RICOH
imagine. change.

Ricoh säkerhetslösningar

Hjälper dig skydda ditt företag

Bristande cybersäkerhet är det största hotet mot överlevnad och framgång för moderna företag. Företag av alla storlekar löper konstant risk att utsättas för fördärvande attacker t.ex. nätfiske, DDoS-attacker eller utpressningstrojaner. Den faktiska kostnaden för dessa attacker uppgår till miljonbelopp. 2017 upptäckte Ponemon-institutet att den globala genomsnittskostnaden för dataöverträdelser var 3,62 miljoner US dollar. Denna kostnad kommer att öka de kommande åren på grund av myndighetsförordningar, såsom GDPR, den nya dataskyddsförordningen som innebär att företag straffas med kraftiga böter om de inte kan säkra sina system och data. För att undvika dessa försvagande straff måste företag kunna bevisa att de kan skydda data.
Detta kräver en helhetssyn av alla sårbara områden inom en verksamhet.

Något som ytterligare ökar företags utmaningar med cybersäkerhet är expansionen och digitaliseringen av den moderna arbetsplatsen samt att datavolymen ökar explosionsartat. Arbetsflöden sprids ofta över flera enheter, nätverk och geografiska platser. Information är som mest utsatt när den flyttas runt inom ett företag. Den måste skyddas för varje steg på sin resa. På grund av risken som detta medför kan moderna företag inte längre fungera utan att ha en grundläggande säkerhet för sina dokument- och datahanteringssystem. Samtidigt har kontorsskrivares och multifunktionsenheters funktioner utvecklats tiofalt de senaste åren. De är nu ansvariga för en mycket stor andel av företags indata, utdata, överföring och lagring. Detta gör dem till en av de farligaste, oftast förbisedda, hotfaktorerna på dagens arbetsplatser.

Många företag säger sig erbjuda säkerhetsmöjligheter men Ricoh har utvecklat säkra arbetsplatslösningar och -tjänster i många årtionden. Våra skrivare har till exempel haft säker överskrivningskapacitet för hårddiskar i över 20 år.

Säkerhet finns i vårt DNA och går som en röd tråd genom alla våra produkter och tjänster. Vi har fler än 4 miljoner kontorsprodukter ute på fältet idag. Varje produkt och varje tjänst som vi erbjuder tillsammans med dem har inbyggda säkerhetsmöjligheter. Vi använder även ett operativsystem som är unikt för Ricoh i många av våra produkter. Detta är en stor del av vårt säkerhetsförsvar som ger kontroll och skydd mot OS-specifika hot som vanliga operativsystem utsätts för.

Ricoh erbjuder en konsekvent världsomspännande tjänste- och supportstruktur för kunder och som ser till att hotinformation delas och hanteras på ett effektivt sätt. IEEE 2600-certifiering är implementerat som standard på alla våra utskriftsenheter. Dessutom är Ricoh en ledande medlem och huvudförfattare för IEEE Standards Association. Ricoh är även ISO 27001-certifierad och engagerad i att fortsätta följa detta hanteringssystem för informationssäkerhet. Vi fokuserar vår produktutveckling på kunders företagsbehov och säkerhetsproblem genom en serie av globala kunddrivna innovationsprogram.

För att möta kraven på effektiva och bevisligt beprövade rutiner för cybersäkerhet, inkluderas säkerhet som standard i alla produkter och tjänster i Ricohs portfölj – det är aldrig något som vi kommer på i efterhand. Vi tror att denna helhetssyn på sårbarhet är väsentlig för överlevnad i en modern företagsverksamhet.

SÄKERHETSUTMANING FÖR KUNDER

TRENDER: När datavolymer ökar, ökar även sårbarheter, attacker och böter.

Att säkra och ge kraft åt digitala arbetsplatser

Ricoh vill möjliggöra och säkra digitaliserat arbete oavsett var folk arbetar. I en modern digital ekonomi betyder detta att man lägger värde på en arbetsplats bortanför ett begränsande traditionellt kontor. Distanskontor och -anställda ökar företags flexibilitet och produktivitet varje dag. De hjälper företag att bättre kunna uppfylla kundförväntningar och tjänstekrav.

Att arbeta vid nätverkets gräns är dock en av de största riskerna för företagssäkerhet. Den data som dessa arbetare genererar och de fjärrenheter som de använder för att insamla denna data måste ha ordentlig säkerhet. Anställda arbetar ofta över flera nätverk och geografiska platser, vilket gör uppgiften ännu mer komplicerad. Något som är avgörande är att myndighetsförordningar såsom GDPR kräver att företag på ett bevisbart sätt kan säkra data genom hela livscykeln. Annars kan de få stränga böter. Allt eftersom arbetsplatser utvecklas och använder digitala arbetsflöden, blir livscykeln för företagsinformation gradvis mer komplicerad. Låt oss undersöka detta steg för steg.

