Ricoh-beveiligingsoplossingen

Wij helpen u om uw organisatie te beveiligen

RICOH
imagine. change.

Cyberbeveiliging is de grootste bedreiging voor het overleven en succes van moderne organisaties. Kleine en grote organisaties lopen constant het risico het slachtoffer te worden van ontwrichtende aanvallen, zoals phishing, DDos-aanvallen en ransomware. De werkelijke kosten van deze aanvallen lopen in de miljoenen. In 2017 berekende het Ponemon Institute dat een gegevenslek wereldwijd gemiddeld € 3,11 miljoen kost. Deze kosten zullen de komende jaren alleen maar toenemen. Wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), bestraffen organisaties namelijk met hoge boetes als ze hun systemen en gegevens niet op de juiste manier beveiligen. Een organisatie moet gegevens aantoonbaar beschermen als het deze straffen wil vermijden. Hiervoor hebben organisaties inzage nodig in alle kwetsbare gebieden.

Andere beveiligingsuitdagingen voor organisaties zijn de uitbreiding en digitalisering van de moderne werkplek. Maar ook de explosieve toename van de hoeveelheid data. Workflows lopen vaak via verschillende apparaten en netwerken, en over verschillende landsgrenzen heen. De meeste risico's liggen op de loer wanneer de informatie rondgaat binnen een organisatie. De informatie moet in elk stadium van het traject worden beveiligd. Met het oog op beveiligingsrisico's kunnen moderne organisaties niet meer functioneren zonder gedegen beveiligde document- en gegevensbeheersystemen. Tegelijkertijd hebben kantoorprinters en multifunctionele printers (MFP's) de afgelopen jaren veel meer mogelijkheden gekregen. Deze apparaten zijn nu belast met een enorm deel van de invoer, uitvoer, overdracht en opslag van bedrijfsgegevens. Dit maakt ze tot een van de grootste bedreigingen op de hedendaagse werkplek. Toch worden deze apparaten vaak over het hoofd gezien.

Hoewel veel spelers op de markt beweren beveiligingsfuncties aan te bieden, ontwikkelt Ricoh al decennialang beveiligde werkplekoplossingen en -services. Onze printers zijn bijvoorbeeld al meer dan 20 jaar voorzien van beveiligingsfuncties voor het overschrijven van harde schijven.

Beveiliging zit in ons DNA en is een integraal onderdeel van ons portfolio voor de digitale werkplek. Momenteel staan meer dan 4 miljoen van onze kantoorproducten bij klanten op de werkvloer. Elk van deze producten is voorzien van ingebouwde beveiligingsfuncties. Dat geldt ook voor elke service die we inzetten in combinatie met deze apparaten. Daarnaast voorzien wij veel van onze producten van ons eigen Ricoh-besturingssysteem. Dit is een belangrijk onderdeel van onze beveiligingsstrategie. Onze producten zijn hierdoor namelijk niet toegankelijk voor bedreigingen die specifiek zijn gericht op de bekende besturingssystemen.

Ricoh biedt overal ter wereld dezelfde service- en supportstructuur. Wij zorgen ervoor dat informatie over bedreigingen efficiënt wordt gedeeld en er adequaat wordt ingegrepen. Standaard voldoen al onze printers en MFP's aan de IEEE 2600-norm. Daarnaast is Ricoh toonaangevend lid van en belangrijke opsteller voor de IEEE-SA (Institute of Electrical and Electronics Engineers Standards Association). Verder is Ricoh gecertificeerd volgens ISO 27001 en vastberaden zich te allen tijde aan deze standaard voor informatiebeveiliging te houden. Wij laten ons bij de ontwikkeling van onze producten leiden door de zakelijke behoeften en beveiligingsproblemen van onze klanten. Dit doen wij door middel van een aantal wereldwijde, klantgerichte innovatieprogramma's.

De basis van al onze producten en services is beveiliging. Ricoh neemt dan ook de best practices voor effectieve en aantoonbare cyberbeveiliging in al zijn ontwerpen mee. Nooit achteraf. En het maakt niet uit hoe veeleisend deze zijn. Volgens ons is een moderne organisatie alleen in staat om te overleven dankzij inzage in alle kwetsbare gebieden.

UITDAGINGEN RONDOM BEVEILIGING

TRENDS: Samen met de toenemende hoeveelheden gegevens neemt het aantal zwakke plekken, aanvallen en boetes ook toe.

Digitale werkplekken beveiligen en versterken

Ricoh wil altijd en overal digitaal werken faciliteren en beveiligen. In een moderne digitale economie betekent dit meerwaarde bieden buiten de grenzen van het traditionele kantoor. Nu werknemers altijd en overal werken, voeren organisaties hun dagelijkse werkzaamheden veel flexibeler en productiever uit. Zo kunnen ze beter voldoen aan de verwachtingen van hun klanten en de eisen die de klant aan hun dienstverlening stelt.

