RICOH
imagine. change.

Ricohs sikkerhetsløsninger

Vi hjelper deg med å beskytte din virksomhet

Datasikkerhet er den største trusselen mot overlevelse og suksess for moderne virksomheter. Bedrifter av alle størrelser er under konstant risiko for å bli offer for ødeleggende angrep som f.eks. phishing, DDoS eller ransomware. Den reelle kostnaden ved slike angrep kan komme opp i millioner av kroner. I 2017 fant Ponemon Institute ut at den globale gjennomsnittskostnaden ved et datainnbrudd var 3, 62 millioner dollar. Denne kostnaden vil fortsette å øke i årene fremover da offentlige reguleringer, slik som EU-forordningen (GDPR), vil straffe virksomheter med høye bøter for å ikke sikre sine systemer og data på en tilstrekkelig måte. For å unngå disse kostbare bøtene, må virksomheten kunne dokumentere sin evne til å beskytte sine data. For å kunne gjøre dette, kreves det et helhetlig bilde av sårbarheten på tvers av hele organisasjonen.

En faktor som ytterligere kompliserer utfordringen ved datasikkerhet for virksomheter, er den økende digitaliseringen ved moderne arbeidsplasser og økningen i mengde data. Arbeidsflyter er ofte spredt på tvers av enheter, nettverk og geografiske områder. Informasjonen er utsatt for høyest risiko når den flyttes rundt i virksomheten. Den må beskyttes i alle stadier på sin reise. På grunn av den sikkerhetsrisikoen dette medfører, kan ikke lenger moderne virksomheter fungere uten grunnleggende sikring av sine dokumenter og datahåndteringssystemer. Samtidig har også funksjonaliteten til kontorskrivere og multifunksjonsenheter økt et ti-talls ganger de siste årene. Disse er står nå for en svært stor del av virksomhetens inndata, utdata, overføring av data og lagring av data. Dette gjør dem til farlige, men ofte oversette, trusselvektorer på dagens arbeidsplasser.

Selv om mange selskaper hevder å tilby sikkerhetsfunksjoner, har Ricoh utviklet sikre arbeidsplassløsninger og -tjenester i flere tiår. For eksempel har våre skrivere hatt muligheten for sikker overskriving av harddisken i mer enn 20 år.

Sikkerhet ligger i DNA-et i hele vår portefølje for en digital arbeidsplass. Vi har mer enn 4 millioner kontorprodukter hos kunder i dag. Alle disse produktene, og alle tjenestene vi leverer med dem, har innebygde sikkerhetsfunksjoner. For mange av våre produkter benytter vi også vårt eget Ricoh-operativsystem. Dette er en viktig del av vårt sikkerhetsforsvar, som gir kontroll og isolering fra OS-spesifikke trusler som ofte har de mer utbredte operativsystemene som mål.

Ricoh har en konsistent, verdensomspennende tjeneste- og supportstruktur for sine kunder. Dette sikrer at trusseletterretning blir delt og behandlet på en effektiv måte. Ikke bare er IEEE 2600-sertifisering implementert som standard på alle våre skrivere-/utdataenheter, men Ricoh er også et ledende medlem og en nøkkelforfatter for IEEE Standards Association. Ricoh er også ISO 27001-sertifisert, og forpliktet til å fortsette å etterkomme dette styringssystemet for informasjonssikkerhet. Vår produktutvikling fokuserer på kundens forretningsbehov og bekymringer for sikkerhet gjennom en rekke globale kundedrevne innovasjonsprogrammer.

For å møte de harde kravene for effektive, dokumenterbare løsninger for datasikkerhet er sikkerhet inkludert i alle produkter og tjenester i Ricohs portefølje gjennom design – aldri som en ettertanke. Vi tror at dette helhetlige bildet på sårbarhet er nøkkelen til overlevelse i moderne forretningsvirksomhet.

SIKKERHETSUTFORDRINGER FOR KUNDEN

TRENDER: Ettersom mengden data øker, vil også sårbarhet, angrep og bøter øke.

Sikre og styrke digitale arbeidsplasser

Ricoh arbeider for å muliggjøre og sikre digitalisert arbeid, uansett hvor folk befinner seg. I en moderne, digital økonomi betyr dette verdiskapning utover rammene til det tradisjonelle kontoret vi møter på arbeidsplasser. Fjerntliggende kontorer og arbeidere gir virksomheter stor fleksibilitet, og produktiviteten øker i den daglige driften. De hjelper selskapene til bedre å møte kundenes forventninger og krav til service.