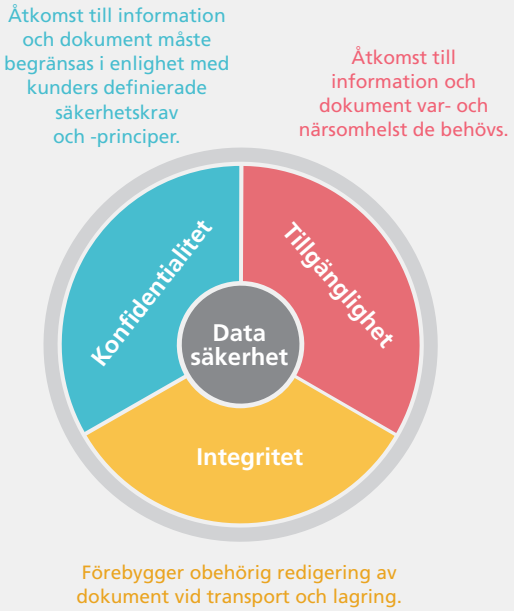
Det första steget är indata- och insamlingsenheter – en viktig komponent i Ricohs säkerhetsförsvar. Härifrån måste data transporteras över nätverk och lagras säkert. I detta steg är det avgörande att dataintegriteten bevaras. Ricohs system begränsar användaråtkomst till enheter och nätverksfunktionalitet för att säkerställa att data inte kan manipuleras när de skickas eller är lagrade på en enhet. Dessa tjänster inkluderar åtkomstkontroll, kryptering och kopieringsskydd. Vi kallar detta steg för Kontroll.

Efter lagring måste dokumenten dock vara lättåtkomliga för de inom företaget som behöver dem. Möjligheten att hämta information när den behövs och visualisera den på ett effektivt sätt beror på denna tillgänglighet. Dataanalys är en viktig komponent i en kraftfull digital arbetsplats. Den ger insyn på ett effektivt sätt för varje del av företaget, från försäljning till HR. Verktyg för behörighetsinfrastruktur ger en snabb och säker åtkomst oavsett var användaren befinner sig eller vilken enhet som används. Det är viktigt att säkerhetsprotokoll inte hindrar innovation och funktionalitet eller riskerar att anställda kämpar emot. Vi kallar detta steg för Bevarande.

Slutligen måste data avyttras på ett säkert och spårbart sätt. Detta steg är väsentligt för överensstämmelse med föreskriftskrav och minimerar risken för datastöld eller förlust. Denna process sker faktiskt löpande genom hela dokumentets livscykel samt vid slutlig radering. Utskrift av filer lämnar dolda bilder på hårddisken på en multifunktionsskrivare (MFP), som måste skrivas över för att förebygga obehörig åtkomst. Ricohs dataavyttringstjänst inkluderar funktioner som rensning av hårddisk, minnesrensning, radering av ej utskrivna filer och radering vid utloggning för att förhindra att hackare sammanställer känslig information från de spår som ett dokument lämnar efter sig. Vi kallar detta steg för Destruktion.

För att effektivt säkra data genom denna livscykel använder sig Ricoh av en så kallad ”CIA”-princip för sekretess och säkerhet: Confidentiality, Availability och Integrity (konfidentialitet, tillgänglighet och integritet). Dessa principer vägleder oss vid utformning av produkter och lösningar för att vi ska uppfylla väsentliga standarder och förordningar. Denna metod möjliggör arbetsplatsinnovation och tillväxt samtidigt som vi bibehåller effektiva och säkra processer.

RICOHS INSTÄLLNING TILL SÄKERHET



Vi bygger runt ”CIA”-principer för sekretess och säkerhet: confidentiality, integrity och availability (konfidentialitet, integritet och tillgänglighet)

Säkerhet ligger i vårt DNA. Varje produkt som byggs och tjänst som tillhandahålls av Ricoh innehåller inbyggda säkerhetsfunktioner och möjligheter

Ricoh erbjuder en komplett uppsättning säkerhetsprodukter och -tjänster för att säkra dokumentskapande från början till slut.

Vi kommer nu förklara varje avgörande steg var för sig: kontroll, bevarande, destruktion och support.

