RAPPORT

INFORMASJONSSIKKERHET I SKANDINAVISKE VIRKSOMHETER

10 Spørsmål til IT-sjefer
om beskyttelse av data

Canon

FORORD

Truslene fra cyberkriminalitet er høy i Skandinavia, og ifølge Center for Cybersikkerhed i Danmark, blir det investert store summer i informasjonssikkerhet. Slik har det vært i mange år, men det dukker opp nye utfordringer hele tiden, senest gjennom den hybride arbeidsplassen. Kontoret er der du er - og det skal være trygt.

Men hva med dokumenter og print? Dokumenthåndtering er en utfordring for sikkerhet og compliance. Det kan være vanskelig å få fullstendig overblikk over brukere og dokumentaktiviteter. Det kan resultere i brudd på informasjonssikkerheten.

Derfor bør virksomhetens informasjonssikkerhetsstrategi understøtte hele dokumentets livssyklus for å være compliant:

- Overblikk over bruker- og dokumentaktiviteter i forbindelse med print.
- Sikre at skannede dokumenter når riktig destinasjon uten datalekkasjer.
- Data og følsomme opplysninger skal oppbevares og håndteres i overensstemmelse med gjeldende regler.
- Utgående kommunikasjon, dokumenter og data skal administreres sikkert. Canon har naturligvis en særlig interesse for dette området og har utviklet løsninger som gjør informasjonssikkerhet og compliance lettere, både når det gjelder dokumenthåndtering, adgangskontrol og printsikkerhet.

Canon har derfor undersøkt dette området og utviklet rapporten du har foran deg. Vi har spurt 263 IT-ansvarlige, hvor langt de er kommet med informasjonssikkerhet - Særlig når det gjelder dokumenthåndtering.

Deltagerne deler vår bekymring. **59%** mener at det er vanskelig å sikre dokumenter og data i virksomheten.

GOD LESING!

Intervjuperiode og datainnsamlingsmetode:
Undersøkelsen er gjennomført i perioden 1. til 5. mai 2023 via internett med utgangspunkt i YouGov-panelet, som består av frivillige undersøkelsesdeltagere, som er nøye utvalgt på bakgrunn av sin profil.

Målgruppe:
Undersøkelsen omfattet 263 dansker i alderen 25-65 år med IT-beslutningsansvar.

Det er sendt ut invitasjoner via e-mail til personer som oppfyller kravene i YouGov-panelet.

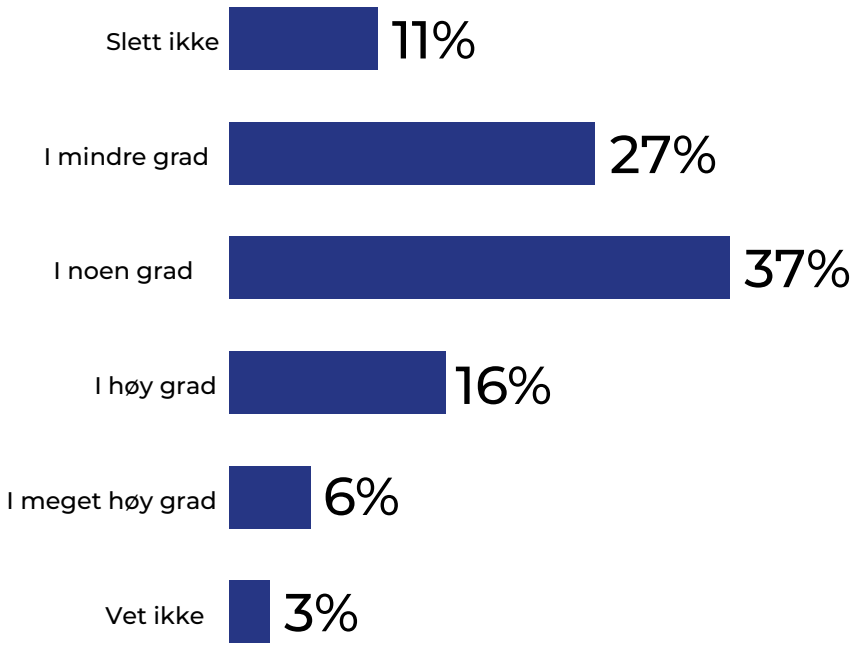
Dataen er innsamlet slik at den utgjør et representativt utvalg av den danske befolkning basert på målgruppen. Canon Norge har valgt å videreformidle disse resultatene da vi anser de som relevante og informative for et norsk/ skandinavisk publikum også

Vekting av data og materialets sammensetning:

Data er vektet på dimensjonene kjønn, alder og geografi ut fra en standard fra Danmarks Statistikk, dermed er resultatene representative for målgruppen.