Flexibel werken vormt echter een van de grootste risico's voor de beveiliging van een organisatie. De gegevens die deze werknemers genereren en de externe apparaten waarop ze deze gegevens opslaan, moeten op passende wijze worden beveiligd. Werknemers werken vaak via verschillende netwerken of over landsgrenzen heen, waardoor deze taak nog ingewikkelder wordt. Van doorslaggevend belang zijn wetgevingen zoals de AVG. Hierin wordt van organisaties geëist dat ze hun gegevens aantoonbaar beveiligd opslaan tot deze niet meer nodig zijn. Zo niet, dan riskeren ze hoge boetes. De werkplek ondergaat een grote verandering en digitale workflows worden steeds normaler. Daarom neemt de complexiteit van de levenscyclus van bedrijfsgegevens gestaag toe. Laten we dat even per stadium bekijken.

Het begint al bij de apparaten waarmee gegevens worden ingevoerd en vastgelegd. Deze apparaten vormen een essentieel onderdeel van Ricoh's beveiligingsstrategie. Daarna moeten gegevens via netwerken worden verstuurd en veilig worden opgeslagen. In dit stadium is het behouden van de gegevensintegriteit van cruciaal belang. Gebruikers krijgen maar beperkt toegang tot de apparaat- en netwerkfuncties van Ricoh-systemen. Dit voorkomt manipulatie van gegevens die onderweg zijn of gegevens in opslag. Hiervoor gebruiken we toegangscontrole, codering en kopieerbeveiliging. We noemen dit het controlestadium.

Medewerkers moeten echter ook snel toegang hebben tot opgeslagen documenten. Ze moeten de informatie kunnen raadplegen wanneer ze die nodig hebben. Daarnaast is gegevensanalyse uitermate belangrijk voor een effectieve digitale werkplek. Aan de hand van gegevensanalyses krijgt een organisatie inzicht in de gegevens op elke afdeling; van sales tot HR. Met autorisatiehulpprogramma's krijgen bevoegden snel en veilig toegang tot gegevens, ongeacht de locatie van de gebruiker en welk apparaat hij of zij gebruikt. Beveiligingsprotocollen

mogen innovatie en functionaliteit absoluut niet hinderen. Dat kan namelijk resulteren in weerstand bij werknemers. We noemen dit het opslagstadium.

Ten slotte moeten deze gegevens op een veilige, controleerbare manier worden verwijderd. Deze stap is van cruciaal belang voor het voldoen aan wet- en regelgeving en een minimale kans op diefstal of verlies. Dit proces vindt gedurende de hele levenscyclus van een document plaats en bij definitieve verwijdering. Als u een bestand afdrukt, wordt er namelijk een verborgen beeld achtergelaten op de harde schijf van MFP's. Dit beeld moet worden overschreven om te voorkomen dat onbevoegden er toegang toe krijgen. De gegevensverwijdering van Ricoh bestaat onder andere uit het opschonen van de harde schijf, het wissen van het geheugen en het verwijderen van niet-afgedrukte bestanden. Ook is verwijderen bij uitloggen standaard ingesteld, om te voorkomen dat hackers gevoelige informatie verzamelen uit de sporen die een document achterlaat. We noemen dit het vernietigingsstadium.

Om de werkplekgegevens effectief te beveiligen tijdens de gehele levenscyclus, maakt Ricoh gebruik van de CIA-principes voor privacy en beveiliging: Confidentiality, Integrity and Availability (Vertrouwelijkheid, Integriteit en Beschikbaarheid). Dit zijn de leidende principes voor ons bij het ontwerpen van onze producten en oplossingen om aan de vereiste normen en wet- en regelgeving te voldoen. Deze benadering zorgt voor innovatie en ontwikkeling van de werkplek met behoud van effectieve, veilige processen.

BEVEILIGINGSBENADERING VAN RICOH

Wij volgen de CIA-principes voor privacy en beveiliging: Confidentiality, Integrity and Availability (Vertrouwelijkheid, Integriteit en Beschikbaarheid)

Beveiliging zit in ons DNA. Alle Ricoh-producten en -services bevatten geïntegreerde beveiligingsfuncties en -opties

Ricoh biedt een complete reeks aan beveiligingsproducten en -services om documenten vanaf het begin tot het einde te beveiligen. We gaan nu alle belangrijke stadia in detail bekijken: controle, opslag, vernietiging en support.

VIER STADIA VOOR DE BEVEILIGING VAN DIGITALE WERKPLEKKEN

1 CONTROLE

Effectieve controle van gegevens is cruciaal om de vertrouwelijkheid en integriteit van gegevens te kunnen waarborgen. Bedrijfsinformatie is het grootste goed van een organisatie en moet worden beschermd. De hardware van tegenwoordig is een informatieterminal die een kwetsbare toegang tot bedrijfsinformatie kan vormen. Daarom gebruikt Ricoh voor het toezicht op en het beveiligen van organisatiegegevens een aantal hulpprogramma's voor gebruikersverificatie en apparaatbeheer. Deze hulpprogramma's maken deel uit van de apparaatinstellingen die de toegang tot bepaalde functies en gegevens toestaan of beperken voor werknemers. Beperking tot informatie die via een MFP op kantoor loopt, is een cruciale stap om de beveiliging van een document te waarborgen. Tot dit stadium behoort ook de beveiliging van apparaten tegen malware. Ricoh hanteert hierbij een drievoudige aanpak die betrekking heeft op de firmware van apparaten.

