



CISO'ENS GUIDE TIL PRINTSIKKERHET

2027

Canon

INNHOLD

Forord	3
Formål med guiden	4
Del 1. Trusselbildet 2026/27: Den nye kjempen i rommet	5
Del 2. Fra perimeter til zero trust: printerens nye rolle	8
Del 3. NSMs grunnprinsipper for IKT sikkerhet	10
Del 4. Identifisere og kartlegge (NSM kategori 1)	12
Del 5. Beskytte og opprettholde (NSM kategori 2)	14
Del 6. Oppdage (NSM kategori 3)	17
Del 7. Håndtere og gjenopprette (NSM kategori 4)	18
Del 8. Supply chain security: firmware og leverandørstyring	20
Del 9. 2027 – hvor bærekraft møter sikkerhet	22
Del 10. Sjekkliste for beredskap	24
Del 11. Totalforsvarsåret 2026	26
Del 12: Nasjonal sikkerhetsmåned 2026: Digital dømmekraft i fokus	28
Del 13: Et tilbakeblikk: Nasjonal sikkerhetsmåned 2025: Digital beredskap	29
Del 14. Cybersikkerhets trusler 2027	30

FORORD

Velkommen til den fjerde utgaven av CISO'ens guide til printsikkerhet. Da vi i Canon ga ut den første utgaven, ble printsikkerhet ofte ansett som en "husk-på-ting" – en teknisk sjekkliste nederst i bunken hos IT-drift. I 2026 er bildet fundamentalt endret. Den moderne multifunksjonsskriveren (MFP) er ikke lenger bare en maskin som flytter blekk og toner til papir; den er en høyt-ytende IoT-server, en inngangsport til skyen og kan fort bli et av de mest sårbare endepunktene i bedriftens nettverk.



I år står vi overfor et skifte i trusselbildet som krever mer enn bare brannmurer og passord. Med inntoget av KI-drevne angrep og stadig mer sofistikerte aktører, har grensen mellom den fysiske og digitale arbeidsplassen blitt visket ut. En usikret printer på et hjemmekontor eller en feilkonfigurert maskin i hjørnet av kontorlandskapet kan være alt en angriper trenger for å omgå år med investeringer i cybersikkerhet.

Denne guiden er, som alltid, leverandør- og plattformuavhengig. Vårt mål er å gi deg som CISO og beslutningstaker det strategiske verktøyet du trenger for å lukke dette kritiske gapet.

Årets utgave tar et viktig steg videre ved å integrere **NSMs grunnprinsipper for IKT-sikkerhet (v2.1)** direkte inn i print-domenet. Ved å bruke et nasjonalt anerkjent rammeverk, gjør vi det enklere å kommunisere risiko til styret og sikre at print-infrastrukturen ikke bare er en driftskostnad, men en herdet del av deres Zero Trust-arkitektur.

Truslene er komplekse, men strategien for å møte dem trenger ikke være det. Årets guide vil vi gi deg innsikten, sjekklistene og arkitekturforståelsen som kreves for å navigere trygt i det kommende året.

God lesing – og god sikring.
Oslo, oktober 2026

A handwritten signature in black ink, reading "Erik Mikalsen". The signature is fluid and cursive.

Erik Mikalsen
Adm Dir
Canon Norge

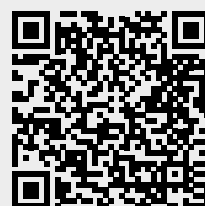
FORMÅL MED GUIDEN

Formålet med denne guiden er å ruste CISO-er og IT-ledere til å navigere i et digitalt trusselbilde som er i ferd med å endre karakter. NSM rapporten Risiko 2026 viser at det ofte er svikt i det helt grunnleggende som feller norske virksomheter. Denne guiden skal hjelpe deg med å forstå hva god printsikkerhet betyr i praksis, hvordan man oppnår det, og hvilke spesifikke trusler man må være oppmerksom på.

Hva guiden har som mål å gi deg svar på:

- **Hva er god printsikkerhet?:** Når digitale trusler får alvorlige konsekvenser i den fysiske verden kan ikke printerflåten lenger være en blindsonesone. God printsikkerhet betyr å behandle hver printer som et kritisk endepunkt med krav til unik identitet, kryptering og streng tilgangsstyring.
- **Trusselbildet i 2027:** Med utgangspunkt i NSM sin advarsel om at kunstig intelligens (KI) gjør angrepene både raskere og mer treffsikre, belyser guiden hvordan automatiserte cyberoperasjoner kan ramme printerflåten.
- **Veien til sikkerhet:** Vi ser på hvordan man tetter gapene NSM har identifisert – fra å fjerne overflødige tilganger til å implementere robuste løsninger som Public Key Infrastructure (PKI) og moderne utskriftsarkitektur. Guiden forklarer hvordan man går fra "mangler i det forebyggende arbeidet" til en herdet infrastruktur.