FYRA STEG FÖR DIGITAL ARBETSPLATSSÄKERHET

1 KONTROLL

Effektiv datakontroll är avgörande för att bibehålla datakonfidentialitet och -integritet. Företagsinformation är en primär tillgång som behöver skyddas. Dagens maskinvaruenheter är informationsterminaler som kan vara sårbara portar för företagsinformation. På grund av detta använder Ricoh flera verktyg för användarautentisering och enhetshantering för att kontrollera och säkra företagsdata. Dessa avser inställningarna på fysiska enheter som tillåter och begränsar åtkomst till vissa funktioner och data. Att begränsa anställdas åtkomst till den information som skickas till och från företagets MFP:er är en avgörande beprövad metod för att bevara dokumentsäkerheten. Kontrollfasen inkluderar även enhetsskydd mot skadlig kod genom Ricohs metod för inbyggd programvara i tre nivåer.

Kontroll för obehörig kopiering

Ricoh erbjuder en lösning som säkerställer att obehörig duplicering av utskrivna dokument inte kan utföras. Kopieringsskyddsfunktionen skriver ut eller kopierar dokument med speciella osynliga mönster som ligger inbäddade i bakgrunden. Om det utskrivna eller kopierade dokumentet kopieras och/eller skannas kommer ett inbäddat mönster att synas på kopiorna. Skyddsmodulen för obehörig kopiering gör det möjligt för MFP:n att upptäcka det inbäddade mönstret och byta ut den kopierade bilden mot en grå bild för att förebygga att information läcks. Denna funktion är användbar vid utskrift av konfidentiell information. Begränsning av duplicering av konfidentiell information förebygger informationsläckor av detta slag.

Säker utskrift

Ett dokument som tas emot från en PC kan lagras på hårddisken i MFP:n. Med Ricohs funktion för säkra utskrifter anges ett lösenord när en användare skickar dokumentet och lösenordet måste sedan anges på MFP:n innan det kan skrivas ut. Eftersom dokumentet inte kan skrivas ut förrän ägaren är vid enheten säkerställer funktionen för säker utskrift att dokumentet hamnar hos rätt ägare.

Avancerad insamlingssäkerhet

Ricohs portfölj med avancerade insamlingslösningar erbjuder varierande skikt med kryptering och dekryptering genom alla behandlingsnivåer i insamlingsprocessens samtliga steg. Administratörer kan tillåta åtkomst för att behandla köer med individuell användarinloggning eller med gruppinloggning. Ytterligare säkerhetsnivåer inkluderar SAML (Security Assertion Markup Language) för ett ramverk med SSO (Single Sign On), PIV (Personal Identity Verification) och kryptering med PKI (Public Key Infrastructure).

Inbäddade autentiseringskontroller

Enhetsåtkomst och identitetsautentiseringsprotokoll för alla Ricoh-produkter kan hanteras centralt. Tillgängliga metoder inkluderar ID-kort, pinkod, nätverksinloggning eller en kombination av dessa metoder. En kombinerad autentisering förbättrar säkerheten men kan sakta ner användare som har mycket att göra. SSO (Single Sign On) underlättar detta genom att tillåta användare att komma åt många enheter sömlöst. Dessutom är Ricohs snabbautentisering, ett autentiseringsprogram baserat på swipe-and-go, förinstallerat på våra enheter, vilket ger användare ett enkelt sätt att komma åt sina dokument. Användning av en NFC-läsare/skrivare gör användarens inloggningsprocess mycket enklare samtidigt som åtkomsten till MFP:n säkras och kontrolleras. Denna form av åtkomst fungerar även tillsammans med befintliga behörighetsinställningar i MFP:n för att begränsa användaråtkomst till enhetsfunktioner som fastställts av kunden.

SLNX (Streamline NX)

Enhetshanterarmodulen inom Ricohs Streamline NX-plattform är Ricohs programvara för hantering och övervakning av enheter inom ett nätverk. Programmet gör det möjligt för administratörer att se eller konfigurera säkerhetsinställningar för enheter med hjälp av befintliga mallar och anpassade parametrar. Avgörande säkerhetsinställningar inkluderar aktiverings/inaktiveringsprotokoll, IP-adressinställningar, lösenord för administratörer, e-postadresser för aviseringar, krypteringsinställningar med mera. SLNX kan också rapportera skrivare som inte uppfyller de principer som kunden har beslutat om.

Enhetsskydd för skadlig kod

Ricoh använder en metod med tre nivåer som skydd mot skadlig kod på sina enheter. För det första fungerar Ricoh-enheter endast med Ricoh-maskinspråk eller operativsystem. För det andra, för att kunna förebygga skadlig manipulering av enhetens programvara, måste uppdateringar av inbyggd programvara skrivas och godkännas på Ricohs maskinspråk. För det tredje måste slutligen alla uppdateringar för inbyggd programvara skrivas under digitalt av Ricoh. Om denna trestegsmetod används kan inbyggd programvara som inte godkänts inte laddas upp på Ricohs enheter, vilket gör att skadlig kod, spionprogram och virus elimineras på ett effektivt sätt.