Imidlertid, å operere slik på kanten av nettverket utgjør en av de største risikoene til virksomhetens sikkerhet. Dataene som blir generert av disse arbeiderne, og de eksterne enhetene som de bruker for å innhente dem, må være hensiktsmessig sikret. Ansatte vil ofte operere på tvers av nettverk og geografiske områder, noe som videre kompliserer denne oppgaven. Det viktigste her er at offentlige reguleringer som GDPR krever at virksomhetene kan dokumentere at deres data er sikret gjennom hele levetiden, hvis ikke kan de stå overfor alvorlige straffer. Ettersom arbeidsplasser utvikler seg og går over til digitale arbeidsflyter, vil livssyklusen til kommersielle data gradvis bli mer komplisert. La oss se på det nå, steg for steg.

Det første steget er inndata og enheter for datafangst – en nøkkelkomponent i Ricohs sikkerhetsforsvar. Herfra må dataene overføres gjennom nettverket for å lagres på en sikker måte. På dette stadiet er det avgjørende å bevare dataintegriteten. Ricohs systemer begrenser brukertilgang til enhets- og nettverksfunksjonalitet for å sikre at det ikke er mulig å påvirke data under transport eller i hvilemodus. Disse tjenestene inkluderer tilgangskontroll, kryptering og kopibeskyttelse. Vi kaller dette steget Kontroll.

Etter de er lagret må likevel dokumentene være raskt tilgjengelig for de i virksomheten som trenger dem. Muligheten til å effektivt gjøre bruk av og se på data når behovet er der, avhenger av tilgjengeligheten. Dataanalyse er en viktig del av en sterk digital arbeidsplass. Den gir effektivt innsikt for hvert ledd i virksomheten fra salg til HR. Verktøy for autorisasjonsinfrastruktur gir rask og sikker tilgang, uavhengig av brukerplassering eller valg av enhet. Det er viktig at sikkerhetsprotokoller ikke hindrer utvikling eller funksjonalitet, eller at de ansatte vegrer seg for dem. Vi kaller dette steget Bevaring.

Til slutt må dataene avhendes på en sikker og dokumenterbar måte. Dette steget er avgjørende for å være i samsvar med regulatoriske krav, og for å minimere muligheten for påfølgende tyveri eller tap. Faktisk skjer denne prosessen gjennom hele dokumentets livssyklus, i tillegg til dets endelige sletting. Utskrift av enhver fil etterlater seg et skjult bilde på harddisken til multifunksjonsskrivere (MFP-er), og disse må overskrives for å hindre uautorisert tilgang. Ricohs tjeneste for dataavhending inkluderer rensing av harddisk, tømming av minne, sletting av filer som ikke er skrevet ut og funksjonalitet for sletting ved utlogging for å hindre hackere fra å samle sammen sensitiv informasjon fra fotavtrykkene som et dokument etterlater seg. Vi kaller dette steget Destruering.

For effektivt å sikre arbeidsplassens data gjennom hele levetiden, bruker Ricoh «CIA»-prinsippet for personvern og sikkerhet: Konfidensialitet, Integritet og Tilgjengelighet (Confidentiality, Integrity and Availability.) Dette er våre rettesnorer når vi designer våre produkter og løsninger, med det mål for øye at de skal imøtekomme de nødvendige standarder og reguleringer. Denne tilnærmingen åpner for innovasjon og vekst på arbeidsplassen, samtidig som effektive og sikre prosesser opprettholdes.

RICOHS TILNÆRMING TIL SIKKERHET

Vi bygger på «CIA»-prinsippet for personvern og sikkerhet: konfidensialitet, integritet og tilgjengelighet

Sikkerhet ligger i vårt DNA. Alle produkter og tjenester fra Ricoh har innebygde sikkerhetsfunksjoner og muligheter

Ricoh tilbyr en komplett pakke med sikkerhetsprodukter og tjenester for å sikre dokumenter fra opprettelse til sletting.

Vi vil nå se på hvert av disse viktige stegene: Kontroll, Bevaring, Destruering og Støtte.

FIRE STADIER AV SIKKERHET PÅ DIGITALE ARBEIDSPLASSER

1 KONTROLL

Effektiv datakontroll er avgjørende for å opprettholde konfidensialitet og integritet. Bedriftsinformasjon er en primærressurs som må beskyttes. Dagens maskinvareenheter er informasjonsterminaler som kan fungere som sårbare innfallsporter til bedriftsinformasjon. Ricoh har derfor flere verktøy for brukerautentisering og enhetshåndtering for å kontrollere og sikre virksomhetens data. Disse angår innstillinger på fysiske enheter som tillater og begrenser tilgang til visse funksjonaliteter og data. Begrensning av ansattes tilgang til informasjon som går via en hvilken som helst multifunksjonsskriver (MFP) er et viktig steg i opprettholdelsen av dokumentsikkerhet. Kontrollfasen inkluderer også beskyttelse mot skadelig programvare for enheter via Ricohs tre-trinns tilnærming til fastvare på enheter.