Controle van onbevoegd kopiëren

Ricoh biedt een slimme oplossing om papieren documenten te beveiligen tegen pogingen tot onbevoegd kopiëren. De kopieerbeveiligingsfunctie kopieert of drukt documenten af met een speciaal, onzichtbaar patroon op de achtergrond. Wanneer het afgedrukte of gekopieerde document wordt gekopieerd en/of gescand, is het patroon op de achtergrond zichtbaar op kopieën. De MFP herkent het patroon op de achtergrond dankzij de beveiligingsmodule voor onbevoegd kopiëren. De gekopieerde tekst of afbeelding wordt dan vervangen door een grijze afbeelding. Zo worden informatielekken voorkomen. Deze functie is handig wanneer vertrouwelijke informatie wordt afgedrukt. Doordat vermenigvuldiging van vertrouwelijke informatie wordt beperkt, wordt een informatielek voorkomen.

Beveiligd afdrukken

Een document dat wordt verzonden via een computer, kan op de harde schijf van de MFP worden opgeslagen. Met behulp van de functie voor beveiligd afdrukken wordt er een wachtwoord vastgelegd wanneer een gebruiker het document verzendt. Dat wachtwoord moet op de MFP worden ingevoerd. Pas dan kan het document worden afgedrukt. Het document wordt niet afgedrukt zolang de persoon die de printopdracht heeft gegeven, niet bij het apparaat is. Zodoende wordt gewaarborgd dat het document onder toezicht van deze persoon blijft.

Geavanceerde beveiliging voor gegevensopslag

Ricoh's aanbod met geavanceerde oplossingen voor gegevensopslag bestaat uit diverse (de)coderingsmogelijkheden op alle verwerkingsniveaus en tijdens alle opslagstadia. Een beheerder kan individuele gebruikers of een gebruikersgroep met behulp van een inlogfunctie toegang geven tot verwerkingswachtrijen. Aanvullende beveiligingsniveaus omvatten Security Assertion Markup Language (SAML) voor eenmalig inloggen, Personal Identity Verification (PIV) en Public Key Infrastructure (PKI).

Embedded verificatiemethoden

Toegang tot apparaten en identiteitsverificatieprotocollen kunnen voor alle Ricoh-producten centraal worden beheerd. Beschikbare verificatiemethoden zijn een ID-kaart, PIN-code, inloggen via een netwerk of een combinatie van deze drie methoden. Een combinatie van de drie verificatiemethoden verhoogt de beveiliging, maar kan de productiviteit van gebruikers verlagen. Dit kan worden opgelost met eenmalig inloggen, waarmee gebruikers probleemloos toegang krijgen tot een reeks apparaten. Daarnaast wordt Quick Authentication van Ricoh standaard geïnstalleerd

op al onze apparaten. Met deze verificatiesoftware kunnen gebruikers eenvoudig een pasje langs het apparaat swipen, waarna ze direct toegang tot hun documenten hebben. Het gebruik van een NFC-lezer/-schrijver vereenvoudigt het inlogproces van de gebruiker aanzienlijk en beveiligt de toegang tot de MFP. Deze manier van toegang werkt ook in combinatie met de geïntegreerde MFP-machtigingsinstellingen. Zo kunt u de toegang van gebruikers tot de apparaatfuncties beperken.

Streamline NX (SLNX)

De module voor apparaatbeheer binnen het Ricoh Streamline NX-platform is authentieke Ricoh-software voor het beheren en monitoren van apparaten op een netwerk. Met deze software kan een beheerder beveiligingsinstellingen voor apparaten bekijken of configureren met behulp van templates of zelf ingestelde parameters. Cruciale beveiligingsinstellingen zijn het in-/uitschakelen van protocollen, IP-adresinstellingen, beheerderswachtwoorden, e-mailadressen voor waarschuwingen, coderingsinstellingen enz. SLNX rapporteert tevens printers die niet voldoen aan uw beleid.

Bescherming van apparaten tegen malware

Ricoh beschermt zijn apparaten tegen malware op drie niveaus. Ten eerste werken Ricoh-apparaten alleen met een Ricoh-apparaattaal of -besturingssysteem. Ten tweede moeten alle firmware-updates uitsluitend in deze Ricoh-apparaattaal worden geschreven en goedgekeurd om manipulatie van de software op het apparaat te voorkomen. Ten slotte moet elke firmware-update digitaal worden ondertekend door Ricoh. Door deze driestappenmethode kan niet-goedgekeurde firmware niet op Ricoh-apparaten worden geïnstalleerd, waardoor malware, spyware en virussen effectief worden geëlimineerd.