Målet er at valgene du tar i dag, basert på denne innsikten, skal avgjøre din virksomhets risiko i morgen.



Les også om
informasjonssikkerhet
på [canon.no](https://www.canon.no)



DEL 1. TRUSSELBILDET DEN NYE KJEMPEN I ROMMET

KI har blitt angriperens nye "Fast-Track"

Kunstig intelligens (KI) er ikke lenger bare et verktøy for å skrive overbevisende phishing-eposter. For moderne trusselaktører fungerer KI som en digital spesialist som kontinuerlig analyserer, tester og identifiserer svakheter i tilkoblede enheter, inkludert printere og multifunksjonssystemer. KI-drevne verktøy kan analysere firmware på sekunder, avdekke ukjente sårbarheter, skape målrettede angrepskoder og utvikle polymorfisk skadevare som kontinuerlig endrer seg for å unngå tradisjonell signaturbasert deteksjon. Dette gjør at printere i økende grad må behandles som forretningskritiske endepunkter på linje med servere og arbeidsstasjoner.

God printsikkerhet reduserer denne risikoen ved å kombinere flere sikkerhetslag. Oppdatert firmware, Secure Boot og integritetskontroll av firmware bidrar til å forhindre manipulering og uautorisert kodekjøring. Nettverkssegmentering og Zero Trust-prinsipper begrenser muligheten for at en kompromittert printer kan brukes som inngangsport til resten av virksomheten. Samtidig bør usikre protokoller deaktiveres, administrasjon sikres med sterke autentiseringsmekanismer og printere

plasseres i egne sikkerhetssoner. Fordi KI-generert skadevare i stadig mindre grad kan oppdages gjennom tradisjonelle signaturer, blir kontinuerlig overvåking, SIEM-integrasjon og atferds basert deteksjon avgjørende for å oppdage mistenkelig aktivitet, uvanlig nettverkstrafikk eller forsøk på manipulering.

Like viktig er beskyttelsen av informasjonen som behandles gjennom utskriftsmiljøet. Kryptering, sikker utskrift med brukerautentisering, automatisk sletting av utskriftsjobber og beskyttelse av lagrede data på harddisker reduserer risikoen for datalekkasjer selv dersom en enhet kompromitteres. Når KI gjør sårbarhetsanalyse og angrepsutvikling raskere enn noensinne, er den mest effektive forsvarsstrategien å redusere angrepsflaten, begrense konsekvensene av et kompromiss og sørge for kontinuerlig synlighet i printermiljøet. Moderne printsikkerhet handler derfor ikke lenger bare om å beskytte dokumenter, men om å beskytte virksomhetens digitale verdier mot en stadig mer automatisert og intelligent trusselaktør.



Kvanteteknologi: Ikke en krise, men en planleggingsoppgave

Kvanteteknologi kan på sikt endre forutsetningene for digital sikkerhet. I den tradisjonelle dataverdenen lagres informasjon som bits, som enten er 0 eller 1, men en kvantedatamaskin bruker **qubits** som kan eksistere i begge tilstander samtidig. Dette fenomenet, kjent som superposisjon, gjør at maskinen kan utføre enormt mange beregninger parallelt i stedet for sekvensielt. Mens en vanlig datamaskin må prøve én dør av gangen i en labyrint, kan en kvantedatamaskin i teorien teste alle veier

samtidig. Dersom teknologien modnes slik mange forskningsmiljøer forventer, vil enkelte av dagens mest brukte kryptografiske mekanismer kunne bli sårbare.

For de fleste virksomheter er ikke dette et problem som må løses i dag, men det er et tema som bør innarbeides i langsiktig teknologi- og sikkerhetsplanlegging. Særlig gjelder dette informasjon som må forbli konfidensiell i mange år fremover.

"Høst nå, dekrypter senere"

En ofte omtalt problemstilling er "Harvest Now, Decrypt Later". Tanken er at angripere kan samle inn kryptert informasjon i dag, med mål om å dekryptere den på et senere tidspunkt dersom fremtidige teknologiske gjennombrudd gjør dette mulig.