Kontroll av uautorisert kopiering

For å beskytte mot forsøk på å lage uautoriserte kopier, tilbyr Ricoh en elegant løsning for å ivareta sikkerheten til papirdokumenter. Kopibeskyttelsesfunksjonen skriver ut eller kopierer dokumenter med spesielle usynlige mønstre på tvers av bakgrunnen. Hvis disse dokumentene blir kopiert og/eller skannet, vil dette mønsteret bli synlig på kopiene. Modulen for beskyttelse mot uautorisert kopiering tillater MFP-en å oppdage det innebygde mønsteret, og erstatte det kopierte bildet med et grått bilde for å unngå informasjonslekkasjer. Denne funksjonen er nyttig når konfidensiell informasjon skal skrives ut. Restriksjoner på duplisering av konfidensiell informasjon hindrer slike typer informasjonslekkasjer.

Sikker utskrift

Et dokument mottatt fra en PC kan lagres på harddisken til MFP-en. Når Ricohs sikker utskriftsfunksjon brukes, må et passord angis når brukeren sender dokumentet. Dette passordet må skrives inn på MFP-en før dokumentet kan skrives ut. Siden dokumentet ikke vil bli skrevet ut før eieren er ved enheten, sikrer denne funksjonen at dokumentet forblir under eierens kontroll.

Avansert sikring ved datafangst

Ricohs portefølje med avanserte løsninger for datafangst tilbyr flere lag av kryptering og dekryptering gjennom prosesslagene, og på tvers av alle nivå i datafangstprosessen. Administratorer kan autorisere tilgang til prosesskøene med individuelle brukerinnlogginger eller flerbrukerinnlogging. Ekstra lag for sikkerhet inkluderer Security Assertion Markup Language (SAML) for et nett med Single Sign On (SSO), Personal Identity Verification (PIV) og Public Key Infrastructure (PKI)-kryptering.

Innebygde autentiseringskontroller

Protokoller for enhetstilgang og identitetsautentisering kan administreres sentralt for alle Ricohs produkter. Tilgjengelige metoder inkluderer ID-kort, PIN-kode, innlogging på nettverk eller en kombinasjon av disse. Godkjenning med flere faktorer øker sikkerheten, men den kan sinke travle brukere. Single Sign On (SSO) forebygger dette ved å gi brukere sømløs tilgang til flere enheter. Ricohs hurtiggodkjenning, et kortbasert «swipe-and-go» autentiseringsprogram, er forhåndsinstallert i våre enheter, og det gir brukerne tilgang til deres dokumenter på en enkel måte. Ved å bruke en NFC-leser/skriver forenkles innloggingen for brukerne enormt, samtidig som den effektivt sikrer og kontrollerer tilgangen til MFP-en. Denne formen for tilgang fungerer også i kombinasjon med eksisterende MFP-innstillinger, og begrenser brukertilgang til enhetsfunksjoner bestemt av kunden.

Streamline NX (SLNX)

Enhetsstyringsmodulen i Ricohs Streamline NX-platform er Ricohs programvare for å administrere og overvåke enheter i et nettverk. Programvaren gir administratorer muligheten til å se eller konfigurere sikkerhetsinnstillinger for enheter ved å bruke forhåndsinstallerte maler og kundeparametere. Kritiske sikkerhetsinnstillinger inkluderer blant annet aktivering/deaktivering av protokoller, innstillinger for IP-adresser, passord for administratorer, e-postadresser for varsler og innstillinger for kryptering. SLNX kan også rapportere de skriverne som ikke tilfredsstiller kravene basert på kundens policy.

Enhetsbeskyttelse mot skadelig programvare

Ricoh har en tre-trinns tilnærming til beskyttelse mot skadelig programvare på sine enheter. For det første, Ricohs enheter kan kun betjenes ved å bruke et maskinspråk eller operativsystem kun for Ricoh-produkter. For det andre, for å hindre skadelig manipulering av programvare på enheter, må all oppdatering av fastvare kun skrives og godkjennes ved bruk av Ricohs eget maskinspråk. Til slutt, alle fastvareoppdateringer må signeres digitalt av Ricoh. Ved å bruke denne tre-trinns metoden kan ikke fastvare som ikke er godkjent lastes opp til Ricohs enheter, så skadelig programvare, spionprogrammer og virus blir effektivt eliminert.