Beveiliging van papieren documenten

Beveiliging hoeft niet altijd ingewikkeld te zijn. Kantoren zijn drukke omgevingen en papieren documenten vormen met het oog op diefstal en nalatigheid van werknemers een wezenlijk risico voor de organisatie. Ricoh biedt ook een aantal extra fysieke beveiligingsopties om onbevoegde toegang tot papieren documenten te voorkomen. Vergrendeling van papierladen verhindert bijvoorbeeld diefstal van gevoelige papiervoorraden zoals receptpapier in de gezondheidszorg. Ook montage van kabelafdekkingen voorkomt geknoei met apparatuur vanuit de interne organisatie. Een beveiligingsoplossing voor documentvrijgave (Follow You) zorgt ervoor dat documenten alleen worden afgedrukt wanneer de persoon aanwezig is die de printopdracht heeft gegeven. Zo wordt gewaarborgd dat het document niet in het bezit van iemand anders komt.

2 OPSLAG

Volgens nieuwe en bestaande wet- en regelweving moeten organisaties de vertrouwelijkheid van informatie waarborgen. Dit voorkomt informatielekken en informatiediefstal. Daarnaast moet de integriteit van de informatie worden gewaarborgd. Er moeten dus geen wijzigingen aan informatie kunnen plaatsvinden. Om dit te bereiken moeten organisaties de toegang tot gevoelige documenten beperken. Dit voorkomt onbevoegde wijziging en vervalsing. Bovendien dient het als beveiliging tegen gerichte of opportune bedreigingen binnen de organisatie.

Mobiel werken maakt cyberbeveiliging nog moeilijker. Er zijn extra beveiligingsmaatregelen nodig om het delen van bestanden vanaf elke locatie mogelijk te maken. Zulke bestanden moeten net zo goed worden beveiligd tijdens de overdracht via netwerken en tussen apparaten als tijdens opslag. Krachtige coderingstechnologie zorgt voor effectieve bescherming en tracering van gegevens gedurende de hele levenscyclus. Dit is natuurlijk van toepassing op documenten, maar geldt ook voor andere wezenlijke elementen die beveiligd dienen te worden, zoals opgeslagen wachtwoorden, macro-instellingen

en adresboeken. Zelfs als hackers toegang tot uw netwerk zouden krijgen, is het dankzij de codering buitengewoon moeilijk om aan bruikbare informatie te komen. In geval van een gegevenslek blijft de integriteit dan behouden.

Een constante uptime is voor veel organisaties van groot belang. Onvoorspelbare gebeurtenissen zoals natuurrampen zijn daarom een direct bedrijfsrisico. Papieren documenten zijn in zo'n geval extra kwetsbaar. Door gebruik te maken van een beveiligde cloudopslag voor gedigitaliseerde documenten, wordt de bescherming tegen menselijke fouten en natuurrampen aanzienlijk verhoogd. Er moeten echter passende beveiligingsmaatregelen worden genomen om deze digitale gegevens te beschermen.

Gegevenscodering is essentieel

Gegevenscodering beschermt informatie die zich van het ene apparaat naar het andere verplaatst. U kunt dan ook instellen of informatie die naar een harde schijf van een Ricoh-MFP wordt verstuurd of daar wordt opgeslagen, moet worden gecodeerd. Ingebouwde software-opties bieden end-to-end-codering voor gescande en afgedrukte bestanden door middel van een PKI-sleutel (Public Key Infrastructure) van de gebruiker. Zo'n sleutel beschermt tegen interne aanvallen binnen uw IT-omgeving.

Voor extra beveiliging worden de afdrukgegevens ook voortdurend overschreven door het Ricoh Data Overwrite Security System (DOSS). Dit proces wordt uitvoeriger beschreven in het vernietigingsstadium van de levenscyclus van gegevens.

BIOS- en besturingssysteembeveiliging

Ricoh-MFP's maken gebruik van een Trusted Platform Module (TPM). Dit is een hardwarebeveiligingsmodule waarmee niet kan worden geknoeid. De TPM voert cryptografische functies uit en slaat cryptografische gegevens veilig op. Ricoh gebruikt de TPM om de rootcoderingssleutel op te slaan die de gegevenscoderingssleutel van de harde schijf en het digitale certificaat van MFP's beschermt. De TPM stelt een beheerder bovendien in staat om een MFP veilig opnieuw op te starten. Hierbij wordt de authenticiteit van de MFP-firmware geverifieerd voordat deze kan worden bediend.

Firmwarevalidatie

De rootsleutel en de cryptografische functies maken altijd deel uit van de TPM. Ze kunnen niet van buiten de firewall worden gewijzigd, waardoor manipulatie of misbruik van Ricoh-producten wordt voorkomen. Dit proces garandeert validatie van de firmware van de MFP, de identiteit van het apparaat en de beveiliging van harde schijven op hoog niveau. Wederom een goed voorbeeld dat Ricoh bij het ontwerpen van MFP's de beveiligingsbelangen van zijn klanten voorop stelt.

Wachtwoordbeheer

Ricoh-apparaten kunnen worden geconfigureerd met meerdere beheerders, elk met verschillende wachtwoorden en bevoegdheden (rollen) op de apparaten. De wachtwoorden van beheerders kunnen op afstand worden geconfigureerd met behulp van webbased beheerhulpprogramma's en kunnen regelmatig worden geverifieerd. Dankzij de rolverdeling is een taakverdeling mogelijk, zoals dat is vastgelegd in een aantal organisatievoorschriften.