Säkerhet för fysiska dokument

Beprövade säkerhetsrutiner är inte alltid komplicerade. Ett kontor är en plats med många olika aktiviteter och dokumentutskrifter är en signifikant företagsrisk både vad gäller informationsstöld och vårdslöshet av anställda. Ricoh har ytterligare ett antal fysiska säkerhetsalternativ för att förebygga obehörig åtkomst av utskrivna dokument. Till exempel kan låsta lådor förebygga stöld av känsliga papper t.ex. receptblanketter inom sjukvården. Genom att montera täckplåtar för alla kablar förebygger man också möjligheten till manipulation från interna hot. En säker lösning för dokumentutgivning (Print-to-me) säkerställer att dokument endast skrivs ut när ägaren är närvarande, vilket eliminerar risken att utskrivna dokument inte hämtas från skrivaren.

2 BEVARANDE

Enligt nya och befintliga föreskriftskrav måste företag säkerställa både konfidentialitet av information, så att den inte kan stjälas eller läckas, och fortlöpande informationsintegritet, så att den inte kan ändras. För att uppnå detta måste företag begränsa åtkomsten till känsliga dokument. Detta förebygger obehörig ändring och förfalskning. Det fungerar även som skydd från planerade eller opportunistiska hot inom företaget.

Mobilt arbete är ytterligare en försvårande omständighet för alla olika cyberhotsscenarion. Ytterligare säkerhetsåtgärder måste finnas för att kunna hantera fildelning från vilken plats som helst. Dessa filer måste vara lika säkra när de skickas över nätverk och mellan enheter som de är vid lagring. Stark krypteringsteknik kan effektivt följa och skydda data genom hela dess livscykel. Detta gäller naturligtvis för dokument men även för avgörande säkerhetselement såsom sparade lösenord, makroinställningar och adressböcker. Även om hackare kan komma åt ditt nätverk måste de kämpa med krypteringen för att kunna extrahera användbar information, vilket bevarar dess integritet i händelse av ett intrång.

Kontinuerlig drift är viktigt för många industrier. Oförutsägbara händelser som t.ex. naturkatastrofer kan därför vara ett direkt hot mot verksamheten. Pappersdokument är särskilt sårbara i ett sådant scenario. Genom att spara digitaliserade dokument på ett moln skyddas de mot naturkatastrofer och andra olyckor. Lämpliga säkerhetssteg måste dock vidtas för att kunna bevara dessa digitala data.

Väsentlig datakryptering

Kryptering skyddar information när den skickas mellan enheter och kan aktiveras för data som skickas till eller som finns sparad på en Ricoh MFP-hårddisk. Inbyggda programalternativ ger kryptering från slutpunkt till slutpunkt för skannade och utskrivna filer via användarens PKI-nyckel (public key infrastructure). Detta skyddar mot MITM-angrepp (man-in-the-middle) i kundens IT-miljö.

För ytterligare säkerhet skrivs data över kontinuerligt av Ricohs DOSS (Data Overwrite Security System), som vi kommer att presentera närmare i stycket om destruktionsfasen.

Skydd för bios och operativsystem

Ricohs MFP:er använder en TPM (Trusted Platform Module), som är en manipuleringssäker säkerhetsmodul för maskinvara. TPM utför kryptografiska funktioner och lagrar kryptografisk data på ett säkert sätt. Ricoh använder TPM till att lagra den rotkrypteringsnyckel som skyddar hårddiskens krypteringsnyckel och MFP:ns digitala certifikat. Den tillåter också administratörer att utföra en betrodd omstart, vilket validerar autenticiteten för MFP:ns inbyggda programvara innan den får tillstånd att köra.

Validering av inbyggd programvara

Rotnyckeln och kryptografiska funktioner finns alltid inbyggda i TPM:en och kan inte ändras utanför brandväggen, vilket förebygger felaktig användning eller skadlig manipulering av våra produkter. Denna process ger en hög valideringsnivå av MFP:ns inbyggda programvara, enhetsidentitet och hårddisksäkerhet. Detta är ännu ett bra exempel på hur Ricohs MFP:er är utformade med Ricohs kunders säkerhetsintresse som högsta prioritet.

Lösenordshantering

Ricohs enheter kan konfigureras med flera administratörer där var och en har olika roller på enheterna och med distinkta lösenord. Lösenorden för dessa användare kan fjärrkonfigureras via webbaserade administratörsverktyg och verifieras regelbundet. Detta möjliggör ”segregering av uppgifter”, något som är ett krav i många företags policyer.

