«White paper» om informasjonssikkerhet

Dokumentsikkerhet

Beskyttelse av bedriftsinformasjon

www.sharp.no

SHARP
Be Original.

Innhold

Innledning 3
Bakgrunn 4
Problem 5
Anbefalinger 7
Konklusjon 10
Referanser 11

Innledning

For organisasjoner som hver dag behandler tusenvis av dokumenter i alle typer formater, er faren overhengende for at noe skal gå tapt, bli stjålet eller kompromittert. Beskyttelse er helt nødvendig.

Sharp definerer dokumentsikkerhet som sikkerheten knyttet til informasjon fra skannede papirdokumenter eller digitale dokumenter (f.eks. Microsoft Office-filer og e-poster) i bedriftens datasamlinger. Sharps løsning for dokumentsikkerhet dekker følgende:

- Dokumentrelaterte forretningsprosesser
- Dokumentoppbevaring (fysiske papirdokumenter og elektroniske arkiver)
- Dokumentlivssyklusen (innhenting → oppbevaring → administrering → bevaring → levering → integrering).

I dette «white paper» ser vi nærmere på utfordringene som bedriftene står overfor når det gjelder dokumentsikkerhet.
De viktigste punktene er:

- **Bakgrunnen**
  Vi undersøker her kompleksiteten i dokumentsikkerhet: fra identifisering av alle typer kontordokumenter og informasjon i de vanligste forretningsprosessene, til differensiering mellom dokumenter i fysisk (papir) og digitalt (elektronisk) format, og beskrivelser av dokumentenes livssyklus.

- **Problemet**
  Vi går her inn på utfordringene som de IT-ansvarlige, sluttbrukerne og lederne i bedrifter kan møte med hensyn til dokumentsikkerhet – særlig ved innhenting, lagring og tilgang til dokumenter og informasjon som er av en forretningssensitiv art. Fokusområdene er følgende:

  - Ustrukturerte data
  - Manuelle oppgaver knyttet til kontordokumenter
  - Generell dokumentsikkerhet

- **Anbefalingene**
  Vi ser her nærmere på hvordan Sharps optimaliserte løsninger, tjenester og beste praksis kan hjelpe deg å skape et sikkert dokumentmiljø og unngå dokumentsikkerhetsrelaterte risikoer som kan føre til driftsforstyrrelser eller brudd på persondatasikkerheten. I tillegg går vi inn på hvordan Sharp kan hjelpe deg å løse komplekse bedriftsproblemer ved å:

  - Få innsikt i hvilken betydning dokumentprosessene spiller
  - Optimalisere papirbaserte arkiver og filbaserte elektroniske datasamlinger
  - Identifisere alle trinnene som trengs for å optimalisere dokumentlivssyklusen eller utarbeide beste praksis og egne retningslinjer for dokumentsikkerhet

- **Konklusjonen**
  Vi gir her en oppsummering av emnet med fokus på følgende:

  - De sentrale utfordringene knyttet til dokumenter i bedriften
  - De viktigste anbefalingene basert på Sharps ekspertise og optimaliserte produkter
  - De neste trinnene som kreves for å utarbeide konsekvente retningslinjer for dokumentsikkerhet
  - Hvordan dokumentsikkerhet kan knyttes til andre kontorrelaterte sikkerhetsaspekter som f.eks. nettverks- og dokumentdatasikkerhet

Bakgrunn

Vi ser i dag en eksponentiell økning både i arbeidstempo og datavolumet vi genererer og forbruker.

Bransjeanalytiker IDC anslår at den globale datagenereringen vil vokse til enorme 163 zettabyte (ZB) innen 2025[1]. Det er en tidobling av datavolumet som ble produsert i 2017.

Hver dag genererer bedriftene kontrakter, fakturaer, tilbud og en rekke andre driftskritiske dokumenter i utallige formater.

