«White paper» om informasjonssikkerhet

Dokumentdatasikkehet

Beskyttelse av utskrevne og elektroniske data

www.sharp.no

SHARP

Be Original.

Innhold

Innledning

Behovet for å beskytte dokumenter som leveres fysisk eller elektronisk fra (multifunksjons)skrivere, er en informasjonssikkerhetsfaktor som ofte overses.

Sharp definerer dokumentdatasikkerhet som sikkerheten knyttet til utskrifter og elektroniske dokumentdata fra multifunksjonsskrivere (MFP-er) eller vanlige skrivere. Denne kategorien omfatter alle utskrevne dokumenter og elektroniske bilder av informasjon i transitt fra en datamaskin til en utskriftsenhet (herunder utskrifter gjennom egne utskriftsservere), skanning (innbefattet skanning til mapper, e-poster, skyen eller HDD) og faks.

De viktigste punktene vi tar for oss i dette «white paper» er:

- **Bakgrunnen**
  Vi går her inn på hvorfor styring av dokumentdata er en informasjonssikkerhetsfaktor som ofte overses. I tillegg fremhever vi potensielle svakheter som IT-administratorene må være oppmerksomme på, deriblant:

  - Det økende antallet organisasjoner som konsoliderer (multifunksjons)skriverparkene sine
  - Det økende antallet tilkoblede brukere som må identifiseres og administreres
  - Det økende antallet dokumenter som produseres og må kontrolleres
  - Mangelen på verktøy til å spore og rapportere all dokumentdata-aktivitet

- **Problemet**
  Vi ser på hvilke utfordringer IT-ansvarlige, sluttbrukere og ledere i bedriftsorganisasjoner kan møte i forbindelse med styring av dokumentdata. Eksempler på slike utfordringer er administrering av brukertilgangen til utskrevne dokumenter, sporing av brukeraktivitet, rapportering av aktivitet, utskriftstilgang fra mobile enheter, skanning til flere destinasjoner, samt faksing av dokumenter utenfor organisasjonen.

  I tillegg går vi inn på forskningsdata som viser kompleksiteten i emnet og omfanget av problemet.

- **Løsningen**
  Vi presenterer her ulike Sharp-produkter (programvareløsninger) samt beste praksis som kan hjelpe deg til å skape et sikkert dokumentdata-miljø og hindre uautorisert tilgang til (multifunksjons)skriverparken, samt dokumentene (innbefattet elektroniske dokumentbilder), kopiene, faksene, skanningene og utskriftene som produseres med og lagres på disse skriverne.

  I tillegg ser vi nærmere på hvordan Sharp kan løse disse problemene ved å hjelpe deg å:

  - Velge en løsning som innfrir dine krav og støtter opp under retningslinjene dine for utskriftssikkerhet. Et system for styring av dokumentdata kan kontrollere tilgang, håndheve utskriftsregler, begrense funksjoner og sikre nøyaktig sporing og rapportering av alle dokumentdata.
  - Velge riktig løsningsleverandør for styring av dokumentdata og relaterte dokumentdata-aktiviteter.

- **Konklusjon**
  Vi gir her en oppsummering med fokus på følgende:

  - De primære sårbarhetene knyttet til alle typer dokumentdata
  - En oppsummering av anbefalingene basert på Sharps sikkerhetsløsninger
  - De neste trinnene som kreves for å få på plass konsekvente retningslinjer for utskriftssikkerhet (innbefattet pålitelige verktøy) som kan brukes på alle aspekter ved virksomheten.

Bakgrunn

Når bedriftene lager lister over potensielle risikoer knyttet til informasjonssikkerhet, tenker de sjelden eller aldri på nettverkstilkoblede (multifunksjons)skrivere – for ikke å snakke om dokumentutskrifter – som noe problem.

