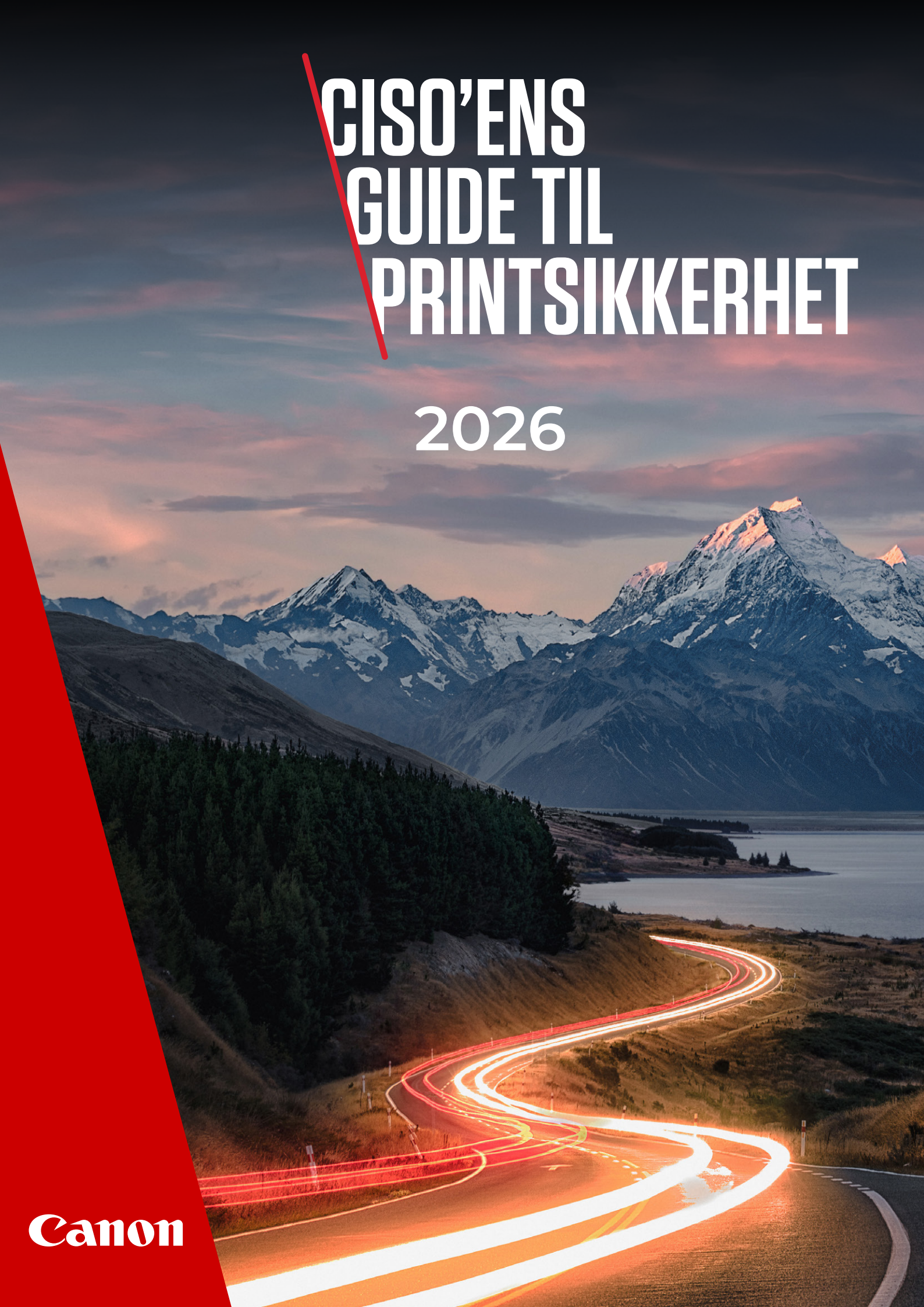
CISO'ENS GUIDE TIL PRINTSIKKERHET

2026



Canon

FORORD

I en tid der digitalisering og trusler mot cybersikkerheten utvikler seg i rekordfart, er det avgjørende at vi ikke overser de fysiske komponentene i vår digitale hverdag. Printere og multifunksjonsenheter er ikke lenger bare kontorverktøy – de er integrerte deler av vår IT-infrastruktur, og dermed også en del av vår sikkerhetsstrategi.

Denne guiden er et viktig bidrag til å styrke bevisstheten og kompetansen rundt printsikkerhet. Den gir CISO'er og sikkerhetsansvarlige et solid rammeverk for å forstå, vurdere og håndtere risikoer knyttet til utskriftsmiljøet – et område som ofte blir undervurdert, men som kan utgjøre en betydelig sårbarhet.

Vi står overfor skjerpede regulatoriske krav, som NIS2 og DORA, og et trusselbilde som krever at vi tenker helhetlig og proaktivt. Printsikkerhet handler ikke bare om teknologi – det handler om kultur, ledelse og ansvar. Det handler om å beskytte verdier, tillit og samfunnets robusthet.

Jeg vil takke alle som har bidratt til denne guiden, og oppfordrer ledere på alle nivåer til å ta printsikkerhet på alvor. Ved å gjøre det, styrker vi ikke bare vår egen virksomhet – vi bidrar også til et tryggere og mer motstandsdyktig Norge.

Erik Mikalsen
Adm Dir
Canon Norge

FORMÅL MED GUIDEN

Denne guiden er utviklet for å gi CISO'er (Chief Information Security Officers) og sikkerhetsledere et strategisk og praktisk rammeverk for printsikkerhet, i et stadig mer komplekst cybersikkerhetslandskap. I en tid preget av økende digitalisering, avanserte trusler og skjerpede regulatoriske krav, er det avgjørende å ha en helhetlig tilnærming til printsikkerhet som beskytter virksomheten og muliggjør innovasjon.

Sammendrag

Cybersikkerhetslandskapet er i rask utvikling, drevet av teknologiske fremskritt, endrede trusselaktører, og nye måter for jobb og samhandling digitalt. For å være i forkant må CISO'er forstå og forholde seg til de mest sentrale trendene som former sikkerhets-strategier frem mot 2026 og videre.

Blant de viktigste utviklingstrekkene er:

Kunstig intelligens og maskinlæring: Brukes både til å styrke forsvar (f.eks. trussel deteksjon, automatisert respons) og av angripere (f.eks. KI-genererte phishing-angrep og deepfakes).

Zero Trust-arkitektur: Et paradigmeskifte fra perimeterbasert sikkerhet, til kontinuerlig verifisering og minste privilegium.

Sikkerhet i sky og multisky-miljøer: Økt kompleksitet krever nye tilnærminger til synlighet, tilgangsstyring og konfigurasjonssikkerhet.

Regulatorisk utvikling: Nye lover og standarder, som EUs NIS2 regulativ og DORA-forordningen og skjerpede krav til rapportering av sikkerhets-hendelser, påvirker hvordan sikkerhet må bygges og dokumenteres.

Styrket samarbeid mellom IT, ledelse og styret, bidrar til en sikkerhetskultur forankret i hele organisasjonen. Ved å kombinere strategisk innsikt med operasjonelle anbefalinger, skal denne guiden fungere som et verktøy for planlegging, implementering og kontinuerlig forbedring av virksomhetens sikkerhets-arbeid.

Les også om informasjonssikkerhet på canon.no

INNHOLD

DEL 1: CISO'ENS TANKER OM SIKKERHETSUTFORDRINGER I 2026 AV QUENTYN TAYLOR, CISO CANON EMEA

Som leder for informasjonssikkerhet er det ofte lett å glemme skriverne i organisasjonen din og risikoen de forårsaker for informasjonssikkerheten. Ofte administreres ikke skriveren engang av IT-teamet, og til tross for de betydelige mengdene informasjon som flyter gjennom den, er det svært ofte man neglisjerer sikkerheten til disse enhetene.

Hvis vi tenker på hva en skriver er, er det grensen mellom det fysiske og det digitale. Data overføres fra å være digital til fysisk papir, og data som er på papiret overføres til digitalt format. I tillegg skriver vi ut eller skanner dokumenter som er viktige. Skriveren blir derfor en dataakkumulator med enorme mengder sensitive data, data som passerer gjennom den og data som lagres på den.

