Veilig werken

RICOH
imagine. change.

Hoe beveiligt u uw werk?

Tegenwoordig bestaan er veiligheidsrisico's voor veel meer apparaten dan enkel pc's, servers en netwerken. Ook printers moeten goed worden afgeschermd. Ze zijn immers uitgegroeid tot enorme doorstroompunten van informatie, waardoor ze op zichzelf al een volwaardig ICT-systeem vormen. De rekenkracht van de groep apparaten die we van oudsher 'printers en kopieerapparaten' noemen, is de afgelopen tijd flink gegroeid. Het nadeel: de risico's voor die groep zijn toegenomen. Denk aan:

- Onbevoegde toegang via netwerken.
- Aftappen of aanpassen van informatie op het netwerk.
- Informatielekken via HDD-opslag.
- Onbevoegde toegang via het bedieningspaneel van een apparaat.
- Ongewenste toegang via fax- en telefoonlijnen.
- Informatielekken via geprinte documenten.
- Schendingen van het beveiligingsbeleid door onzorgvuldigheid.

Informatie is goud voor een organisatie. Het is belangrijk om deze goed te beschermen. Ricoh helpt u bij het organiseren en creëren van informatie en kan deze informatie ook voor u beveiligen.

Ricoh's aanpak

Het kloppend hart van ons beveiligingsmodel is het apparaat zelf. Het besturingssysteem (OS, Operating System) van Ricoh-apparaten hebben we speciaal ontwikkeld en getest voor gebruik in onze eigen apparatuur. Daarnaast voldoen veel van onze Multifunctionele Printer (MFP)-modellen aan Devices IEEE 2600.2-beveiligingsnorm voor de bescherming van printapparatuur. De meeste modellen zijn standaard al geschikt voor het coderen van harde schijven en overschrijfbeveiliging. Daardoor blijven vertrouwelijke gegevens die worden verwerkt daadwerkelijk vertrouwelijk. Ook het nieuwe Smart Operation Panel (SOP) is zodanig ontwikkeld dat het geen beveiligingsrisico's met zich meebrengt en werkt op het unieke Ricoh-besturingssysteem. Ricoh installeert nooit onnodige onderdelen en toegang tot de broncodes is niet mogelijk. Geïntegreerde toepassingen moeten altijd aan onze compatibiliteitstests voldoen en digitaal worden ondertekend, voordat ze met het Smart Operation Panel kunnen worden gebruikt. Ricoh wil samen met onze klanten producten en diensten ontwikkelen, die perfect aansluiten op uw beleid op het gebied van IT en netwerkbeveiliging. We hanteren een aantal technieken om MITM-aanvallen (man-in-the-middle) en interne dreigingen te weren, waaronder end-to-end-codering van print- en scanbestanden, codering van gegevens op servers en een scheiding van beheerderstaken. Om al die beveiligingsmaatregelen heen zit een frontlinie van verschillende beveiligingsdiensten, zoals advies en beheer, zodat we de document- en informatieveiligheid effectief kunnen monitoren, optimaliseren en beheren.

Gebruikersinterface (Smart Operational Panel)

- Beveiligd Ricoh-besturingssysteem met specifieke modulen
- Onnodige tools en onderdelen worden niet geïnstalleerd
- Aangepaste kernel en diensten
- Toegang tot broncodes is niet mogelijK

Geïntegreerde toepassingen

- Bieden uitgebreide functies
- Zijn getest op compatibiliteit, gecertificeerd en digitaal ondertekend door Ricoh
- Voorbeelden: verificatie, beveiligd printen, codering, workflow

Netwerk (transport en gegevenslagen)

- Benut en voldoet aan het netwerk-gerelateerde beveiligingsbeleid en de maatregelen van de klant
- End-to-end-codering van print- en scanbestanden als verdedigingsmiddel tegen MITM-aanvallen