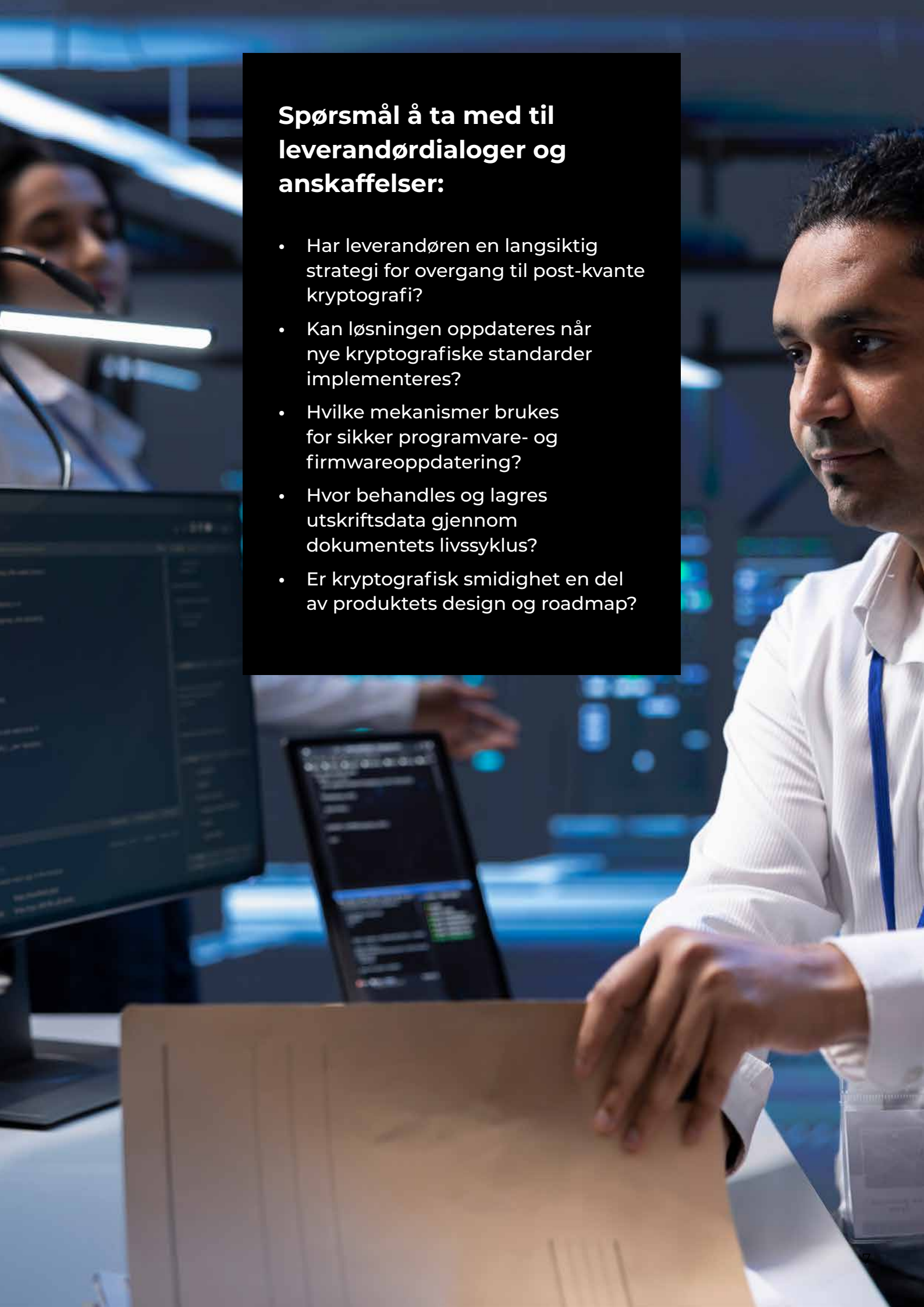
For virksomheter betyr dette at vurderingen ikke bare handler om dagens trusselbilde, men også om hvor lenge informasjonen skal beskyttes. Dokumenter som inneholder forretningshemmeligheter, forskningsresultater, personopplysninger eller kritiske kontrakter kan ha verdi langt utover levetiden til dagens kryptografiske løsninger.

Hva betyr dette for utskriftsmiljøet?

Printmiljøet er en del av virksomhetens informasjonsflyt. Dokumenter lagres, behandles og overføres mellom klienter, servere, skytjenester og multifunksjonsheter. Derfor bør utskriftsinfrastrukturen inngå når virksomheten vurderer sin fremtidige overgang til post-kvante kryptografi. For CISO-er er det særlig tre områder som fortjener oppmerksomhet:

- **Kryptografisk smidighet:** Evnen til å oppdatere kryptografiske mekanismer uten å bytte ut hele infrastrukturen.
- **Leverandørrisiko:** Innsikt i hvordan kritiske teknologileverandører planlegger overgangen til nye kryptografiske standarder.
- **Levetid på informasjon:** Identifisere hvilke dokumenttyper som krever beskyttelse i 10 år eller mer.



A man in a white shirt and blue lanyard is looking at a document in a server room. In the background, there are computer monitors and server racks. The text is overlaid on a dark rectangular box.

Spørsmål å ta med til leverandørdialoger og anskaffelser:

- Har leverandøren en langsiktig strategi for overgang til post-kvante kryptografi?
- Kan løsningen oppdateres når nye kryptografiske standarder implementeres?
- Hvilke mekanismer brukes for sikker programvare- og firmwareoppdatering?
- Hvor behandles og lagres utskriftsdata gjennom dokumentets livssyklus?
- Er kryptografisk smidighet en del av produktets design og roadmap?