Begränsad användaråtkomst

Ricohs användarhanteringsverktyg gör det möjligt för systemadministratörer att begränsa behörigheten för användaråtkomst. Till exempel kan administratören skapa behörigheter som ger valda användare åtkomst till en MFP:s registrerade adressbok. Detta blockerar obehöriga att komma åt personlig information och arkiv som lagras på kontorets enheter.

Funktion för utelåsning av användare

När fel lösenord anges flera gånger under en inloggningsprocess kan Ricohs MFP:er utvärdera om någon försöker knäcka lösenordet. Detta triggar låsfunktionen som blockerar användarnamnet i fråga. Det blockerade användarnamnet kan inte autentiseras även om det till slut kombineras med korrekt lösenord. Låset kan bara öppnas efter en viss tid eller av en administratör, vilket effektivt hindrar förmodade hackare.

3 DESTRUKTION

Säker dataavyttring är en väsentlig del av ett omfattande cybersäkerhetsförsvar. Det är lätt att missta sig och tro att företagets ansvar slutar när data lämnar organisationen. Många förordningar stipulerar dock att dataavyttring måste vara en omfattande process som eliminerar alla risker för stöld eller felaktig användning. Tills detta kan bevisas är ett företags ansvar inte över.

Kontorsenheter som avyttras vid utgånget kontrakt kan ofta vara en risk för företagsinformation som man inte tänker på. Ricoh erbjuder en certifierad och spårbar tjänst för borttagning av data från de skrivare vars kontrakt går ut. Detta inkluderar förbisett material såsom sparade nätverksinställningar, användardata, hårddiskdata eller även etiketter på enheten. Om denna rensning inte utförs kan företaget riskera att exponera konfidentiell information om både företaget och de anställda. Men för att kunna upprätthålla överensstämmelse med gällande föreskrifter måste denna process även ske löpande under en enhets livscykel. Detta säkerställer att företag har maximal kontroll över den data som de är ansvariga för.

Skriva över bild: DOSS (Data Overwrite Security System)

MFP-hårddiskar fungerar effektivt i och med att de sparar dolda bilder av dokumentdata i sitt minne för jobbehandling. Ricohs DOSS-lösning säkerställer att dessa bilder alltid skrivs över innan nästa jobb startar. På detta sätt kan de dataspår som lämnas kvar efter tidigare jobb inte kommas åt om någon med ont uppsåt skulle få åtkomst till hårddisken. På Ricoh är vi stolta över att ha erbjudit denna beprövade säkerhetsmetod i över 20 år.

Rensningstjänst vid utgånget kontrakt

Ricoh erbjuder en tjänst för fullständig datarensning, Ricoh Data Cleansing Service, en tjänst för MFP:er och skrivare vars kontrakt går ut, där minnesmoduler och lagringsutrymmen i enheterna raderas bortom återhämtning med branschcertifierade säkerhetslösningar. Ricohs IT-tjänster erbjuder även en omfattande avyttringstjänst för utrustning och som inkluderar flera steg av certifierade datarensningstjänster.

Utbyte av hårddisk och flyttbar lagring

Ricoh erbjuder också en avyttringstjänst för hårddiskar som låter kunder behålla sin hårddisk och istället ersätter den mot en ny tom hårddisk när de lämnar tillbaka utrustningen när kontraktet går ut. Detta garanterar företag en fullständig och spårbar kontroll av sin datamiljö.

4 SUPPORT

Allteftersom ett företag växer, ökar oundvikligen även antalet anslutningar mellan enheter och nätverk. Företag måste ha strategier som säkerställer att denna infrastrukturtillväxt inte leder till en säkerhetsrisk. De måste vara medvetna om svagheter i sitt system och vidta åtgärder för att förebygga planerade och opportunistiska attacker.

Specialiserad IT-säkerhet krävs ofta för att analysera ett företags infrastruktur och identifiera dessa sårbarheter. För många företag är det svårt att ha en egen IT-avdelning som besitter den kunskap som behövs för att hantera sina cybersäkerhetsmiljöer. Det är helt enkelt för dyrt och ineffektivt, vilket ofta tvingar dessa företag att vara farligt overksamma.

Ricohs IT-supporttjänst erbjuder tjänster för IT-upphandling och konfigurering samt fjärrövervakning, support och överföra hanteringsmöjligheter för att ytterligare ge stöd åt cybersäkerhetsprocessen. Cybersäkerhet är beroende av att ha en samlad förståelse för företagsrisker. Ricohs SIRT (Security Incident Response Team) säkerställer att information om viktiga hot delas med kunder över hela världen, vilket gör att effektiva åtgärder kan koordineras omedelbart.