SPØRSMÅL 1

I HVILKEN GRAD ER DET EN UTFORDRING Å SIKRE DOKUMENTER OG DATA I HVERDAGEN PÅ DIN ARBEIDSPLASS



Det er generelt en utfordring å sikre dokumenter og data. Hele 59 % finner det vanskelig å sikre dokumenter i varierende grad. Bare 11 % mener at det ikke er en utfordring. Det er ganske tydelige tall.

Men det er ikke en enkel oppgave. Et typisk scenario kan være et sensitivt papirdokument som ligger i skriveren og deretter enten blir tatt av feil person eller rett og slett glemt, slik at fortrolig informasjon blir sett av personer den ikke var ment for. Dette kan lett skje. Mange har opplevd det.

Det samme gjelder for dokumenter som kan være spredt over hele virksomheten og brukes av ansatte i mange forskjellige roller og scenarioer. Noen i permer, andre på intranettet, filservere, forretningssystemer eller til og med i skyen. IT-avdelingen står overfor vanskelige oppgaver med å sikre informasjonshåndteringen – spesielt med dokumenter lagret i e-poster, både i innboksen og blant slettede meldinger.

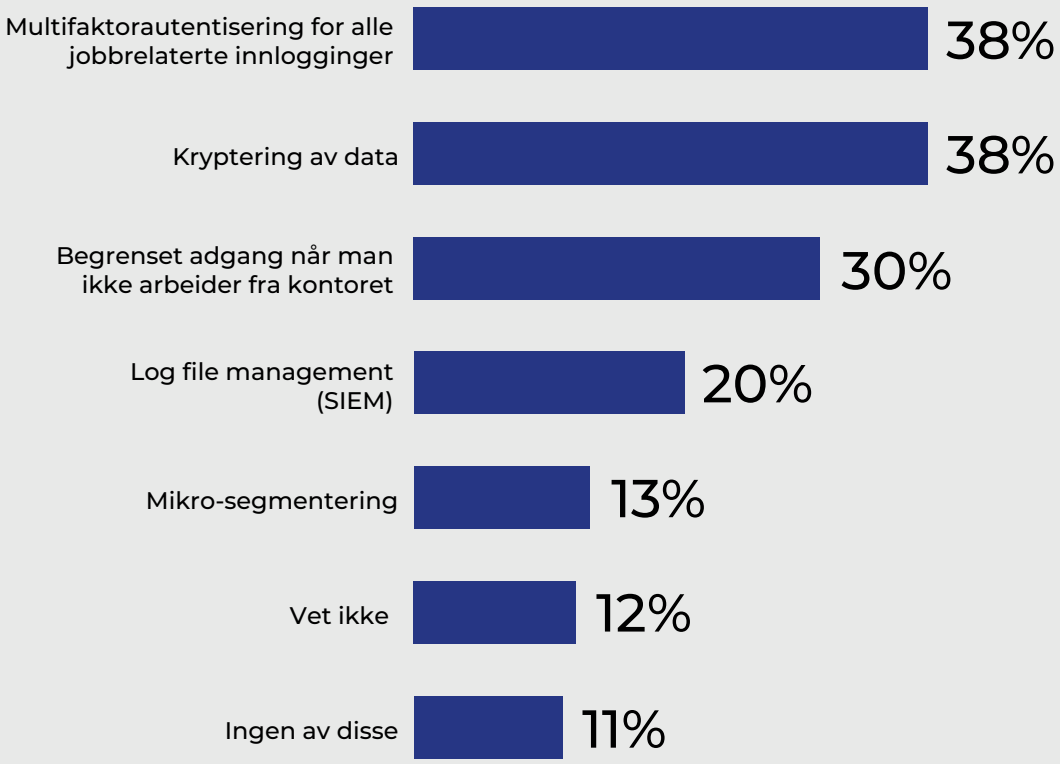
Se hvordan IKT Valdres økte sin printsikkerhet!

IKT-Valdres har tatt i bruk Canon herdingstjeneste for å øke robustheten i sitt printmiljø.

Scann QR-koden
Eller klikk her

SPØRSMÅL 2 – DU KAN VELGE FLERE SVAR

HAR DERE INNFØRT ET ELLER FLERE AV FØLGENDE TILTAK PÅ DIN ARBEIDSPLASS DE SISTE 3 ÅRENE?