Ifølge analyseinstituttet Quocirca, har 60 % av organisasjonene opplevd minst ett brudd på persondatasikkerheten som følge av utrygge utskriftsrutiner, og både små og store bedrifter kan bli rammet[1]. Selv om du implementerer sikkerhetsløsninger for å beskytte dataene dine mot hackere eller cyberkriminelle som bruker avansert teknologi, er det ikke alltid tilstrekkelig.

Noen av de vanligste sikkerhetsbruddene er så enkle som at en dokumentutskrift plukkes opp av feil person. Hvis sensitive dokumenter blir liggende for lenge i en (multifunksjons)skriver, kan hvem som helst få tak i og bruke dem til sin fordel. Dette kan skape alvorlige problemer.

56 % av bedriftene tar ikke med skriverne i sin strategi for endepunktsikkerhet.[2]

Sett fra tyvens ståsted er utskuffen det helt klart enkleste stedet å stjele konfidensiell informasjon fra. En ofte undervurdert utfordring for IT-administratorene er derfor å sørge for at dokumentutskrifter ikke blir liggende igjen oppå en usikret (multifunksjons)skriver og dermed kan havne i feil hender.

Utfordringene som alle moderne organisasjoner står overfor når det gjelder dokumentdata-sikkerhet, vokser imidlertid for hver dag som går. Dette har flere årsaker:

1. **Stadig større enhetsparker**
   Stadig flere organisasjoner konsoliderer (multifunksjons)skriverparkene sine, og bedriftene ønsker samkjøring og standardisering. Dette skaper flere utfordringer på grunn av mangelen på verktøy til å styre (multifunksjons)skriverne med:

   - Funksjonalitet
   - Dokumentdata
   - Sikkerhet (som del av nettverket)

2. **Antall (nettverks)tilkoblede brukere**
   I organisasjoner med mange medarbeidere kan det være hundrevis av brukere som skriver ut fra 10 til mer enn 100 enheter. Kombinert med det økende antallet sikkerhetsforskrifter (deriblant GDPR), kan det by på betydelige utfordringer med hensyn til følgende:

   - Brukerautentisering
   - Administrering av brukerkontoer (innbefattet kontroller av antall tilkoblede bruker)
   - Integrering av brukere i eksisterende kontorsystemer
   - Begrensninger i hvordan organisasjonene kan administrere brukeridentifiserbare data i systemene sine (f.eks. brukerredigering iht. personvernforordningen)

3. **Antall dokumentutskrifter som må kontrolleres**
   Med stadig flere brukere og en fortløpende økning i gjennomsnittlig antall utskrevne sider per bruker, er det en enorm mengde dokumentutskrifter å kontrollere.

   - Kopierte dokumenter
   - Utskrevne dokumenter

- Skannede dokumenter
- Faksede dokumenter
- Dokumenter som er skrevet ut via smarttelefon og nettbrett (mobilutskrifter / bruk av egen enhet (BYOD)).

4. **Mangel på kontrollverktøy**
   Det skorter generelt på verktøy som kan gi nøyaktig sporing og rapportering av alle dokumentdata.

Problem

Alle moderne bedrifter som bruker (multifunksjons)skrivere, bør ha dokumentdata-sikkerhet som ett av sine viktigste fokuspunkter.

Tilby riktig verktøy

Forskningsanalytikere fremhever behovet for å implementere egnede verktøy og tiltak for å håndtere utfordringen knyttet til at flere brukere skriver ut flere filer på flere utskriftsenheter.

Sikre dokumentdata-tilgang

En utfordring som alle IT-administratorer møter, er hvordan man skal håndtere de mange kontoene og brukerne som er registrert i bedriftsnettverket. Antallet brukere påvirker naturlig nok den administrative arbeidsbelastningen. I tillegg kompliserer det administreringen av brukerne samt de dokumentdata-relaterte brukeraktivitetene som f.eks. kopiering, utskrifter, skanning og faksing. Utfordringen ligger her i å håndtere sikkerheten av dokumentdata på en effektiv måte.