Hvis vi ser på noen av angrepene som har skjedd de siste årene, ser vi ikke angrep som bruker KI og kvantedatabehandling, men vi ser angrep som fokuserer utelukkende på det grunnleggende. Mange angrep er avhengige av stjålne legitimasjonsopplysninger, der angriperen ganske enkelt kjøper logg-ons fra det mørke nettet og deretter bruker de til å kompromittere offerbedriften. I tillegg finner vi ofte angrep som bruker uovervåkede maskiner som er koblet til Internett. Det er synd, men vi ser fortsatt skrivere som er koblet til Internett og som ikke er konfigurert, og som representerer en betydelig risiko for bedrifter.

Jeg anbefaler alltid at bedrifter ikke bare har en veldig god oversikt over perimeternettverket sitt ved å bruke et av verktøyene med åpen kildekode som finnes der ute på Internett, men også forstår at skriverne deres er en del av sikkerhetsstrukturen deres, og hvis de ikke er konfigurert, kan de være en risiko, men hvis de er riktig konfigurert, kan de forbedre sikkerheten til dataene dine og bedriften din betraktelig.

Som leder for intern informasjonssikkerhet og produktsikkerhet hos Canon, liker jeg å sørge for at alle lærdommene vi lærer internt, også gis til kundene våre. Mange, om ikke alle, av utskriftssikkerhetstjenestene du ser hos Canon, er enten konseptualisert internt eller brukes internt i Canon for å beskytte kundenes data i dag og hver dag. Produktsikkerhetsteamet og det interne sikkerhetsteamet jobber i harmoni for å gi det aller beste nivået av informasjonssikkerhet, ikke bare for våre egne data, men også for kundene våre og for produktene våre.

Hva er printsikkerhet?

Printsikkerhet handler om å beskytte informasjon som behandles gjennom utskriftsenheter; printere, skannere, kopimaskiner og multifunksjonsmaskiner. Dette inkluderer digital og fysisk sikkerhet knyttet til dokumenter som skrives ut, skannes og/eller kopieres. I mange virksomheter er slike enheter en integrert del av IT-infrastrukturen, men de blir ofte oversett når det gjelder sikkerhetstiltak.

I dag er printere langt mer avanserte enn tidligere. De er koblet til nettverk, har egne operativsystemer, og kan lagre data lokalt. Dette gjør dem sårbare for både interne og eksterne trusler. Eksempler på slike trusler inkluderer:

Uautorisert tilgang til utskrifter: Dokumenter som blir liggende i utskriftskuffen kan enkelt plukkes opp av feil person.

Datainnbrudd via printere: Hackere kan utnytte sårbarheter i printerens programvare for å få tilgang til hele nettverket.

Manglende sletting av lagrede data: Mange printere lagrer dokumenter på interne harddisker. Hvis disse ikke slettes sikkert, kan sensitiv informasjon bli gjen-opprettet.

Feilkonfigurerte nettverksprintere: Uten riktig tilgangskontroll kan hvem som helst sende utskrifter til en printer, eller hente dokumenter fra den.

Printsikkerhet er spesielt viktig i bransjer som håndterer sensitiv informasjon, som helsevesen, finans, offentlig sektor og juridiske tjenester. Et sikkerhetsbrudd kan føre til alvorlige konsekvenser, som brudd på personvernlovgivning (for eksempel GDPR), økonomiske tap, tap av tillit og skade på omdømmet.

Hva kan man gjøre for å oppnå god printsikkerhet?

For å sikre en trygg og robust utskriftsinfrastruktur, må virksomheter implementere en rekke tekniske og organisatoriske tiltak. Her er noen av de viktigste:

1. Sikker utskrift (pull printing)

Dette innebærer at brukeren må autentisere seg ved printeren – for eksempel med ID-kort, PIN-kode eller mobilapp – før dokumentet faktisk skrives ut. Dette forhindrer at dokumenter blir liggende i utskriftsskuffen og plukket opp av uvedkommende.

2. Kryptering av data

All kommunikasjon mellom datamaskiner og printere bør være kryptert. Dette gjelder både data som sendes til utskrift og data som lagres midlertidig på printerens interne lagring. Kryptering beskytter informasjonen mot avlytting og manipulering.

3. Tilgangskontroll og autentisering

Printere bør være konfigurert slik at kun autoriserte brukere har tilgang til bestemte funksjoner. For eksempel kan man begrense hvem som får skrive ut i farger, skanne til e-post eller bruke USB-porter.

4. Sletting av lagrede data

Printere med intern lagring bør ha funksjoner for automatisk sletting av midlertidige filer etter bruk. Ved avhending eller utskifting av enheter bør harddiskene slettes på en sikker måte eller fysisk destrueres.

5. Programvareoppdateringer og sikkerhetsoppdateringer

Produsenter av printere utgir jevnlig oppdateringer for å tette sikkerhetshull. Det er viktig å holde enhetene oppdatert for å beskytte mot kjente sårbarheter.

6. Overvåking og logging

Ved å loggføre utskriftsaktivitet kan man oppdage uvanlig bruk, som store utskriftsmengder utenfor arbeidstid eller forsøk på å skrive ut sensitive dokumenter. Dette gir også sporbarhet ved sikkerhetsbrudd.

7. Opplæring av ansatte

Menneskelige feil er ofte den største sikkerhetsrisikoen. Ansatte bør få opplæring i håndtering av konfidensielle dokumenter, hvordan de bruker sikre utskriftsløsninger, og hva de skal gjøre hvis de oppdager mistenkelig aktivitet.

8. Sikker avhending av utskrifter

Dokumenter som ikke lenger er nødvendige, bør makuleres eller destrueres på en sikker måte. Å kaste sensitive papirer i vanlig søppel kan føre til datalekkasjer og brudd på lovverk som GDPR.

Hvordan KI og SIEM kan styrke printsikkerheten

Både KI (kunstig intelligens) og SIEM (Security Information and Event Management) kan spille en viktig rolle i å styrke printsikkerheten. Vi har sett på hvordan de fungerer, hvor krevende det er å ta i bruk, og hvilke fordeler det kan gi.

Kunstig intelligens (KI)

KI kan brukes til å analysere utskriftsmønstre og oppdage unormal aktivitet. Eksempler:

Anomalideteksjon: KI kan lære hva som er ”normal” utskriftsatferd for en bruker eller avdeling, og varsle hvis noen plutselig skriver ut store mengder dokumenter, sensitive filer utenfor arbeidstid, eller fra uvanlige lokasjoner.

Prediktiv analyse: Ved å analysere historiske data kan KI forutsi risikoer og foreslå tiltak før et sikkerhetsbrudd skjer.

Automatisert respons: KI kan kobles til sikkerhetssystemer for å automatisk blokkere eller begrense tilgang hvis mistenkelig aktivitet oppdages.

SIEM-systemer

SIEM samler inn og analyserer logger fra ulike enheter – inkludert printere – i sanntid. Dette gir:

Sentralisert overvåking: Alle hendelser knyttet til utskrift, autentisering og nettverkstilgang loggføres og analyseres.

Krysskorrelasjon: SIEM kan koble sammen hendelser fra printere med annen IT-infrastruktur (f.eks. innlogginger, filtilgang), og dermed oppdage mer komplekse angrepsmønstre.

Varsling og rapportering: Ved avvik eller brudd på policyer kan SIEM sende varsler til IT-avdelingen og generere rapporter for revisjon og etterforskning.

Er det vanskelig å ta i bruk KI og SIEM?

Det kommer an på organisasjonens størrelse og modenhet:

For små og mellomstore bedrifter: Det kan være krevende å implementere KI og SIEM fra bunnen av, men det finnes skybaserte og brukervennlige løsninger som krever lite teknisk kompetanse.

For større virksomheter: Disse teknologiene kan integreres med eksisterende IT-sikkerhetsinfrastruktur, men krever ofte dedikert IT-personell og god planlegging.

Fordeler med å bruke KI og SIEM i printsikkerhet

- Tidlig varsling av trusler
- Du kan oppdage og reagere på sikkerhetsbrudd før de får alvorlige konsekvenser
- Redusert menneskelig feil
- Automatisering reduserer risikoen for at ansatte overser viktige hendelser
- Bedre etterlevelse av regelverk
- SIEM gir dokumentasjon og sporbarhet som er nyttig ved revisjoner og for å overholde GDPR og andre krav
- Effektiv ressursbruk
- KI og SIEM kan håndtere store datamengder raskt og effektivt, noe som sparer tid og ressurser
- Forbedret innsikt og kontroll
- Du får bedre oversikt over hvordan printere brukes, og kan optimalisere både sikkerhet og drift

DEL 2: HVORFOR ER PRINTSIKKERHET ET STADIG VIKTIGERE OMRÅDE?

