RICOH
imagine. change.

Sikkerhedsløsninger fra Ricoh

Vi hjælper med at beskytte din forretning

Cybersikkerhed er den største trussel mod moderne virksomheders overlevelse og succes. Organisationer af enhver størrelse er i konstant risiko for at blive udsat for angreb i form af f.eks. phishing, DDoS eller ransomware, og omkostningerne kan løbe op i millioner. I 2017 kortlagde Ponemon Institute, at den globale gennemsnitsomkostning for en datalækage var 24 mio. kroner. I de kommende år vil reguleringer som den nye EU-persondataforordning (GDPR) kunne straffe virksomheder med gigantiske bøder for utilstrækkelig sikring af deres systemer og data. For at undgå dette skal enhver virksomhed kunne demonstrere deres evne til at beskytte data, og det kræver fuldt overblik over alle sårbarheder på tværs af organisationen.

En yderligere udfordring er digitaliseringen af den moderne arbejdsplads samt den eksplosive udvikling i datamængder. Arbejdsgange spreder sig ofte på tværs af enheder, netværk og geografisk placering. Informationer udsættes for størst risiko, når de flyttes rundt i virksomheden, da de skal beskyttes på ethvert trin af deres rejse. Det betyder, at moderne virksomheder ikke længere kan fungere uden sikre dokument- og datahåndteringssystemer. Samtidig er funktionaliteten på kontorprintere og MFP'er blevet tidoblet i løbet af de seneste år. De håndterer en betydelig del af virksomhedens datainput, -output, -overførsel og -lagring, hvilket gør dem til en af de farligste, men samtidig mest oversete, trussel mod sikkerheden på den moderne arbejdsplads.

Selv om mange virksomheder hævder at tilbyde sikkerhedsfunktioner, har Ricoh udviklet sikre arbejdspladsløsninger og -tjenester i årtier. Vores printere har f.eks. indeholdt mulighed for sikker overskrivning af harddiske i mere end 20 år.

Sikkerhed er i vores DNA og dækker alle vores løsninger til den digiale arbejdsplads. Vi har mere end 4 mio. kontorprodukter på markedet i dag. Ethvert af disse produkter, samt alle tilhørende tjenester, indeholder indbyggede sikkerhedsfunktioner. Vi anvender desuden Ricohs eget styresystem på tværs af mange af vores produkter. Dette udgør en stor del af vores sikkerhedsforsvar, idet det kontrollerer og isolerer mod trusler, som er målrettet mere udbredte operativsystemer.

Ricoh giver kunderne en ensartet service- og supportstruktur på verdensplan, hvilket sikrer, at efterretninger om trusler deles og håndteres effektivt. Ikke alene er IEEE 2600-certificeringen implementeret som standard på tværs af vores printerenheder, Ricoh er også et førende medlem og en nøgleaktør i IEEE Standards Association. Ricoh er desuden ISO 27001-certificeret og forpligtet til kontinuerligt at overholde dette system til håndtering af informationssikkerhed. Vi holder vores produktudvikling fokuserer på kundernes forretningsbehov og sikkerhedsproblemer gennem en serie globale kundedrevne innovationsprogrammer.

For at opfylde de høje krav til effektiv og målbar best practise inden for cybersikkerhed er beskyttelse en integreret del af designfasen for alle Ricohs produkter og tjenester – aldrig som en eftertanke – idet vi mener, at en holistisk tilgang til sårbarheder er afgørende for overlevelse i det moderne erhvervsliv.

SIKKERHEDSUDFORDRINGER

TENDENS: Efterhånden som datamængden øges, øges også sårbarheder, angreb og bødestraffe

Sikring af den digitale arbejdsplads

Ricoh forsøger at fremme og sikre digitale processer, hvor som helst mennesker interagerer. I en moderne digital økonomi betyder det tilføring af værdi ud over rammerne for det traditionelle kontor på innovative arbejdspladser. Fjernkontorer og fjernmedarbejdere gør det muligt at opnå store fleksibilitets- og produktivitetsgevinster i den daglige drift. Digitalisering hjælper også virksomheder med bedre at leve op til kundernes forventninger og servicekrav.