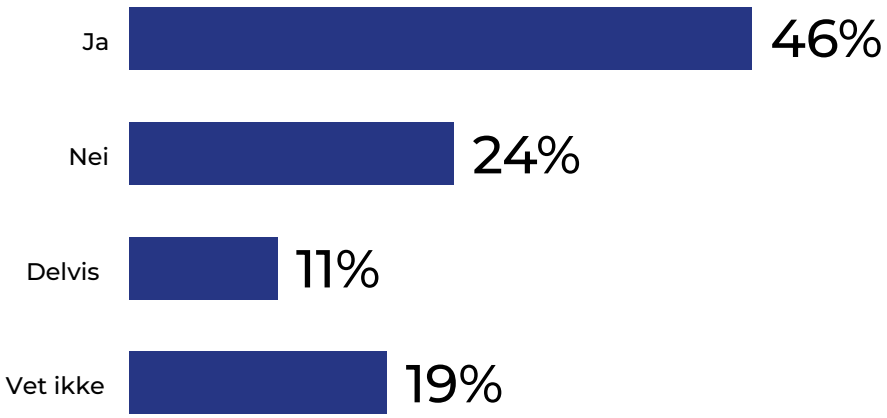


Det er ikke overraskende at det har blitt investert mye i IT-sikkerhet de siste 3 årene- spesielt Multifaktor Autentisering (MFA) og datakryptering, som 38 % har investert i. Det samme gjelder adgangsstyring og brukerkontroll for ansatte utenfor kontoret – noe som sannsynligvis er en direkte konsekvens av økt cyberkriminalitet og, kanskje i enda større grad, hybride arbeidsplasser. Faktisk er det overraskende at tallene ikke er høyere.

Spesielt når det gjelder SIEM, en kategori løsninger for å overvåke og følge med på aktivitetene i virksomheten. Dette er spesielt viktig når det er behov for å åpne opp for omverdenen. For eksempel når de ansatte jobber hjemmefra.
MFA, kryptering, tilgangskontroll og SIEM er også viktig i forbindelse med utskrift og skanning, som er en integrert del av IT-infrastrukturen, der store mengder sensitiv data passerer gjennom hver dag.

SPØRSMÅL 3

HAR DIN ARBEIDSPLASS INNLEMMET PRINT- OG SCANNINGSLØSNINGER I DERES IT-SIKKERHETSSTRATEGI?



Kun 46% har tatt inn print- og scannings-løsninger i sin IT-sikkerhetsstrategi. Ytterligere 11% har gjort det delvis. Det er bemerkelsesverdig få tatt i betraktning trusselen for datainnbrudd.

Medarbeidere arbeider med kontrakter, salgsdokumenter, personsensitiv informasjon om kollegaer, forretnings-hemmeligheter og lignende. Hundrevis, om ikke tusenvis av dokumenter blir berørt, hver dag. Disse opplysningene bør ikke glemmes i utskriftshyllen eller trekkes ut av harddisken på en multifunksjonsprinter.

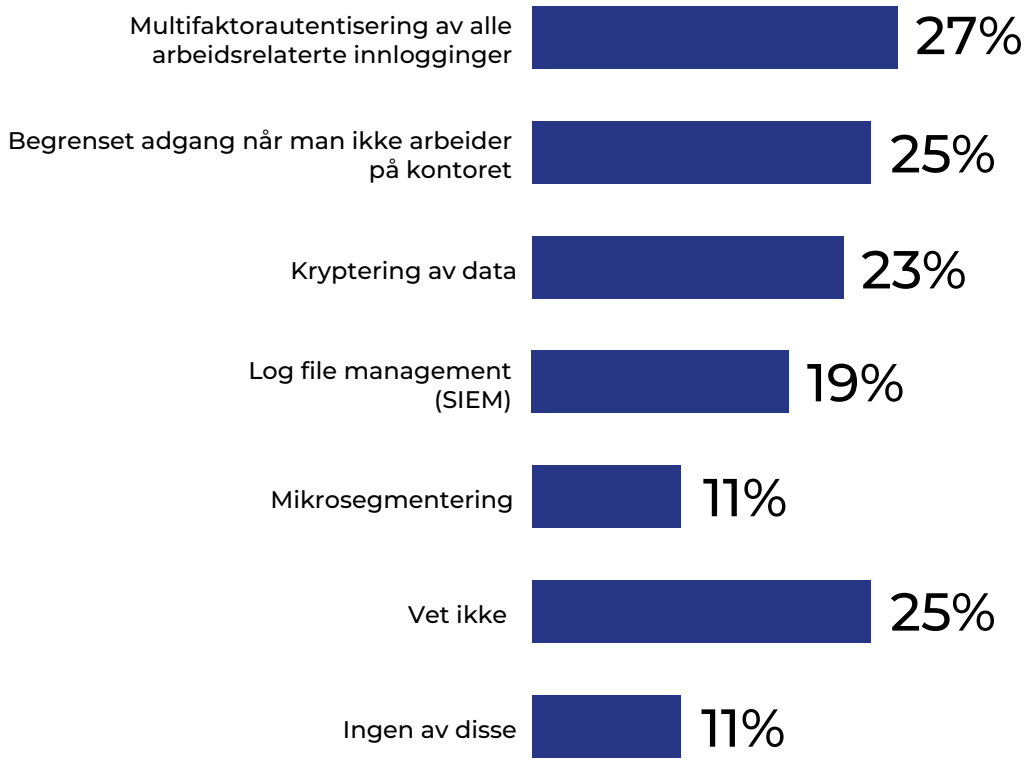
Derfor er det bekymringsverdig, at 43% ikke har en informationssikkerhetsstrategi på print og scan eller ikke vet om de har en.