Bruk av PIN-koder, pålogging, passord, kort og nøkkelbrikker er her populære og effektive måter å sikre dokumentdataene på. Hvis disse metodene er dårlig implementert og administrert, kan de imidlertid fort bli et mareritt for IT-administratorene. Særlig ettersom mange IT-administratorer også prøver å koble enheter og dokumentdata til eksisterende systemer som f.eks. Microsoft-kontoer.

Antall dokumenter og utskrifter som blir liggende uten tilsyn

Det økende antallet utskrifter er en formidabel utfordring. Man må her ta med i beregningen både tradisjonelle papirdokumenter som skrives ut eller kopieres på enhetene, samt elektroniske dokumenter som sendes til (multifunksjons)skriverne enten via bedriftsnettverket eller skanne- og faksfunksjonene.

Med innføringen av nye forskrifter som for eksempel personvernforordningen (GDPR), har det dukket opp en rekke spørsmål om hvordan man skal beskytte ubevoktede utskrifter og hvor trygt den personlige informasjonen i kommunikasjonskanalene ovenfor faktisk oppbevares.

Forstå risikoene

For å kunne tilby effektiv beskyttelse må man forstå fullt ut hvilke risikoer de ulike aktivitetene medfører:

- **Kopiering**
  Kopiering var den mest populære måten å dele dokumenter på på 1980- og 1990-tallet, men i dag er det mer vanlig å ta utskrift. Like fullt er kopiering fortsatt et viktig område å kontrollere gjennom systemer for styring av dokumentdata, særlig med hensyn til sensitive forretningsdokumenter.

- **Utskrift**
  Utskrifter er i dag en svært vanlig måte å distribuere forretningsdokumenter på, men risikoene er mange når det skrives ut uten kontroller eller sentral styring. Eksempler på slike risikoer er:

  - Usikret og ikke-kontrollert tilgang til multifunksjonsskrivere/skrivere og enhetsfunksjoner (f.eks. harddisker)
  - Utskrevne dokumenter som ligger åpent tilgjengelige for alle kontorbrukere/medarbeidere (og kanskje også besøkende)
  - Manglende mulighet til å spore og rapportere brukeraktiviteter (f.eks. hvem som har skrevet ut hva i et bestemt tidsrom)
  - Manglende mulighet til å spore og forebygge brudd på persondatasikkerheten, noe som kan føre til store bøter eller straffer på grunn av strenge sikkerhetsforskrifter (deriblant personvernforordningen)
  - Manglende mulighet til å spore mobilbrukere og utskrifter fra mobilenheter som f.eks. smarttelefoner og nettbrett

- **Skanning**
  Skanning kan by på vanskeligheter for sikkerhetsprosessen, ettersom dokumenter ikke bare kan skannes til nettverksmapper og e-poster, men også til eksterne, skybaserte systemer. I tillegg kommer følgende risikoer:

  - Skanning av sensitive forretningsdokumenter til eksterne destinasjoner (f.eks. skanning til personlige e-postadresser i stedet for bedriftsadresser)
  - Skanning til flere mapper i stedet for til valgte personlige bedrifts- eller nettverksmapper, uten en måldestinasjon og struktur som er godkjent av IT-administratoren
  - Skanning uten indeksering – dette kan gjøre det uhyre vanskelig å finne og revidere skannede dokumenter og skannerelatert aktivitet (hva som skannes og til hvor)

- **Faksing**
  I likhet med skanning kan også faksing være et sårbart punkt med hensyn til dokumentdata-sikkerhet. Uansett om de sendes analogt eller via e-post, er faksede dokumenter like utsatt for brudd på datasikkerheten som skannede dokumenter.