Toegangsrechten van gebruikers beperken

Met het hulpprogramma voor gebruikersbeheer van Ricoh kunnen beheerders de toegangsrechten van gebruikers beperken. Zo kan de beheerder rechten instellen om geselecteerde gebruikers toegang te geven tot een geregistreerd adresboek van een MFP. Hierdoor wordt de toegang tot persoonlijke gegevens en records die op kantoorapparaten zijn opgeslagen, geblokkeerd voor onbevoegden.

Blokkering van gebruikers

Als er tijdens het inloggen meerdere keren een onjuist wachtwoord wordt ingevoerd, kan een Ricoh-MFP beoordelen of iemand het wachtwoord probeert te kraken. In zo'n geval wordt de betreffende gebruikersnaam geblokkeerd. Ook met het juiste wachtwoord kan de geblokkeerde gebruikersnaam niet meer worden geverifieerd. De blokkering kan pas na een bepaalde tijd of door een beheerder worden opgeheven, zodat potentiële hackers worden tegengehouden.

3 VERNIETIGING

Veilige verwijdering van gegevens is een essentieel onderdeel van elk cyberbeveiligingsbeleid. Veel organisaties denken dat de verplichting tot bescherming eindigt wanneer een organisatie de gegevens niet meer nodig heeft. Verschillende wet- en regelgeving bepalen echter dat de vernietiging van gegevens een allesomvattend proces moet zijn. Zo wordt diefstal of misbruik uitgesloten. De organisatieverplichtingen zijn daarom nog niet voorbij, zolang gegevensvernietiging niet kan worden bewezen.

Kantoorapparaten die zijn afgedankt of teruggegeven, vormen vaak een onbekend risico op het uitlekken van bedrijfsinformatie. Ricoh biedt een gecertificeerde service voor het verwijderen van gegevens van afgedankte printers. Dit proces is tevens geschikt voor audits. De service bestaat onder meer uit het verwijderen van vergeten gegevens, zoals opgeslagen netwerkinstellingen, gebruikersgegevens, hardeschijfgegevens of zelfs stickers die op het apparaat zijn geplakt. Als deze gegevens niet worden verwijderd, bestaat er een groot risico voor de organisatie dat vertrouwelijke organisatie- en persoonsgegevens op straat komen te liggen. Om voor compliance te zorgen, moet dit proces gedurende de volledige levenscyclus van een apparaat continu worden uitgevoerd. Dit zorgt voor een maximale mate van controle over de gegevens waarvoor organisaties verantwoordelijk zijn.

Overschrijven van gegevens: Data Overwrite Security System (DOSS)

Harde schijven van MFP's functioneren efficiënt door verborgen documentgegevens in hun geheugen op te slaan voor taakverwerking. Het DOSS-systeem van Ricoh zorgt ervoor dat zulke gegevens altijd worden overschreven, voordat de volgende taak begint. Als iemand kwaadwillend toegang tot de harde schijf zou krijgen, heeft hij/zij geen toegang tot de 'voetafdruk' van gegevens, omdat deze niet zijn achtergebleven van eerdere taken. Bij Ricoh zijn we er trots op dat we deze veiligheidsmaatregel al meer dan 20 jaar aanbieden.

Volledige gegevensvernietiging aan het einde van de contractduur

Onze Data Cleansing Service, een service voor het veilig vernietigen van resterende gegevens op printers en MFP's, vernietigt alle resterende gegevens, zodat ze niet kunnen worden hersteld. Ricoh gebruikt hiervoor gecertificeerde beveiligingsoplossingen. Ricoh IT Services biedt ook een allesomvattende verwijderingsservice die uit diverse niveaus van gecertificeerde gegevensverwijdering bestaat.

Vervanging van de harde schijf en externe geheugens

Ricoh biedt ook een vernietigingsservice voor harde schijven aan. De harde schijf wordt dan aan het einde van een leaseovereenkomst vervangen door een nieuwe, lege harde schijf wanneer u de apparatuur aan ons teruggeeft. Op deze manier kunnen organisaties aantonen dat ze volledige controle over hun gegevensomgeving hebben.

4 SUPPORT

Wanneer organisaties groeien, is de groei van het aantal verbindingen tussen apparaten en netwerken ook onvermijdelijk. Organisaties hebben strategieën nodig om ervoor te zorgen dat deze groei van de infrastructuur geen beveiligingsrisico vormt. Zij moeten zich bewust zijn van de zwakke punten in hun systeem. Zo kunnen er maatregelen worden genomen om doelgerichte en opportune aanvallen te voorkomen.

Vaak is gespecialiseerde IT-beveiligingskennis nodig om de infrastructuur van een organisatie te analyseren en deze zwakke punten te identificeren. Voor veel organisaties is het geen optie om intern IT-personeel met de nodige kennis van cyberbeveiligingsbeheer aan te houden. De kosten en inefficiëntie leiden er vaak toe dat organisaties geen intern personeel aannemen voor zulke taken. En dat kan gevaarlijk zijn.