Hvorfor bør alle virksomheter prioritere printsikkerhet som en del av sin IT-sikkerhetsstrategi?
Se videoen med mnemonic, skandinavias største it-sikkerhetsselskap, som demonstrerer i praksis, hvordan hackere kan komme seg inn på og hente ut informasjon fra multifunksjonsprintere.

› Se videoen her

SPØRSMÅL 4 – DU KAN VELGE FLERE SVAR

HVILKE AV FØLGENDE FUNKSJONER UNDERSTØTTER PRINTERE PÅ DIN ARBEIDSPLASS?



Informasjonssikkerhet kan være en utfordring når det gjelder utskrift. Store mengder sensitive data passerer gjennom printeren hver dag, og hver gang er det en risiko for datalekkasje.

Derfor er det viktig å ha sikkerhetstiltak som MFA, som identifiserer og autentiserer brukere, slik at sensitive dokumenter bare skrives ut til riktig person. Det samme gjelder for brukertilgang og isolering av alle enheter, inkludert skrivere og skannere, i mikrosegmenter for å redusere skaden fra eventuelle angrep. Som vi så i spørsmål 2, er det fokus på dette, men risikoen ved skrivere ser ut til å være undervurdert.

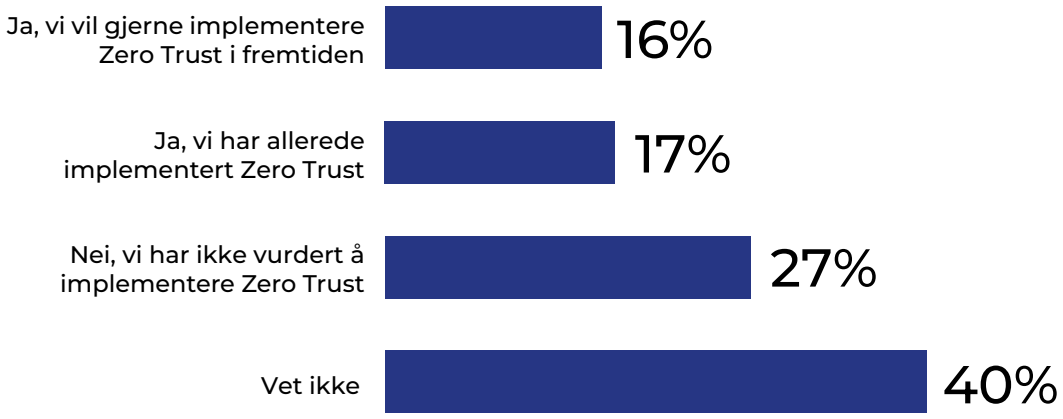
Kun 27 % har implementert MFA i forbindelse med utskrift, og 75 % begrenser ikke tilgangen til utskrift når de er borte fra kontoret. Dessuten krypterer kun et mindretall av dataene som sendes til skriveren. Dette er et problem hvis disse dataene skulle bli stjålet, hacket eller på annen måte kompromittert.

Det generelle bildet er at informasjonssikkerhet ikke blir prioritert høyt nok rundt utskrift og skanning, noe som kan bli problematisk.


Canon

SPØRSMÅL 5

HAR DIN ARBEIDSPLASS PLANER OM Å INNFØRE EN ZERO TRUST-STRATEGI?



Zero Trust er en tilnærming innen IT-sikkerhet som antar at IT-trusler kan komme både utenfra og innenfra. Zero Trust krever verifisering av enhver forespørsel, som om den kommer fra et åpent nettverk og derfor potensielt er en trussel. Alle tilgangsforespørsler må være fullstendig autentisert, autorisert og kryptert.

Zero Trust som konsept preger mange IT-sikkerhetsstrategier i dag og krever blant annet:

-Least-privilege access (PoLP): betyr at en bruker kun får tilgang til det mest nødvendige.

-Mikrosegmentering: IT-infrastrukturen er delt inn i mindre sikkerhetssoner, så sikkerhetsbrudd – som hackerangrep – begrenses til en enkelt sone.

-Multifaktorautentisering: brukere må identifisere seg med flere metoder før de blir logget inn, for eksempel passord kombinert med fingeravtrykk eller en token.

Mange anser Zero Trust for å være fundamentalt for bedrifters IT-sikkerhet nå og i fremtiden. Men blant de spurte bedriftene har kun 17 % allerede implementert Zero Trust-paradigmet. 16 % vurderer det, men hele 67 % har ikke innført Zero Trust og har muligens ingen planer om det.