DEL 2. FRA PERIMETER TIL ZERO TRUST: PRINTERENS NYE ROLLE

I flere tiår har IT-sikkerhet vært bygget som en middelalderborg: tykke murer (brannmurer) beskyttet alt på innsiden. Printere ble plassert dypt inne i dette "betrodde" nettverket, ofte med åpne porter og ukrypterte protokoller, under den feilaktige antakelsen om at dersom du hadde fysisk tilgang til kontoret, var du en trygg bruker.

I dag er denne modellen død. Med fremveksten av hybride sky-løsninger, ansatte som printere fra usikre hjemmenettverk, og sofistikerte trusselaktører som bruker printere som brohode for lateral bevegelse, må vi adoptere **Zero Trust-modellen: "Aldri stol på, alltid verifiser"** (som vi også nevnte i fjorårets utgave av CISO Guiden). I takt med at Zero Trust-prinsippene blir standard, flyttes sikkerhetskontrollene nærmere selve informasjonen. Dokumenter klassifiseres automatisk, tilgang styres dynamisk og utskrift kan begrenses basert på identitet, lokasjon eller sikkerhetsnivå. Resultatet er færre kopier av sensitiv informasjon og bedre kontroll med hvordan informasjon brukes.

Hvorfor interne soner er en risiko:

- **Lateral bevegelse:** En infisert laptop kan skanne det interne nettverket for printere med kjente sårbarheter. Når printeren er kompromittert, blir den en permanent "lyttepost" som er vanskeligere å oppdage enn en infisert laptop.
- **Protokoll-svakheter:** Mange printere bruker fortsatt utdaterte protokoller (som SNMP v1/v2 eller eldre SMB-versjoner) som sender informasjon i klartekst. I et åpent internt nettverk kan dette enkelt avlyttes.
- **IoT som blindvei:** Printere har ofte svakere logger og kortere support-sykluser enn servere, noe som gjør dem til ideelle skjulesteder for skadevare som ønsker å unngå deteksjon fra sentrale sikkerhetssystemer.

Printeren som en uavhengig identitet

I en Zero Trust-arkitektur endres printerens rolle fra å være en passiv ressurs til å bli en aktiv, identifisert aktør. Dette krever et fundamentalt skifte i hvordan vi håndterer tilgang.

1. Mikrosegmentering: En brannmur per enhet

I stedet for å plassere alle printere i ett felles VLAN, bruker vi mikrosegmentering. Hver printer tildeles en unik sikkerhetspolise som definerer nøyaktig hvem den kan snakke med.

Eksempel: En printer i personalavdelingen skal kun akseptere trafikk fra HR-serveren og autoriserte ansatte, og den skal aldri kunne initiere kontakt med finanssystemet.

2. Sertifikatbasert autentisering (802.1X)

Vi kan ikke lenger stole på IP-adresser alene, ettersom disse kan forfalskes gjennom såkalt spoofing. Med sertifikatbasert autentisering må hver printer presentere et gyldig maskinsertifikat for å få tilgang til nettverket. Dersom enheten ikke kan autentiseres, eller sertifikatet er utløpt eller ikke lenger er tillitsverdig, kan nettverkstilgangen automatisk nektes eller begrenses.

3. Kontinuerlig verifisering av tillit

Tillit er ikke lenger noe man får én gang ved pålogging; det må kontinuerlig vurderes basert på tilgjengelig sikkerhetsinformasjon.

Kontroll av enhetens integritet: Ved oppstart verifiseres at printeren kjører godkjent firmware. I tillegg overvåker Trellix fortløpende at programvaren som kjører på enheten er intakt og ikke er manipulert.

Kontekstuell tilgang: Tilgang kan begrenses basert på faktorer som tid, sted og risikonivå. For eksempel kan en utskriftsjobb med sensitivt innhold blokkeres dersom brukeren forsøker å hente den ut fra en enhet eller lokasjon som ikke oppfyller virksomhetens sikkerhetskrav.



“Overgangen til Zero Trust for print handler om å eliminere implisitt tillit. Ved å isolere printeren som et eget endepunkt, reduserer du angrepsflaten dramatisk. Skulle en printer bli kompromittert i en Zero Trust-modell, vil angriperen være låst inne i et digitalt ”isolasjonskammer” uten mulighet til å nå resten av organisasjonen. Målet er at en printer skal være like sikker på en kaffebar som den er på hovedkontoret. Det er arkitekturen, ikke lokasjonen, som skal stå for sikkerheten.”