Sikring av fysiske dokumenter

Den beste tilnærmingen til sikkerhet trenger ikke være komplisert. Kontorer er travle steder, og papirkopier representerer en vesentlig forretningsrisiko når det gjelder både tyveri og uaktsomhet fra ansatte. Ricoh gir en rekke alternativer for ekstra fysisk sikring for å hindre uautorisert tilgang til papirdokumenter. For eksempel hindrer låsing av papirskuffene tyveri av sensitivt materiale, slik som resepter i helsevesenet. Montering av blindplater foran alle kabler forhindrer muligheten for manipulering fra interne trusler. En sikker utskriftsløsning (Print-to-me) sørger for at dokumentet kun skrives ut når eieren er tilstede. På denne måten elimineres risikoen med utskrifter som ikke hentes.

2 BEVARING

Nye og eksisterende reguleringer gjør at virksomheter må sikre både informasjonens konfidensialitet, slik at den ikke blir stjålet eller lekket, og dens integritet, slik at den ikke kan endres. For å oppnå dette må virksomheter begrense tilgangen til sensitive dokumenter. Dette forhindrer uautorisert modifisering og forfalskning. Det fungerer også som beskyttelse mot målrettete eller opportunistiske trusler innenfor virksomheten.

Mobile arbeidsplasser gjør alle scenarier ved datasikkerhet mer kompleks. Ekstra sikkerhetstiltak må være på plass for å imøtekomme fildeling fra enhver lokalisering. Disse filene må være like sikre under overføring via nettverk og på tvers av enheter, på samme måte som når de er på lager. Sterk krypteringsteknologi kan effektivt følge og beskytte data gjennom livssyklusen. Dette gjelder naturligvis for dokumenter, men strekker seg også til viktige sikringselementer som lagrede passord, makroinnstillinger og adressebøker. Selv om hackere skulle klare å få tilgang til ditt nettverk, vil de streve med å trekke ut brukbar informasjon hvis kryperingen er på plass. Dette sikrer dataintegriteten i tilfelle et brudd skulle oppstå.

Kontinuerlig oppetid er overordnet i mange industrier. Uforutsette hendelser, slik som naturkatastrofer, kan derfor være en direkte forretningsrisiko. Papirdokumenter er særlig utsatte i et slikt scenario. Bruk av et sikkert, skybasert oppbevaringssted for digitale dokumenter gir ekstra motstandsdyktighet mot natur- og menneskeskapte katastrofer. Uansett må hensiktsmessige sikkerhetstiltak tas for å sikre digitale data.

Kryptering av essensiell data

For å beskytte informasjon som forflyttes mellom enheter kan kryptering aktiveres for hvilke som helst data som flyttes til, eller befinner seg på en Ricoh MFP harddisk. Muligheter innebygd i programvaren gir ende-til-ende-kryptering for skannede og utskrevne filer ved hjelp av brukerens PKI (public key infrastructure)-nøkkel. Dette beskytter mot angrep fra "mellommenn" innenfor kundens IT-miljø.

For ekstra sikkerhet blir utskriftsdata kontinuerlig overskrevet av Ricohs Data Overwrite Security System (DOSS), som vi skal se nærmere på i fasen «destruering» for livssyklusen til data.

Beskyttelse av BIOS og operativsystem

Ricohs MFP-er bruker en TPM (Trusted Platform Module), som er en inngrepssikker modul for sikring av maskinvare. TPM-en utfører krypteringsfunksjoner og lagrer kryptografiske data på en sikker måte. Ricoh bruker TPM-en til å lagre rotkrypteringsnøkkelen som beskytter krypteringsnøkkelen for harddiskdata og det digitale sertifikatet for MFP-ene. Dette gjør at administratorer kan foreta en pålitelig oppstartsoperasjon som validerer MFP-ens fastvareautentisitet før den blir gitt tillatelse til å fungere.

Validering av fastvare

For å forhindre misbruk av, eller skadelige inngrep på våre produkter, er rotnøkkelen og de kryptografiske funksjonene alltid bevart innenfor TPM-en, og kan ikke endres fra utsiden av brannveggen. Denne prosessen gir validering på høyt nivå av MFP-ens fastvare og enhetsidentitet, samt sikkerhet til harddisken. Dette er enda et godt eksempel på hvordan Ricohs produkter er skapt med fokus på Ricohs kunders sikkerhetsbehov.

Administrering av passord

Ricohs enheter kan konfigureres med flere administratorbrukere, hver med ulike roller for enheten og egne passord. Passordene for disse brukerne kan fjernkonfigureres ved bruk av et nettbasert administrasjonsverktøy, og kontrolleres regelmessig. Dette muliggjør «ansvarsfordeling», noe som er et krav i mange forretningsforskrifter.