Men at arbejde på kanten af netværket medfører nogle af de største risici i forhold til sikkerheden. Dataene, som disse medarbejdere genererer, og enhederne, de benytter til at opfange dem, skal være sikret tilstrækkeligt. Mobile medarbejdere opererer desuden ofte på tværs af netværk og geografisk placering, hvilket komplicerer opgaven yderligere. Helt afgørende er, at love og regler som EU's persondataforordning (GDPR) vil kræve dokumentation for at virksomhederne sikrer deres data gennem hele levetiden. Efterhånden som arbejdspladsen udvikler sig og i stigende omfang benytter sig af digitale arbejdsgange, bliver livscyklussen for forretningsdata stadig mere kompliceret. Lad os kigge på det trin for trin.

Det første trin er datainput og scanningsenheder – en afgørende del af Ricohs sikkerhedsforsvar. Herfra skal data transporteres over netværk og lagres sikkert. På dette trin er bibeholdelse af dataintegriteten altafgørende. Ricohs systemer begrænser brugeradgang til enheds- og netværksfunktionalitet for at sikre, at data ikke kan manipuleres i transit eller under lagring. Disse tjenester omfatter adgangskontrol, kryptering og kopibeskyttelse. Vi kalder dette Kontrol.

Når dokumenterne er gemt, skal de samtidig være lettilgængelige for de personer i virksomheden, som skal bruge dem. Muligheden for at hente informationer, når det er nødvendigt, og at visualisere dem effektivt, afhænger af denne tilgængelighed. Dataanalyse er en afgørende komponent i den digitale arbejdsplads, da den giver et effektivt indblik i alle forretningsområder fra salg til HR. Godkendelsesværktøjer giver hurtig og sikker adgang, uanset brugerens lokation eller valg af enhed. Men det er afgørende, at sikkerhedsprotokoller ikke hæmmer innovation, funktionalitet eller fleksibiliteten hos medarbejderne. Vi kalder dette Bevarelse.

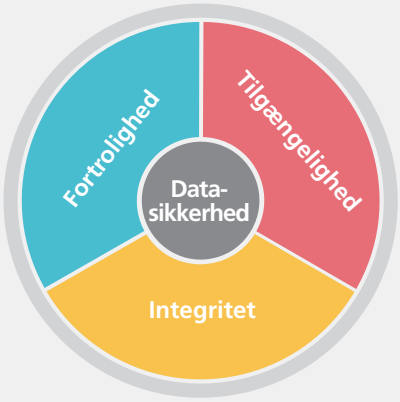
Endelig skal dataene kunne bortskaffes på en sikker og sporbar måde. Dette trin er afgørende for overholdelse af bestemmelser og minimerer muligheden for efterfølgende tyveri eller tab. Denne sikring sker faktisk gennem hele et dokuments levetid såvel som ved dets endelige sletning. Udskrivning af en fil efterlader et latent billede på harddisken i multifunktionsprintere (MFP'er), som skal overskrives for at hindre lækage. Ricohs tjeneste til databortskaffelse omfatter rensning af harddisken, sletning af hukommelsen, sletning af ikke-udskrevne filer og en funktion til sletning ved logout, som hindrer hackere i at indsamle følsomme oplysninger fra de spor, et dokument efterlader. Vi kalder dette Destruktion.

For effektivt at sikre forretningsdata gennem hele denne livscyklus anvender Ricoh "CIA"-principperne til sikring af data: Confidentiality, Availability og Integrity. Ovenstående er vores vejledningsprincipper, når vores produkter og løsninger designes til at overholde de nødvendige standarder. Denne tilgang muliggør innovation og vækst, mens processerne forbliver effektive og sikre.

RICOHS TILGANG TIL SIKKERHED

Adgang til information og dokumenter skal begrænses i henhold til kundens definerede sikkerhedskrav og politikker.

Adgang til information og dokumenter hvor og når, det kræves.



Hindring af uautoriseret dataredigering under transport eller lagring

Denne tilgang bygger på vores principper om privatliv og sikkerhed: fortrolighed, integritet og tilgængelighed

Sikkerhed er i vores DNA. Alle Ricohs produkter og tjenester indeholder indbyggede sikkerhedsfunktioner og egenskaber

Ricoh tilbyder et komplet udvalg af sikkerhedsprodukter og -tjenester til at sikre dokumenter i alle faser. Vi vil nu kigge nærmere på hvert enkelt trin: kontrol, bevarelse, destruktion og support.