DEL 3. NSMS GRUNNPRINSIPPER FOR IKT SIKKERHET

(4 kategorier, 21 prinsipper)



1. Identifisere og kartlegge

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer
- 1.2 Kartlegg enheter og programvare
- 1.3 Kartlegg brukere og behov for tilgang

2. Beskytte og opprettholde

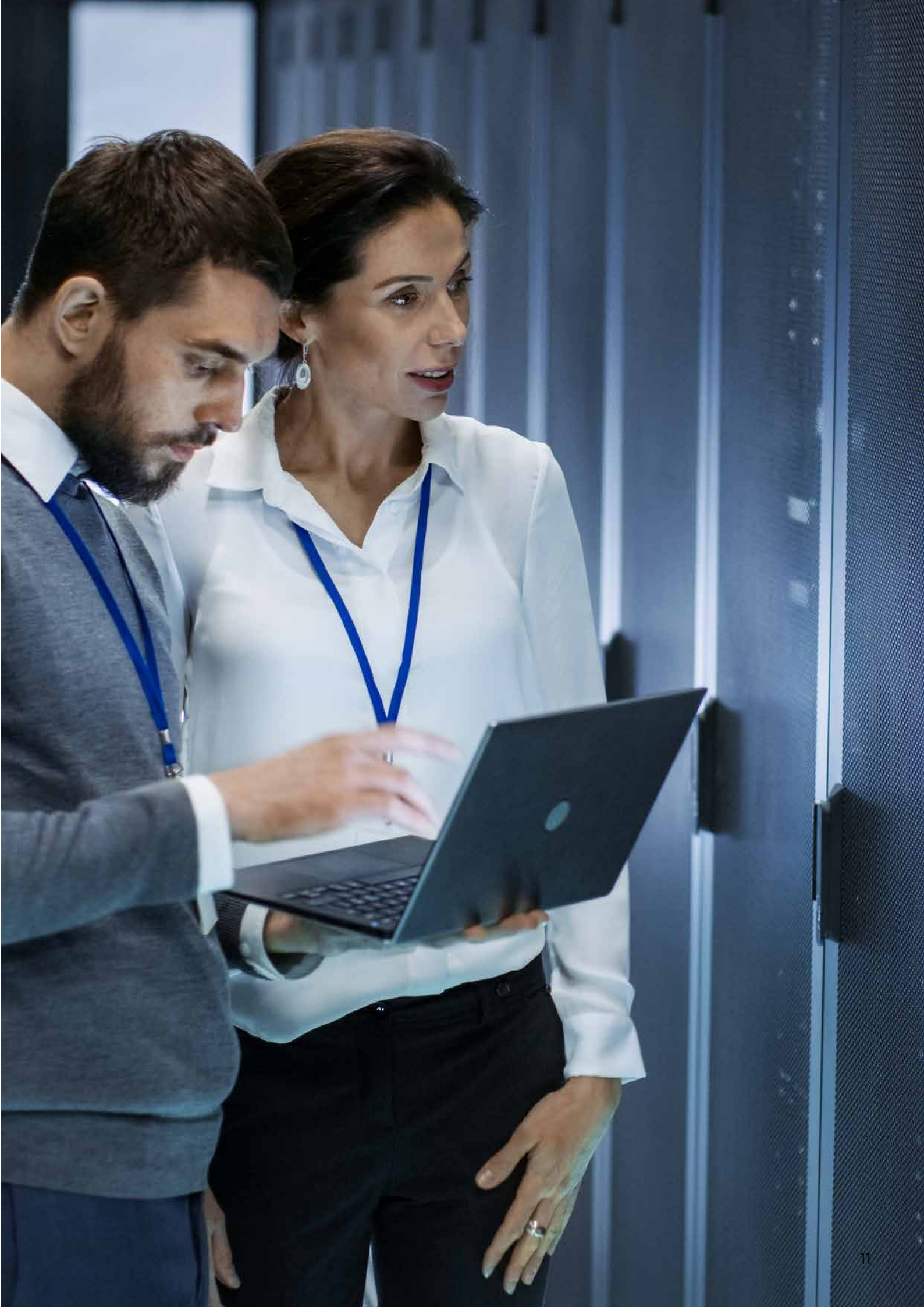
- 2.1 Ivareta sikkerhet i anskaffelser og utviklingsprosesser
- 2.2 Etabler en sikker IKT-arkitektur
- 2.3 Ivareta sikker konfigurasjon
- 2.4 Beskytt virksomhetens nettverk
- 2.5 Kontroller dataflyt
- 2.6 Ha kontroll på identiteter og tilganger
- 2.7 Beskytt data i ro og i transitt
- 2.8 Beskytt e-post og nettleser
- 2.9 Etabler evne til gjenoppretting av data
- 2.10 Integrer sikkerhet i endringshåndtering

3. Oppdage

- 3.1 Oppdag og fjern kjente sårbarheter
- 3.2 Etabler sikkerhetsovervåkning
- 3.3 Analyser data fra sikkerhetsovervåkning
- 3.4 Gjennomfør inntrengningstester

4. Håndtere og gjenopprette

- 4.1 Forbered virksomheten på hendelseshåndtering
- 4.2 Vurder og klassifiser hendelser
- 4.3 Kontroller og håndter hendelser
- 4.4 Evaluer og lær av hendelser



DEL 4. IDENTIFISERE OG KARTLEGGE (NSM KATEGORI 1)

I dag er "oversikt" et langt mer komplekst begrep enn for få år siden. NSMs grunnprinsipp 1 krever at virksomheten har oversikt over alle enheter og systemer. For en CISO betyr dette at man må gå fra et passivt "inventar-ark" til en dynamisk, sanntidsoversikt over alle enheter som kan prosessere virksomhetens data.