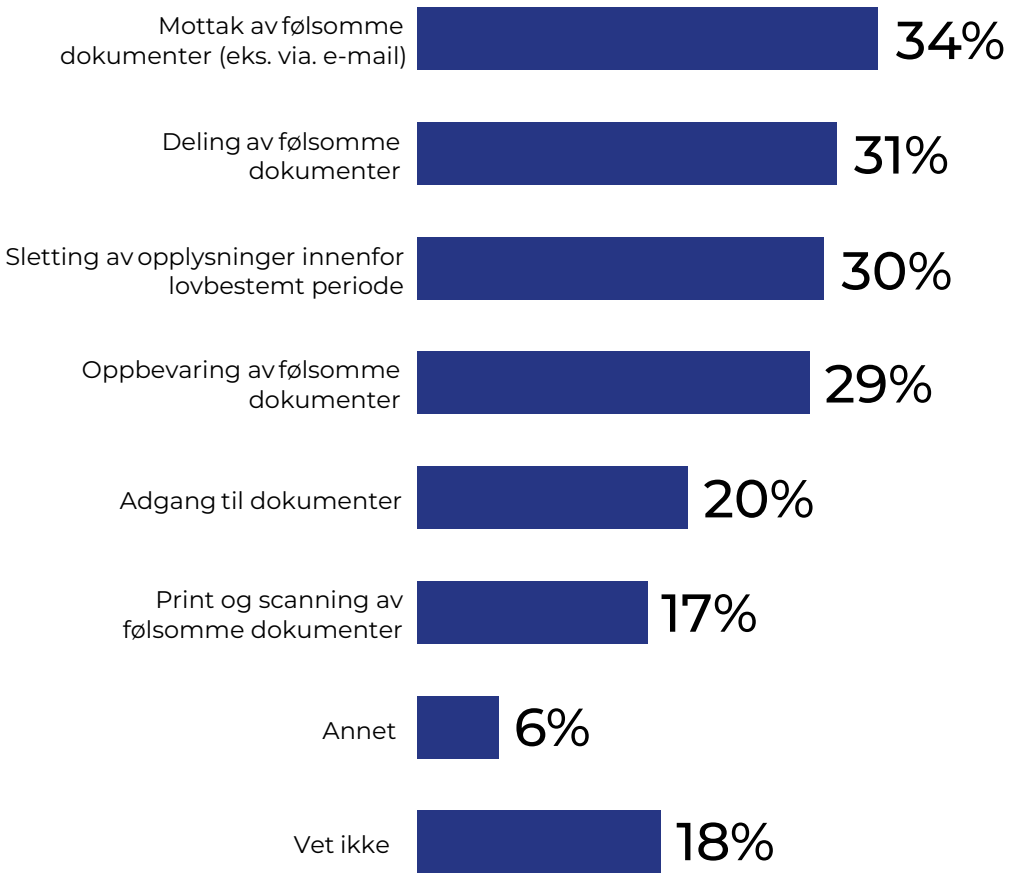
Det ser ut til at mange ennå ikke er fullt ut kjent med fordelene ved Zero Trust. Minst 40 % vet ikke om deres bedrift vil innføre Zero Trust.

Canons løsninger for dokumenthåndtering og utskrift/skanning støtter en Zero Trust-strategi og kan integreres med din eksisterende tilgangskontroll og MFA for å inkludere dokumenter når de skrives ut og skannes.

Sikker print bygget på Zero trust-prinsipper!
Les mer om uniFLOW Online her:

› Les mer

HVA ER DE STØRSTE UTFORDRINGENE DU/DIN ARBEIDSPLASS OPPLEVER I FORBINDELSE MED GDPR?



Siden innføringen av GDPR i 2018 har både myndigheter og bedrifter prioritert sikkerheten rundt behandling av personsensitive data høyt. Denne oppgaven er utfordrende, fordi vi jobber med mange dokumenter og typer data som kan være sensitive på flere nivåer. Disse dataene må kunne arkiveres på riktig måte, og hvis personen ønsker det, også slettes.

Retten til å bli glemt er et sentralt element i GDPR. Som bedrift må du kunne redegjøre for hvilke data du har samlet inn, dokumentere beskyttelsestiltakene, og forklare prosedyrene som trer i kraft ved eventuelle uhell.

Svarene fra spørsmål 6 understøtter disse utfordringene. Omtrent en tredjedel støter på problemer med mottak og behandling av sensitive dokumenter. Likevel opplever virksomhetene utfordringer ved lagring og sletting av dokumenter for å sikre overholdelse av GDPR.

Det er avgjørende for bedrifter å ha effektive dokumenthåndteringssystemer. Disse systemene bør enkelt, og eventuelt automatisk, kunne arkivere og sortere dokumenter, så de er både sikkert lagret og enkle å finne. På den måten kan dokumenter alltid gjenfinnes og slettes, om nødvendig. Uten et slikt system kan prosessen bli betydelig mer komplisert.