I en tid hvor digitalisering og cybersikkerhet står høyt på agendaen, er det lett å glemme at fysiske dokumenter og utskriftsenheter fortsatt utgjør en betydelig sikkerhetsrisiko. Printsikkerhet er beskyttelse av informasjon som behandles via printere, skannere og kopimaskiner – og det har blitt et stadig viktigere område av flere grunner:

1. Økt digital kompleksitet og nettverkstilkobling

Moderne printere er ikke enkle maskiner. De er avanserte, nettverkstilkoblede enheter med egne operativsystemer, lagringskapasitet og tilgang til skybaserte tjenester. Dette gjør dem til potensielle inngangspunkter for cyberangrep, på lik linje med datamaskiner og servere. Uten riktig sikring kan en printer bli brukt til å hente ut sensitiv informasjon eller til å spre skadevare i et nettverk.

2. Strengere krav til personvern og datasikkerhet

Med innføringen av personvernforordningen GDPR i 2018, har virksomheter fått et større ansvar for å beskytte personopplysninger – også når de behandles fysisk. En glemt utskrift i en felles printer kan være et brudd på regelverket, med potensielle bøter og omdømmetap som konsekvens. Printsikkerhet er derfor ikke bare et teknisk spørsmål, men også et juridisk og etisk ansvar.

3. Økende mengde sensitiv informasjon i omløp

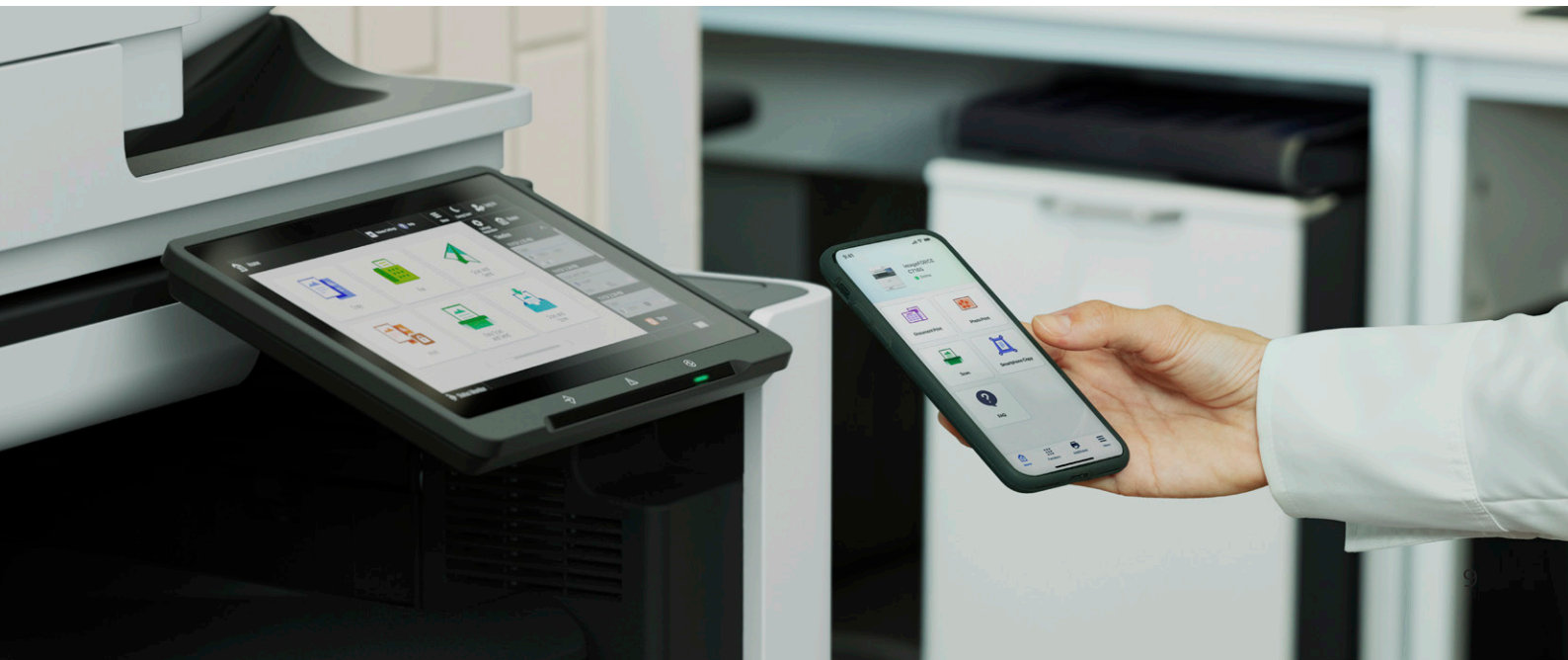
Virksomheter håndterer i dag store mengder konfidensiell informasjon – alt fra kundedata og kontrakter, til helseopplysninger og interne strategidokumenter. Når slike dokumenter skrives ut, skannes eller kopieres, må det sikres at de ikke havner i feil hender. Dette gjelder i kontormiljøer og i hjemmekontorsituasjoner, hvor kontrollen ofte er svakere.

4. Flere hybride og desentraliserte arbeidsformer

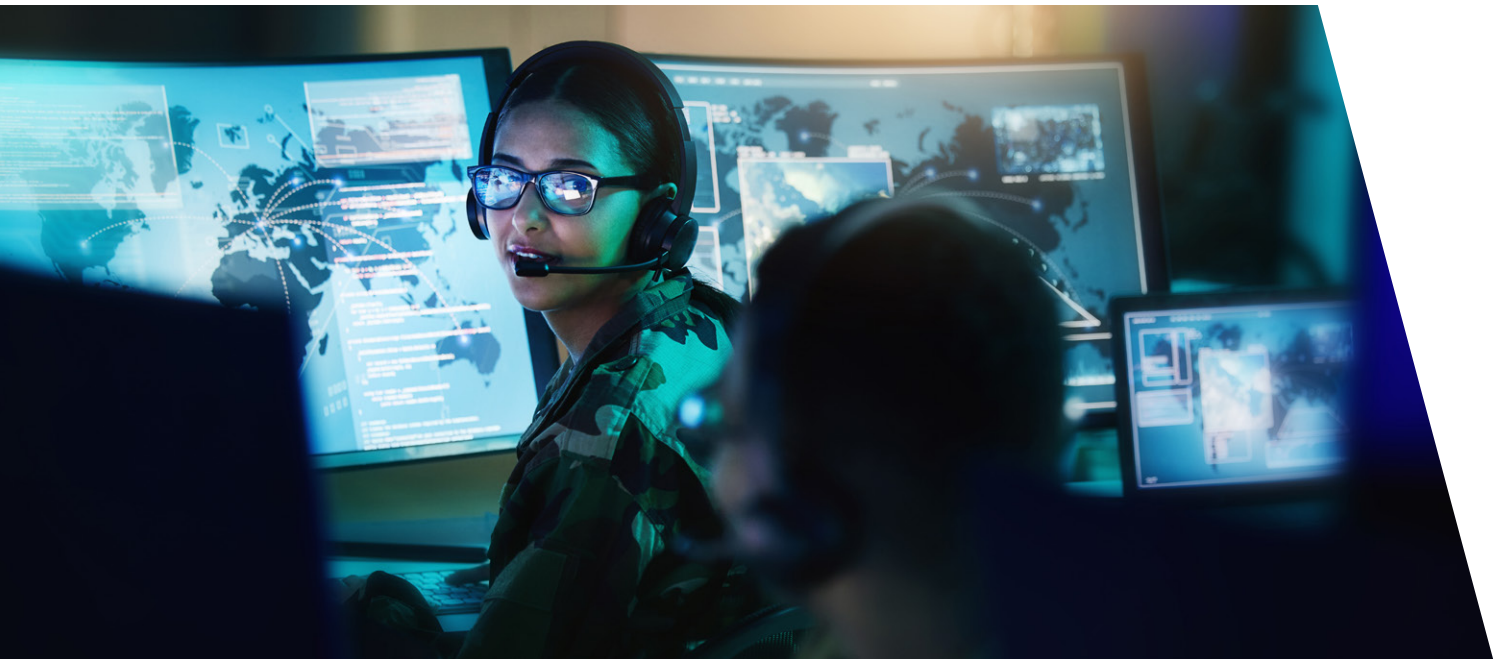
Etter pandemien har mange organisasjoner gått over til hybride arbeidsmodeller. Dette har ført til økt bruk av mobile og skybaserte utskriftsløsninger, som øker risikoen for at dokumenter blir sendt til feil enhet, lagret usikkert eller glemt i en felles printer. Printsikkerhet må derfor tilpasses en mer fleksibel og desentralisert arbeidshverdag.