Serverbeveiliging

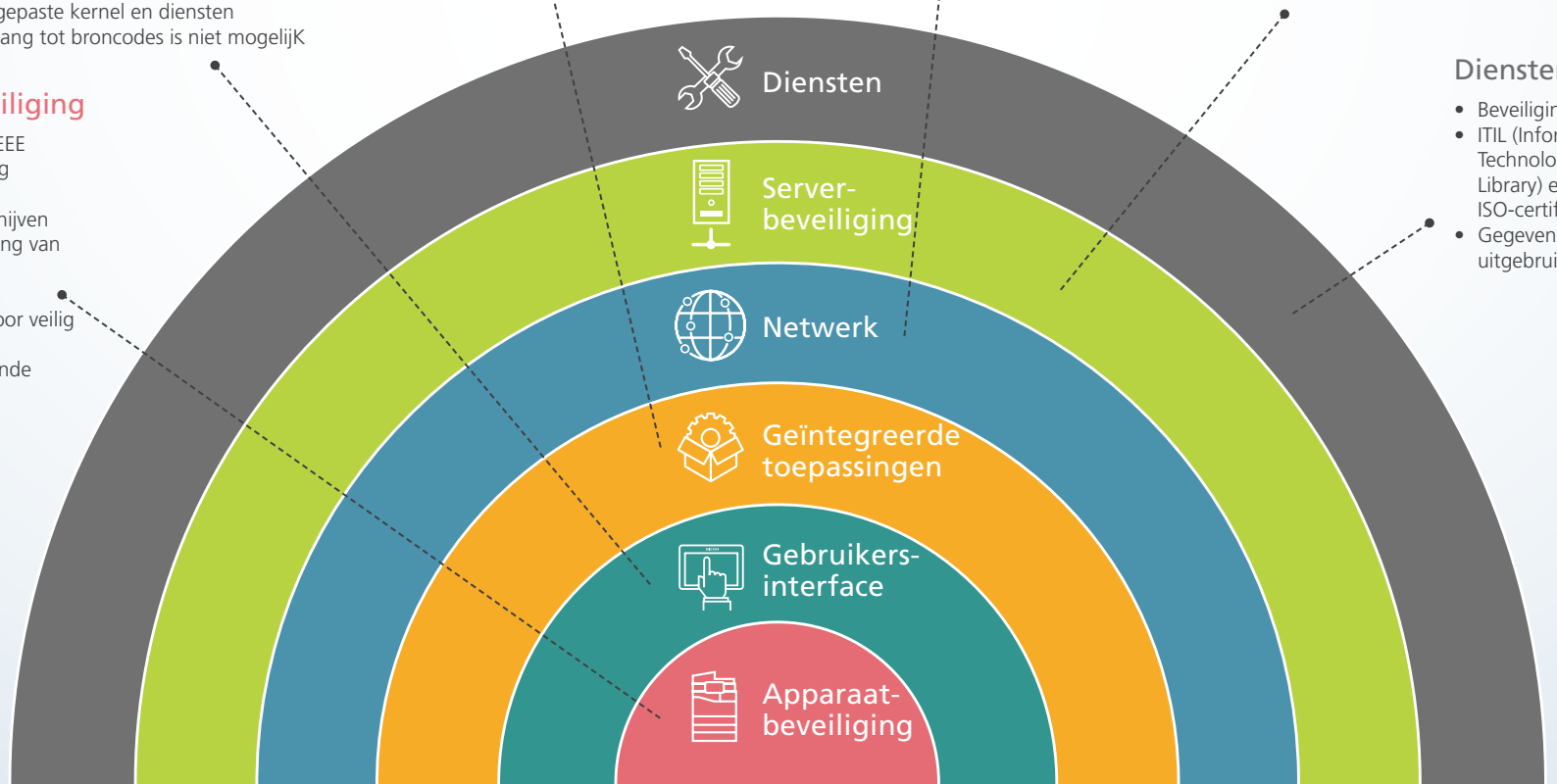
- Benut en voldoet aan het server gerelateerde beveiligingsbeleid en de maatregelen van de klant
- Gecodeerde bestanden
- Scheiding van beheerdersfuncties

Apparaatbeveiliging

- ISO-/IEEE 15408-/IEEE
- 2600.2-certificering
- Uniek Ricoh-OS
- Codering harde schijven
- Overschrijfbeveiliging van schijven
- Betrouwbare platformmodule voor veilig opstarten
- Digitaal ondertekende firmware-updates

Diensten

- Beveiligingsoptimalisatie
- ITIL (Information Technology Infrastructure Library) en processen met ISO-certificering
- Gegevens verwijderen bij uitgebruikname apparatuur



Beveiliging zit in ons DNA

Ricoh ontwerpt, produceert en implementeert zijn apparaten met veiligheid als een harde eis. Veiligheid is in het gehele traject verweven, van de conceptfase tot de uiteindelijke verkoop. Beveiliging zit in ons DNA en maakt onlosmakelijk deel uit van onze ontwerpvisie en toewijding aan continue verbeteringen, zodat we onze klanten oplossingen kunnen bieden voor de modernste dreigingen.

Apparaat-beveiliging

- Digitaal ondertekende firmware-updates
- Harde schijven codering
- Gegevens wissen harde schijven
- IEEE 2600-certificering
- Beveiligd faxen
- Verificatie apparaat-gebruikers

Gegevens-beveiliging

- Beveiligd scannen
- Beveiligd kopiëren
- Beveiligd printen
- Document classificatie
- Inzicht, rapportage,- en bewaking van print- en kopieergebruik

Netwerk-beveiliging

- Verificatie netwerk-gebruikers
- Codering printinformatie
- Sluiten ongebruikte netwerkpoorten
- @Remote
- Netwerk-codering
- Device Manager NX

Programma's en resources

- Ondersteunende documentatie over beveiliging
- Nationale/ internationale technische ondersteuning
- Programma's uitgebruikname apparatuur
- Trainingen voor eindgebruikers en beheerders

Apparaat-beveiliging

Met onze technologie voor beveiliging kunnen we multifunctionele apparaten en laserprinters tegen potentiële risico's beschermen. Daaronder vallen bijvoorbeeld kwetsbare firmware, de harde schijf van het apparaat, het niet-vluchtige geheugen, open netwerkpoorten en een verificatiesysteem. Ricoh beschikt voor allerlei producten over Common Criteria-certificeringen (ISO/EIC 15408). Dit houdt in dat de beveiligingsfuncties van het apparaat getest zijn door onafhankelijke, externe, gelicentieerde laboratoria. Zo kunnen we garanderen dat alle beveiligingsfuncties naar behoren werken, conform de normen van zowel overheden als de branche zelf.

Wij willen dat uw informatiesystemen tegen dreigingen zijn beschermd. Daarom ontwikkelen en bieden we onder andere informatiegerelateerde functies en producten, waarmee u uw digitale en geprinte documenten achter slot en grendel houdt, zonder dat de gebruiksvriendelijkheid van uw processen en de productiviteit in het geding komen.

Onveilige firmware kan voor cybercriminelen een ingang zijn

Digitaal ondertekende firmware-updates

Als de firmware, oftewel de ingebouwde software, van een MFP of printer, wordt aangepast of gekraakt, kan het apparaat worden gebruikt als ingang in het bedrijfsnetwerk, als middel om het apparaat schade toe te brengen of als platform om het bedrijf op een andere manier te benadelen. Alle apparaten van Ricoh werken met de unieke Trusted Platform Module (TPM). Zodra het systeem merkt dat de firmware is gekraakt, kan het apparaat omwille van de beveiliging niet meer opstarten. TPM is een hardwarematige Ricoh-beveiligingsmodule waarmee verschillende zaken worden geverifieerd, zoals de controller kernprogramma's, het besturingssysteem, de BIOS, de bootloader en de firmware van applicaties.