Begrensning av brukertilgang

Ricohs brukeradministrasjonsverktøy lar systemadministratorer begrense rettigheter på brukertilganger. For eksempel kan administratoren sette opp rettigheter for å gi utvalgte brukere tilgang til en MFP-registrert adressebok. Dette blokkerer uautorisert tilgang til personlig informasjon og dokumenter lagret på kontorenheter.

Funksjon for blokkering av bruker

Når feil passord tastes inn flere ganger på rad ved innlogging, kan en Ricoh MFP evaluere om noen prøver å knekke passordet. Dette utløser blokkeringsfunksjonen som vil blokkere det aktuelle brukernavnet. Det blokkerte brukernavnet kan deretter ikke autentiseres selv med det korrekte passordet. Blokkeringen vil kun opphøre etter en gitt tid, eller av en administrator, og er effektivt for å hindre at noen prøver å hacke passordet.

3 DESTRUERING

Sikker dataavhending er en essensiell del av alle omfattende forsvarssystemer for datasikkerhet. Det er lett å gå i den fellen å tro at forretningsansvaret slutter når data forlater organisasjonen. Det er likevel mange forskrifter som fastsetter at destruering av data må være en omfattende prosess som eliminerer all risiko for senere tyveri eller misbruk. Frem til dette kan bevises, er ikke bedriftens ansvar for sine data over.

Utgåtte og returnerte kontorenheter kan ofte utgjøre en risiko for bedriftens forretningsinformasjon. Ricoh tilbyr en sertifisert og ettersynbar tjeneste for fjerning av data fra disse utgåtte skriverne. Dette inkluderer oversett informasjon som lagrete nettverksinnstillinger, brukerdata, harddiskdata og til og med klistermerker på enheten. Hvis dette ikke gjøres vil virksomhetene ha en betydelig risiko for at konfidensiell informasjon om virksomheten eller personalet avdekkes. For å kunne opprettholde overholdelse må denne prosessen også skje konstant gjennom enhetens levetid. Dette sikrer at virksomhetene har maksimal kontroll over de data de er ansvarlige for.

Overskriving av bilde: Data Overwrite Security System (DOSS)

MFP-enes harddisker fungerer effektivt ved å lagre et skjult bilde av dokumentdata i minnet for utføring av jobben. Ricohs Sikkerhetsløsning for dataoverskriving sikrer at dette hele tiden blir overskrevet før den neste jobben starter. På denne måten vil ingen kunne se «fotavtrykket» til data fra foregående jobber, selv om de skulle få tilgang til harddisken med ondsinnete tanker. Hos Ricoh er vi stolte av å ha tilbudt dette sikkerhetstiltaket som beste praksis i over 20 år.

Dataslettingstjenester for livssyklusslutt

Ricoh tilbyr en full dataslettingstjeneste, en slutt-tjeneste hvor utgåtte MFP-er og skrivere får minnemoduler og lagringsdisker på enheten slettet fullstendig, uten mulighet for gjenoppretting, ved bruk av industrisertifiserte sikkerhetsløsninger. Ricohs IT-tjenester tilbyr også en omfattende avhendingstjeneste for utstyr, som inkluderer flere nivå med sertifiserte datafjerningstjenester.

Utskiftning av harddisk og fjernbare lagringsenheter

Ricoh tilbyr en avhendingstjeneste for harddisker som lar kunden beholde sin harddisk. Denne blir erstattet med en ny, tom harddisk når de returnerer utstyret etter endt leieperiode. Dette garanterer virksomhetene en komplett, dokumenterbar kontroll over sitt datamiljø.

4 STØTTE

Etterhvert som virksomhetene vokser, er det ikke til å unngå at antall tilkoblinger mellom enheter og nettverk også øker. Virksomheter behøver strategier for å sikre at veksten i denne infrastrukturen ikke utgjør en sikkerhetsrisiko. De må være oppmerksom på de svake punktene i sine systemer, og ha tiltak for å hindre målrettete og opportunistiske angrep.

Det er ofte behov for spesialisert ekspertise på IT-sikkerhet for å analysere virksomhetens infrastruktur, og identifisere disse sårbare punktene. For mange virksomheter er det ikke et alternativ å ha en egen IT-avdeling med nødvendig kunnskap for administrering av datasikkerhet. Kostnadene og ineffektiviteten ved en slik tilnærming leder ofte disse virksomhetene til en farlig passivitet.