- **Mobilutskrifter – bruk av egen enhet (BYOD)**
  Mobilitet blir av mange ansett som en av grunnpilarene for utskriftsaktivitet i fremtiden. For bedriftene byr det imidlertid på utfordringer med hensyn til hvordan de mobile utskriftsløsningene skal integreres og hvordan man får til en nøyaktig sporing og administrering av aktivitetene til mobilbrukerne. Et annet sentralt spørsmål er hvordan en mobil utskriftsstrategi passer inn i organisasjonens overordnede strategi. Mange bedrifter vegrer seg dessverre mot å innse at medarbeidermobilitet er en økende trend eller et reelt forretningskrav. Behovet for utdatasikkerhet på dette området blir derfor ofte oversett.

- **Sporing og rapportering**
  Utfordringen for bedriftene ligger ikke bare i å skulle sikre kanalene for dokumentdata, men også i å spore og rapportere dokumentdata-informasjonene.

  I tillegg er det viktig at revisjonsrapporten er nøyaktig og sikker:

  - Hvem har tilgang?
  - Er dataene nøyaktige?
  - Er redigering/manipulering mulig?
  - Hvem administrerer systemet?

Anbefalinger

Det er svært viktig å ha i bakhodet at sikkerheten av dokumentdata bare er ett av mange områder for kontorsikkerhet, og at det vil være variasjoner fra organisasjon til organisasjon.

Enkelte bedrifter kommer kanskje til at tiltakene de allerede har for nettverkssikkerhet, er tilstrekkelige så lenge de tas på alvor og implementeres grundig. Etter hvert som disse bedriftene vokser, øker imidlertid også antall genererte dokumenter, og sikkerhetsutfordringene blir automatisk større.

For å takle dette kreves en bredere sikkerhetstilnærming der man ikke bare sikrer selve nettverket, men også alt av informasjon og dokumenter som genereres og deles utenfor organisasjonen.

Det er med andre ord avgjørende å sikre både nettverket og tilkoblede perifere enheter. Dokumentdata-sikkerhet er et naturlig trinn å ta for å forbedre nettverkssikkerheten i alt fra store organisasjoner til små- og mellomstore bedrifter som er i hurtig vekst.

Programmer for dokumentdata -/utskriftsstyring (f.eks. Sharps løsninger for optimalisert utskrift eller skanning) hjelper deg å sikre alt av kontor dokumentdata, integrere enhetene dine i eksisterende systemer (f.eks. Windows) og raskt implementere konsekvente sikkerhetsretningslinjer for utskrift og skanning.

Den viktigste faktoren når det gjelder dokumentdata-sikkerhet, er kontroll: alt du kan kontrollere, kan måles og dermed sikres. Systemene våre gir deg full kontroll over alt av dokumenter og informasjon som kopieres, skrives ut, skannes og fakses.

Takket være den sømløse integreringen i den eksisterende skriverparken din, gjør styringen av dokumentdata at du sparer mye kostbar tid. Det er for eksempel raskt og enkelt å importere samtlige brukere gjennom Lightweight Directory Access Protocol (LDAP). Alle kan legges til, identifiseres og integreres i systemet på bare sekunder. All påloggingsinformasjon overføres dessuten ved hjelp av Transport Layer Security (TLS) for å unngå at den kommer uvedkommende i hende.

Det beste med dette systemet for dokumentdata-sikkerhet er likevel de avanserte funksjonene som gjør livet så mye enklere både for IT-administratorene og sluttbrukerne:

- **Brukerautentisering**
  Dette er den første og viktigste faktoren i hvordan du får tilgang til et system for dokumentdata-sikkerhet. Programvaren gir deg flere alternativer å velge mellom for hvordan du vil identifisere brukerne og gi dem tilgang til de tilkoblede enhetene. De raskeste og mest populære metodene per i dag er kort og brikker med berøringsfri funksjon. Disse lagrer alle personopplysninger, og autentiseringen gjøres med en kortleser som er installert på enheten. IT-administratorene kan dessuten velge mellom en rekke forskjellige autentiseringsmetoder, innbefattet PIN-kode, brukerpålogging, passord og biometrisk avlesning.