FIRE TRIN TIL SIKKERHED PÅ DEN DIGITALE ARBEJDSPLADS

1 KONTROL

Effektiv datakontrol er afgørende for at beskytte fortrolige data og deres integritet. Forretnings-information er et vigtigt aktiv, som skal beskyttes. Nutidens hardware er informationsterminaler, der kan agere som sårbare indgange til virksomhedens oplysninger. Derfor anvender Ricoh flere redskaber til brugergodkendelse og enhedsadministration. Databeskyttelsen omfatter indstillinger på de fysiske enheder, som enten tillader eller begrænser adgang til visse funktioner og data. En begrænsning af medarbejdernes adgang til oplysninger, der føres gennem enhver MFP, er et vigtigt best practice-trin til opretholdelse af dokumentsikkerheden. Kontrolfasen omfatter desuden beskyttelse af enheder mod malware via Ricohs tredelte tilgang til firmware på enhederne.

Kontrol af uautoriseret kopiering

Som et værn mod forsøg på uautoriseret kopiering tilbyder Ricoh en elegant løsning, der garanterer sikkerheden for fysiske dokumenter. Når dokumenter udskrives eller kopieres, bliver usynlige mønstre indlejret i baggrunden. Hvis det udskrevne eller kopierede dokument fotokopieres og/eller scannes, bliver det indlejrede mønster synligt på kopien. Med denne funktion kan MFP'en registrere det indlejrede mønster og erstatte det fotokopierede billede med en grå farve for at forhindre lækage. Funktionen er nyttig, når der udskrives fortrolige oplysninger. Ved at begrænse duplikering af fortrolige oplysninger kan denne type datalækage minimeres betydeligt.

Låst udskrivning

Et dokument modtaget fra en pc kan lagres på MFP'ens harddisk. Med Ricohs låsefunktion angives der en adgangskode, når en bruger sender dokumentet, og samme adgangskode skal indtastes på MFP'en, før dokumentet kan udskrives. Da dokumentet ikke kan udskrives, før ejeren når frem til enheden, sikrer denne funktion, at dokumentet forbliver under ejerens kontrol.

Avancereret sikkerhed

Ricohs udvalg af avancerede capture-løsninger tilbyder forskellige lag af kryptering og dekryptering gennem alle proceslag og på tværs af hele gengivelsesprocessen. Administratorer kan autorisere adgang til proceskøer via individuelt bruger-login eller gruppe-login. Yderligere sikkerhedslag omfatter SAML (Security Assertion Markup Language) i et SSO-miljø (Single Sign On), PIV (Personal Identity Verification) og kryptering via PKI (Personal Key Infrastructure).

Integreret godkendelsesstyring

Enhedsadgang og protokoller til identitetsgodkendelse på tværs af Ricohs produkter kan styres centralt. Tilgængelige metoder omfatter id-kort, pinkode, netværks-login eller en kombination af disse i form af multifaktorgodkendelse. Multifaktorgodkendelse øger sikkerheden, men kan være et irritationsmoment for travle brugere. SSO (Single Sign On) afhjælper dette ved at give brugerne adgang til et udvalg af enheder. Desuden er Ricohs kortbaserede "swipe-and-go"-godkendelsessoftware forhåndsinstalleret på tværs af vores enheder, hvilket giver brugerne nem og hurtig adgang til deres dokumenter. Brugen af en NFC-kortlæser forenkler loginprocessen markant, mens den samtidig sikrer og kontrollerer MFP-adgangen. Denne form for adgangkontrol virker også sammen med eksisterende MFP-adgangstilladelser, så adgangsbegrænsingen fungerer som fastlagt af kunden.

Streamline NX (SLNX)

Device Manager-modulet i Ricohs Streamline NX-platform er Ricohs software til håndtering og overvågning af enheder på et netværk. Med softwaren kan administratorer se eller konfigurere sikkerhedsindstillinger for enheder via forhåndsdefinerede skabeloner og tilpassede parametre. Afgørende sikkerhedsindstillinger omfatter aktivering/deaktivering af protokoller, indstilling af IP-adresser, administratoradgangskoder, e-mailadresser til varsling, krypteringsindstillinger m.v. SLNX kan også rapportere om printere, der ikke er i overensstemmelse med kundens sikkerhedspolitik.

Malwarebeskyttelse af enheder

Ricoh anvender en trelagstilgang til beskyttelse af enheder mod malware. For det første kan Ricoh-enhederne kun betjenes ved hjælp af Ricohs eget maskinsprog eller operativsystem. For det andet skal alle firmwareopdateringer være skrevet og godkendt i dette Ricoh-maskinsprog for at hindre manipulering med enhedens software. Endelig skal alle firmwareopdateringer signeres digitalt af Ricoh. Ved hjælp af denne tretrinsmetode kan ikke-godkendt firmware ikke indlæses på Ricoh-enheder, så malware, spyware og virus elimineres effektivt.