IT-support van Ricoh omvat het aanschaffen en configureren van de IT-omgeving, monitoren op afstand en servicedesk- en overgangsbeheer. Zo ondersteunen we het cyberbeveiligingsproces. Cyberbeveiliging vereist een holistische benadering van organisatierisico's. Ricoh's Security Incident Response Team (SIRT) zorgt ervoor dat kennis over vitale bedreigingen wordt gedeeld met klanten over de hele wereld. Zo kan er effectief en snel worden ingegrepen.

Evaluatie van de beveiliging van de infrastructuur

De functie voor apparaatbeheer van Ricoh Streamline NX (SLNX) is zeer geschikt voor audits en is daarmee een onmisbare beveiligingsbeleidsfunctie. SLNX heeft een functie waarmee IT-managers apparaten op basis van het organisatiebeleid kunnen instellen. Ze kunnen instellingen distribueren en analyseren aan de hand van een rapport. SLNX kan het management ook waarschuwen als een apparaat niet voldoet aan het organisatiebeleid.

Print Security Optimisation

Naast Print Security Optimisation (PSO) biedt Ricoh tevens een professionele en managed consultancy-service om apparaatgerelateerde beveiligingslekken te identificeren. Dit is een webbased hulpprogramma met een grafische wizard die een overzicht geeft van de actuele toestand. Met dit hulpprogramma kan Ricoh producten aanbevelen om risico's tot een minimum te beperken.

Product Security Incident Response Team (PSIRT)

De reactie van Ricoh op nieuwe bedreigingen en de ontwikkeling van effectieve tegenmaatregelen wordt beheerd door het PSIRT-team van Ricoh. Dit is een programma dat Ricoh gebruikt om ervoor te zorgen dat het volledige productaanbod (hardware en software) van Ricoh voortdurend wordt geüpdatet en beschermd tegen nieuwe bedreigingen en zwakke plekken. Dit helpt ons om wereldwijd een hoog serviceniveau te handhaven en problemen met de kwetsbaarheid van producten van Ricoh te beperken.

Ondersteunende documentatie

Voorbereiding en training is een wezenlijk onderdeel van elk goed cyberbeveiligingsbeleid. U ontvangt back-updocumentatie, gebruikershandleidingen, beveiligingswhitepapers en training. Zoals bij veel elementen van cyberbeveiliging is aantoonbare compliance van cruciaal belang. Deze documentatie speelt daarbij een doorslaggevende rol voor organisaties.

HOE KAN RICOH U HELPEN?

Ricoh bevindt zich in een unieke positie bij het leveren van toonaangevende beveiligingsoplossingen voor de gehele afdruk- en IT-omgeving vanwege onze kennis over de veranderende markt. Vervolgens passen wij onze koers hierop aan. Onze oplossingen zijn ontworpen om alle informatie gedurende de volledige levenscyclus te beschermen. Ze sluiten dan ook nauw aan op de vier stadia van gegevensbeveiliging die in dit rapport worden genoemd.

We beschikken over toegewijde vakinhoudelijke experts die verantwoordelijk zijn voor het analyseren van de marktbehoeften, inclusief sectorspecifieke eisen. Vervolgens ontwerpen we nieuwe oplossingen of passen we bestaande oplossingen aan.

Bovendien streven we ernaar om onze interne capaciteit te vergroten, zodat we beveiligingsgerichte oplossingen kunnen bouwen en implementeren.Met dit doel voor ogen hebben we toegewijde teams in onze serviceorganisatie opgericht die zich richten op het ontwikkelen van nieuwe overheids-, risicomanagement-, compliance- en cyberbeveiligingsservices.

Gebruikersverificatie en -autorisatie

- Beveiligd afdrukken
- Standaard embedded verificatiesoftware
- Gebruikersverificatie/Toegangsbeperking
- Eenmalig inloggen
- Meerdere beheerdersrollen
- Wachtwoordbeveiliging voor PDF-bestanden (wachtwoord voor gescand document)
- Beveiliging tegen onbevoegd kopiëren
- Toegangscontrole op basis van IP-bereik
- Veilig apparaat- en afdrukbeheer
- PKI (Public Key Infrastructure)/Ondersteunt smartcards
- Veilig afdrukken (Follow You/beveiligd afdrukken)

Bescherming van apparaten tegen malware

- Servers
- Niet/minder gevoelig voor malware
- Smart Operation Panel met beveiligde versie van Android
- Eigen Ricoh-versie van besturingssysteem (besturingstaal van apparaat) voor MFP's
- In 3 lagen - digitale handtekening, downloaden via Ricoh-hulpprogramma, moet in specifieke besturingstaal worden geschreven

Vernietiging van harde schijven

- Vernietiging van harde schijven, afbeeldingen overschrijven
- Volledige service voor gegevensvernietiging (Data Cleansing Service)
- Vernietiging van gegevens op geheugenmodules en in opslag aan einde van contractduur

Apparaatbeheer

- Limieten instellen/accountlimieten
- DMNX: één geïntegreerde beheerinterface voor beveiligingsaudits, wachtwoordbeheer, monitoren, versturen van alerts

Bescherming van BIOS en besturingssysteem

- Veilig opstarten met Trusted Platform Module (TPM)