Canons Therefore-løsning er et dokument-håndteringssystem som forenkler prosessen for virksomheter å arbeide med, dele og samarbeide om dokumenter og data, samtidig som man overholder GDPR-lovgivningen. Ved bruk av Therefore eForms eller uniFLOW Online kan brukere laste opp eller skanne dokumenter direkte til plattformer som SharePoint, Teams, OneDrive, med flere. På denne måten unngås GDPR-compliance-problemer forbundet med skanning av konfidensielle dokumenter som ender opp i brukerens e-postinnboks. uniFLOW Online oppretter en kryptert PDF-fil og tilbyr muligheten for passordbeskyttelse. Med follow-me-utskrift sikres det at utskrivingen først skjer når brukeren autentiserer seg ved skriveren.

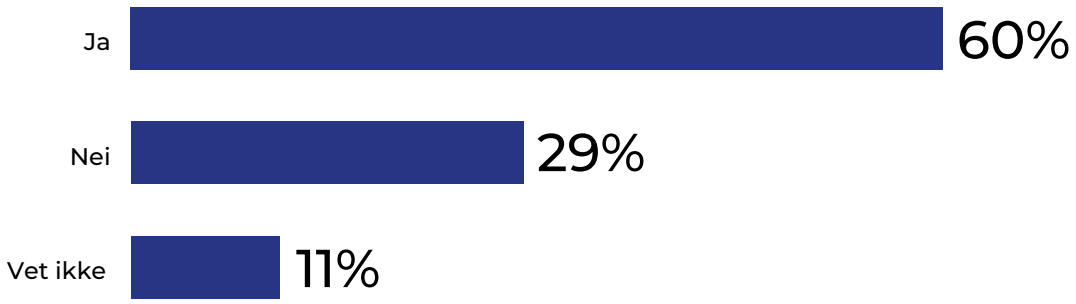
Dette forhindrer uautoriserte brukere i å se, redigere eller skrive ut dokumentet og beskytter informasjonen mot potensielle trusler.

Vil du finne ut mer om Therefore? Besøk vår produktside her!

Scann QR-koden eller klikk her

SPØRSMÅL 7

HAR DIN ARBEIDSPLASS ET OVERBLIKK OVER HVEM SOM PRINTER OG HVA SOM PRINTES?



En børsnyhet har blitt lekket for tidlig. Forretningshemmeligheter har blitt solgt. Konfidensielle dokumenter har blitt skrevet ut. Men hvem står bak?

Dette er alvorlige, men dessverre ikke urealistiske scenarier. Virksomheten rammes spesielt hardt hvis det ikke er mulig å spore hvem som har skrevet ut hva. Bare 60 % er sikre på at de alltid vet hvem som skriver ut, og hva de har skrevet ut.

For de resterende 40 % kan det være en god idé å se nærmere på et system som uniFLOW for å overvåke utskriftsaktiviteter. Med dette systemet mottar virksomheten løpende rapporter, som gir en oversikt over utskrifts-, kopierings-, faks- og skanningsaktiviteter, samt kostnadsoversikt via uniFLOW accounting.

uniFLOW Online-portalen tilbyr ulike illustrerte rapporttyper som kunder kan generere basert på brukerinformasjon, enhetsinformasjon, avdelingsinformasjon eller lokasjon.

De sammenfattede rapportene viser data fra det foregående året, mens andre rapporter viser data fra de siste seks månedene.

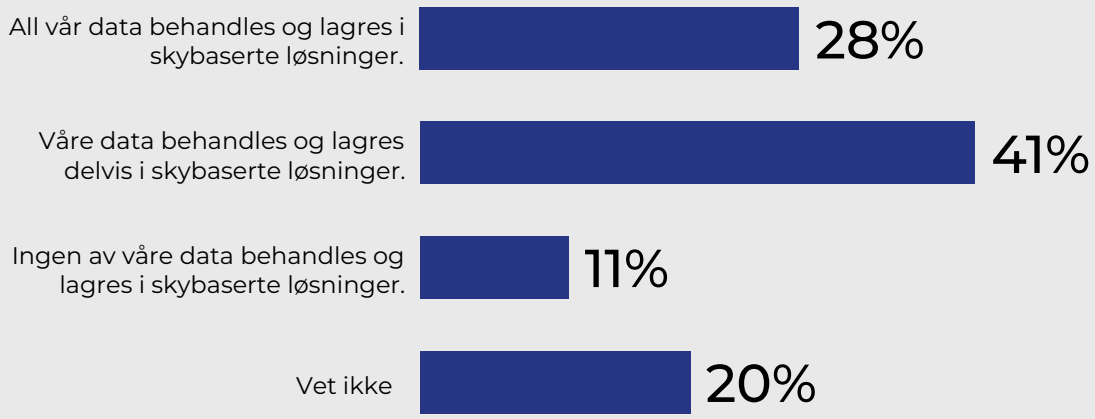
Mer om uniFLOW:
Virksomheter bør ha en generell oversikt over hvem og hva som skrives ut av flere viktige grunner. Blant annet kan implementeringen av passende tilgangskontroll og sikkerhetstiltak sikre konfidensialiteten til utskrevne dokumenter.