Full oversikt: Mer enn bare serienummer

En moderne enhetsoversikt må inneholde langt mer enn fysisk lokasjon og modellnavn. For å tilfredsstille kravene til sikkerhetsstyring, må kartleggingen inkludere:

Programvare- og firmware-versjon: Hvilke enheter kjører utdatert kode med kjente sårbarheter, og hvordan skal enheten være konfigurert?

Eierskap og ansvar: Hvem "eier" risikoen for den spesifikke enheten?

Data-klassifisering: Hvilken type informasjon er tillatt å sende til denne maskinen? (F.eks. er maskinen i resepsjonen godkjent for sensitive personopplysninger?)

Trusselen fra "Skyggeprintere"

Hjemmekontoret har blitt en permanent del av infrastrukturen for de fleste, men det representerer også en enorm blindsones. "Skyggeprintere" – ansattes private printere koblet til bedriftens laptop-er er ofte den svakeste inngangen for angripere.

Problemet: Private printere mangler bedriftens sikkerhetskontroller, mottar sjelden firmwareoppdateringer og er ofte koblet til usikre hjemmenettverk med standardpassord på ruter.

Kartleggingsstrategi: Virksomheten må implementere verktøy som identifiserer lokalt tilkoblede printere via USB eller WiFi når den bærbare maskinen er tilkoblet VPN.

Tiltak: Guiden anbefaler en "Zero Trust-agent" på endepunktet som rapporterer hvilke utskriftsenheter som benyttes, slik at disse kan inkluderes i risikovurderingen (NSM 1.2).

Maskin-identiteter: Enheten som subjekt

Et sentralt fokusområde er overgangen til Non-Human Identities (NHI). I en moderne arkitektur holder det ikke at en bruker logger på; selve printeren må ha en verifiserbar identitet.

Hvorfor NHI er kritisk for print:

- **Sertifikatbasert tillit:** Hver maskin må tildeles et sertifikat (f.eks. via SCEP-protokollen) som beviser at den er en autorisert enhet eid av selskapet.
- **Unngå impersonering:** Uten en sterk maskin-identitet kan en angriper koble en ondsinnet enhet til en nettverksport og "late som" den er en godkjent printer for å fange opp utskriftsjobber (Man-in-the-Middle).
- **Automatisert livssyklus:** Kartleggingen må inkludere en plan for utskifting av sertifikater. En printer med et utløpt eller trukket tilbake sertifikat skal automatisk miste tilgangen til utskriftskøen.

Praktisk sjekkliste for NSM Kategori 1:

- **Automatisk oppdagelse:** Har vi verktøy som kontinuerlig skanner nettverket for nye, ukjente printere?
- **Hjemmekontor-kontroll:** Har vi oversikt over hvilke ansatte som printer hjemmefra, og hvilke enheter de bruker?
- **Sertifikat-oversikt:** Er alle våre MFP-er registrert med unike maskin-identiteter i vårt Identity & Access Management (IAM)-system?
- **Logisk kartlegging:** Vet vi hvilke skytjenester (f.eks. Microsoft Universal Print eller andre SaaS-løsninger) hver enkelt fysisk printer snakker med?

A woman with brown hair, wearing a dark blazer, is shown in profile, looking back over her shoulder while holding a laptop. She is in a server room, with rows of server racks and glowing blue lights visible in the background. A black text box is overlaid on the image.

“NSM Kategori 1 er ikke en engangsjobb. I dag må dette være en automatisert prosess. ”Skygge IT” i form av en billig printer kjøpt på den lokale elektronikk butikken til et prosjektkontor kan være nok til å kompromittere hele avdelingen.”

DEL 5. BESKYTTE OG OPPRETTHOLDE (NSM KATEGORI 2)

Der kategori 1 handlet om å vite hva man har, handler kategori 2 om å bygge forsvarsverkene. Vi følger NSMs prinsipper for å transformere printeren fra et sårbart endepunkt til en sikker festning.

Sikker arkitektur: Fra VLAN til mikrosegmentering

Den tradisjonelle metoden med å legge alle printere i et eget VLAN er i dag utilstrekkelig. Hvis én printer blir kompromittert, vil en angriper kunne infisere hele flåten via dette VLAN-et.