  Det er også mulig å benytte kort som allerede brukes for tilgang til bygninger, bestemte avdelinger eller beskyttede rom i bedriften. Det finnes en rekke kort- og kortleserstandarder som bruker ulike kommunikasjonsmetoder og -frekvenser. Vi anbefaler derfor at du rådfører deg med vår løsningskonsulent, slik at du kan få hjelp til å velge riktig system for din bedrift.

- **Sikker kø**
  Når et dokument sendes til utskrift på vanlig måte via en datamaskin, starter kommunikasjonen mellom styringen av dokumentdata og driveren på datamaskinen. Bare registrerte brukere kan skrive ut til systemet, og da bare gjennom lisensierte enheter som er konfigurert med den

nødvendige programvaren. Brukeren sender jobben til serveren for utdatastyring, og blir ved pålogging på enheten (ved hjelp av et kort med berøringsfri funksjon, en PIN-kode eller brukerpålogging med passord) identifisert som registrert bruker med utskriftsrettigheter.

- **Pull print**
  En av de store fordelene med å ha en sikker kø og kunne holde jobber på en server, er muligheten til å bruke Pull print-funksjonen gjennom en hvilken som helst tilkoblet enhet. Sluttbrukeren kan dermed skrive ut fra en vilkårlig enhet – i en annen avdeling, i en annen etasje eller sågar i en annen bygning (forutsatt at den er på samme nettverk) – eller hvor som helst der systemet for styring av dokumentdata er installert.

  Pull print innebærer dessuten mindre utskriftsrelatert nedetid for bedriften. Hvis en av utskriftsenhetene er ute av drift eller vedlikeholdes, kan du ganske enkelt gå til nærmeste tilgjengelige enhet og skrive ut jobbene dine der.

- **Automatisk sletting av jobber**
  Det store antallet sider som lagres midlertidig før utskrift eller indeksering, byr ofte på ekstra utfordringer for IT-administratorene. Men ikke hvis det brukes styring av dokumentdata. Takket være en funksjon for automatisk sletting av jobber, kan IT-administratorene konfigurere retningslinjer for dokumentoppbevaring. Hvis et dokument f.eks. ble skrevet ut kl. 8 om morgenen og ikke frigitt på enheten innen 24 timer, slettes det automatisk fra serverkøen. Denne funksjonen er fullt konfigurerbar ut fra hva hver enkelt organisasjon trenger.

84 % av organisasjonene har angitt sikkerhet som topprioritet frem til 2025, og for 58 % vil sikkerhetsekspertisen være det utslagsgivende kriteriet for valg av leverandør.[3]

- **Eliminering av dupliserte utskrifter**
  En annen fordel med å implementere løsninger for utdatastyring, er at du unngår dupliserte utskrifter. Etter autentisering og pålogging på valgt enhet, kan brukerne se hele listen over filer som er sendt inn. De finner da raskt ut om et dokument har blitt sendt flere ganger, og kan avgjøre hvilke dokumenter som skal skrives ut, og hvilke som skal forkastes. I tillegg kan brukerne velge om de vil skrive ut og slette et dokument fra køen eller skrive ut og beholde dokumentet i køen.

- **Sikker skanning, faksing og kopiering**
  Styring av dokumentdata gir deg mulighet til å kontrollere alle funksjonene som er tilgjengelige på enheten. Kopierings-, skanne- og fakseaktivitetene kontrolleres gjennom samme brukertilgang til enheten og kan overvåkes deretter. I tillegg kommer følgende:

  - For å gi sikker e-postkommunikasjon bruker Sharp-enhetene TLS-protokollen for SMTP- og S/MIME-kryptering av e-poster.
  - LAN-nettverksgrensesnittkomponenten av MFP-kontrolleren er fullstendig isolert fra PSTN-telefonlinjen for faks. Dette hindrer at hackere får tilgang til de interne systemene på multifunksjonsskriveren eller det lokale nettverket.