Med en Follow Me-løsning for utskrifts-administrasjon forhindres uautorisert tilgang til utskrevne dokumenter, og informasjonens konfidensialitet beskyttes.

Les mer her

SPØRSMÅL 7

I HVILKET OMFANG BEHANDLES OG OPPBEVARES ARBEIDSPLASSENS DATA I SKY-BASERTE LØSNINGER?



69% av de spurte virksomhetene behandler og lagrer data i sky-baserte løsninger. Det gir naturligvis virksomhetene en lang rekke fordeler, som skalerbarhet, lavere omkostninger, sikkerhet mot nedetid, mobilitet og mulighet til å nå data hvor som helst. Det stiller høye krav til IT-sikkerheten, som riktignok ofte også er på et høyt nivå hos de fleste skyleverandører.

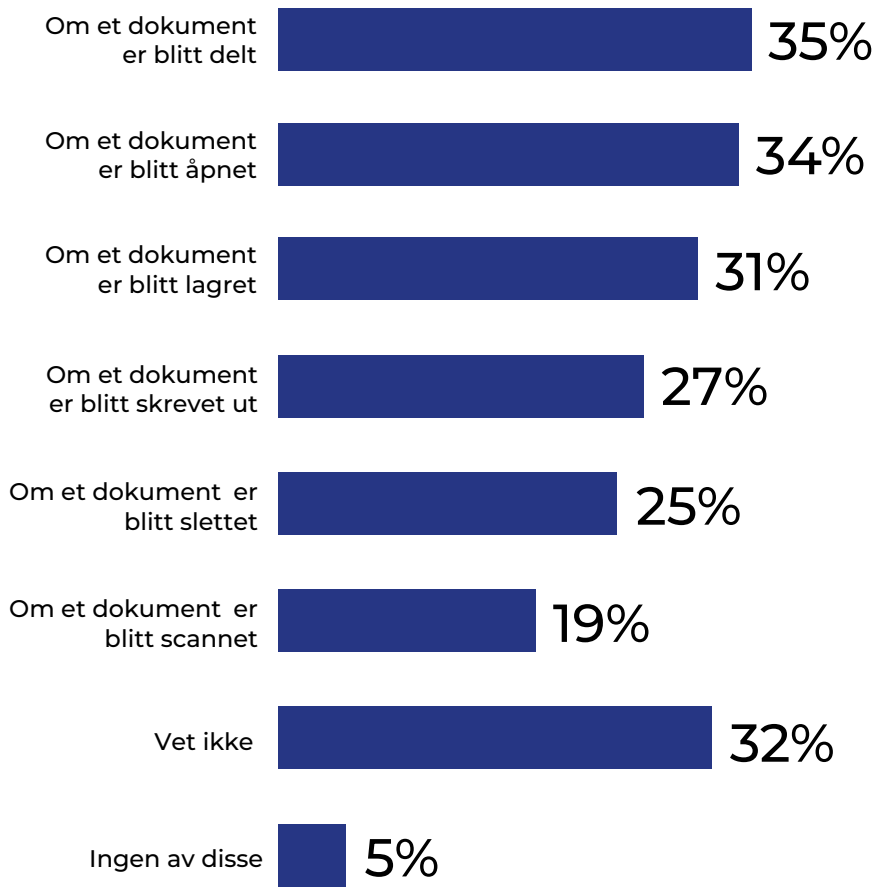
Mange av de samme fordelene oppnår du hvis du flytter print management og dokumenthåndtering til skyen, f.eks. med cloud-løsningen Therefore Online, som gir mulighet til å konfigurere automatiserte policyer som styrer hvem som kan få adgang til dokumenter, og hvordan opplysninger skjermes, deles eller redigeres.

Det betyr, at virksomheter med en ambisjon om en 100% sky-strategi - eller tett på - også kan flytte kritiske data og arbeidsflyter til skyen.

Her ser det ut til, at det blir strategien for mange. Kun 11% har ingen skyløsninger.

SPØRSMÅL 9 – DU KAN VELGE FLERE SVAR

HVILKE AV FØLGENDE OPPLYSNINGER KAN DIN ARBEIDSPLASS SPORE TIL REVISJONSFORMÅL?



Dokumentovervåkning og -håndtering fremstår som en betydelig utfordring for virksomhetene som deltok i undersøkelsen. Mer enn 65 % mangler oversikt over om et dokument har blitt delt, åpnet, arkivert, skrevet ut, slettet eller skannet. Dette etterlater virksomhetene i en situasjon hvor de ikke kan avgjøre eller dokumentere hvem som har hatt tilgang til informasjon som kanskje skulle ha vært konfidensiell. Derfor har de heller ikke mulighet til å reagere raskt på mistenkelig oppførsel.