Fysisk dokumentsikkerhed

Best practice for sikkerhed er ikke altid kompliceret. Kontorer er travle arbejdspladser, og fysisk dokumentation udgør en betydelig erhvervsrisiko, både hvad angår tyveri og medarbejdernes uagtsomhed. Ricoh anvender et antal ekstra valgmuligheder for fysisk sikkerhed til at forhindre uautoriseret adgang til fysiske dokumenter. F.eks. kan aflåsning af papirskuffer forhindre tyveri af følsomme dokumenter som f.eks. receptskabeloner i et lægefagligt miljø. Montering af kabelplader kan også forhindre muligheden for intern manipulering. En Print-to-me-løsning sikrer, at dokumenter kun udskrives, når ejeren er til stede, hvilket eliminerer risikoen for manglende afhentning af dokumenter.

2 BEVARELSE

Ifølge nye og eksisterende lovkrav skal virksomhederne sikre, at deres informationer er beskyttet, så de ikke kan stjæles eller lækkes, og at dataintegriteten bevares, så de ikke kan manipuleres. For at opnå dette skal virksomhederne begrænse adgangen til følsomme dokumenter. Dette forhindrer uautoriserede ændringer og forfalskninger. Det fungerer desuden som beskyttelse mod målrettede eller opportunistiske trusler fra virksomheden selv.

Mobile arbejdspladser tilføjer kompleksitet til ethvert cybersikkerhedsscenarie. Yderlige sikkerhedsforanstaltninger skal være på plads for at håndtere fildeling fra enhver lokalitet. Disse filer skal være lige så sikret under transit via netværket og via enheder, som de er, når de er lagret. Teknologi med stærk kryptering kan effektivt følge og beskytte data gennem hele livscyklussen. Dette gælder naturligvis for dokumenter, men kan også udvides til vigtige sikkerhedselementer som adgangskoder, makroindstillinger og adressebøger. Med krypteringen på plads vil eventuelle hackere have svært ved at udtrække brugbare oplysninger, hvilket bevarer dataintegriteten, selv i tilfælde af et sikkehedsbrud.

Kontinuerlig oppetid er altafgørende i mange brancher. Uforudsigelige hændelser, som f.eks. naturkatastrofer, udgør derfor en direkte erhvervsrisiko. Papirdokumenter er særligt udsatte i dette scenarie. Ved hjælp af et sikkert, cloudbaseret opbevaringssted til digitaliserede dokumenter tilføjes et vigtigt værn mod naturlige og menneskeskabte katastrofer. Der skal dog træffes passende sikkerhedsforanstaltninger for at beskytte disse data.

Essentiel datakryptering

For at beskytte oplysninger i transit mellem enheder, krypteres alle data, der transporteres til eller er gemt på en Ricoh MFP-harddisk. Indbyggede softwarefunktioner yder fuld kryptering af scannings- og printfiler via brugerens PKI-nøgle. Dette beskytter mod angreb i kundens eget it-miljø.

Som en yderligere sikkerhed overskrives printdata kontinuerligt af Ricohs Data Overwrite Security System (DOSS), som vi vil beskrive mere detaljeret i afsnittet om destruktion.

Beskyttelse af BIOS og operativsystem

Ricohs MFP'er anvender et TPM (Trusted Platform Module), som er et hardwarebaseret sikkerhedsmodul, der ikke kan manipuleres. TPM udfører krypterings-funktioner og opbevarer de krypterede data på en sikker måde. Ricoh anvender TPM til at opbevare root-krypteringsnøglen, der beskytter krypteringsnøglen til data på harddisken og MFP'ernes digitale certifikater. Modulet gør det også muligt for administratorer at udføre en betroet boot-operation, om validerer MFP'ens ægthed, før den kan betjenes.

Validering af firmware

Rodnøglen og krypteringsfunktioner er altid en del af TPM'en og kan ikke ændres fra den eksterne side af firewall'en, hvilket forhindrer misbrug eller manipulation af vores produkter. Denne proces yder high level-validering af MFP'ens firmware, identitet og harddisk-sikkerhed. Dette er endnu et godt eksempel på, hvordan Ricohs MFP-produkter er konstrueret med fokus på kundesikkerhed.