Kontrakter definerer f.eks. forretningsforholdet mellom organisasjonen og kundene, mens fakturaer gir bedriftene inntekt når de betales. For å lykkes som bedrift, er det avgjørende at denne informasjonen administreres, ivaretas og gjøres tilgjengelig for riktig vedkommende i organisasjonen.

90 % av dagens data ble generert i løpet av de siste to årene – det vil si 2,5 trillioner byte med data per dag.[2]

Volumet, kompleksiteten og mangfoldet av informasjon som bedriftene genererer og forbruker, skaper utfordringer med hensyn til administrering og kontroll. For å håndtere denne situasjonen må bedriftene forstå og kartlegge de ulike typene dokumenter, hvordan de brukes, hvilken rolle de spiller i forretningsprosessene samt hvordan de lagres, administreres, distribueres og forvaltes.

De fleste av disse utfordringene er knyttet direkte til følgende tre problemer:

- **Ustrukturerte data**
  Ustrukturerte data er informasjon som enten mangler en forhåndsdefinert datamodell, eller som ikke er organisert på en forhåndsdefinert måte. Brukere vil ofte lagre transaksjonsdokumenter som f.eks. e-poster og kontordokumenter i mappestrukturer de oppretter uten en standardisert navnekonvensjon eller beskrivende metadata.

  Dette gjør det svært vanskelig å få en enhetlig oversikt og kunne svare på følgende:

  - Hvordan blir dokumentene lagret, administrert og kontrollert?
  - Hvor enkelt er det å finne, revidere og distribuere dokumentene?
  - Hvordan håndheves tilgangsrettigheter og filtillatelser?

- **Manuelle rutineoppgaver**
  Manuelle rutineoppgaver som f.eks. behandling av fakturaer, håndtering av utgifter eller administrering av HR-dokumenter, forekommer i så å si alle bedrifter. Ved hjelp av teknologi kan disse prosessene automatiseres for å øke effektiviteten, nøyaktigheten, sporbarheten og sikkerheten.

- **Forstå dokumentenes livssyklus i bedriften**
  Alle dokumenter eller dokumenttyper følger sin egen livssyklus fra innhenting til destruering. For å kunne iverksette de riktige sikkerhetstiltakene for forskriftssamsvar og samtidig bevare nødvendig fleksibilitet til å jobbe effektivt, gjelder det å forstå, kartlegge og optimalisere livssyklusene til de ulike dokumenttypene.

Dette er sentrale områder som bedriftene bør tenke over når de definerer og implementerer retningslinjer for dokumentsikkerhet.

Problem

Moderne bedrifter behandler store mengder informasjon, men mangler ofte klart innsyn i hvordan informasjonen produseres, lagres og gis tilgang til. Dette kan føre til potensielle sikkerhetsbrister.

Selv om de fleste organisasjoner benytter digital generering og lagring av innhold, blir dokumenter ofte lagret både i elektronisk (digitalt) format og papirformat:

- **Filer og journaler i papirformat**
  Dokumenter i papirformat utgjør en betydelig sikkerhetsrisiko ettersom det ofte er vanskelig å dokumentere hvor de kommer fra eller vise et tydelig revisjonsspor. I tillegg til denne manglende sporbarheten, blir den fysiske sikkerheten ofte oversett: sensitive prosessdokumenter arkiveres på feil sted, går tapt eller oppbevares på utrygge steder.

- **Filer og journaler i elektronisk format**
  Elektroniske journaler som lagres i distribuerte, og i enkelte tilfeller isolerte lagringssystemer, medfører egne sikkerhetsutfordringer – ofte rett og slett på grunn av mengden og de mange potensielle lagringssystemene/-stedene. For å kunne få på plass prosesser og sikkerhetsretningslinjer som gjelder hele bedriften, er man nødt til å forstå dokumentenes livssyklus.