5. Målrettede angrep og avanserte trusler

Cyberkriminelle blir stadig mer sofistikerte, og printere har i flere tilfeller blitt brukt som inngangsport for angrep. Eksempler inkluderer utnyttelse av sårbarheter i printerens programvare, eller sosial manipulering der ansatte lures til å skrive ut eller hente ut sensitiv informasjon. Printsikkerhet handler om å beskytte seg mot avanserte trusler og målrettede angrep.



Zero Trust



Zero Trust er et buzz-word de fleste har fått med seg når vi snakker om sikkerhet, men hva betyr det?

Zero Trust er en sikkerhetsmodell som bygger på prinsippet om at ingen – verken brukere, enheter eller systemer – skal stoles på automatisk, selv om de befinner seg innenfor organisasjonens nettverk. I stedet må alle forespørsler om tilgang verifiseres kontinuerlig basert på identitet, kontekst og risiko. Dette prinsippet er svært viktig for å styrke print-sikkerheten.

Tradisjonelt har printere blitt sett på som "trygge" enheter innenfor det interne nettverket. I en Zero Trust-tilnærming behandles også printere som potensielle risikoelementer. Dette innebærer at tilgang til utskriftsfunksjoner må kontrolleres og overvåkes på samme måte som tilgang til sensitive systemer og data. Ved å anvende Zero Trust-prinsipper på utskriftsmiljøet, reduseres risikoen for datalekkasjer, misbruk og uautorisert tilgang. Det gir en mer robust og fremtidsrettet tilnærming til print-sikkerhet – spesielt i en tid med økende trusler og hybride arbeidsformer.

Slik kan Zero Trust brukes for å ivareta printsikkerhet:

Autentisering før utskrift: Brukere må identifisere seg (f.eks. med ID-kort eller tofaktorautentisering) før de får tilgang til å skrive ut dokumenter. Dette hindrer uautorisert tilgang.

Minimering av tilgang: Brukere får kun tilgang til de printerne og funksjonene de faktisk trenger, basert på rolle og behov.

Kontinuerlig overvåking: All utskriftsaktivitet logg-føres og analyseres for å oppdage unormal atferd, som store utskriftsmengder eller forsøk på å skrive ut sensitive dokumenter.

Segmentering av nettverk: Printere plasseres i egne nettverkssoner med begrenset tilgang, slik at de ikke kan brukes som inngangsport til resten av systemet.

Veien videre for CISO'er

For å lykkes med Zero Trust i praksis, bør CISO'er:

- Starte med identitet: Etabler sterk autentisering og sentralisert tilgangsstyring.
- Prioritere synlighet: Skaff oversikt over alle brukere, enheter og applikasjoner.
- Bygge bro mellom IT og forretning: Knytt Zero Trust-tiltak til forretningsrisiko og regulatoriske krav.
- Bruke etablerte rammeverk: Følg anbefalinger fra f.eks. NIST SP 800-207 og ENISA.

Zero Trust er ikke et produkt – det er en kontinuerlig prosess. En moden tilnærming gir ikke bare bedre sikkerhet, men også større fleksibilitet og tillit i en mer digital og distribuert verden.

Windows Protected Print

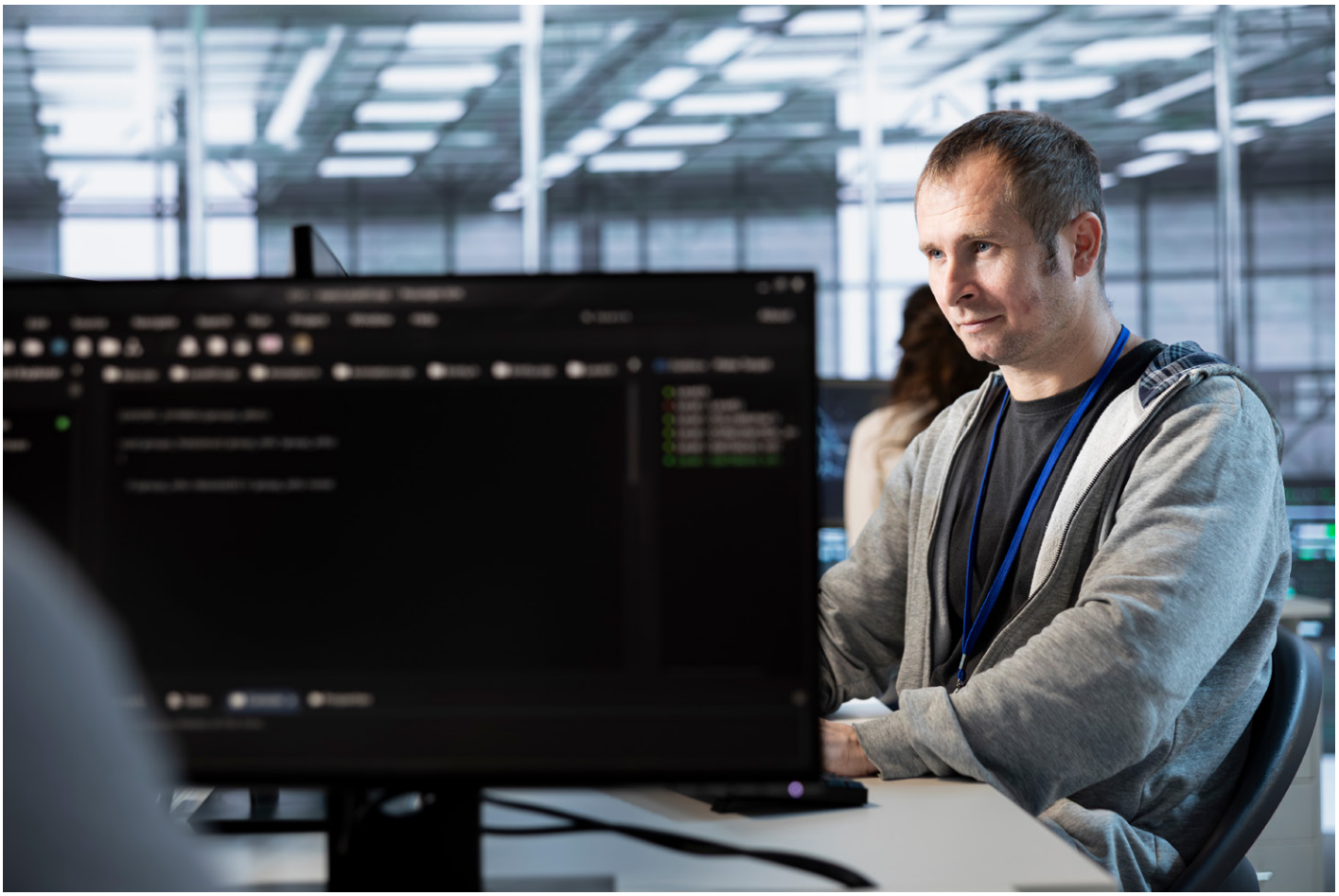
Vi kan ikke snakke om printsikkerhet uten å nevne Windows Protected Print som er på vei inn.

Windows Protected Print Mode (WPP) er en ny funksjon som forbedrer sikkerheten ved utskrift ved å eliminere behovet for tredjeparts drivere, noe som reduserer risikoen for sikkerhetssårbarheter. WPP forenkler administrasjonen ved å bruke en universell driver og er kompatibel med de fleste moderne skrivere som er Mopria-sertifiserte. Dette gjør utskriftsprosessen enklere og mer pålitelig. En utfordring kan være at eldre skrivere som ikke er Mopria-sertifiserte, kanskje ikke støttes. WPP er allerede tilgjengelig i de nyeste versjonene av Windows (Windows 11 H2), og kan aktiveres via innstillingene for skrivere og skannere. Ved å implementere WPP kan virksomheter sikre et tryggere og mer effektivt utskriftsmiljø. Vær obs på at ved å aktivere WPP vil de tradisjonelle skriverdriverne ikke lenger fungere, og det kan bety at de eksisterende sikkerprint løsningene ikke lenger vil fungere. Snakk med printleverandøren før dere aktiverer WPP funksjonen, for har dere først aktivert det, så kan det ikke skrus av igjen.

Dette gjelder alle printere, uavhengig av merke. Det betyr at hver leverandør må utvikle sin egen app som ivaretar de funksjonalitetene dere har i dag, f.eks stifting, bretting, valg av papirskuff etc. Dette begynte i juli 2025, og vil være standard i 2027, så det er viktig å forberede seg nå.