Administration af adgangskoder

Ricoh-enheder kan konfigureres med flere administratorer, hver med sin rolle, og forskellige adgangskoder. Adgangskoderne for disse brugere kan fjernkonfigureres via webbaserede admin-værktøjer og verificeres regelmæssigt. Dette muliggør adskillelse af ansvarsområder, som er et krav i en lang række brancher.

Begrænsning af brugeradgang

Med Ricohs brugerstyringsværktøj kan administratorer begrænse brugeradgange. Administratoren kan fx give udvalgte brugere adgang til MFP'ens registrerede adressebog. Dermed blokeres uautoriseret adgang til personlige oplysninger, som er gemt i kontorprinterne.

Funktion til brugerlåsning

Hvis forkerte adgangskoder indtastes flere gange ved login, kan en Ricoh MFP vurdere, om en person er i færd med at knække adgangskoden. Dette udløser låsefunktionen, der blokerer det pågældende brugernavn. Den blokerede bruger kan ikke godkendes, selv hvis den korrekte adgangskode indtastes efterfølgende. Låsningen kan udelukkende frigøres efter et bestemt tidsrum eller af en administrator, hvilket effektivt stopper potentielle hackere.

3 DESTRUKTION

Sikker destruktion af data er en vigtig del af ethvert omfattende cybersikkerhedsforsvar. Det er nemt at falde i den fælde, der hedder, at virksomhedens ansvar slutter, når data forlader organisationen. Mange bestemmelser anfører dog, at datadestruktion skal være en altomfattende proces, som eliminerer enhver risiko for efterfølgende tyveri eller misbrug. Indtil dette er bevist, er virksomhedens dataansvar ikke bortfaldet.

Kontormaskiner, som enten er udtjent eller sendt retur, er en ofte overset risiko, når det gælder forretningsoplysninger. Ricoh tilbyder en certificeret og sporbar tjeneste til fjernelse af data fra disse enheder ved kontraktudløb. Det omfatter overset materiale som fx gemte netværksindstillinger, brugerdata, harddiskdata og endda mærkater efterladt på enheden. Undladelse af at gøre dette udsætter virksomheden for en betydelig risiko for at miste fortrolig information og personlige oplysninger. For at overholde lovmæssige krav bør denne proces dog foregå kontinuerligt gennem hele enhedens levetid. Det sikrer, at virksomheden har den størst mulige kontrol over data, man har ansvaret for.

Billedoverskrivning: DOSS (Data Overwrite Security System)

MFP-harddiske fungerer effektivt ved at opbevare latente billeder af dokumentdata i hukommelsen til brug for jobbehandling. Ricohs DOSS-løsning sikrer, at billeder konstant overskrives, før næste job begynder. Såfremt nogen fik ondsindet adgang til harddisken, er vedkommende på den måde ikke i stand til opsnappe "fodspor" efter data fra tidligere jobs. Hos Ricoh er vi stolte over at have tilbudt denne best practice-sikkerhedsforanstaltning i mere end 20 år.

Rensning af udstyr ved kontraktudløb

Ricoh tilbyder en fuld rensningstjeneste til MFP'ere og printere, hvor alle hukommelsesmoduler og diske på enheden slettes ved hjælp af branchecertificerede metoder, så dataene ikke kan genskabes. Ricohs IT Services tilbyder også en omfattende tjeneste til bortskaffelse af udstyr, herunder flere niveauer af tjenester til certificeret datasletning.

Udskiftning af harddiske og flytbart lager

Ricoh tilbyder desuden harddiskbortskaffelse, som lader kunderne beholde deres harddisk. Harddisken udskiftes med en ny, tom harddisk, når kunden returnerer udstyret ved kontraktudløb. Det sikrer, at virksomheden har fuld, dokumenterbar kontrol over datamiljøet.

4 SUPPORT

Når virksomheder vokser, vokser antallet af forbindelser mellem enheder og netværk også. Det betyder, at de har brug for strategier til at sikre, at den voksende infrastruktur ikke udgør en sikkerhedsrisiko. De skal være opmærksomme på svage punkter i deres systemer og tage skridt til at forebygge målrettede og opportunistiske angreb.

Ofte kræves der specialiseret it-sikkerhedsekspertise for at analysere en virksomheds infrastruktur og identificere disse sårbarheder. For mange virksomheder er opretholdelse af en intern it-afdeling med den nødvendige viden til håndtering af cybersikkerhedsmiljøet ikke en reel mulighed. De forbundne omkostninger ved denne tilgang tvinger derfor ofte disse virksomheder ud i en farlig mangel på aktivitet.