Hvis dokumentene er lagret forskjellige steder i virksomheten på filservere, intranett eller i skybaserte løsninger, vil oppgaven også være nesten umulig. Det kan også være ulike varianter og versjoner av det samme dokumentet som man ikke kan holde styr på eller kontrollere tilgangen til.

For å adressere disse utfordringene, er en dokumenthåndteringsløsning nødvendig. Med en slik løsning vil virksomheten være i stand til å overvåke alle de nevnte dokumentaktivitetene, hvilket til syvende og sist sikrer at man effektivt kan beskytte sensitive data og minimere risikoen for datalekkasjer.

SPØRSMÅL 10 – DU KAN VELGE FLERE SVAR

HVILKE AV FØLGENDE AUTOMATISERTE PROSESSER HAR DIN ARBEIDSPLASS IMPLEMENTERT?

GDPR er et omfattende arbeid. Det krever mange ressurser å sikre at alle regler følges, at personsenitive opplysninger ikke kompromitteres, og at data slettes hvis de ikke brukes, eller kan slettes hvis personen ønsker det.

Heldigvis finnes det systemer som kan automatisere mange av de GDPR-relaterte oppgavene i forbindelse med dokument- og datahåndtering, slik at du unngår manuelle prosesser og kan sove trygt om natten med vissheten om at loven overholdes.

Likevel indikerer undersøkelsen at en stor del av virksomhetene ennå ikke har tatt skrittet til å investere i disse automatiserte løsningene.

Overraskende nok påpeker 11 % av dem at de fortsatt stoler på manuelle metoder. Mellom 21 % og 33 % angir at de har investert i teknologier som adresserer noen eller alle av de tidligere nevnte utfordringene.

Automatisering av prosesserer en måte å frigi tid og ressurser på som kan brukes mer produktivt andre steder. Håndtering av sensitive data i overensstemmelse med GDPR er en av prosessene mange finner kompliserte og tidkrevende.

Med Canon kan du være sikker på at all data blir fjernet fra gamle enheter- det gir en ting mindre å bekymre seg over!

› Find ut hvordan her

KONKLUSJON

IT-sikkerhet er på agendaen overalt. Cyberkriminelle og spionasje utgjør en stor trussel. Center for Cyber Security sier trusselen er "svært høy". Dokumentstyring, som inkluderer både utskrift og skanning, er en integrert del av mange bedrifters IT-landskap. Dermed er de også potensielt sårbare for cyberangrep og risikoen for for datalekkasjer. For å sikre overholdelse og beskyttelse, må bedriftens informasjonssikkerhetsstrategi dekke hele dokumentets livssyklus:

- Overvåkning av brukeraktiviteter og dokumenthåndtering i forbindelse med utskrift.
- Garanti for at skannede dokumenter når deres tiltenkte destinasjon uten lekkasjer.
- Datasikring og korrekt håndtering av sensitive opplysninger i samsvar med gjeldende regler.
- Sørge for at all utgående kommunikasjon, inkludert dokumenter og data, håndteres sikkert.

Ifølge undersøkelsen er beskyttelsen av dokumenter og data en betydelig utfordring. Dette bekreftes av 59 % av respondentene som deltok. Selv om et betydelig antall har implementert multifaktorautentisering, kryptering, og SIEM, er det ikke alle som har tatt disse skrittene. Dette er spesielt tydelig når det gjelder dokumenter utskrift og skanning; kun omtrent en fjerdedel oppnår et høyt sikkerhetsnivå på disse områdene. Som et resultat av dette er mange bedrifter ennå ikke nær en Zero Trust- tilnærming innen informasjonssikkerhet. Faktisk har kun 33 % innført denne tilnærmingen.

Når det gjelder dokumentsikkerhet, er det stadig rom for forbedring. Omtrent 60 % har oversikt over hvem som skriver ut og innholdet av det som skrives ut. Men kun omtrent en tredjedel har kapasiteten til å overvåke ytterligere handlinger med dokumentene – som for eksempel hvis de åpnes, deles, slettes eller skannes.

GDPR kan ingen unngå, men mange gjør oppgaven mer besværlig for seg selv ved å holde fast ved manuelle prosesser fremfor å benytte en automatisert løsning som blant annet håndterer 'retten til å bli glemt'.

Overordnet sett er det helt klart at deltagerne har fokus på IT-sikkerhet. Likevel ser det ut til at sikkerheten rundt dokumenter, utskrift og skanning ofte ligger et skritt bak. I praksis kan dette etterlate en åpen dør for cyberkriminelle, og samtidig kan bedriften risikere å ikke overholde GDPR-reglene.

Vil du vite mer om hvordan Canons løsninger kan hjelpe deg med sikkerhet og compliance i deres organisasjon?

› Les mer her