Ivaretakelse av dokumentsikkerheten

Dokumentsikkerhet (eller mangel på sådan) er svært bredt definert, og må vurderes ut fra et livssykluserspektiv. Dette gjelder særlig med hensyn til brudd på persondatasikkerheten, ustrukturerte data, usikrede filer, menneskelig svikt, uautorisert lagringstilgang osv.

Dokumentenes livssyklus består av de seks hovedfasene innhenting, lagring, administrering, forvaltning, levering og integrering:

- **Trinn 1: Innhenting**
  Innhenting er prosesstrinnet der informasjon samles inn gjennom enten skanning av papirdokumenter, overvåkning av en «overvåket» innboks eller oppretting og lagring av dokumenter fra et program:
  - **Skanning** er den vanligste metoden for å overføre innhold fra papirformat til elektronisk format. Selv om skanning er praktisk, kan det by på utfordringer med hensyn til sikkerhet og juridisk holdbarhet. Uten kontroller er ikke prosessen sporbar, og dette kan føre til at dokumentene ikke består testen for bevisverdi og juridisk holdbarhet.
  - **Indeksering** er metoden som brukes for å beskrive dokumenter ved hjelp av metakoder eller fulltekst (tekst). Indeksering muliggjør raske fil- og datasøk, noe som er særlig praktisk ved evaluering av innhold med hensyn til forskriftssamsvar.
  - **Ruting** er prosessen som brukes for å sende innhentede dokumenter til riktig lagringssted. Uten dokumentruting kan det skje ved vanvare at dokumenter lagres på feil sted eller på et utrygt sted.

- **Trinn 2: Lagring**
  Et sikkert lagringssted kan være et papirbasert eller elektronisk filsystem, men mange bedrifter er ikke bevisst på hvilke krav som stilles til type lagring, plassering og sikkerhet:
  - Papirbaserte lagringssystemer er fortsatt svært vanlige, men mangler ofte nødvendige sikkerhetskontroller. I tillegg er det svært vanskelig å vise revisjonsinformasjon for papirdokumenter.
  - Elektronisk baserte lagre implementeres ofte med en forventning om at de er den beste løsningen. Uten egnet utforming og administrering oppstår det imidlertid utfordringer knyttet til bl.a. hvordan man beskytter slike systemer i bedriftsnettverket, hvordan man konfigurerer tilgangsrettigheter og hvordan man overvåker eller begrenser bruken.

- **Trinn 3: Administrering**
  Dokumentstyring omfatter tillatelser, versjonssporing og revisjonsspor:

  - Med tillatelser administreres brukernes dokumenttilgang slik at man bevarer et sikkert dokumentmiljø. Selv om tillatelser gjerne er enkle å forstå, kan de være vanskelige å innføre og administrere hvis man ikke har de riktige systemene. For å kunne implementere tillatelser effektivt, må bedriften i første omgang forstå hvordan brukernes aktivitet er relatert til informasjonen de trenger tilgang til, og prosessene de er involvert i.
  - Versjonssporing sikrer at brukerne jobber med de nyeste dokumentene, samtidig som eldre dokumentversjoner kan bevares ved behov. Dette er særlig nyttige i strategiske eller juridiske situasjoner der man kan bruke tidligere dokumentversjoner til å bevise opprinnelsen til et dokument. Versjonssporing er avgjørende for å bevare et sikkert og juridisk holdbart digitalt dokumentarkiv.
  - Et revisjonsspor lagrer oppføringer av alle aktiviteter og transaksjoner knyttet til et dokument, innbefattet hvem som har opprettet, redigert, sett eller laget en ny versjon av det. Revisjonsspor gjør det mulig å dokumentere aktivitet knyttet til lagrede dokumenter, og er avgjørende for å bevare sikkerhet – særlig i tilfelle brudd på persondatasikkerheten.