De MFP's en printers van Ricoh werken met digitale ondertekening om de status van firmware te valideren. De openbare sleutel die voor deze verificatiemethode wordt gebruikt, staat op een niet-vluchtig TPM-gedeelte dat niet kan worden overschreven. De TPM bevat daarnaast een broncoderingssleutel en cryptografische functies. Deze kunnen niet extern worden aangepast.

Ricoh werkt met een Trusted Boot-procedure, waarbij twee methoden worden gebruikt om de programma's en firmware te valideren.

1. Detectie van aanpassingen.
2. Validatie van digitale handtekeningen.

Een Ricoh-apparaat start pas op als het heeft gecontroleerd dat de programma's en firmware authentiek en gebruiksveilig zijn.

Tijdelijke gegevens zijn kwetsbare gegevens

DataOverwriteSecurity-systeem (DOSS)

Als u een document scant of gegevens van een computer ophaalt, kunnen er tijdelijk gegevens op de harde schijf of in het geheugen van het apparaat worden opgeslagen. Het kan daarbij gaan om afbeeldingsbestanden van scans, afdrukken en documenten alsook gegevens of instellingen van de gebruiker. Deze tijdelijke - ook wel 'latente' - gegevens vormen een mogelijk risico voor uw informatieveiligheid.

Met het DataOverwriteSecurity-systeem (DOSS) dekt Ricoh dit risico af. Na iedere printopdracht worden de tijdelijke gegevens op de harde schijf van de MFP actief overschreven met willekeurige enen en nullen. Tijdelijke gegevens worden actief overschreven en dus telkens verwijderd, zodra er een opdracht wordt uitgevoerd.

Toegang tot latente gegevens van kopieer-, print-, scan- en faxopdrachten zodra deze zijn overschreven, is nagenoeg onmogelijk. Het overschrijfproces kan 1 tot 9 keer worden herhaald.

Codering dient als beschermingsmiddel tegen gegevensdiefstal

Harde schijven codering

Ook als de harde schijf uit een Ricoh-apparaat wordt verwijderd, kunnen de gecodeerde gegevens niet worden gelezen. Met codering van de harde schijf kunt u de gegevens op de harde schijf van een MFP beschermen tegen diefstal. Tegelijkertijd kan uw organisatie gemakkelijker het beveiligingsbeleid in acht nemen. Ook de gegevens in het adresboek van een systeem worden gecodeerd. Voor de werknemers, klanten en leveranciers van een bedrijf betekent dit een lager risico dat hun gegevens door cybercriminelen worden gehackt. De volgende soorten gegevens worden in het niet-vluchtige geheugen of op de harde schijf van MFP's opgeslagen en kunnen worden gecodeerd:

- Het adresboek.
- Verificatiegegevens van gebruikers.
- Opgeslagen documenten.
- Tijdelijk opgeslagen documenten.
- Logbestanden.
- Instellingen voor netwerkinterfaces.
- Configuratiegegevens.

Ricoh werkt met codering van harde schijven aan de hand van AES-methodologie (Advanced Encryption Standard) tot 265 bits.

Beveiligd faxen

Volledig gebruiksveilig

Als u de faxfunctie van een apparaat inschakelt, kan het apparaat via de telefoonlijn verbinding met de buitenwereld maken. Daarom moet worden voorkomen dat kwaadwillenden zich via de fax toegang tot uw bedrijfsnetwerk kunnen verschaffen. De geïntegreerde software van Ricoh verwerkt alleen de juiste soorten gegevens, dus in dit geval alleen faxgegevens, en stuurt die rechtstreeks door naar de juiste functies van het apparaat. Omdat faxgegevens alleen via de faxlijn kunnen worden ontvangen, bestaat er geen risico dat iemand zich via de faxlijn toegang tot het netwerk of de apparaatprogramma's verschaft.

Ricoh zorgt er op meerdere manieren voor dat alle faxfuncties volledig gebruiksveilig zijn:

- De faxcontroller bevat geen gegevensmodem, maar enkel een faxmodem, waardoor alle communicatie via het G3-faxprotocol verloopt.
- Beeldgegevens worden niet in het paginageheugen van de enginecontroller of een tijdelijk opslaggeheugen geplaatst. Daardoor is het niet mogelijk om via de faxcontroller toegang tot deze gegevens te krijgen.
- De gegevens die in het paginageheugen van de enginecontroller of een tijdelijk opslaggeheugen worden opgeslagen, worden alleen naar de printeenheid verzonden.
- Er bestaat geen actieve verbinding tussen de videobussen van de print- en scanfuncties en de enginecontroller. Daardoor kan er geen toegang worden verkregen tot de gegevens in het paginageheugen van de enginecontroller of het tijdelijk opslaggeheugen van de faxcontroller.
- De locatiegegevens van het paginageheugen worden verwijderd zodra een opdracht is uitgevoerd.

Onafhankelijke beveiligings-certificering

IEEE 2600

In de IEEE 2600-beveiligingsnorm worden de minimumvereisten uiteengezet voor beveiligingsfuncties van apparaten, waarbij een hoge mate van documentbeveiliging vereist is. Dankzij deze norm bestaat er een duidelijk minimumniveau van wat er mag worden verwacht van de beveiligingsfuncties van MFP's en printers. Om te garanderen dat een apparaat aan specifieke normen voldoet, buigt een onafhankelijk extern laboratorium zich over het testen en eventueel goedkeuren van de beveiligingsfuncties die de fabrikant heeft aangebracht.