Mikrosegmentering: Vi gjennomfører logiske skiller som hindrer printere i å kommunisere med

hverandre. En printer skal kun ha "Line of Sight" til utskriftsserveren eller sky-gatewayen.

Software-Defined Networking (SDN): Bruk av identitetsbaserte brannmurregler som følger enheten, uavhengig av hvilken fysisk port den plugges inn i. Dette støtter NSMs krav om å begrense skadepotensialet ved et kompromiss.



Sikker konfigurasjon: Digital herding

En printer som kommer rett fra esken er en sikkerhetsrisiko. NSM 2.3 anbefaler at alle enheter herdes før de settes i drift.

- **Deaktivering av "Legacy"-protokoller:** Nå er det ingen unnskyldning for å kjøre Telnet, FTP, HTTP (port 80) eller eldre versjoner av SNMP. Disse er åpne dører for angripere. Kun krypterte varianter (SSH, SFTP, HTTPS, SNMPv3) bør tillates.
- **Utrydding av standardpassord:** Automatiserte verktøy må brukes for å sikre at ingen enhet beholder fabrikkinnstillingene. Passord skal være unike.
- **Firmware-integritet:** Aktiver funksjoner for "Self-healing" der printeren automatisk sjekker sin egen BIOS, firmware og all programvare som enhver tid kjører på enheten, og nekter å starte dersom koden er manipulert.

Identitet og tilgang: Den menneskelige barrieren

I en Zero Trust-verden er det ikke nettverket som gir tilgang, men identiteten din.

Secure Release (Pull-Print): Dette skal være standardkonfigurasjon, ikke et tilvalg. Dokumenter blir liggende kryptert i køen og skrives kun ut når eieren fysisk autentiserer seg ved maskinen. Dette eliminerer risikoen for sensitive utskrifter som blir liggende uavhentet i papirskuffen.

Data i ro og transitt: Kryptering som grunnmur

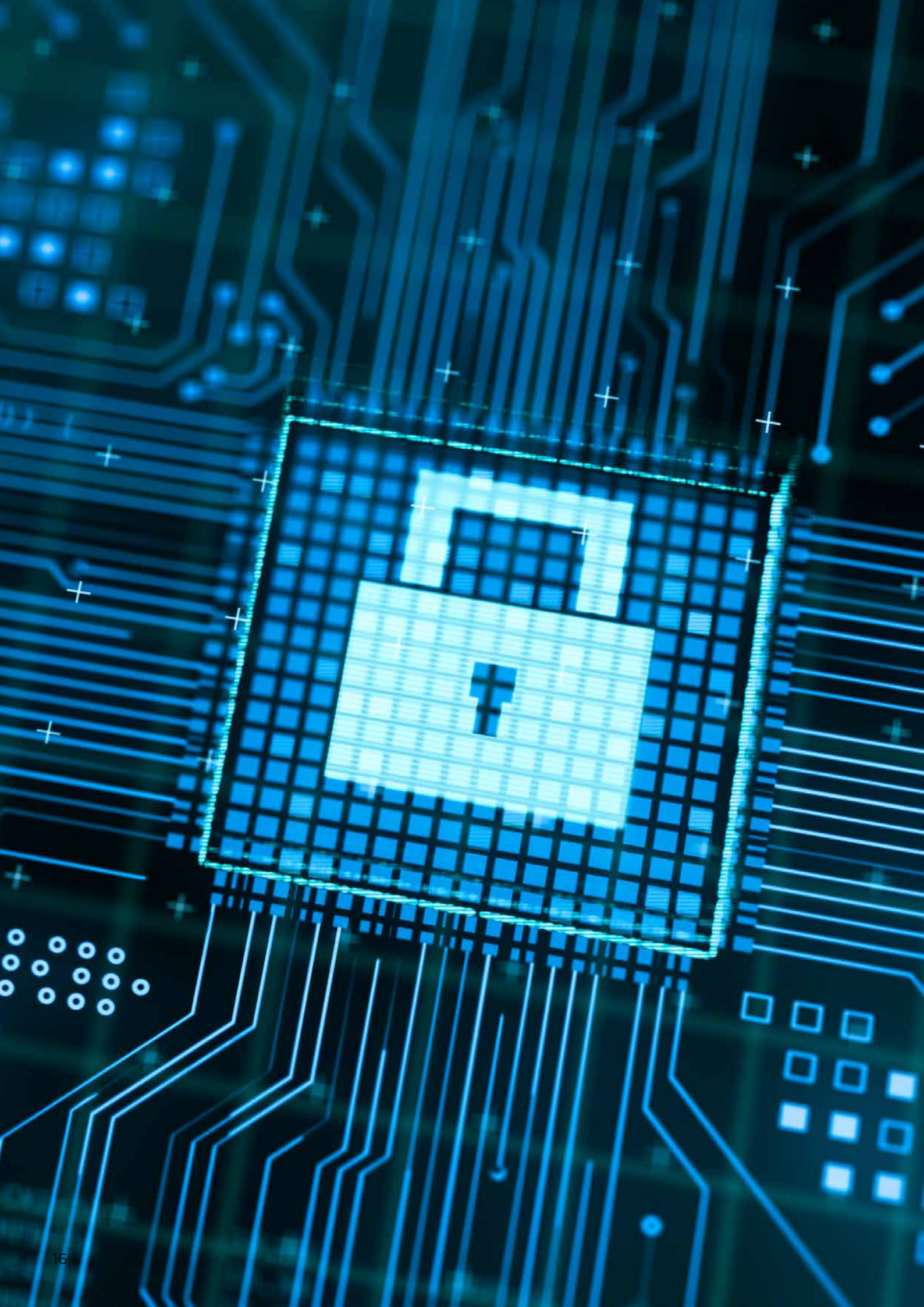
Informasjon på avveie skyldes ofte at data fanges opp underveis eller hentes ut fra avhendede maskiner.