Säkerhetsutvärdering av infrastruktur

Funktionen i Ricohs SLNX (Streamline NX) enhetshanterare är utformad att utföra en ovärderlig granskningsfunktion för säkerhetsprinciper. SLNX tillhandahåller en funktion som IT-ansvariga kan aktivera för att ställa in enheter baserat på ett företags principer, distribuera dessa inställningar och analysera dem med en visualiserad rapport. SLNX kan också avisera ledningen när en enhet inte följer företagets principer.

Optimering av utskriftssäkerhet

Ricoh erbjuder en omfattande PSO-tjänst (Print Security Optimisation) tillsammans med professionella och hanterade konsulttjänster för att identifiera enhetsrelaterade säkerhetsluckor. Detta är ett webbaserat verktyg med en grafisk guide som visar det aktuella tillståndet och gör det möjligt för Ricoh att erbjuda produktrekommendationer som kan reducera riskerna.

PSIRT (Product Security Incident Response Team)

Ricohs aktiva svar på nya hot och hur effektiva motåtgärder kan utvecklas, hanteras av Ricohs PSIRT (Product Security Incident Response Team). Detta är ett program som Ricoh använder för att säkerställa att hela produktutbudet (maskinvara och programvara) uppdateras kontinuerligt och skyddas mot nya identifierade hot och sårbarheter. Detta hjälper oss att bibehålla en konsekvent hög servicenivå globalt sett och minimerar den inverkan som sårbarhetsproblem har på Ricoh-produkter.

Stöddokument

Förberedelse och utbildning är avgörande element i alla cybersäkerhetsstrukturer. Dokumentation om säkerhetskopior, användarhandböcker, säkerhetsdokument och utbildning ska levereras till kunden. Som med många andra delar av cybersäkerhetsmiljön är en spårbar överensstämmelse av avgörande betydelse och denna dokumentation är en central del i att säkra ett företags intäkter.

HUR KAN RICOH HJÄLPA TILL?

Ricohs unika position att leverera branschledande säkerhetslösningar över hela IT- och utskriftsmiljön baseras delvis på bibehållandet av en stark förståelse för hur marknadsvillkor förändras och att kunna utveckla vår riktning i enlighet med det. Våra lösningar är utformade att skydda all information genom hela livscykeln och fokuserar på de fyra områden inom datasäkerhet som presenteras i denna rapport.

Vi har dedikerade ämnesexperter som är ansvariga för att analysera marknadsbehov, vilket inkluderar industrispecifika behov för vilka nya lösningar som kan utvecklas eller befintliga lösningar som kan anpassas.

Vi är även engagerade i att utveckla vår interna kapacitet att utveckla och lansera centrala säkerhetslösningar. För att uppnå detta har vi skapat dedikerade team inom vår tjänsteutvecklingsorganisation som fokuserar på att utveckla nya tjänster för styrning, riskhantering, överensstämmelse och cybersäkerhet.

Autentisering av och behörighet för användare

- Säker utskrift
- Inbäddad programvara för autentisering som standard
- Användarautentisering/begränsning av åtkomst
- En inloggning
- Flera administratörsroller
- Lösenordsskydd för PDF (lösenord för skannade dokument)
- Skydd mot obehörig kopiering
- IP-områdesbaserad åtkomstkontroll
- Säker enhets- och utskriftshantering
- PKI (Public Key Infrastructure)/SmartCard-support
- Säker utskriftshantering (print2me/säker utskrift)

Enhetsskydd för skadlig kod

- Servrar
- Inte alls eller mindre mottaglig för skadlig kod
- SOP – assimilerad version av Android
- Ricoh-version av maskin-OS (maskinkontrollspråk) för MFP
- Metod med 3 nivåer – digital signatur, ladda ner via Ricoh-verktyg, måste skrivas på specifikt kontrollspråk

Avyttring av hårddisk

- Avyttring av hårddisk, överskrivning av bild
- Fullständig datarensningstjänst
- Tjänst vid utgånget kontrakt: destruktion av data på minnesmoduler, lagring

Enhetshantering

- Inställning av kvot/kontogräns
- DMNX – säkerhetsgranskning med enkel glasruta, lösenordshantering, övervakning, avisering

Skydd för bios och operativsystem

- Säker omstart med TPM (Trusted Platform Module)

Överskrivning av bild och flyttbar lagringsmedia

- DOSS (Disk Overwrite Security System)
- Flyttbar hårddisk

Datakryptering

- Hårddiskkryptering via TPM
- Krypteringsnycklar via TPM
- Slutpunkt till slutpunkt-kryptering för utskrivna och skannade filer som använder PKI-nyckel
- FIPS-certifierad HDD (Federal Information Processing Standards)
- Slutpunkt till slutpunkt-kryptering för utskrift
- Slutpunkt till slutpunkt-kryptering för skanning