Ricoh heeft bij veel apparaten ervoor gezorgd dat de volgende aspecten, waarvan duidelijk is dat er een hoger risico op gegevensdiefstal aan kleeft, aan de IEEE 2600-norm voldoen en kunnen worden ingeschakeld:

- Systemen voor gebruikersidentificatie en -verificatie.
- Gegevenscodering voor MFP's.
- Validatie van de systeemfirmware.
- Scheiding van de analoge faxlijn en de controller voor scan-, print- en kopieeropdrachten.
- Validatie van algoritmen voor gegevenscodering.
- Beveiliging tegen gegevensoverschrijving.

Het Ricoh-assortiment telt een breed gamma aan MFP's en printers met een IEEE 2600-beveiligingscertificering. We passen de producten in ons assortiment regelmatig aan, zodat we kunnen blijven beantwoorden aan de klantvraag.

Grip op de toegang

Verificatie van apparaatgebruikers

Dankzij verificatiefuncties hebben bevoegde gebruikers wél toegang tot een Ricoh-apparaat, terwijl gebruikers zonder de juiste aanmeldgegevens de toegang wordt geweigerd. Ricoh biedt u ook de mogelijkheid om per groep of gebruiker specifieke rechten toe te kennen. U kunt bijvoorbeeld aanpassingen aan de apparaatinstellingen en het adresboek niet toestaan of toegang geven tot specifieke scanprocessen, documentservers en andere functies. Daarnaast vormt de blokkeerfunctie van gebruikers - die wordt ingeschakeld als iemand zich buitensporig vaak aanmeldt of probeert aan te melden - een extra beveiligingsmiddel tegen DoS- of bruteforce-aanvallen.

De verificatiemethoden bestaan onder andere uit:

- Eenvoudige verificatie: de gebruiker voert een gebruikersnaam en wachtwoord in. Deze worden beide in het lokale adresboek van de MFP opgeslagen.
- Verificatie via gebruikerscodes: de gebruiker voert een code van maximaal acht cijfers in. Deze code wordt vervolgens vergeleken met de gegevens die in het adresboek zijn opgeslagen.
- Verificatie via Windows/LDAP: de toegang tot MFP's van Ricoh kan ook verlopen via domeincontrollers van Windows® of LDAP-servers.
- Kaartverificatie: de gebruiker voert ter verificatie geen gebruikersnaam en wachtwoord in, maar houdt een geregistreerde kaart tegen een optionele kaartlezer aan.

Gegevens-beveiliging

Informatie lekken is venijnig eenvoudig. Als iemand bij een multifunctionele printer een document laat rondslingeren, kan dat net zo'n groot risico vormen als een onderschept digitaal bestand of een menselijke fout. De multifunctionele printers van Ricoh beschermen uw gegevens, of u nu documenten print, scant, kopieert of faxt.

Ricoh beschermt uw gegevens met behulp van allerlei technologieën en functies die specifiek zijn ontwikkeld als aanvulling op beveiligingsbeleid, als bescherming tegen misbruik of onzorgvuldigheid en als prikkel om de compliance verantwoordelijkheid in een organisatie bij een persoon of afdeling te beleggen.

Bescherming van digitale documenten

Beveiligd scannen

Het digitaliseren van fysieke documenten en het aansluitend doorsturen van de elektronische bestanden - of dat nu via back-endsystemen of per e-mail verloopt - vormen bij gebrekkige beveiliging een gelegenheid voor cybercriminelen om de gegevens te onderscheppen. Scanprocessen zijn natuurlijk ingericht op optimaal gebruikersgemak, maar mogen niets te wensen overlaten als het gaat om de veiligheid van verstuurde informatie. De eerste stap naar degelijke processen: de toegang beperken. U kunt met behulp van verschillende verificatiemethoden, zoals aanmelden via het netwerk, optionele Kerberos-verificatie of SSO-kaarttechnologie (Single Sign-On), scanprocessen alleen voor specifieke gebruikers toestaan.

Als u daarnaast de scannen-naar-mailgegevens codeert, neemt het risico op gegevensdiefstal af. Verstuur e-mails met behulp van cryptografie met openbare sleutels en gecertificeerde gebruikersverificatie, waarbij het certificaat is opgenomen in het adresboek van de scanner. U kunt spoofing en aanpassingen aan berichten voorkomen door berichten elektronisch te ondertekenen met behulp van een geheime sleutel, die wordt gegenereerd op basis van het apparaatcertificaat.

De multifunctionele printers, kopieerapparaten en scanners van Ricoh zijn voorzien van twee protocollen: SSL (Secure Sockets Layer) en TLS (Transport Layer Security). Daarnaast werken ze met effectieve coderingsalgoritmen (256-bits AES en SHA-2), ondersteuning voor herleidbaarheid en beheerdersfuncties.

Rondslingerende documenten kunnen een informatielek veroorzaken

Beveiligd printen

Wanneer er een geprint document in de papierlade blijft liggen of elders rondslingert, kan iedereen het meenemen. Daardoor komt de veiligheid van de informatie op het document in het geding. Het risico neemt exponentieel toe als de rondslingerende documenten gevoelige informatie bevatten. Met beveiligd afdrukken biedt Ricoh een manier om gecodeerde documenten op de harde schijf van het apparaat te bewaren totdat de eigenaar van het document op het apparaat zelf de juiste pincode invoert. Ricoh biedt naast de op stuurprogramma's gebaseerde functie voor beveiligd afdrukken ook Enhanced Locked Print. Deze technologie is gekoppeld aan gebruikersaccounts en kan worden gecombineerd met kaartverificatie. Voor nog meer functionaliteit kunt u met software zoals Ricoh Streamline NX (te zien op de afbeelding) profiteren van de compromisloze, veilige vrijgave van documenten, waardoor gebruikers hun eigen takenwachtrij kunnen aanpassen, terwijl de beheerder alle controle behoudt.