- **Trinn 4: Forvaltning**
  Forvaltning av dokumenter og informasjon er et annet vesentlig aspekt ved det å ivareta et sikkert dokumentmiljø. Arkiver og elektroniske datasamlinger må imidlertid vedlikeholdes konstant, i og med at lagringsplassen er begrenset. Følgende rutiner er derfor av avgjørende betydning:

  - **Dokumentoppbevaring**
    Visse dokumenter må (iht. gjeldende lovkrav) oppbevares et bestemt antall år. Dette medfører blant annet følgende utfordringer:

    - Å sørge for en arkivføring som sikrer at man kun fjerner dokumenter med utløpt oppbevaringsperiode
    - Å påse at samtlige dokumentversjoner som omfattes av retningslinjene for oppbevaring, er gjort rede for
    - Å bestemme om dokumentene skal administreres sentralt eller lokalt

  - **Destruering av dokumenter**
    Bedriftene må utarbeide retningslinjer for å sikre at alt av papirinformasjon, elektroniske filer og elektroniske biblioteker destrueres på en trygg måte når de ikke lenger er aktuelle eller oppbevaringsperioden er utløpt:

    - Makulering av fysiske dokumenter i samsvar med ett av sikkerhetsnivåene som er angitt i DIN-standarden for makulering, er den tradisjonelle måten å håndtere papirer på. Det kan imidlertid være både kostnads- og tidkrevende.
    - Elektronisk makulering sørger for sikker og dokumenterbar sletting av elektroniske dokumenter fra harddisker, DVD-er, disketter osv.

- **Trinn 5: Levering**
  På dette trinnet angis hvordan et elektronisk dokument kan deles med andre brukere eller forretningspartnere. Særlig hvis:

  - Dokumentdeling gjøres ofte ved hjelp av delte mapper eller stasjoner, men uten korrekt administrering kan dette føre til at uautoriserte brukere eller brukergrupper får tilgang til filene.
  - Tilgang til dokumenter på mobilenheter kan også være en del av leveringstrinnet, og man står da overfor langt mer komplekse utfordringer med hensyn til hvordan man sikrer tilgangen.

- **Trinn 6: Integrering**
  Integrering er prosessen som brukes for å utveksle informasjon med andre bedriftsprogrammer som f.eks. bokførings- eller ERP-systemer.

  For at integreringen skal bli vellykket, må alle de forutgående trinnene være riktig og fullstendig gjennomført, slik at det kan leveres konsekvente og nøyaktige data. Eventuelle problemer knyttet til ett eller flere av de angitte punktene, vil få direkte konsekvenser for virksomhetsprosessen.

Anbefalinger

Sharp kan levere en rekke løsninger og programmer som hjelper organisasjoner å utarbeide retningslinjene de trenger for datasikkerhet.

Dokumentsikkerhet er et svært komplekst emne, men ved å definere dokumentlivssyklusen blir det enklere å se hva som eventuelt trenger å endres eller forbedres:

- Å skulle optimalisere prosesser eller definere dokumentsikkerhet fra grunn av kan være både vanskelig og tidkrevende – særlig med hensyn til kartlegging av prosesser og innhenting av relevant informasjon om prosessene og bedriftsrollene. I våre profesjonelle tjenester blir erfaringen vår innenfor dokumentløsninger kombinert med sofistikerte verktøy for dokument-/informasjonsoppdagelse og kartlegging av arbeidsflyt.

- Sharp bruker en trinnvis prosess for å gi bedriftene innsikt i egen dokumentsyklus og relaterte utfordringer, og tar deretter utgangspunkt i disse for å utvikle prosesser og prosedyrer rettet mot de to hovedmålene for dokumentsikkerhet:

    - Å skape struktur i ustrukturerte data
    - Å effektivisere rutineoppgaver

    .

Kom raskt og enkelt i gang

- Sharp hjelper kundene å skape robuste dokumentmiljøer og retningslinjer for sikkerhet. Løsningene våre, der Sharps multifunksjonsskrivere brukes til innhenting og den optimaliserte programvareporteføljen vår brukes til dokumentlagring og -styring, gir kundene trygg forvissning om at de har både en sikker og sporbar dokumentinfrastruktur.