Ricohs IT-supporttjeneste tilbyr IT-tjenester for anskaffelse og konfigurasjon, i tillegg til fjernovervåking, service-desk og administrerende tjenester i overgangsfasen for ytterligere å støtte prosessen for datasikkerhet. Datasikkerhet er avhengig av en helhetlig forståelse av forretningsrisikoene. Ricohs Security Incident Response Team (SIRT) sikrer at viktig trusseletterretning blir delt med klienter i hele verden, og at en effektiv respons kan iverksettes umiddelbart.

Sikkerhetskartlegging av infrastrukturen

Funksjonaliteten til Ricohs Streamline NX (SLNX) enhetsbehandler er designet for å utføre en uvurderlig ettersynsfunksjon på sikkerhetsretningslinjene. SLNX gir en funksjonalitet som IT-ledere aktiverer for å sette opp enheter basert på selskapets retningslinjer, distribuere disse innstillingene og analysere dem ved bruk av en visualisert rapport. SLNX kan også varsle ledelsen når en enhet ikke samsvarer med selskapets retningslinjer.

Optimalisering av utskriftssikkerhet

Ricoh tilbyr en omfattende Print Security Optimisation (PSO)-tjeneste, samt konsultasjonstjenester slik at alle enhetsrelaterte brudd på sikkerheten kan identifiseres. Dette er et nettbasert verktøy med en grafisk veiviser som gir et bilde på den nåværende tilstanden, og som gir Ricoh muligheten til å gi produktanbefalinger.

Product Security Incident Response Team (PSIRT)

Ricohs respons til nye trusler og utviklingen av effektive tiltak, er styrt av PSIRT. Dette er et program som Ricoh bruker for å sikre at hele vår produktserie (maskinvare og programvare) kontinuerlig blir oppdatert og beskyttet mot nylig identifiserte trusler og sårbarheter. Dette hjelper oss til å opprettholde et konsekvent høyt servicenivå globalt, og minimere effekten av sårbarheter på Ricohs produkter.

Dokumentasjon

Forberedelse og opplæring er et viktig element i alle oppsett for datasikkerhet. Støttedokumentasjon, brukermanualer, sikkerhetspublikasjoner og opplæring skal gis til kunden. Som ved mange aspekter av et datasikkerhet er dokumenterbar overholdelse avgjørende, og denne dokumentasjonen spiller en nøkkelrolle i sikringen av fortjeneste.

HVORDAN KAN RICOH HJELPE DIN BEDRIFT?

Ricohs unike posisjon som leverandør av industriledende sikkerhetsløsninger på tvers av hele IT- og utskriftsmiljøet, er delvis forutsatt av å opprettholde en sterk forståelse for endrede markedsbetingelser og å utvikle oss i samsvar med disse. Våre løsninger er skapt for å beskytte all informasjon gjennom hele dens livssyklus, og å følge de fire områdene for datasikkerhet som er tatt opp i denne rapporten.

Vi har dedikerte fageksperter som er ansvarlige for å analysere behovene i markedet, inkludert industrispesifikke standarder som nye løsninger kan bygges etter, eller som eksisterende løsninger kan tilpasses til.

Vi er også forpliktet til å utvikle vår interne kapasitet for å konstruere og levere sikkerhetsfokuserte løsninger. Med dette mål for øyet har vi opprettet dedikerte arbeidsgrupper innen tjenesteutvikling som skal fokusere på nye retningslinjer, risikostyring og datasikkerhetstjenester.

Brukerautentisering og autorisering

- Sikker utskrift
- Standard innebygget S/W for autentisering
- Brukerautentisering / tilgangsbegrensning
- Enkel pålogging
- Flere administratorroller
- PDF passordbeskyttelse (passord for skannede dokumenter)
- Beskyttelse mot uautorisert kopiering
- Tilgangskontroll basert på IP-adresser
- Sikker enhets- og utskriftsstyring
- PKI (Public Key Infrastructure) / SmartCard-støtte
- Sikre utskrifter (print2me / sikker utskrift)

Enhetsbeskyttelse mot malware

- Servere
- Ikke/lite utsatt for skadelig programvare
- SOP – forsterket versjon av Android
- Ricohs egen versjon av OS (kontrollspråk for maskin) for MFP
- 3-nivås tilnærming – digital signatur, nedlasting via Ricohs verktøy, må skrives i spesifikt kontrollspråk

Avhending av harddisk

- Avhending av harddisk, overskriving av bilde
- Full dataslettingstjeneste
- Tjenester ved livssyklusslutt: destruering av data i minnemoduler, lager

Enhetsstyring

- Kvoteinnstillinger / kontobegrensning
- DMNX – sikkerhetsrevisjon via et skjermbilde, passordstyring, overvåking, varsling

Beskyttelse av BIOS og operativsystem

- Sikker oppstart ved bruk av TPM (Trusted Platform Module)