Uppdatering av inbyggd programvara och lösenordshantering

- Fjärrgranskning av lösenord
- Funktion för att blockera användare
- Validering av inbyggd programvara via TPM

Överensstämmelse med branschstandarder

- ISO 27001-certifiering
- IEEE 2600.2-certifiering för valda produkter
- ISO 15408-certifiering för valda produkter
- Säkerhetsdokumentation och utbildning

RICOHS NIVÅINDELADE METOD FÖR ENHETSSÄKERHET

Det råder inget tvivel om att MFP-leverantörens roll har utvecklats långt bortom det transaktionsbaserade, endimensionella tillhandahållandet av maskinvara till faktisk datahantering. MFP:ers funktioner inkluderar nu allt från insamling av information från många kanaler till klassificering av insamlad data och arbetsflödesintegrering samt säker lagring och analys. I detta komplexa nät av stränga regler med många föreskrifter och kvarhållningskrav – tillsammans med interna och externa hot som utsätter arkiv för risk för förlust, förstörelse eller manipulering – använder vi en nivåindelad metod för enhetssäkerhet för att kunna säkerställa att din MFP och systemet det ansluter till ger dig det bästa möjliga skyddet.

1. Enheten

Enheten är den centrala delen i Ricohs alla modeller. Den är utformad, tillverkad och implementerad med säkerhet som grundläggande krav. Ricohs egna operativsystem är inte lika sårbara som många vanliga kommersiella operativsystem och våra enheter är certifierade enligt standarden IEEE2600.2. Hårddiskkryptering och disköverskrivningssäkerhet säkerställer att all data som behandlas fortsätter att vara konfidentiell.

2. Den smarta användarpanelen SOP (Smart Operation Panel) tillhandahåller användargränssnittet

På liknande sätt som MFP:erna använder SOP Ricohs egna operativsystem. Inga onödiga komponenter installeras och det finns ingen rotåtkomst. Ricoh har jobbat hårt med att säkerställa att enhetssäkerhet inte försvagas av introduktionen av SOP.

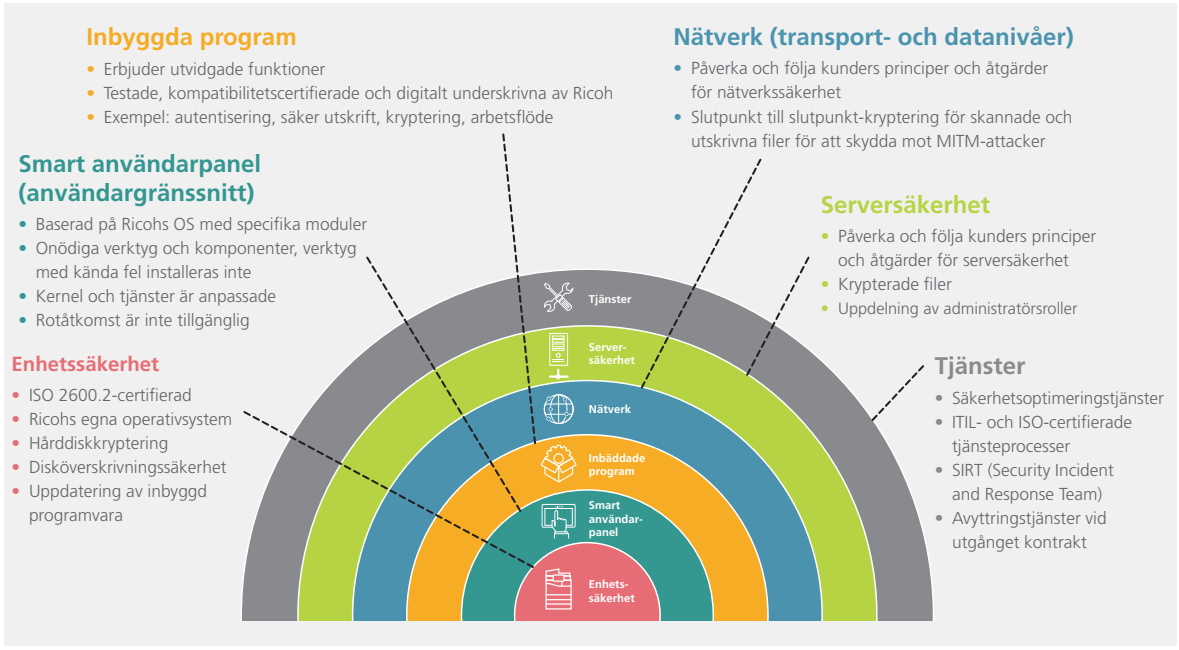
3. Smarta program

Dessa kan vara inbäddade i SOP och tillhandahåller ytterligare funktionalitet för användaren, vilket inkluderar arbetsflöde och datainsamling. Vissa program har väsentliga säkerhetsfunktioner. Dessa inkluderar säker utskriftskapacitet, kortåtkomst och kryptering. Program utvecklas av Ricoh eller Ricoh Developer Programme-medlemmar. Alla program måste genomgå Ricohs kompatibilitetstestning och måste signeras digitalt innan de kan köras på SOP:en.