- Endringene kan i første omgang innføres i avdelinger der det brukes svært mye papir (juridisk avdeling samt personal- og økonomiavdelingen), før man så trinnvis utvider prosessen og prosedyrene til å omfatte også andre deler av virksomheten.

Enklere innhenting og lagring av dokumenter

- For å sørge for trygg skanning anbefaler Sharp på det sterkeste at kundene bare skanner sikre, interne datasamlinger og valgte e-postgrupper eller brukere. Alt dette er ting som IT-administratorene kan konfigurere på multifunksjonsskriverne fra Sharp. Slike trygge rutiner er særlig viktig i et GDPR-perspektiv.

- I tilfeller der det er behov for mer sofistikerte funksjoner (f.eks. for å sikre juridisk holdbarhet), kan disse fås gjennom Sharps optimaliserte produktportefølje.
  Sharp tilby en rekke forskjellige løsninger som effektiviserer prosessene hos små, mellomstore og store organisasjoner, og muliggjør direkte integrering i bedriftsprogrammer.

- Sharps optimaliserte løsninger gjør det mulig å indeksere alle innhentede dokumenter:

    - Legg til metadata direkte fra multifunksjonsskriveren
    - Legg til metadata i programgrensesnittet før lagring og behandling

- Sharps optimaliserte løsninger inkluderer rutingalternativer som skal sikre at alle brukere skanner og innhenter dokumenter på samme strukturerte måte og deretter lagrer dem på riktig sted og i klarerte programmer.

Brukerroller og -tillatelser

Ved utarbeiding av retningslinjer for dokumentsikkerhet er brukertillatelser og -roller avgjørende for å bevare konfidensialitet og kontroll.

- Sharp anbefaler å bruke ett sentralt dokumentadministrasjonssystem der

«rollene» er koblet til medarbeiderens behov i bedriften. For eksempel:

  - Kun medlemmer på styrenivå har tilgang til alle forretningsdokumenter
  - Bare HR-avdelingen har tilgang til personaljournalene
  - Prosjektledere har tilgang til prosjektrelaterte dokumenter
  - Salgsrepresentanter har tilgang til salgsrelaterte filer som f.eks. brosjyrer og skjemaer

- Tillatelser defineres ut fra rolle eller gruppe for å avgrense hva brukerne kan gjøre med dokumenter eller delsett (opprette, vise, endre eller slette). En bruker kan dermed f.eks. kun ha tillatelse til å vise dokumenter.

- Versjonssporing er avgjørende. Med Sharps optimaliserte løsninger kan du sjekke hvilken versjon av dokumentet du jobber på, og revidere eller gjenopprette eldre dokumentversjoner.

- Dokumentstyringen sørger for at mens en medarbeider redigerer et dokument, vil andre i personalet kun ha lesetilgang til dette dokumentet.

- For å påse at målene om sikkerhetssamsvar nås, kan IT-administratorene bruke et sofistikert revisjonssporverktøy (loggføringsspor) som registrerer all dokumentaktivitet, innbefattet informasjon om når et dokument ble endret, hvem som utførte endringen og hvor lenge en bestemt bruker har jobbet med dokumentet.

Riktig informasjon til riktig tid

- Utarbeid retningslinjer for dokumentoppbevaring ut fra type dokument og hvilke avdelinger som behandler informasjonen.

- Ved utløp av dokumentoppbevaringstiden skal dokumentene destrueres. Avhengig av hvilken type datasamlinger som er i bruk, kan dataene fjernes fra systemene på flere ulike måter:

  - For papirdokumenter anbefaler Sharp å bruke en profesjonell makuleringstjeneste som har en DIN-rating på 5 eller høyere.
  - For elektroniske data anbefaler Sharp en profesjonell tjeneste for sletting av elektroniske data
  - For data som er lagret på HDD-er (med lokal dokumentstyring og interne datasamlinger), anbefaler Sharp en totrinns prosess med datasletting etterfulgt av fysisk destruering, for å sikre at ingen kan få tilgang til harddiskene.