Ricohs tilbyder en it-indkøbs- og konfigurationstjeneste samt mulighed for fjernovervågning, service desk og transitionshåndtering for yderligere at understøtte sikkerhedsprocessen. Cybersikkerhed kræver en holistisk forståelse af de forretningsmæssige risici. Ricohs Security Incident Response Team (SIRT) sikrer, at vitale trusselsefterretninger deles med kunder over hele verden, og effektive modforholdsregler kan koordineres øjeblikkeligt.

Sikkerhedsvurdering af infrastruktur

Ricohs Streamline NX (SLNX)-funktion til enhedshåndtering er konstrueret til at yde en uvurderlig revision af sikkerhedspolitikken. SNLX tilbyder en funktion, der gør det muligt for it-chefer at konfigurere enheder baseret på virksomhedens politik, distribuere disse indstillinger og analysere dem vha. en visualiseret rapport. SLNX kan desuden alarmere ledelsen, hvis en enhed ikke overholder virksomhedens sikkerhedspolitik.

Optimering af printsikkerhed

Ricoh tilbyder en omfattende tjeneste til optimering af printsikkerhed (PSO) sammen med professionelle og administrerede konsulenttjenester til identifikation af enhedsrelaterede sikkerhedsmangler. Der er tale om et webbaseret værktøj med en grafisk guide, der viser den aktuelle tilstand og en række Ricoh-produktanbefalinger med det formål at reducere risikoen.

Product Security Incident Response Team (PSIRT)

Ricohs aktive svar på nye trusler og udviklingen af effektive modforanstaltninger håndteres af Ricohs Product Security Incident Response Team (PSIRT). Det er et program, som Ricoh anvender til at sikre, at vores samlede produktsortiment (hardware og software) konstant er opdateret og beskyttet mod nye trusler og sårbarheder. Det hjælper os med at opretholde et konsistent højt serviceniveau på globalt plan og at minimere konsekvenserne af sårbarhedsproblemer på Ricoh-produkter.

Understøttende dokumentation

Forberedelse og vejledning er afgørende elementer i ethvert cybersikkerheds-setup. Såvel backup-dokumentation, brugervejledninger som sikkerhedshåndbøger og uddannelse skal tilbydes kunden. Som med andre elementer i sikkerhedsmiljøet er en dokumenterbar overholdelse af regler afgørende for at sikre virksomhedens bundlinje.

HVORDAN KAN RICOH HJÆLPE?

Ricohs enestående position som branchens førende leverandør af sikkerhedsløsninger på hele it- og printområdet er delvist baseret på en stor forståelse af markedet og en løbende udvikling af sortimentet i forhold til de ændrede behov. Vores løsninger er designet til at beskytte information i alle stadier og er tæt knyttet til de fire faser for databeskyttelse, der er omtalt i denne rapport.

Vi har dedikerede fageksperter med ansvar for at analysere markedsbehov, herunder branchespecifikke krav, som nye løsninger kan bygge på, eller som eksisterende løsninger kan skræddersys til.

Vi har også forpligtet os til at udvide vores interne muligheder for at udvikle og installere sikkerhedsbaserede løsninger. Til dette formål har vi oprettet dedikerede teams i vores udviklingsorganisation med fokus på tjenester til risikohåndtering, overholdelse af regler samt cybersikkerhed.

Brugergodkendelse og -autorisation

- Låst print
- Integreret software til godkendelse som standard
- Brugergodkendelse/adgangsbegrænsning
- Enkeltlogon
- Opsplitning af administratorroller
- Beskyttelse med PDF-password (til scannede dokumenter)
- Hindring af uautoriseret kopiering
- IP-områdebaseret adgangskontrol
- Sikker enheds- og printstyring
- PKI (Public Key Infrastructure)/SmartCard-understøttelse
- Sikker print (Print2Me/låst udskrivning)

Beskyttelse af BIOS og operativsystem

- Sikker opstart med Trusted Platform Module (TPM)

Billedoverskrivning

- DOSS (Disk Overwrite Security System)
- Flytbar harddisk

Malwarebeskyttelse

- Servere
- Ikke/mindre sårbare overfor malware
- SOP: Avanceret version af Android
- Ricoh-version af maskin-OS (maskinkontrolsprog) til MFP
- Tre sikkerhedslag: Digital signatur, download via Ricoh-værktøj, skrivning i særligt kontrolsprog