Afbeeldingen overschrijven en verwijderbaar geheugen

- Disk Overwrite Security System (DOSS)
- Verwijderbare harde schijf

Gegevenscodering

- Hardeschijfcodering met TPM
- Coderingssleutels met TPM
- End-to-end-codering van afgedrukte en gescande bestanden met PKI-sleutel
- FIPS-gecertificeerde harde schijf (Federal Information Processing Standards)
- End-to-end-codering voor afdrukken
- End-to-end-codering voor scannen

Firmware-updates en wachtwoordbeheer

- Wachtwoordaudit op afstand
- Functie voor blokkeren van gebruikers
- Firmwarevalidering via TPM

Compliance met industriestandaarden

- ISO 27001-certificering
- IEEE 2600.2-certificering voor geselecteerde producten
- ISO 15408-certificering voor geselecteerde producten
- Beveiligingsdocumentatie en training

RICOH'S GELAAGDE AANPAK VOOR APPARAAT-BEVEILIGING

De rol van de MFP-leverancier omhelst ondertussen zonder twijfel meer dan alleen de transactionele, eendimensionale levering van hardware. Het omvat tegenwoordig ook gegevensbeheer. De mogelijkheden van MFP's reiken tegenwoordig van informatieopslag vanaf meerdere bronnen, classificatie van opgeslagen gegevens en workflowintegratie, tot aan veilige opslag en analysefuncties. Ricoh hanteert een gelaagde aanpak voor apparaatbeveiliging, zodat uw organisatie zo goed mogelijk wordt beschermd. En dat is wel nodig in het huidige, complexe landschap van strenge wet- en regelgeving en retentievereisten. Om nog maar niet te spreken over de interne en externe bedreigingen die een risico vormen voor verlies, vernietiging of manipulatie van bedrijfsgegevens.

1. Het apparaat

De kern van elk Ricoh-model is het apparaat zelf. Beveiliging is een basisvereiste bij het ontwerp, de productie en de implementatie van een apparaat. De zwakke punten van veel commerciële, seriematige besturingssystemen komen niet voor in het eigen Ricoh-besturingssysteem. Bovendien zijn onze apparaten standaard gecertificeerd volgens IEEE 2600.2. De hardeschijfcodering en de overschrijfbeveiliging van de schijf zorgen ervoor dat de gegevens die worden verwerkt, vertrouwelijk blijven.

2. De gebruikersinterface: Smart Operation Panel (SOP)

Net als de MFP maakt het SOP gebruik van een eigen Ricoh-besturingssysteem. Er worden geen onnodige componenten geïnstalleerd en toegang tot de root is niet mogelijk. Ricoh heeft hard gewerkt om ervoor te zorgen dat de beveiliging van het apparaat niet is verslechterd door de introductie van het SOP.