Bescherming tegen onbevoegde kopieeropdrachten

Beveiligd kopiëren

Ricoh biedt functies om onbevoegde kopieeropdrachten te weigeren om zo mogelijke informatielekken te voorkomen. De kopieerbescherming zorgt ervoor dat afgedrukte en gekopieerde documenten van een onzichtbaar achtergrondpatroon worden voorzien. Als het afgedrukte of gekopieerde document nogmaals wordt gekopieerd, wordt het patroon zichtbaar op de kopieën.

De bescherming tegen onbevoegde kopieeropdrachten werkt op twee manieren. Bij Masked Type for Copying-bescherming worden er een maskeringspatroon en een boodschap aan het afgedrukte document toegevoegd. Bij onbevoegde kopieën verschijnt de boodschap op de kopie. Dat kan bijvoorbeeld de naam van de auteur of een waarschuwing zijn. Data Security for Copying vormt een beveiligingslaag om de daadwerkelijke informatie. Als een Ricoh-apparaat het maskeringspatroon herkent, wordt de afgedrukte informatie afgedekt door een grijs kader dat de hele pagina bedekt, op 4 mm bij de randen na.

Anonieme documenten zijn moeilijk te beheren

Document classificatie

Zet op documenten een stempel met belangrijke identificerende gegevens, voor meer helderheid en beheermogelijkheden. Verplicht veilig informatie printen is een functie waarbij veiligheidsinformatie, zoals wie een document wanneer en op welk apparaat heeft afgedrukt, bij printopdrachten automatisch aan het document wordt toegevoegd. U kunt deze functie inschakelen bij kopieer-, print-, fax- en documentserveropdrachten. Beheerders kunnen instellen in welke positie en met welke informatietypen documenten automatisch worden afgedrukt. Tot de mogelijkheden behoren:

- De datum en het tijdstip waarop de afdruktaak is uitgevoerd.
- De naam of gebruikers-ID van degene die de afdruktaak heeft uitgevoerd.
- Het IP-adres en/of serienummer van het gebruikte apparaat.

Apparaten beveiligen tegen misbruik

Inzicht, rapportage,- en bewaking van print en kopieergebruik

Ongecontroleerd gebruik van apparatuur kan tot onverwachte kosten en schendingen van het bedrijfsbeleid leiden. De cost- en accountingsoftware van Ricoh volgt het gebruik tot aan individuele gebruikers. Alle kosten worden automatisch aan de juiste gebruikers en afdelingen toegekend. Stel gebruikers- en accountlimieten in voor meer herleidbaarheid.
Stel gebruikersbevoegdheden in om de toegang tot bepaalde functies te koppelen aan de daadwerkelijke behoefte daarvoor, zoals printen in kleur. Als u de controle heeft over wie met behulp van welke verificatie en bevoegdheden apparatuur kan gebruiken, is er minder risico op wangebruik en komt u over nuttige gebruiksinformatie ter beschikking.

Netwerk-beveiliging

Multifunctionele printers versturen en ontvangen via netwerken gevoelige informatie van en naar computers en servers. Als die informatie niet is beschermd, loopt u het risico dat kwaadwillenden met toegang tot het netwerk er aanpassingen aan maken. De producten en technologieën van Ricoh bevatten functies om onbevoegden buiten uw netwerk te houden. Daartoe gebruiken we verschillende technieken, zoals codering van alle netwerkcommunicatie en het printverkeer, netwerkverificatie en een breed scala aan beheermaatregelen, zoals de sluiting van netwerkpoorten en proactief apparaatbeheer.

Met de beveiligingsfuncties van Ricoh loopt u minder risico op misbruik of informatieverlies via het netwerk als gevolg van gekraakte multifunctionele printers of apparaten.

Onbevoegde gebruikers kunnen een risico vormen

Verificatie netwerkgebruikers

Ricoh-apparaten ondersteunen verificatie van netwerkgebruikers, waardoor enkel bevoegde gebruikers toegang hebben. Zo kan met verificatie via Windows® de identiteit van een gebruiker bij de multifunctionele printer worden geverifieerd. De aanmeldingsgegevens (gebruikersnaam en wachtwoord) worden vergeleken met de database van bevoegde gebruikers. Die database bevindt zich op de Windows-netwerkserver. Bij toegang tot een wereldwijd adresboek wordt de gebruiker met behulp van LDAP-verificatie vergeleken met de LDAP-server (Lightweight Directory Access Protocol). Zo kunnen alleen gebruikers met geldige aanmeldingsgegevens de e-mailadressen op de LDAP-server doorzoeken en selecteren.

Met software zoals Ricoh Streamline NX - een modulair pakket voor scannen, faxen, printen, apparaatbeheer, beveiliging en accounting - beschikt u over aanvullende mogelijkheden voor netwerkverificatie. Denk daarbij aan verificatie via LDAP, Kerberos of een beschikbare SDK voor verificatie op maat.