Datakryptering

- Harddiskkryptering via TPM
- Krypteringsnøgler via TPM
- Fuld kryptering af print- og scanningsfiler med PKI-nøgle
- FIPS-certificeret harddisk (Federal Information Processing Standards)
- Fuld kryptering ved udskrivning
- Fuld kryptering ved scanning

Bortskaffelse af harddisk

- Bortskaffelse af harddisk, billedoverskrivning
- Fuld datarensning
- Efter kontraktudløb: Destruktion af data i hukommelse/lager

Firmwareopdatering og passwordhåndtering

- Fjernkontrol af passwords
- Brugerlåsfunktion
- Firmwarevalidering via TPM

Enhedshåndtering

- Indstilling af printkvoter/maks.forbrug
- DMNX: Én løsning til sikkerhedskontrol, passwordstyring og overvågning

Overholdelse af industristandarder

- ISO 27001-certificering
- IEEE 2600.2-certificering af udvalgte produkter
- ISO 15408-certificering af udvalgte produkter
- Sikkerhedsdokumentation og -vejledning

RICOHS LAGDELTE TILGANG TIL DATABESKYTTELSE

Der er ingen tvivl om, at rollen for en MFP-leverandør har udviklet sig langt udover den transaktionsbaserede, endimensionelle levering af hardware. MFP-mulighederne spænder nu fra opfangning af information via flere inputkanaler til klassificering af de modtagne data, integration i arbejdsgange samt sikker dataopbevaring og -analyse. I denne komplekse verden af strenge lovgivningsmæssige krav til opbevaring kombineret med interne og eksterne trusler, der udgør en risiko for datatab, -destruktion eller -manipulation, anvender vi en lagdelt tilgang for at sikre, at din MFP og de forbundne systemer giver dig den bedst mulige beskyttelse.

1. Enheden

I centrum af enhver Ricoh-model har vi enhederne. Disse designes, produceres og implementeres med sikkerhed som et kernekrav. Det dedikerede Ricoh-operativsystem deler ikke sårbarheder med de mange kommercielle operativsystemer, og vores enheder er som standard certificeret i henhold til IEEE2600.2. Harddisk-kryptering og overskrivning sikrer, at de behandlede data forbliver fortrolige.

2. Egen brugerflade (Smart Operation Panel/SOP)

Som for selve MFP'en anvender SOP et dedikeret Ricoh-operativsystem. Der installeres ingen overflødige moduler, og root-adgang er ikke tilgængeligt. Ricoh har arbejdet hårdt på at sikre, at enhedssikkerheden ikke svækkes i forbindelse med introduktionen af SOP.