***Hva er Mopria?**

Mopria er en teknologi som gjør det enkelt å skrive ut eller skanne fra en hvilken som helst Mopria-sertifisert enhet uten å måtte installere ekstra programvare eller drivere. Det fungerer med mange moderne skrivere og skannere, og er integrert i mange Android-enheter og Windows-systemer. Dette gjør utskrift og skanning raskt og enkelt, uansett hvor du er.



DEL 3: PERSONVERNSPERSPEKTIVET

Vi må ikke glemme viktigheten av personvern når vi snakker om printsikkerhet. Her er det flere viktige hensyn som må tas for å sikre at sensitive og personlige opplysninger ikke kommer på avveie.

1

Beskyttelse av personopplysninger

Utskrifter kan inneholde navn, adresser, fødselsnumre, helse-opplysninger, lønnsdata og annen sensitiv informasjon. Hvis slike dokumenter blir liggende i printeren eller havner i feil hender, kan det utgjøre et brudd på personvernlovgivningen.

2

Dokumentkontroll og sporbarhet

Det må være mulig å dokumentere hvem som har skrevet ut hva, når og hvor. Dette gir sporbarhet og ansvarlighet, og er viktig ved revisjoner eller ved mistanke om brudd på personvernet.

3

Tilgangsstyring

Bare autoriserte personer skal kunne skrive ut eller hente dokumenter med personopplysninger. Dette krever autentisering ved skriveren (f.eks. med ID-kort eller PIN-kode) og rollebasert tilgang til utskriftsfunksjoner.

4

Sikker behandling av dokumenter

Personopplysninger på papir må behandles like sikkert som digitale data. Det betyr at dokumenter som ikke lenger trengs, må makuleres eller destrueres på en sikker måte – ikke kastes i vanlig søppel.

5

Sikker lagring og sletting

Mange printere lagrer dokumenter midlertidig. Det er viktig at disse slettes automatisk etter bruk, og at enhetene er konfigurert til å ikke lagre sensitive data unødvendig.

6

Etterlevelse av regelverk

Virksomheter må kunne vise at de har iverksatt tekniske og organisatoriske tiltak for å beskytte personopplysninger – også i utskriftsmiljøet. Dette er et krav i GDPR og andre relevante lover.

DEL 4: DORA – DIGITAL OPERATIONAL RESILIENCE ACT

I CISO-guiden for 2026 retter vi blikket mot DORA-forordningen – Digital Operational Resilience Act. DORA trådte i kraft allerede 17. januar 2025, men har ikke fått like mye oppmerksomhet som NIS2. Likevel representerer begge regelverkene ikke bare regulatoriske utfordringer, men også muligheter for å styrke og forbedre printsikkerheten.

For å forstå forskjellen mellom de to regelverkene er det viktig å merke seg at NIS2 er et direktiv, mens DORA er en forordning. Dette har betydning for hvordan de implementeres og håndheves i EU-landene. (Se tabell for sammenligning.)

Forordning (Regulation)

Gjelder direkte i alle EU/EØS-land uten at nasjonale myndigheter trenger å vedta egne lover.

Har umiddelbar rettskraft – altså samme virkning som en nasjonal lov.

Eksempel: DORA-forordningen er en EU-forordning som gjelder direkte i hele EU (og EØS etter tilpasning).

Fordel: Ensartet regelverk i hele EU.
Ulempe: Mindre fleksibilitet for nasjonale tilpasninger.

Direktiv (ofte kalt regulativ i dagligtale)

Setter mål som medlemslandene må oppnå, men landene velger selv hvordan de vil gjennomføre det i nasjonal lovgivning.

Må implementeres gjennom nasjonale lover innen en gitt frist.

Eksempel: GDPR startet som et direktiv før det ble en forordning.

Fordel: Gir rom for nasjonale tilpasninger.

Ulempe: Kan føre til ulik praksis mellom land.

DORA er en EU-forordning som trådte i kraft 17. januar 2025. Målet med forordningen er å styrke den digitale operasjonelle motstandsdyktigheten i finanssektoren. Dette inkluderer evnen til å motstå, håndtere og komme seg etter IKT-relaterte hendelser som cyber-angrep, systemfeil og datalekkasjer.

DORA omfatter:

- Banker, forsikringsselskaper, verdipapirforetak og andre finansinstitusjoner
- Betalingsforetak og e-pengeforetak
- Kritiske IKT-leverandører til finanssektoren, som datasentre, skytjenester og IT-driftspartnere
- Norge implementerte DORA gjennom EØS-avtalen som ny Lov om digital operasjonell motstandsdyktighet. Denne ble vedtatt av Stortinget og trådte i kraft 1. juli 2025

DORA stiller krav innen fem hovedområder:

- IKT-risikostyring – systematisk identifisering og håndtering av digitale risikoer
- Hendelseshåndtering og rapportering – krav til varsling og dokumentasjon av IKT-hendelser
- Testing av digital motstandsdyktighet – jevnlig sikkerhetstesting og simuleringer
- Tredjepartsrisiko – strengere krav til styring av IKT-leverandører
- Informasjonsdeling – samarbeid om trussel-informasjon og beste praksis

Hvordan er dette relevant for printsikkerhet?

Selv om printere ikke nødvendigvis nevnes eksplisitt, omfattes de av DORA dersom de:

- Er koblet til nettverk og behandler sensitiv informasjon
- Leveres som en del av en IKT-tjeneste til finansinstitusjoner
- Kan utgjøre en risiko for digital operasjonell motstandsdyktighet

Eksempler:

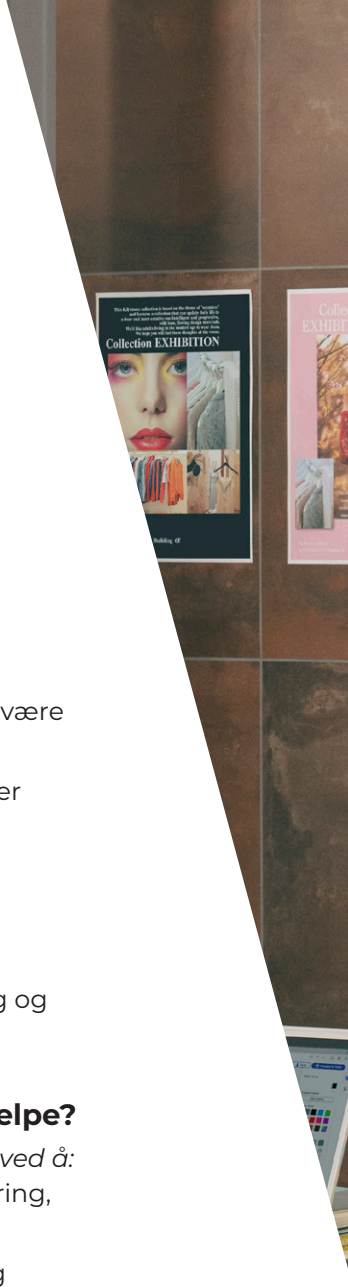
- En kompromittert printer kan gi angripere tilgang til nettverket
- Utskrifter med personopplysninger kan føre til brudd på GDPR.
- Manglende logging og kontroll på utskrifter kan svekke hendelseshåndtering

Hvordan kan printleverandører bidra til å etterleve DORA?

Printleverandører kan bidra til etterlevelse av DORA ved å:

- Tilby sikre utskriftsløsninger med autentisering, logging og kryptering
- Sørge for regelmessige sikkerhetsoppdateringer og sårbarhetstesting
- Dokumentere risikohåndtering og kontinuitetsplaner for sine tjenester
- Tilby sikker sletting av data og sikker avhending av maskinvare
- Delta i trusselinformasjonssamarbeid med kundene

Oppdatering på NIS2 – Digitalsikkerhetsloven



NIS2 (Network and Information Security Directive 2) er et EU-direktiv som bygger videre på det opprinnelige NIS-direktivet fra 2016. Det ble vedtatt i EU i 2022 og skal styrke cybersikkerheten i kritiske og viktige sektorer i hele EU og EØS. I Norge trådte dette i kraft samtidig som CISO'ens Guide til Printsikkerhet 2026 kommer ut - 1. oktober 2025.

Hvor kommer det fra?