Apparaten ‘onzichtbaar’ maken voor de buitenwereld

Sluiten van ongebruikte netwerkpoorten

Fabrikanten willen dat hun klanten gemakkelijk apparaten aan een netwerk kunnen toevoegen. Daarom leveren ze veel systemen met netwerkondersteuning automatisch met alle poorten open. Dat is gebruiksvriendelijk, maar ook riskant, aangezien open poorten op printers en MFP’s een beveiligingsgat kunnen veroorzaken. Een open poort kan een netwerkingang vormen voor allerlei externe dreigingen, met alle gevolgen van dien: verwijderde of aangepaste gegevens, DoS-aanvallen, virussen en malware. De oplossing voor dit veelvoorkomende probleem is eenvoudig, maar wordt toch vaak over het hoofd gezien: sluit de poorten. Beheerders van Ricoh-apparaten kunnen eenvoudig ongebruikte netwerkpoorten sluiten, waardoor de apparaten als het ware onzichtbaar worden voor hackers. Daarnaast kunt u specifieke protocollen, zoals SNMP en FTP, volledig uitschakelen, waardoor hackers er geen misbruik meer van kunnen maken.

Ongecodeerde netwerkgegevens lopen risico

Netwerkcodering

Een hacker met kennis van zaken kan gegevens die via het netwerk worden verplaatst onderscheppen en zo ongecodeerde gegevensstromen, bestanden en wachtwoorden buitmaken. Zonder bescherming kan concrete informatie worden gestolen, aangepast of vervalst en weer worden teruggeplaatst in het netwerk met de bedoeling om schade te veroorzaken. Ricoh werkt met robuuste beveiligingsprotocollen voor netwerken. Die protocollen kunnen eenvoudig aan de behoeften van klanten worden aangepast. We gebruiken het TLS-protocol (Transport Layer Security) om te voorkomen dat er tussen twee eindpunten met gegevens kan worden geknoeid.

Ricoh-apparaten zijn compatibel met WPA2 en WPA2-PSK met AES-codering (Wi-Fi Protected Access). Deze coderingsmethoden zijn bedoeld voor draadloze netwerken en bieden meer veiligheid dan traditionele WEP-codering (Wired Equivalent Privacy). WPA2 en WPA2-PSK werken met CCMP (AES), een vorm van gebruikersverificatie en een coderingsprotocol waarbij de coderingssleutel op gezette tijden wordt aangepast.

Gegevens naar printers zijn kwetsbaar voor misbruik

Codering van printinformatie

Gegevens die naar een printer worden verstuurd, kunnen tijdens het verplaatsen worden buitgemaakt als ze niet zijn gecodeerd. Ricoh kan printgegevens coderen met behulp van Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP). Zo worden de gegevens die van werkstations naar netwerkapparaten en multifunctionele printers worden gestuurd veilig gecodeerd. Dit systeem werkt met IPP via SSL/TLS. Dit is een protocol ter bescherming van de integriteit van gegevens. Pogingen om de gegevensstromen te onderscheppen, resulteren daardoor alleen maar in onleesbare gegevens voor de hacker.

Het beheer van apparaten

Device Manager NX

Het kan veel tijd kosten om apparaten te beheren. Wanneer het beheer niet goed wordt aangepakt, kunnen er onbedoeld gaten in de beveiliging ontstaan. Met de Ricoh-software voor apparaatbeheer, waaronder Device Manager NX en Streamline NX, krijgen IT-beheerders een centraal toegangspunt waarmee ze een nagenoeg onbeperkte hoeveelheid printapparaten via het netwerk kunnen volgen en beheren. Het maakt daarbij niet uit als het netwerk over meerdere servers of landen is verspreid. Het zicht op de status van apparaten en diensten verloopt via SNMPv3-codering, compleet met gebruikersverificatie en gegevenscodering waarmee de gebruikersgegevens en informatie over netwerkapparaten worden beschermd.

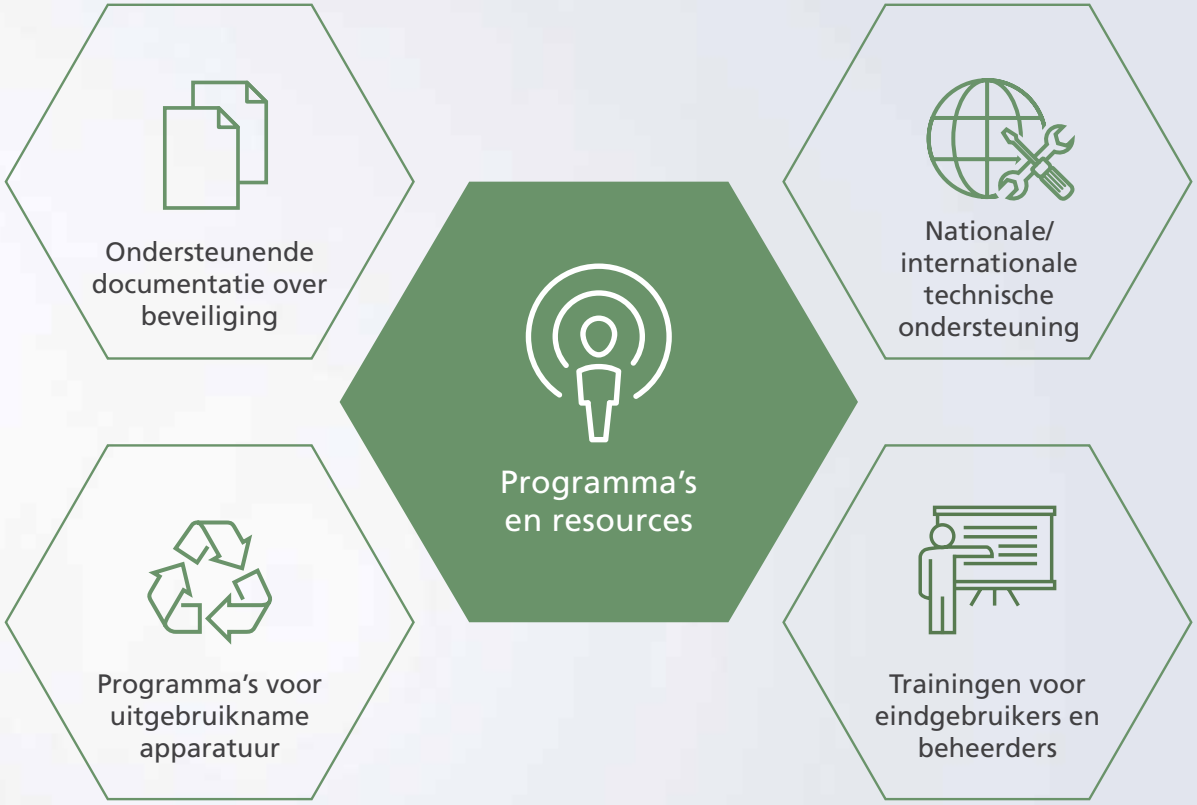
Dankzij het centrale beheer kunnen beheerders zelf bepalen wie er toegang heeft tot een apparaat of multifunctionele printer, hebben ze zicht op de DOSS-instellingen (DataOverwriteSecurity Solution) en kunnen ze apparaatcertificaten beheren. Dankzij automatisering neemt bovendien het risico van verouderde firmware af. De apparaatfirmware van Ricoh wordt vergeleken met de door de klant goedgekeurde firmwareversie of de nieuwste firmwareversie die via het Global Software Center van Ricoh voor het apparaat beschikbaar is. Bestaat er een verschil in de firmwareversies, dan kan de juiste versie automatisch op het apparaat worden geïnstalleerd.