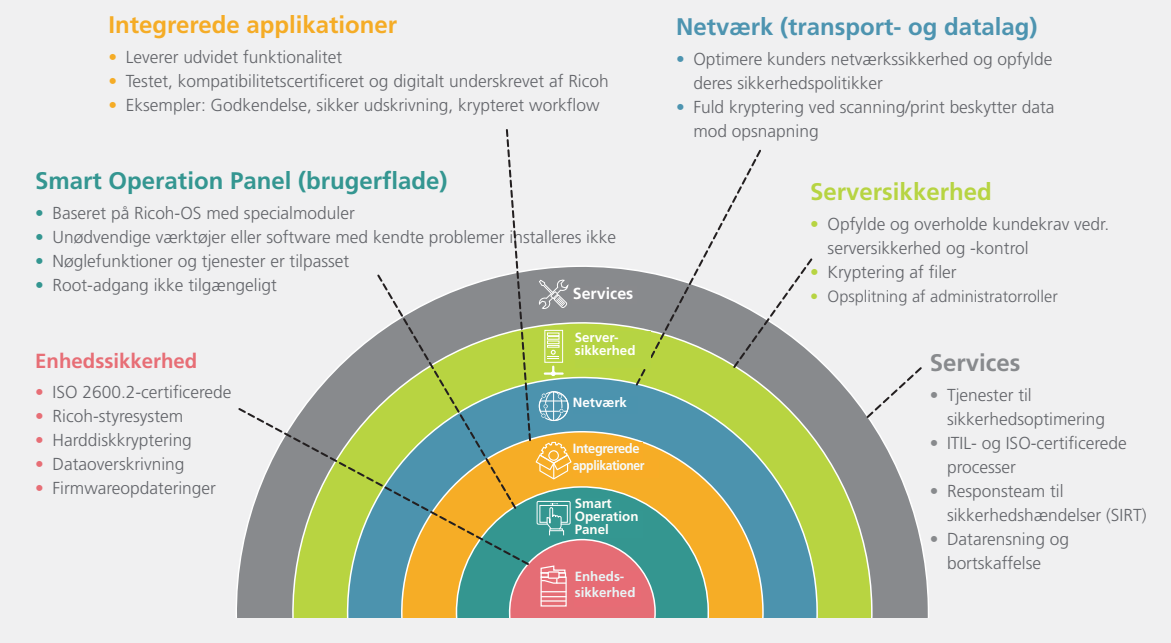
3. Smart-applikationer

Kan integreres i SOP og tilbyder ekstra funktionalitet til brugerne, herunder workflow-værktøjer og dataopfangning. Visse applikationer tilbyder vigtige sikkerhedsfunktioner. Disse omfatter sikker udskrivning, kortadgang og kryptering. Applikationerne udvikles af Ricoh eller medlemmer af Ricoh Developer Programme, og alle applikationer skal bestå Ricohs kompatibilitetstest og signeres digitalt, før de kan køre på vores SOP.

4. Netværk og servere

Uanset hvem der administrerer it-infrastrukturen, sikrer Ricoh, at vores produkter og tjenester overholder dine politikker for it- og netværkssikkerhed. Fuld kryptering af print- og scanningsfiler, kryptering af data på servere og opsplitning af administratorroller er teknikker, der anvendes til at beskytte mod "man-in-the-middle" eller "inside jobs".

Vi tilbyder en omfattende række sikkerhedstjenester som supplement til vores produkter. Dette omfatter rådgivning og administrerede services, der hjælper kunderne med at overvåge, optimere og administrere deres dokument- og informationssikkerhed. Vi tilbyder også en række tjenester, der sikrer, at RAM og harddiske i kasserede enheder renses for data før bortskaffelse.



SÅDAN SIKRER RICOH DEN DIGITALE ARBEJDSPLADS

Vores kunder oplever en række sikkerhedsudfordringer, som alle er baseret på det faktum, at efterhånden som datamængden øges, øges også sårbarheder, angreb og bødestraffe. At holde data fortrolige og sikre er en konstant kamp. Hos Ricoh afviser vi fx ca. 8 mia. firewall-angreb om måneden. Der findes titusindvis af globale, nationale og branchespecifikke dataregler, og virksomhederne skal være i stand til løbende at dokumentere overholdelse. Organisationer af alle størrelser søger derfor en partner, de kan have tillid til – en der kan hjælpe dem med at opretholde sikkerheden på tværs af den digitale arbejdsplads.

Ricoh har udviklet en lang række løsninger, der afbøder de forskellige risici, virksomhederne er udsat for. Da truslerne mod informationssikkerhed udvikler sig med lynets hast, anvender Ricoh sit "voice of the customer"-program til yderligere udvikling og levering af tjenester.

Vores Customer Advisory Boards fungerer som vigtige strategiske fokusgrupper. Vi anvendes grupperne til at få en bedre forståelse af de tendenser og prioriteringer, der former vores kunders forretninger. Vores Technology Advisory-konferencer giver os vigtige efterretninger fra fremtrædende beslutningstagere. Ricohs tekniske eksperter og R&D-teams bruger disse konferencer til at opnå værdifuld kundefeedback om idéer, koncepter og prototyper. Og endelig samarbejder Ricoh med individuelle kunder om at udvikle nye og avancerede sikkerhedsfunktioner til vertikale sektorer og det generelle marked. Denne kundedrevne tilgang hjælper os med at evaluere vores produktplaner og giver vores kunder fordel i form af et globalt netværk af tjenester og support.

Den moderne digitale arbejdsplads skal være lige så dynamisk som de cybertrusler, den står overfor, og lige så fleksibel som de arbejdsmetoder, den promoverer. Det er derfor, vi mener, at sikkerhed skal fungere problemfrit på tværs af de teknologier, vores kunder vælger at anvende på arbejdspladsen. Med udbredelsen af ISO 27001 gennem hele vores organisation og IEEE 2600-certificering på tværs af vores produkter, samt det dedikerede Ricoh-styresystem til vores MFP'er, kan du være sikker på, at du med Ricoh får markedets bedste sikkerhedsløsninger, uanset hvordan du vælger at strukturere og vækste din forretning.

Kombinationen af sikkerhedstrusler og lovgivnings-mæssige krav betyder, at riskoen for skader på økonomi og omdømme aldrig har været større. Det er derfor nu, du bør investere i sikkerhed via en partner, du har tillid til.

RICOH
imagine. change.

www.ricoh.dk