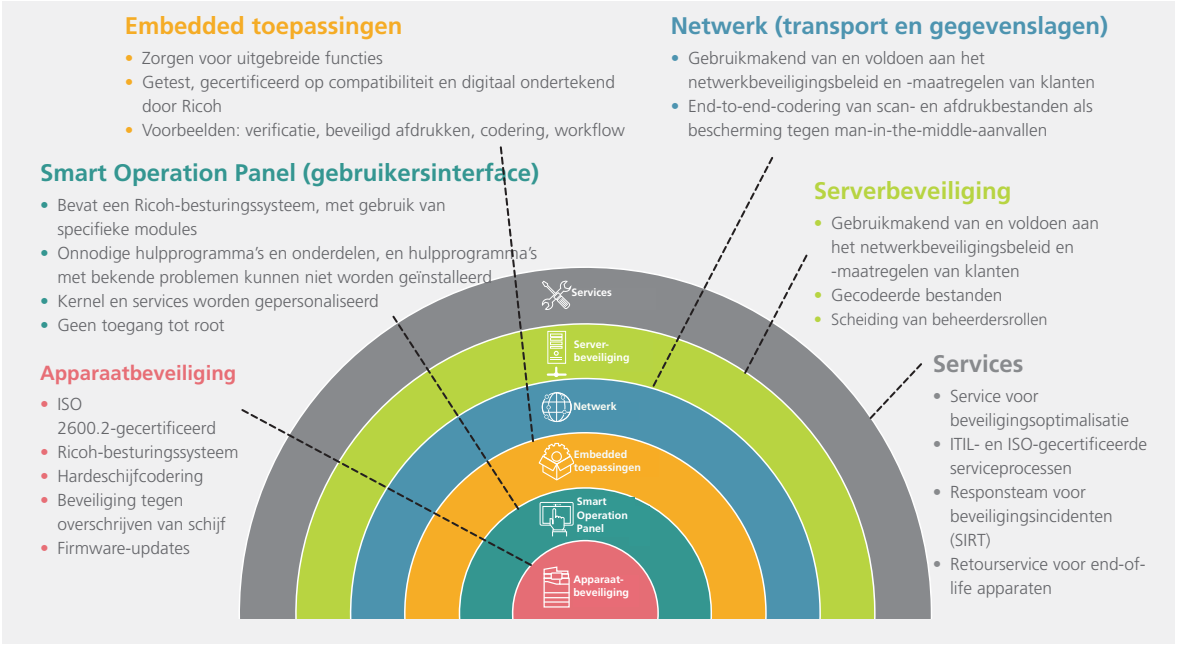
3. Smart toepassingen

Deze toepassingen kunnen in het SOP worden geïntegreerd en bieden extra functionaliteit voor gebruikers, zoals workflows en gegevensopslag. Sommige toepassingen bieden essentiële beveiligingsfuncties. Hiertoe behoren beveiligd afdrukken, toegang via een pasje en codering. Toepassingen worden door Ricoh of door medewerkers van het Ricoh-ontwikkelingsprogramma ontwikkeld. Alle toepassingen moeten de compatibiliteitstesten van Ricoh doorstaan en digitaal worden ondertekend voordat ze op het SOP mogen draaien.

4. Netwerk en servers

Ongeacht wie de IT-infrastructuur beheert, garandeert Ricoh dat onze producten en services voldoen aan uw IT- en netwerkbeveiligingsbeleid. End-to-end-codering van afdruk- en scanbestanden, codering van gegevens op servers en verschillende beheerderstaken zijn methoden die uw organisatie tegen een interne aanval of man-in-the-middle-aanvallen beschermen.

Ons volledige aanbod omvat een uitgebreid assortiment beveiligingsservices. Hiertoe behoren consultancy en managed services om u te ondersteunen bij het monitoren, optimaliseren en beheren van uw document- en informatiebeveiliging. We hebben ook verschillende vernietigingsservices voor aan het einde van de contractduur van een apparaat. Zo weet u zeker dat alle gegevens op het RAM en de harde schijf van afgedankte apparaten worden gewist.



HOE RICOH DE DIGITALE WERKPLEK BESCHERMT

Onze klanten ervaren grotendeels dezelfde beveiligingsproblemen. Dit komt door de toenemende hoeveelheid gegevens, waardoor ook het aantal zwakke plekken, aanvallen en boetes toeneemt. Organisaties bevinden zich in een continue strijd om gegevens vertrouwelijk en beveiligd houden. Er mag niet met gegevens kunnen worden geknoeid. Bij Ricoh worden per maand bijvoorbeeld 8 miljard aanvallen op firewalls geweerd. Er zijn tienduizenden wereldwijde, nationale en industriële gegevenswetten. Organisaties moeten te allen tijde kunnen bewijzen dat ze aan al die wetten voldoen. Het is daarom begrijpelijk dat kleine en grote organisaties een partner willen hebben die ze kunnen vertrouwen. Dit moet een partner zijn die helpt bij de beveiliging van de gehele digitale werkplek.

Ricoh heeft een breed scala aan oplossingen ontwikkeld om de verschillende risico's voor organisaties te beperken. Aangezien de bedreigingen voor informatiebeveiliging zich ongelooflijk snel ontwikkelen, richt Ricoh zich op programma's die samen met klanten zijn ontwikkeld. Zo verbeteren wij de ontwikkeling en levering van onze services.

Onze klantenadviescommissies fungeren als belangrijke strategische focusgroepen. Deze commissies helpen ons om een beter inzicht te krijgen in de trends, stimulansen en prioriteiten die vorm geven aan de organisaties van onze klanten. Onze technologie-adviesconferenties leveren ons essentiële informatie van belangrijke besluitvormers. Ricoh's engineering- en R&D-teams gebruiken deze conferenties om waardevolle feedback van klanten over ideeën, concepten en prototypen te krijgen. Ten slotte werkt Ricoh samen met individuele klanten om nieuwe en geavanceerde beveiligingsfuncties te ontwikkelen voor klanten uit specifieke verticale markten, maar ook voor de algehele markt. Deze klantgerichte aanpak helpt ons om het stappenplan voor een product te valideren. Daarnaast profiteren onze klanten van een wereldwijd netwerk van services en support.

De moderne digitale werkplek moet net zo dynamisch zijn als de cyberbedreigingen waarmee de werkplek wordt geconfronteerd. En deze moet ook kunnen meebewegen met veranderende manieren van werken. Daarom zijn wij ervan overtuigd dat cyberbeveiliging naadloos moet integreren met alle technologie die door onze klanten op hun werkplek wordt gebruikt. Ricoh past de ISO 27001-norm door de hele organisatie toe en al onze producten voldoen aan de IEEE 2600-certificering. Bovendien zijn al onze producten voorzien van ons eigen Ricoh-besturingssysteem. Wij passen dus de best practices op het gebied van beveiliging toe bij onze klanten, ongeacht de structuur en groeimogelijkheden van hun organisatie.

De kans op reputatieschade en financiële schade door cyberrisico's is nog nooit zo groot geweest. De oorzaken zijn divers: veiligheidsbedreigingen, wet- en regelgeving en complexe industrienormen. Het is daarom tijd om op zoek te gaan naar een betrouwbare beveiligingspartner. Zo beschermen we samen het grootste goed van uw organisatie: uw bedrijfsgegevens. En bent u verzekerd van een mooie toekomst.

RICOH
imagine. change.

www.ricoh.nl