@ Remote

Met @Remote Connector NX van Ricoh wordt u op een veilige manier tijdig op de hoogte gebracht van de behoefte aan essentieel onderhoud. Op afstand kunnen firmware-updates vooruit worden gepland en dringende updates meteen via de connector geïnstalleerd. De @Remote Connector verzamelt ook informatie van de apparaatmeters en maakt die samen met meldingen over het verbruik op gezette tijden inzichtelijk, voor een nog betere uptime van de machine en minder administratie.

Programma's en resources

Organisaties die medische, financiële, persoonlijke of andere soorten gevoelige informatie opslaan en gebruiken, zijn gebonden aan verschillende wettelijke vereisten, zoals de GDPR. Als uw organisatie aan externe vereisten moet voldoen of moet aantonen haar eigen beveiligingsbeleid na te leven, kunt u op Ricoh rekenen. Wij voorzien onze klanten van programma's en hulpmiddelen waarmee ze hun specifieke juridische uitdagingen het hoofd kunnen bieden.



Bij Ricoh ondersteunen we klanten met de juiste technische assistentie, kennis, trainingen en beveiligingsdocumentatie voor onze apparaten. Daarnaast kunnen we ook gegevens verwijderen van apparatuur die wordt afgeschreven.

Programma’s voor uit gebruik genomen apparatuur

Informatie die op afgeschreven apparatuur is achtergebleven, kan een beveiligingsrisico vormen. De enige oplossing is de gegevens volledig te wissen. Komen die gegevens in de verkeerde handen, dan kan dat leiden tot een ernstiger beveiligingsprobleem. De programma’s van Ricoh verwijderen de informatie van een apparaat zodra de levensduur ervan is verstreken of zodra het aan het eind van een lease- of huurovereenkomst wordt terug geleverd.

Overschrijving van harde schijven

Deze stap wordt meestal gezet aan het eind van de levensduur van een apparaat of als een leaseovereenkomst is verlopen. Met de Data Overwrite Service weet u zeker dat alle klantgegevens op de harde schijf van het apparaat worden overschreven. De gegevens kunnen op verschillende manieren worden overschreven. Daarnaast wordt het NV-RAM teruggezet naar de standaardinstellingen, om zo te voorkomen dat er leesbare informatie in achterblijft, zoals IP-adressen, adresboeken en andere gegevens van administratieve aard. Zo krijgen derden er geen toegang toe.

Uitgebruikname van harde schijven

Met het Hard Drive Surrender Program heeft u de mogelijkheid om de harde schijf van een MFP of printer te behouden tegen de tijd dat de leaseovereenkomst verloopt of het apparaat wordt afgeschreven. Een gecertificeerde Ricoh-technicus verwijdert de harde schijf voordat het apparaat wordt opgehaald en geeft de schijf vervolgens af aan een vertegenwoordiger van de klant. Zo behoudt de klant de controle over zijn informatie en kan deze zelf kiezen hoe de schijf wordt vernietigd.

MFP Data Cleansing Service

Met de MFP Cleansing Service van Ricoh kan alle herkenbare informatie van een MFP of printer worden verwijderd voordat het apparaat bij de klant op locatie wordt weggehaald. De informatie in het geheugen van het apparaat, zoals adresboeken en netwerkadressen, wordt verwijderd. Ook identificerende informatie, zoals stickers met afdelingsnamen, IP-adressen en onderhoudsinformatie, wordt verwijderd, samen met gegevens over eventueel specifiek klantpapier. Doordat we dit soort informatie verwijderen, is er minder risico dat kwaadwillenden IT-informatie van een organisatie kunnen verkrijgen.

Nationale/ internationale technische ondersteuning

Ricoh beschikt in iedere regio over technologiecentra waarmee we over de hele wereld snel en efficiënt technische ondersteuning kunnen bieden. Het Ricoh Global Services-team levert gestandaardiseerde en consistente totaaloplossingen. We bedienen zo'n 200 landen en regio's ter wereld en hebben ruim 30.000 onderhoudsspecialisten in dienst. Ons ongeëvenaarde ondersteunende netwerk van partners voor rechtstreekse verkoop en wederverkopers is zo uitgebreid dat we maar liefst 95% van de Fortune Global 500-bedrijven kunnen bedienen. Dat betekent voor u dat u bij ons kunt rekenen op één partner met internationale slagkracht. En doordat we in zo veel landen wereldwijd over vestigingen en onderhoudsspecialisten beschikken, kunnen we razendsnel inspelen op vragen van klanten, waar die zich ook bevinden.