Sømløs informasjonstilgang og -deling

Alle retningslinjer som innføres for dokumentsikkerhet i bedriften, skal beskrive hvordan brukere/medarbeidere kan få tilgang til dokumenter og dele data med andre.

Sharps optimaliserte løsninger gjør det mulig å levere dokumenter via dokumentstyringsplattformer på flere forskjellige måter:

- Én mulighet er å dele en tidsbegrenset kobling til filen på e-post. Detaljert informasjon om delingsaktiviteten blir loggført, og det er mulig å deaktivere koblingen manuelt. Alternativt deaktiveres koblingen automatisk etter en forhåndskonfigurert utløpstid.

- Et annet alternativ er å dele mapper i systemet med registrerte brukere fra samme organisasjon. Du kan angi hvilke tillatelser mottakerne skal ha til å jobbe med dokumentene i mappen (lesetillatelse, lese- og skrivetillatelse eller lese-, skrive- og slettetillatelse). Disse rettighetene og retningslinjene kan også fastsettes ved utarbeidelse av de generelle retningslinjene for dokumentadministrasjonssystemet og dokumentsikkerhet.

- Mesteparten av systemfunksjonene kan gjøres tilgjengelig også for bruk på mobil (enten Android eller iOS). Sharp anbefaler at bedriftene vurderer fordelene med sikker mobilbruk i jobbsammenheng.

Få optimalt utbytte av dataene dine

Sharp har utviklet en rekke integreringer som gjør at data som innhentes via multifunksjonsskrivere fra Sharp, overvåkede mapper eller tilknyttede programmer, kan integreres i forretningssystemer som for eksempel Sage, QuickBooks og SharePoint.

Her er noen av avdelingsområdene som Sharp har fokusert på:

- **Optimalisert arbeidsflytprogramvare for leverandørgjeld**

Med denne løsningen brukes optisk tegngjenkjenning (OCR) for å hente ut data fra registrerte fakturaer, og validerings- og godkjenningsprosessene automatiseres. Avdelingene som håndterer leverandørgjeld, vil dermed kunne jobbe mer produktivt, nøyaktig og effektivt.

Les mer om integrering for håndtering av leverandørgjeld her (eksempel fra Storbritannia).

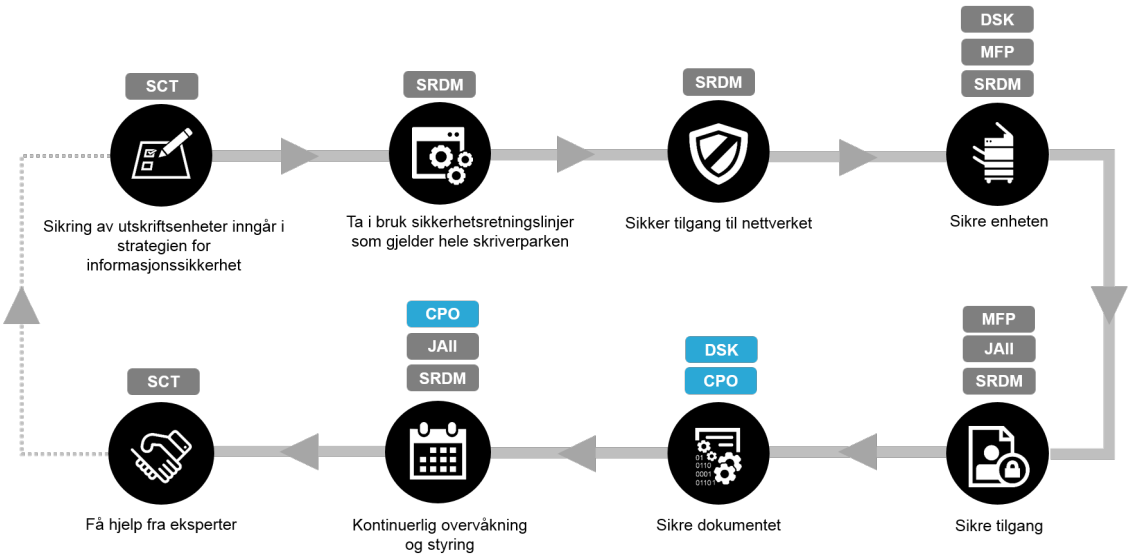
- **Optimalisert arbeidsflytprogramvare for digitale postrom**
  Denne løsningen sørger for at innkommende papir- og digitalpost rutes elektronisk til riktig vedkommende hvis den angitte mottakeren er borte fra kontoret. Bedriftene vil dermed kunne sortere og distribuere store mengder post på en rask og effektiv måte, slik at personalet jobber maksimalt produktivt.