Overskriving av bilde og fjernbare lagringsmedier

- Disk Overwrite Security System (DOSS)
- Fjernbar harddisk

Datakryptering

- Harddisk kryptering via TPM
- Krypteringsnøkler via TPM
- Ende-til-ende kryptering av utskrifter og skannete filer ved bruk av PKI-nøkkel
- FIPS sertifisert HDD (Federal Information Processing Standards)
- Ende-til-ende kryptering for utskrift
- Ende-til ende kryptering for skanning

Fastvareoppdateringer og administrering av passord

- Fjernstyrt passordkontroll
- Funksjon for blokkering av brukere
- Fastvarevalidering via TPM

Overholdelse av industristandarder

- ISO 27001 Sertifisering
- IEEE 2600.2 Sertifisering for utvalgte produkter
- ISO 15408 Sertifisering for utvalgte produkter
- Sikkerhetsdokumentasjon og opplæring

RICOHS LAGVISE TILNÆRMING TIL ENHETSSIKRING

Det er ingen tvil om at rollen til MFP-leverandøren har utviklet seg fra en mer transaksjonell rolle som forhandler, til å faktisk være ansvarlig for selve datahåndteringen. Funksjonaliteten til MFP-ene spenner seg nå fra å innhente data fra flere kilder til klassifisering av de innhentete data og integrering av arbeidsflyt, til en trygg, sikker lagring og analyse. I dette sammensatte bildet med strenge regler og krav til oppbevaring – sammen med interne og eksterne trusler som setter data i fare for tap, ødeleggelse eller manipulering – tar vi en lagvis tilnærming til enhetssikkerhet, for å sikre at din MFP og de systemene den er koblet til gir deg best mulig beskyttelse.

1. Enheten

I kjernen av alle Ricoh-modeller har vi enheten. Disse er designet, produsert og implementert med sikkerhet som et kjernekrav. Vårt eget Ricoh operativsystem deler ikke sårbarheten som er tilstede i mange kommersielle hylleprodukter for operativsystemer, og våre produkter er sertifisert til IEEE2600.2 som standard. Kryptering av harddisk og sikkerhet ved overskriving av disk, sikrer at data som behandles forblir konfidensiell.

2. Smartpanelet (SOP) sørger for brukergrensesnittet

Smartpanelet vårt bruker også et eget Ricoh operativsystem, på samme måte som MFP-ene. Ingen unødvendige komponenter er installert, og rottilgang er ikke tilgjengelig. Ricoh har jobbet hardt for å sikre at enhetssikkerheten ikke er svekket av introduksjonen av SOP-et.