Ondersteunende documentatie over beveiliging

Ricoh kan klanten van technische documentatie voorzien die ze kunnen inzetten om hun beveiliging te versterken. We bieden onder andere IEEE 2600- en ISO15408-certificeringsdocumentatie voor specifieke producten. Met deze documentatie kunnen onafhankelijke, externe partijen beveiligingsclaims controleren. We verstrekken deze documentatie op verzoek. Daarnaast kunnen we onze klanten beveiligingswhitepapers over apparaat- en netwerkinstellingen bieden alsook gidsen over de configuratie van beveiligingsinstellingen. In deze gidsen wordt uitgebreid beschreven hoe Ricoh-apparatuur intern met gegevens omgaat en hoe die gegevens via het netwerk worden gebruikt.

Trainingen voor eindgebruikers en beheerders

Wie wil kunnen rekenen op maximale voorzichtigheid en naleving van het beveiligingsbeleid, moet niet alleen kunnen terugvallen op technologie, maar ook op mensen. Daarom biedt Ricoh ook trainingen waarbij eindgebruikers en beheerders leren omgaan met onze apparaten. Gewapend met de juiste kennis en informatie kunnen uw mensen optimaal gebruikmaken van de verschillende beveiligingsmaatregelen. Daarnaast wordt het ze dankzij de training duidelijk waarom het voor de veiligheid van de organisatie zo belangrijk is om informatie af te schermen en het beleid na te leven.

Staat u voor een lastige beveiligingssituatie? Met Ricoh vindt u de juiste oplossing.

Gegevensverlies en -diefstal

Gegevensverlies vormt een van de grootste zorgen van de C-suite. Het blijft een eeuwige strijd om gegevens achter slot en grendel te houden. Cybercriminelen zijn continu op zoek naar gaten in uw verdediging. De beeldapparatuur van Ricoh kan een belangrijke rol spelen bij de preventie van gegevensverlies.

Beschadiging of aanpassing van gegevens

Virusaanvallen halen regelmatig de voorpagina van de krant. Met die media-aandacht wordt onderschreven hoe kwetsbaar organisaties voor cybercriminelen zijn. Populaire platformen met bekende kwetsbaarheden worden regelmatig doelwit van malware, virussen, Trojan Horses en wormen. De platformen van Ricoh zijn weliswaar ook populair, maar draaien op ons eigen besturingssysteem, omdat we op die manier pogingen tot geknoei met gegevens kunnen afweren.

Gegevensbeschikbaarheid

Wie informatie en gegevens wil verspreiden, moet toegang en afscherming met elkaar in evenwicht zien te brengen. Daar komt heel wat bij kijken. De producten van Ricoh zijn voor beide geschikt. De geoorloofde uitwisseling van informatie vindt in rap tempo plaats door middel van afdrukken, kopiëren, scannen en routering, naast afgedwongen controle over die processen. Daarbij worden doorgestuurde gegevens gecodeerd en kan de beheerder bepalen wie de informatie op onze apparaten mag verwerken.

Inzicht in regelgeving

Moderne organisaties moeten aan allerlei nationale, internationale en branche gerelateerde regelgeving voldoen, naast het verplichte beveiligingsbeleid van de organisatie zelf en de vereisten in het kader van audits. Ricoh heeft de kennis en middelen in huis om klanten bij compliance te ondersteunen.

Compliance zichtbaar maken

De boetes voor niet-naleving zijn hoog, terwijl de eventuele consequenties voor het bedrijf nog veel ernstiger worden vanwege nieuwe regelgeving. De juiste documentatie vormt een harde voorwaarde voor wie effectief wil laten zien dat de compliance in orde is. Met de IEEE 2600-certificering wordt voorzien in een onafhankelijke, externe controle van IT-gerelateerde beveiligingsclaims. Ricoh kan die certificering bieden, alsook andere documentatie.

Neem contact op met onze deskundigen

Klanten willen met organisaties werken die ze kunnen vertrouwen, hun beveiliging op orde krijgen en hun compliance-inspanningen zichtbaar maken. Ricoh heeft zich ten doel gesteld zijn klanten met de beste technologie, diensten, programma's en hulpmiddelen te ondersteunen. Daarnaast zorgen we ervoor dat onze klanten hun eigen beveiligingsbeleid in de praktijk kunnen brengen.
Heeft u vragen of wilt u meer informatie? Neem dan contact op met uw Account Manager of ga naar de website.

Ga voor meer informatie naar www.ricoh.nl.

Waarom Ricoh

Niet voor niets is Ricoh wereldwijd marktleider op het gebied van duurzame IT- en documentmanagement-oplossingen. Wij bewijzen dat bedrijven van elke omvang efficiënter, duurzamer en productiever kunnen werken. Daarnaast kunt u kosten besparen en beter beheersen.

Door intensief samenwerken, creatief denken, adviseren en trainen komen we tot oplossingen. Daarmee vereenvoudigt u al uw documentintensieve processen en kunt u informatie beter beheren. Ook verbetert de beveiliging van uw documenten.

Zo vertalen we uw wensen in slimme ideeën en concrete oplossingen. *imagine. change.*

RICOH
imagine. change.

Ricoh Nederland B.V.
Postbus 93150, 5203 MB 's-Hertogenbosch
Tel.: +31 (0)73 - 645 1111

www.ricoh.nl