- **Sporing og rapportering**
  For mange organisasjoner er sporing og rapportering de viktigste faktorene å ta hensyn til. Med et system for utdatastyring spores samtlige aktiviteter. Uansett om du skriver ut, skanner, kopierer eller fakser, registreres samtlige jobber i systemet. Det kan utarbeides detaljerte rapporter basert på din personlige konto, avdeling eller spesifikke alternativer for kundefakturering.

- **Brukerredigering iht. personvernforordningen (GDPR)**
  Artikkel 17 i personvernforordningen gir detaljerte instruksjoner for håndtering av personopplysninger. Dette innbefatter retten som brukeren har til å kreve at kontrolløren sletter brukerens personopplysninger uten unødvendig opphold, og plikten som

kontrolløren har til å etterkomme et slikt krav. Med Sharps system for styring av dokumentdata er ikke dette noe problem. Det gir deg mulighet til å redigere samtlige brukerdata for å innfri de strenge forskriftskravene. Selv om brukerdataene er fjernet, kan IT-administratorene fortsatt generere bruksrapporter ut fra visse utskriftsopplysninger og -statistikker.

- **Mobil utskrift**
  Dette er et svært enkelt konsept som går ut på at brukerne kan skrive ut som vanlig fra sine egne smarttelefoner eller nettbrett (et konsept som er kjent som Bring Your Own Device, BYOD) IT-administratorene kan avgjøre hvilket program som er best egnet for organisasjonen. Sharps optimaliserte mobilprogram har en omfattende konfigurasjon som muliggjør sporing gjennom styring av dokumentdata, slik at alle mobilutskrifter rapporteres i systemet og kan brukes i forbindelse med statistikker og generering av rapporter.

Skjerpet sikkerhet

Utdatastyring spiller en sentral rolle når det gjelder å definere, utarbeide og implementere egne retningslinjer for utskriftssikkerhet:

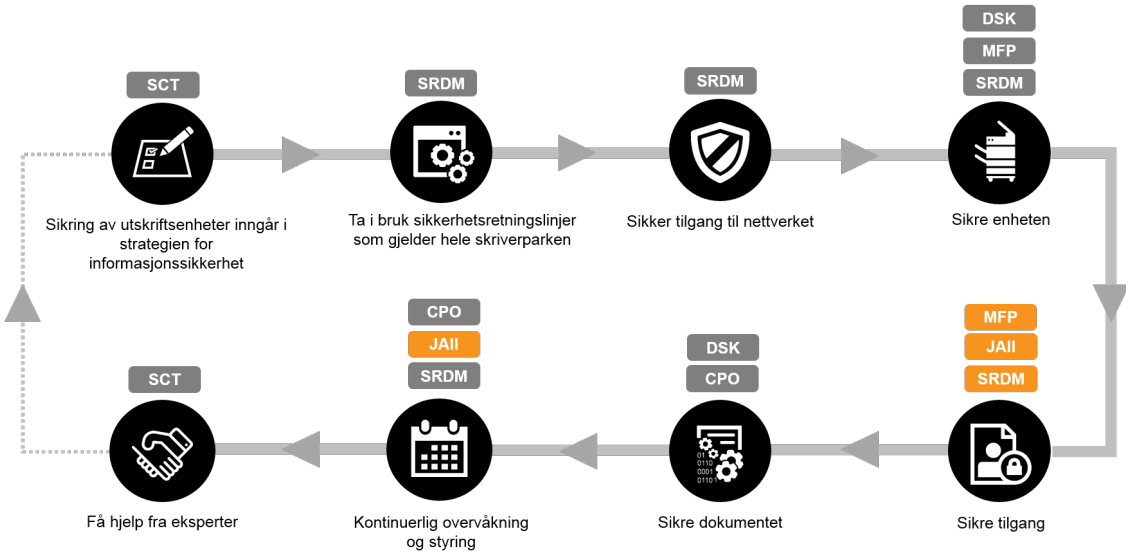
- Produktene for utdatastyring fra Sharps optimaliserte portefølje er av enorm nytte ved implementering av slike retningslinjer – først og fremst med hensyn til trinnene «Sikring av tilgang» og «Pågående overvåkning og administrering».