4. Nätverk och servrar

Oavsett vem det är som hanterar IT-infrastrukturen säkerställer Ricoh att våra produkter och tjänster uppfyller dina säkerhetsprinciper för IT och nätverk. Slutpunkt till slutpunkt-kryptering för utskrivna och skannade filer, kryptering av data på servrar och uppdelning av administratörsuppgifter är tekniker som används för att skydda mot MITM-attacker eller insiderjobb.

Ett omfattande utbud av säkerhetstjänster täcker allt vi erbjuder. Detta inkluderar konsult- och förvaltningstjänster för att assistera kunder att övervaka, optimera och hantera sin dokument- och informationssäkerhet. Vi har även ett utbud av tjänster för avyttring av enheter som säkerställer att RAM och HDD av gamla kundenheter rensas innan de avyttras.



HUR RICOH SKYDDAR DEN DIGITALA ARBETSPLATSEN

Våra kunder har ett antal huvudsakliga säkerhetsfrågor som styrker företags uppfattning om att när datavolymer ökar, ökar även sårbarheter, attacker och lagstadgade böter. Det krävs mycket jobb att hålla data konfidentiell, säker och fri från manipulering. Till exempel avvisar vi på Ricoh runt 8 miljarder brandväggsattacker per månad. Det finns tiotusentals dataförordningar (globala, nationella och branschspecifika) och företag måste kunna bevisa kontinuerlig överensstämmelse med var och en av dem. Naturligtvis letar organisationer av alla storlekar efter en partner som de kan lita på – en partner som kan hjälpa dem att vara säkra och med en portfölj som täcker hela den digitala arbetsplatsen.

Ricoh har utvecklat ett brett utbud av lösningar för att mildra alla de olika risker som företag utsätts för. Informationssäkerhetshot utvecklas otroligt snabbt och Ricoh använder sig av ”kundens röst”-program för att ytterligare kunna utveckla och leverera våra tjänster.

Våra kundrådgivande paneler fungerar som främsta strategiska fokusgrupper. Vi använder dessa för att få en bättre förståelse för trender, drivande faktorer och prioriteringar som formar våra kunders företag. Våra tekniska rådgivande konferenser ger viktig information från centrala beslutsfattare. Ricohs tekniska och F&U-grupper använder dessa konferenser till att få ovärderlig kundfeedback för idéer, koncept och prototyper. Slutligen samarbetar Ricoh med enskilda kunder för att utveckla nya och avancerade säkerhetsfunktioner för kunder på den vertikala och generella marknaden. Denna kunddrivande metod hjälper oss att validera vår produktplan och hjälper våra kunder att dra fördel av ett globalt nätverk av tjänster och support.

Den moderna digitala arbetsplatsen måste vara lika dynamisk som cyberhoten och lika flexibel som arbetsmetoderna inom den. Det är därför vi anser att cybersäkerhet ska fungera sömlöst med den teknik som våra kunder väljer för sin arbetsplats. Oavsett hur du väljer att strukturera och utveckla ditt företag använder vi oss av beprövade rutiner för säkerhetskontroller. Detta garanteras av vårt åtagande av ISO 27001 som genomsyrar hela vår organisation och IEEE 2600-certifieringen för våra produkter, tillsammans med Ricohs egna operativsystem som finns i dem.

En kombination av säkerhetshot, lagstadgade krav och komplexa branschstandarder betyder att risken för skadat rykte och ekonomiska förluster på grund av cyberrisker är större än någonsin. Nu är det hög tid att arbeta med en betrodd partner som kan hjälpa dig att säkra ditt företags mest sårbara tillgångar och skydda dina framtida ambitioner.

RICOH
imagine. change.

www.ricoh.se

Fakta och siffror i denna broschyr relaterar till specifika företagsfall. Individuella omständigheter kan ge olika resultat. Alla företags-, märkes-, produkt- och tjänstenamn är registrerade varumärken tillhörande sina respektive ägare. Med ensamrätt © 2017 Ricoh Europe PLC. Med ensamrätt Denna broschyr, dess innehåll och/eller layout får inte modifieras och/eller anpassas, kopieras i del eller i helhet och/eller inkluderas i annat arbete utan skriftlig tillåtelse från Ricoh Europe PLC.