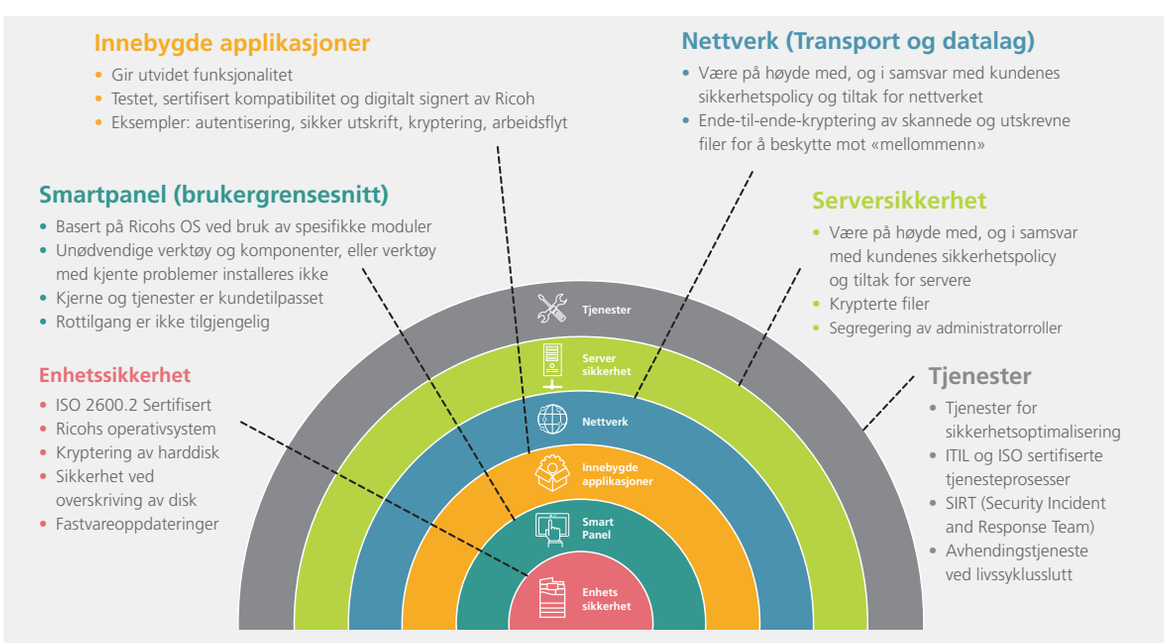
3. Smarte applikasjoner

Disse kan legges inn i SOP-et, og gir ekstra funksjonalitet til brukeren, inkludert arbeidsflyt og datafangst. Noen applikasjoner gir essensielle sikkerhetsfunksjoner. Dette inkluderer muligheten for sikker utskrift, korttilgang og kryptering. Applikasjonene er utviklet av Ricoh, eller medlemmer av Ricoh Developer Programme, og alle applikasjoner må passere Ricohs kompatibilitetstesting og signeres digitalt før de kan kjøres på SOP-et.

4. Nettverk og servere

Uavhengig av hvem som styrer IT-infrastrukturen, sikrer Ricoh at våre produkter og tjenester er i samsvar med dine retningslinjer for IT- og nettverkssikkerhet. Ende-til-ende-kryptering av utskrevne og skannete filer, kryptering av data på servere og segregering av administrasjonsansvar er teknikker som brukes for å beskytte mot «mellommenn» eller «innsidejobber».

En omfattende serie med sikkerhetstjenester favner hele vårt tilbud. Dette inkluderer konsultasjoner og administrative tjenester for å hjelpe kunder å overvåke, optimalisere og styre sin dokumentasjons- og informasjonssikkerhet. Vi har også en rekke tjenester ved livssyklusslutt som vil sikre at RAM og HDD til kundeenheter som er gått ut på dato blir renset før avhending.



HVORDAN RICOH BESKYTTER DEN DIGITALE ARBEIDSPLASSEN

Våre kunder har et antall grunnleggende sikkerhetsbekymringer, alle understøttet av det faktum at mengden sårbarhet, angrep og reguleringer øker i takt med volumet. Det er en konstant kamp å holde dine data konfidensielle, sikre og trygge for manipulering. Hos Ricoh avverger vi for eksempel rundt 8 milliarder angrep på brannmuren hver måned. Det er titusener av globale, nasjonale og industrielle dataforskrifter, og virksomheter må være i stand til kontinuerlig å dokumentere sin overholdelse til hver og en av dem. Det er forståelig at virksomheter i alle størrelser ser etter en partner de kan stole på – en som kan hjelpe dem til å forbli sikret på tvers av en portefølje som dekker hele den digitale arbeidsplassen.

Ricoh har utviklet et bredt spekter av løsninger for å begrense de ulike risikoer som virksomhetene møter. Ettersom trusselbildet rundt informasjonssikkerhet utvikler seg utrolig raskt, ser Ricoh til sine «kundens stemme»-programmer for videre å utvikle og levere våre tjenester.

Våre kundegrupper fungerer som viktige fokusgrupper. Vi bruker disse for å få en bedre forståelse av trendene, de drivende kreftene og prioriteringene som former våre kunders virksomheter. Våre teknologikonferanser gir viktig innsikt fra beslutningstakere. Ricohs forskning og utviklingsteam benytter disse konferansene til å få verdifulle tilbakemeldinger fra kunder på ideer, konsepter og prototyper. I tillegg samarbeider Ricoh med individuelle kunder for å utvikle nye og avanserte sikkerhetsfunksjoner. Denne kundedrevne tilnærmingen hjelper oss å vurdere vårt «veikart» for produktene, og hjelper våre kunder å dra nytte av et globalt nettverk av tjenester og support.

Den moderne, digitale arbeidsplassen må være så dynamisk som de truslene den står overfor, og så fleksibel som arbeidsrutinene tillater det. Derfor mener vi at datasikkerheten må virke sømløst på tvers av den teknologien våre kunder velger for å bruke på sin arbeidsplass. Vår organisasjons forpliktelser til ISO 27001, og IEEE 2600-sertifisering for våre produkter sammen med Ricohs eget operativsystem installert i disse, betyr at de beste løsningene for sikkerhetskontroll er på plass, uansett hvordan du velger å strukturere og utvide din virksomhet.

En kombinasjon av sikkerhetstrusler, lovkrav og komplekse industristandarder betyr at potensialet for skade på omdømme og finansielle skader fra datarisiko, aldri har vært større. Tiden er nå inne for å arbeide med en trygg partner som kan hjelpe deg med å sikre din virksomhets mest sårbare eiendeler, og beskytte dine fremtidige ambisjoner.

RICOH
imagine. change.

www.ricoh.no