- Initiert av EU-kommisjonen som svar på økende digitale trusler
- En del av EUs digitale sikkerhetsstrategi
- I Norge implementeres det gjennom digitalsikkerhetsloven, og arbeidet ledes av Justis- og beredskapsdepartementet, med støtte fra NSM og DSB

NIS2 stiller krav til:

- Risikostyring og sikkerhetstiltak
- Hendelseshåndtering og rapportering (ofte innen 24 timer)
- Sikkerhet i leverandørkjeden
- Ledelsesansvar og styring
- Regelmessige revisjoner og ROS-analyser

Hvem gjelder det for?

Kritiske og viktige sektorer, som:

- Energi, transport, helse, finans, vannforsyning, digital infrastruktur
- Virksomheter med over 50 ansatte og/eller over 10 millioner euro i omsetning
- Leverandører til disse sektorene, inkludert IKT- og printleverandører

Hvordan er det relevant for print?

Printsystemer er ofte:

- Integrert i nettverk og kan være inngangsport for cyberangrep
- Brukerdata og dokumenter som kan være sensitive
- Del av verdikjeden for kritiske tjenester (f.eks. helse, offentlig sektor)

Derfor må printløsninger:

- Ha tilstrekkelig sikkerhetsnivå
- Være overvåket og oppdatert
- Inngå i virksomhetens risikovurdering og hendelseshåndtering

Hvordan kan printleverandører hjelpe?

Printleverandører kan støtte etterlevelse ved å:

- Tilby sikre printløsninger med kryptering, autentisering og logging
- Dokumentere sikkerhetskontroller og oppdateringsrutiner
- Bistå med ROS-analyse og sikkerhets-vurdering av printmiljøet
- Tilby beredskapsplaner og støtte ved hendelser

I NIS2-sammenheng er ROS-analyse:

- Et krav for virksomheter i kritiske sektorer
- Grunnlaget for tilpassede sikkerhetstiltak
- Viktig for å dokumentere etterlevelse og forberede seg på tilsyn

Egenskap	Forordning (Regulation)	Direktiv (Regulativ)
Gjelder direkte?	☑ Ja	☒ Nei
Krever nasjonal lov?	☒ Nei	☑ Ja
Fleksibilitet?	☒ Lav	☑ Høy
Ensartethet?	☑ Høy	☒ Varierer mellom land


Special Sale!

Viktigheten av ROS-analyse

En ROS-analyse (risiko- og sårbarhetsanalyse) er et sentralt verktøy for å identifisere og vurdere trusler knyttet til printsikkerhet. Printere er ofte koblet til nettverk og de kan håndtere sensitive data. Det er avgjørende å forstå hvilke risikoer som finnes – og hvordan de kan håndteres.

Gjennom en ROS-analyse kartlegges hvilke verdier som behandles i utskriftsmiljøet (f.eks. person-opplysninger, kontrakter, helseopplysninger), hvilke trusler som kan påvirke disse (som uautorisert tilgang, datalekkasjer eller tap av dokumenter), og hvilke sårbarheter som finnes i dagens systemer og rutiner. Analysen er et grunnlag for iverksettelse av målrettede tiltak, som for eksempel autentisering ved printer, logging av utskrifter, kryptering av data og opplæring av ansatte. Analysen hjelper din virksomhet med å etterleve krav i regelverk som GDPR, NIS2 eller DORA, og gir dokumentasjon som kan brukes i revisjoner og ved sikkerhetsbrudd.

En ROS-analyse gjør det mulig å gå fra reaktiv til proaktiv sikkerhet. Den gir innsikt, prioritering og trygghet – og er en forutsetning for et sikkert og ansvarlig utskriftsmiljø. En ROS-analyse er en viktig del av bedriftens forretningsplan (Business Continuity Plan, også kalt BCP).

Cyber resilience og forretningsplan (Business Continuity Plan - BCP)

Hvorfor er en ROS-analyse, cyber resilience og en forretningsplan (BCP) relevant for printsikkerhet? Her er hvordan de henger sammen: BCP

BCP handler om å sikre at virksomheten kan opprettholde kritiske funksjoner under og etter en krise – som strømbrudd, cyberangrep eller system-feil. Utskriftsfunksjoner er ofte nødvendige i slike situasjoner, spesielt i helsevesen, finans og offentlig sektor.

Printsikkerhet i BCP-sammenheng innebærer:

- Å ha redundante og sikre utskriftsløsninger tilgjengelig
- Å sikre at sensitive dokumenter ikke går tapt eller havner på avveie under kriser
- Å inkludere printere og dokumenthåndtering i beredskapsøvelser og gjenopprettingsplaner

Cyber resilience handler om en organisasjons evne til å forhindre, oppdage, håndtere og komme seg etter digitale trusler, inkludert angrep, feil og datalekkasjer. Printere og utskriftsmiljøer blir ofte oversett, men de kan være sårbare punkter i IT-infrastrukturen.

Printsikkerhet bidrar til cyber resilience ved å:

- Hindre uautorisert tilgang til sensitive dokumenter
- Oppdage mistenkelig utskriftsaktivitet (f.eks. via SIEM eller KI)
- Redusere risikoen for at printere brukes som inngangsport for cyberangrep
- Sørge for at utskriftsdata ikke kompromitterer resten av nettverket

Printsikkerhet er ikke bare et teknisk tiltak – det er en strategisk del av virksomhetens evne til å stå imot og komme seg etter digitale angrep. Ved å inkludere utskriftsmiljøet i både cyber resilience-strategier og BCP-planer, styrker man helheten i sikkerhets-arbeidet.

DEL 5: NASJONAL SIKKERHET – ET FELLES ANSVAR

Den geopolitiske situasjonen i 2025 er preget av krig i Europa, økt stormaktsrivalisering og sammensatte trusler fra statlige aktører som Russland, Kina og Iran. Ifølge Nasjonal Sikkerhetsmyndighet (NSM) og Politiets Sikkerhetstjeneste (PST) er sabotasje, påvirkning og etterretning reelle og sannsynlige trusler mot Norge. Dette gjelder ikke bare militære mål, men også sivile virksomheter, leverandørkjeder og kritisk infrastruktur.

Rapportene understreker at alle offentlige og private virksomheter har et ansvar for å beskytte sine verdier, og redusere sårbarheter. Dette gjelder spesielt virksomheter som leverer samfunnskritiske tjenester eller inngår i totalforsvaret. Trusselaktører vil ofte angripe via "svake ledd", som små leverandører eller underleverandører – og her kan selv en printer utgjøre en inngangsport.

Printsikkerhet som del av nasjonal sikkerhet

I en digitalisert hverdag er printere og multifunksjons-maskiner koblet til nettverk, de lagrer data og håndterer sensitiv informasjon. Hvis slike enheter ikke sikres, kan de:

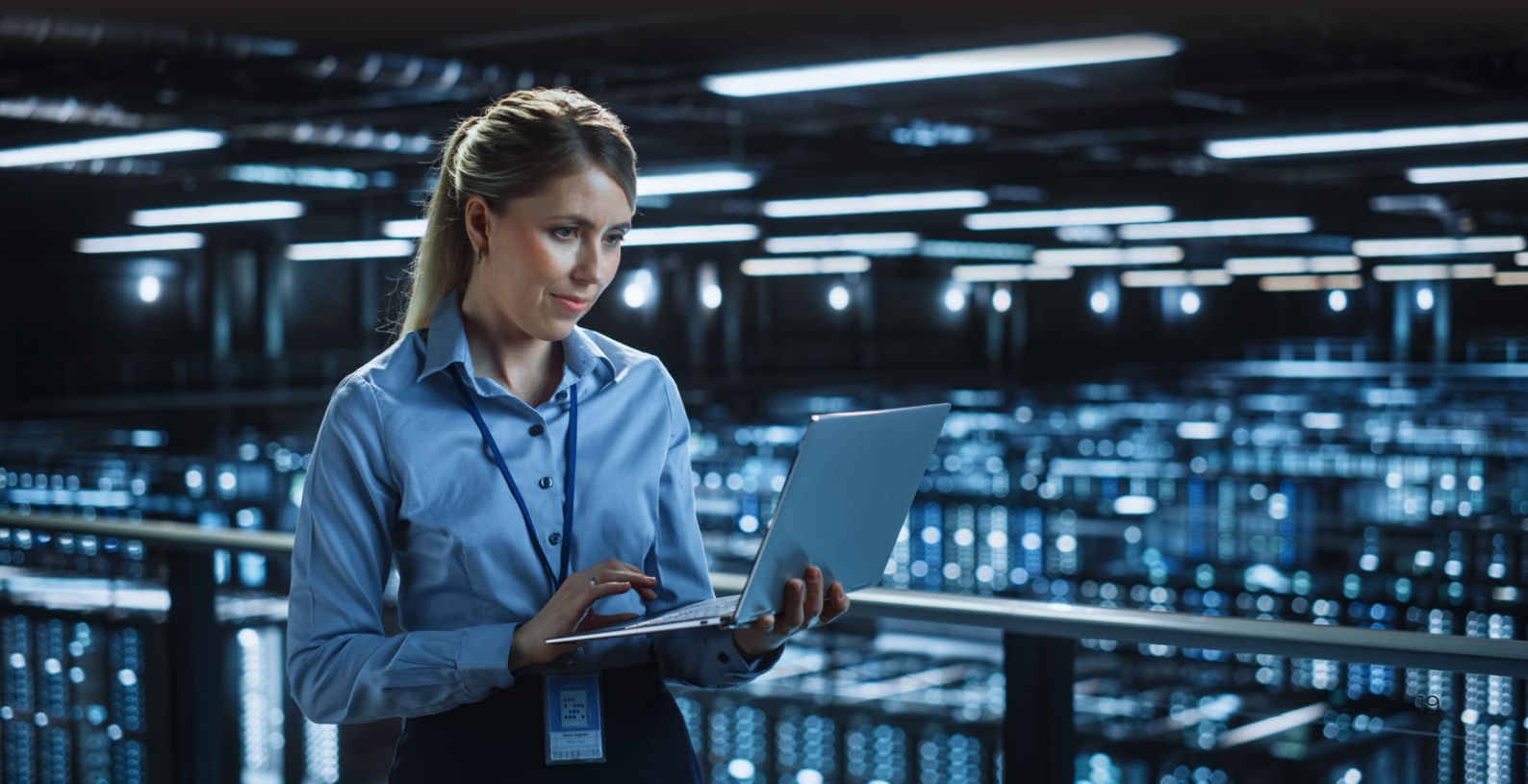
- Lekke personopplysninger og konfidensiell informasjon
- Bli brukt som inngangsport for cyberangrep
- Utnyttes av innsidere eller sabotører
- Kompromittere beredskapsplaner og informasjonsflyt

Dette gjør printsikkerhet til en del av det digitale risikobildet og til en viktig komponent i virksomheters beredskap og motstandsdyktighet.

Hvordan printsikkerhet bidrar til felles trygghet

- Reduserer risiko for datalekkasjer og sabotasje
- Styrker tillit til offentlige og private tjenester
- Understøtter totalforsvaret og samfunnets robusthet
- Bidrar til etterlevelse av sikkerhetsloven og GDPR
- Gir bedre beredskap ved kriser og hendelser

Nasjonal sikkerhet er ikke bare et ansvar for myndighetene – det er et felles prosjekt. Når virksomheter tar ansvar for sin egen sikkerhet, inkludert noe så tilsynelatende enkelt som utskrifter, bidrar de til å beskytte hele samfunnet. Printsikkerhet er derfor ikke bare IT-sikkerhet – det er beredskap, tillit og nasjonal motstandskraft i praksis.



Nasjonal sikkerhetsmåned 2025

Årets tema er "Digital beredskap", valgt av Norsk senter for informasjonssikring (NorSIS).

I en stadig mer digitalisert verden er vår avhengighet av teknologi total. Alt fra produksjon og kundeservice, til økonomi og kommunikasjon er tett knyttet til digitale systemer. Men hvor godt forberedt er vi egentlig på det som kan gå galt?

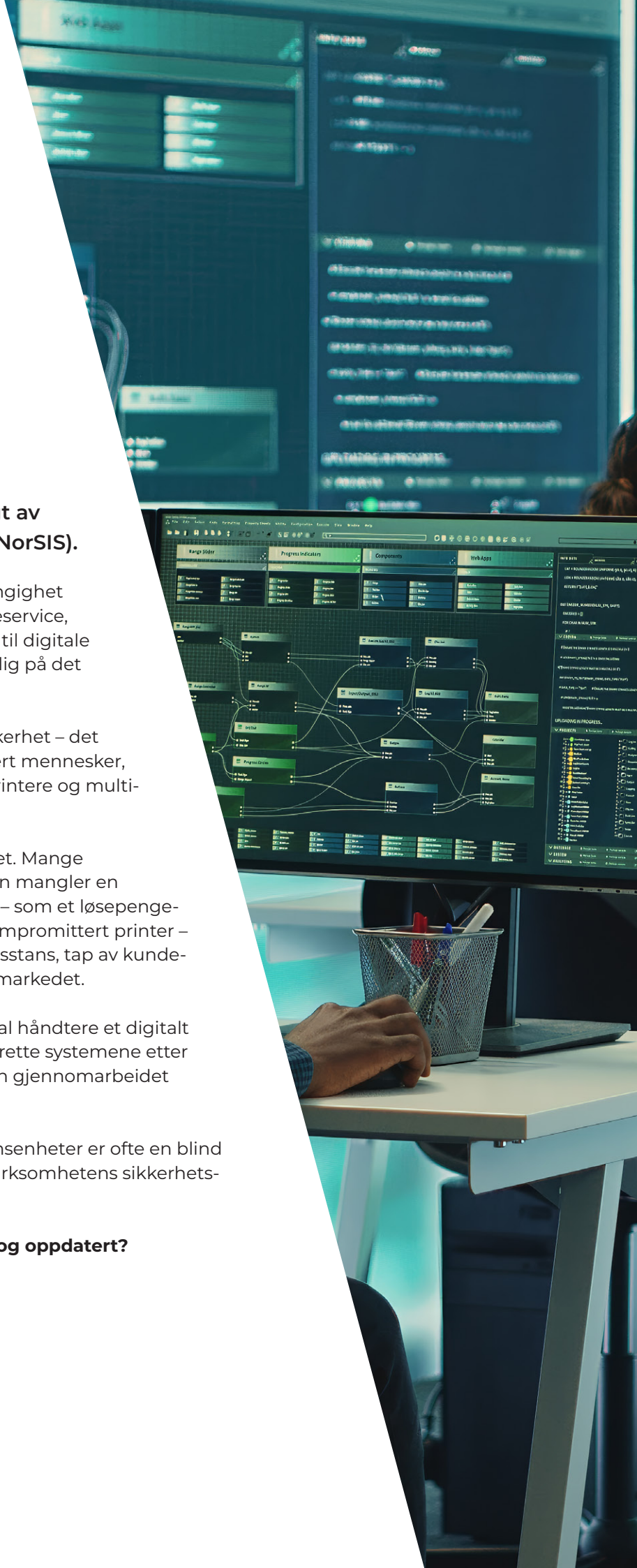
Digital beredskap handler ikke bare om IT-sikkerhet – det handler om å sikre hele virksomheten, inkludert mennesker, prosesser, teknologi og fysiske enheter som printere og multifunksjonsmaskiner.

Det dreier seg om mer enn bare cybersikkerhet. Mange virksomheter har gode tekniske løsninger, men mangler en helhetlig beredskapsplan. Én enkelt hendelse – som et løsepengevirus, en feilkonfigurert skytjeneste eller en kompromittert printer – kan føre til alvorlige konsekvenser: produksjonsstans, tap av kundedata, brudd på personvern eller svekket tillit i markedet.