- Ved å legge til flere produkter fra porteføljen vår – for eksempel multifunksjonsskrivere fra Sharp, Data Security Kit (DSK), Sharp Remote Device Manager (SRDM) og Cloud Portal Office (CPO) – kan du skape et unikt, robust og konsekvent sikkerhetssystem som fungerer perfekt både for IT-teamet og bedriften.

For å oppnå høyest mulig sikkerhet bør bedriftene samarbeide med leverandører som ikke bare kan levere håndgripelige fordeler med hensyn til styring av dokumentdata, men som samtidig er pålitelige og erfarne integratorer.

Sharp har årelang erfaring med produksjon av markedets sikreste (multifunksjons)skrivere, utvikling av programmer for styring av dokumentdata og implementering av komplekse løsninger. Vi har derfor svært gode forutsetninger for å gi kundene råd og veiledning om alle sikkerhetsaspekter, innbefattet retningslinjer for utskrifts- og dokumentdata-sikkerhet.

Sharps løsninger for dokumentdata-sikkerhet og utarbeidelse av retningslinjer for utskriftssikkerhet



SCT – Sharp Consulting Team, **SRDM** – Sharp Remote Device Manager, **DSK** – Data Security Kit, **MFP** – multifunksjonsskriver, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Konklusjon

Situasjonen i dag er den at hver gang noen skriver ut, kopierer, skanner eller fakser et dokument, har man en risiko for at dokumentet stjeles eller kompromitteres.

Bedriftene må være mye mer bevisst på risikoene det innebærer å la fysiske eller elektroniske kopier av sensitive dokumenter og filer ligge uten tilsyn. Hovedpunktene er som følger:

- Dokumentdata-sikkerhet er avgjørende for enhver moderne bedrift uansett størrelse. Det økende antallet dokumenter som bedriftene genererer, medfører betydelige utfordringer for styringen av IT-miljøet. Særlige eksempler her er administreringen av et økende antall brukere, større filer, økt informasjonsdeling, overbelastning av nettverket og skriverparken.

- Et system for dokumentdata-sikkerhet gir deg maksimal fleksibilitet med hensyn til konfigurering. I tillegg til å begrense tilgangen til lukkede grupper av kontorbrukere, kan IT-administratorene spore all aktivitet på multifunksjonsskriverne – innbefattet kopiering, utskrift, skanning og faksing.

- Sharp forstår hvor viktig sikkerheten i et moderne kontor er, og tilbyr derfor en altomfattende løsningstilnærming. Denne spenner fra en nettverkssikkerhet som dekker samtlige bedriftsnettverk og tilkoblede perifere enheter, til dokumentdata-sikkerheten som omhandles i dette «White paper», og samtlige aspekter ved den dokumentrelaterte sikkerheten.

- Med en så vidtspennende sikkerhetstilnærming vil organisasjonen samtidig ha en maksimal overholdelse av de nyeste sikkerhetsforskriftene, innbefattet personvernforordningen (GDPR).

Sikkerhetsrammeverk fra Sharp

For å unngå potensielle svakheter i andre deler av bedriften, anbefaler vi at du leser mer om hvordan du kan innføre ytterligere sikkerhetstiltak knyttet til

- nettverkssikkerhet
- dokumentsikkerhet
- samsvar med personvernforordningen

i delen om informasjonssikkerhet på nettstedet vårt:
https://www.sharp.no/cps/rde/xchg/no/hs.xsl/-/html/informasjonssikkerhet.htm

Alternativt kan du kontakte en løsningskonsulent fra Sharp.

Referanser

1. «Print 2025: Print Security in the IoT Era», Quocirca, 2018
2. «Annual Global IT Security Benchmark Tracking Study», Ponemon Institute, mars 2015
3. «Print 2025: The future of print in the digital workplace», Quocirca, 2018

www.sharp.no

SHARP

Be Original.