  Du kan lese mer om programvaren for optimalisering av digitalpost her (eksempel fra Storbritannia).

- **Optimalisert arbeidsflytprogramvare for personaladministrasjon**
  Denne løsningen sørger for en svært sikker og godt administrert lagring av konfidensiell personaldokumentasjon. Bedriftene kan effektivisere behandlingen av HR-dokumentere, kontrollere tilgangen til dokumenter og sikre etterlevelse av gjeldende person- og datavernlover.

  Les mer her (eksempel fra Storbritannia).

Utarbeidelse av retningslinjer for utskriftssikkerhet samt Sharps løsninger for dokumentsikkerhet



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

Konklusjon

Ingen har råd til å ta lett på informasjonssikkerheten – særlig ikke når dokumenter er involvert. De utgjør organisasjonens intellektuelle rikdom, og kan være katastrofale å miste.

Dokumentsikkerheten er ett av de viktigste aspektene ved sikkerheten i enhver bedrift. Dessverre kan utarbeidelse av retningslinjer for dokumentsikkerhet være en tidkrevende og kompleks prosess. Det er her Sharp kommer inn i bildet.

Vår årelange erfaring med dokumentløsninger har gjort oss i stand til å utvikle en tilnærming til bedriftsdatasikkerhet som omfatter hele spekteret fra nettverks- til utdata- og dokumentsikkerhet.

Som globalt ledende på kontorsikkerhet ønsker vi å bruke ekspertisen vår til å hjelpe kundene å integrere robust og forskriftsmessig sikkerhet i sine bedriftsprosesser.

Med vår dokumentert effektive tilnærming til dokumentsikkerhet sørger vi for at bedriftene kan få på plass unike og skreddersydde systemer og prosesser for hvert av trinnene i dokumentlivssyklusen (innhenting, lagring, administrering, forvaltning, levering og integrering) og dermed innfri nye sikkerhetsforskrifter som f.eks. EUs personvernforordning (GDPR).

Sharps optimaliserte løsninger er laget for å levere maksimal funksjonalitet og sikkerhet samt rask investeringsavkastning.

Nøkkelsektorene våre er offentlig sektor, utdannelsessektoren, juridisk og finansiell sektor, helsevesenet, hotellnæringen og virksomhetssektoren, men vi kan levere skreddersydde og robuste løsninger til alle typer bedrifter.

For at du skal unngå potensielle svakheter på andre områder i organisasjonen din, kan vi hjelpe deg å innføre ytterligere sikkerhetstiltak fra Sharp-porteføljen. På den måten kan du sørge for at hvert eneste aspekt av virksomheten beskyttes fullt ut:

Sikkerhetsrammeverk fra Sharp

- Dokumentsikkerhet
- Nettverkssikkerhet
- Utdatasikkerhet
- Samsvar med personvernforordningen

Du finner mer informasjon om emnene ovenfor i «white paper» -biblioteket og under 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. «Data Age 2025», IDC, mars 2017
2. «Data Never Sleeps 5.0», DOMO, 2018

www.sharp.no

SHARP

Be Original.