispozícii bez ohľadu na to, ako sa ho rozhodnete štruktúrovať a rozvíjať.

Kombinácia bezpečnostných hrozieb, legislatívnych požiadaviek a zložitých priemyselných noriem znamená, že hrozba finančných škôd a škôd na dobrom mene z kybernetických útokov nikdy nebola vyššia. Teraz nastal čas spolupracovať s dôveryhodným partnerom, ktorý vám pomôže zabezpečiť najzraniteľnejšie aktíva vašej firmy a ochrániť vaše budúce ambície.

RICOH
imagine. change.

www.ricoh.cz