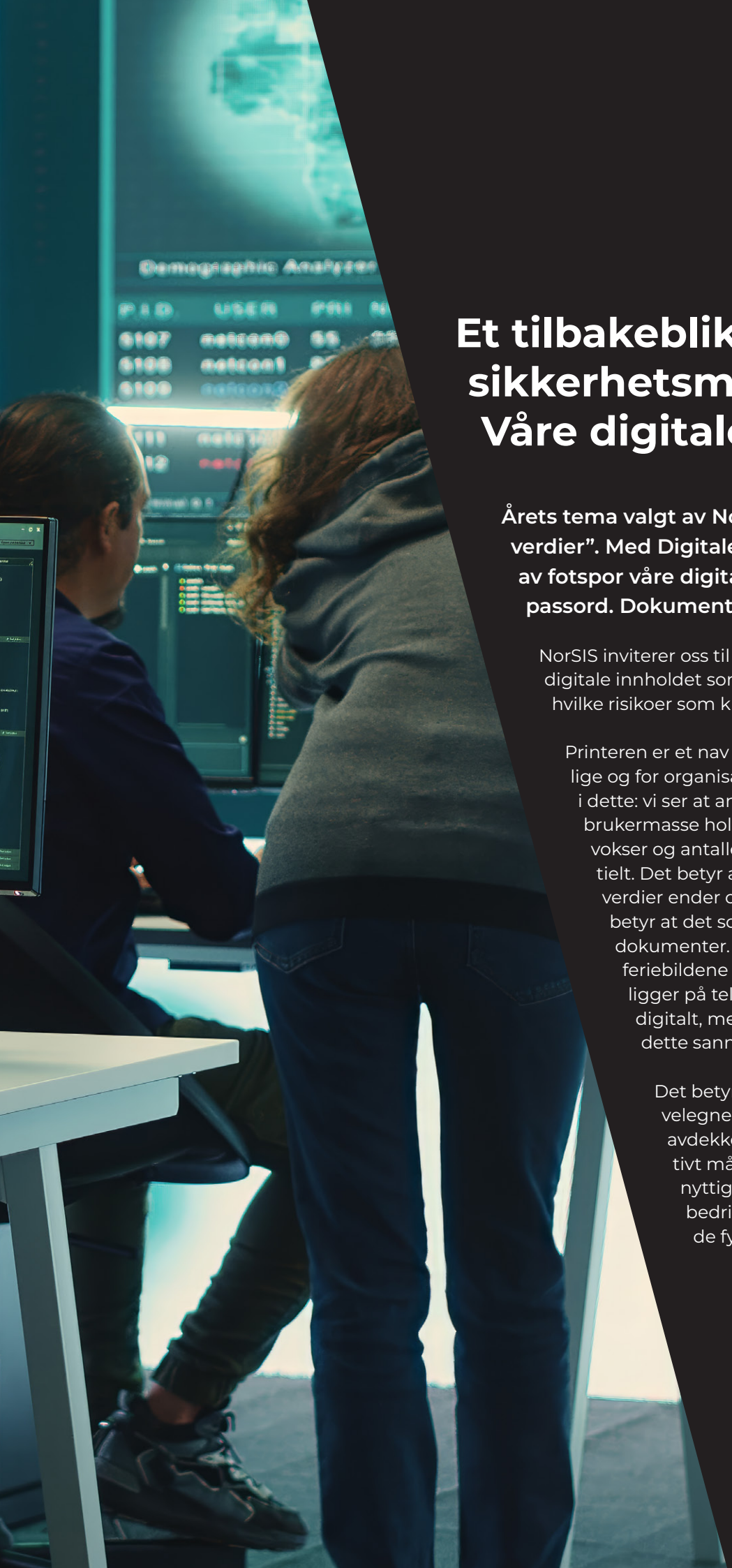
Har virksomheten en plan for hvordan dere skal håndtere et digitalt angrep? Vet dere hvor raskt dere kan gjenopprette systemene etter et brudd – og hvem som har ansvar for hva? En gjennomarbeidet forretningsplan bør besvare dette.

Som belyst tidligere, printere og multifunksjonsenheter er ofte en blind sone i sikkerhetsarbeidet. Ikke overse dette i virksomhetens sikkerhetsarbeid.

Er din digitale beredskapskasse komplett – og oppdatert?



NorSIS



Et tilbakeblikk: Nasjonal sikkerhetsmåned 2024: Våre digitale verdier

Årets tema valgt av NorSIS er "Våre digitale verdier". Med Digitale verdier mener NorSIS alt av fotspor våre digitale liv skaper, som bilder, passord. Dokumenter og forretningsinformasjon.

NorSIS inviterer oss til å reflektere over verdien av alt det digitale innholdet som utgjør vårt digitale fotavtrykk, og hvilke risikoer som knytter seg opp mot disse.

Printeren er et nav for digitale verdier, både personlige og for organisasjoner. Det finnes et paradoks i dette: vi ser at antallet sider som printes i vår brukermasse holder seg stabilt, men befolkningen vokser og antallet digitale filer øker eksponentielt. Det betyr at en lavere andel av våre digitale verdier ender opp på papir, samtidig som det betyr at det som ender opp på papir er viktige dokumenter. Det er kanskje bare de aller fineste feriebildene som printes, ikke de 2000 som ligger på telefonen. Mange avtaler signeres digitalt, men skal en printe ut en avtale er dette sannsynligvis en ekstra viktig avtale.

Det betyr at printere kan sees på som velegnede mål for datainnbrudd. For å avdekke om printeren kan være et attraktivt mål i din organisasjon, kan det være nyttig å kartlegge hva printerne i din bedrift benyttes til, sammen med hvor de fysisk befinner seg.

Cybersikkerhets trusler 2026

Spørsmålet “alle” stiller seg: hva må vi være mest oppmerksomme på i 2026? Det er all grunn til å tro at dagens trusler vil være med oss inn i 2026 og videre, trolig med mer sofistikerte verktøy.

1. KI-drevne angrep

Kunstig intelligens brukes aktivt av angripere til å lage mer overbevisende phishing-e-poster, deepfakes og selvlærende malware. Disse angrepene tilpasser seg forsvarsmekanismer i sanntid, noe som gjør dem vanskeligere å oppdage og stoppe.

2. Deepfake-svindel og sosial manipulering

Ved hjelp av stemmegenerering og video-manipulasjon kan angripere etterligne ledere eller ansatte, og lure brukere til å overføre penger eller gi fra seg sensitiv informasjon.

3. Ransomware 2.0

Løsepengevirus blir stadig mer sofistikerte. Angrepene kombineres ofte med datatyveri og trusler om publisering, noe som øker presset på ofrene. Angrepene er ofte målrettede og rammer kritisk infrastruktur og SMB-markedet.

4. Sårbarheter i skybaserte systemer

Ettersom flere virksomheter flytter til skyen, øker risikoen for feilkonfigurasjoner, tilgangsfeil og utnyttelse av API-er. Angripere retter seg mot svakheter i skyinfrastruktur og SaaS-løsninger.

5. Kontoovertakelser og identitetstyveri

Stjålne brukernavn og passord fra tidligere datainnbrudd brukes til å ta over kontoer. Gjenbruk av passord og manglende tofaktorautentisering gjør dette til en vedvarende trussel.

6. Utnyttelse av smarthjem og IoT-enheter

Flere enheter kobles til nettverk uten tilstrekkelig sikkerhet. Dette gjelder både i hjem og på arbeidsplassen, og gir angripere nye inngangspunkter.

7. Desinformasjon som en tjeneste

Organiserte aktører tilbyr desinformasjon og manipulasjon som betalte tjenester, noe som kan påvirke både virksomheter og samfunnsdebatten.

REFERANSER

NSM “Risiko 2025 Et sikkert Norge i en usikker verden”

https://nsm.no/getfile.php/1314212-1738741587/NSM/Filer/Dokumenter/Rapporter/Risiko 2025.pdf

PST “Nasjonal trusselvurdering 2025”

https://www.regjeringen.no/contentassets/6290dec36c374ee191e5c7dbba18a258/nasjonal-trusselvurdering-2025_no_web.pdf

NorSIS “Nasjonal sikkerhetsmåned 2025”

https://norsis.no/nasjonal-sikkerhetsmaned/

SIKRING AV PRINTENHETER FRA CANON:

Tiltak for å redusere risikoen for uautorisert tilgang på multifunksjonsprintere (Engelsk)

global.canon/en/support/security/pdf/mpf-office-production.pdf

Herdingsguide imageRUNNER Advance (Engelsk)

https://canon.a.bigcontent.io/v1/static/Canon_imageRUNNER_ADVANCE_Hardening_Guide_Brochure_EM_Digital_Final_DIGI

Sikkerhetswhitepaper- veiledning for herding av Canonprintere i tråd med NIST SP 800-171 og -172 (engelsk)

http://downloads.canon.com/nw/pdfs/solutions/NIST-Cybersecurity-Whitepaper.pdf

Canon brukermanual på nett

global.canon/en/support/security/pdf/mpf-office-production.pdf
https://oip.manual.canon/

CANONS SIKKERHETSINITIATIV OG SIKKERHETSTJENESTER:

Sikre utskriftsløsninger fra Canon

https://www.canon.no/business/solutions/security/secure-printing/

Temaside personvern i Canon

https://www.canon.no/privacy/

Vi hjelper deg gjerne med spørsmål rundt sikkerhet.

Kontakt oss via sikkerhet@canon.no

Våre øvrige kontaktopplysninger er

Besøksadresse:

Hallagerbakken 110

1256 OSLO

Postadresse:

P.O.Box 33, Holmlia N-1201 OSLO

Fakturaadresse:

Canon Norge AS

Postboks 1 Youngstorget 0028 Oslo Norway

Tlf. sentralbord:

+47 22 62 92 00

Printet på Canon imagePress C850