- **Data kryptering:** All data fra PC/mobil til print-server, og videre til printeren, skal være kryptert med TLS 1.2 eller bedre. Dette sikrer mot "sniffing" på lokalnettverket.
- **Harddisk-beskyttelse:** Moderne MFP-er har store lagringsenheter. Disse må ha kryptert intern lagring.
- **Automatisert sletting:** Konfigurer enhetene til å utføre "Secure Overwrite" av alle midlertidige data umiddelbart etter at en jobb er fullført, eller ved et uventet stopp (grunnet feil, papirstopp eller tom for toner). Ved endt leasingperiode må det fremlegges et sertifikat på at disken er slettet i henhold til NSMs standarder for destruksjon av data.

Praktisk sjekkliste for NSM Kategori 2:

- **Mikrosegmentering:** Er printere isolert slik at de ikke kan kommunisere direkte med hverandre?
- **Zero Trust-nettverk:** Har alle printere kun tilgang til nødvendige tjenester og systemer?
- **Sikker konfigurasjon:** Er Telnet, FTP, HTTP og andre usikre protokoller deaktivert?
- **Sterk autentisering:** Benyttes HTTPS, SNMPv3 og andre krypterte administrasjonsprotokoller?
- **Unike administratorpassord:** Har enhetene et ikke-standard administratorpassord?
- **Firmware-integritet:** Er Secure Boot, firmware-validering eller tilsvarende integritetskontroller aktivert?
- **Secure Release:** Kreves autentisering ved maskinen før dokumenter skrives ut?
- **Maskinidentiteter:** Har alle printere gyldige sertifikater?
- **Kryptering:** Er all kommunikasjon mellom printer og andre kontaktflater kryptert med TLS?
- **Datasletting:** Er automatisk sletting av midlertidige utskriftsdata aktivert etter hver jobb?
- **Harddiskbeskyttelse:** Er lagrede data kryptert på printerens interne lagringsmedier?
- **Patch-management:** Finnes det en prosess som sikrer rask oppdatering av firmware og sikkerhetsfikser?

"Beskyttelse handler ikke om å bygge høyere murer, men om å sørge for at hver eneste printer kan forsvare seg selv, selv om resten av nettverket faller."



DEL 6. OPPDAGE (NSM KATEGORI 3)

Denne delen av guiden flytter fokus fra forebygging til situasjonsforståelse. I dagens trusselbilde er det ikke et spørsmål om en enhet blir forsøkt angrepet, men når. NSM Kategori 3 handler om å ha de digitale "overvåkningskameraene" på plass. Mange organisasjoner har avansert overvåking av servere og klienter, men printerflåten forblir ofte et "sort hull" i sikkerhetsloggene. I dag er integrasjon av print-infrastrukturen i virksomhetens sentrale sikkerhetsovervåking (SOC) et absolutt krav.

Integrasjon med SIEM og XDR

For å oppdage sofistikerte angrep må printerloggene ut av de proprietære produsentverktøyene og inn i bedriftens Security Information and Event Management (SIEM) eller Extended Detection and Response (XDR)-plattform.

- **Sanntids-strømming av logger:** Bruk av kryptert Syslog eller API-integrasjoner for å sende hendelsesdata umiddelbart.
- **Korrelering:** En isolert hendelse på en printer kan se uskyldig ut, men sett i sammenheng med en uvanlig pålogging fra en administrator-konto, kan det indikere et pågående angrep.

Identifisering av avvikende atferd

Deteksjon handler mindre om faste regler og mer om UEBA (User and Entity Behavior Analytics). Systemet må lære seg hva som er "normalt" for din organisasjon for å kunne flagge mistenkelige avvik:

- **Massiv dataeksport nattestid:** Hvis en printer som normalt produserer 50 sider om dagen plutselig "skanner" 5000 sider til en ekstern skydestinasjon klokken 03:00, må XDR-systemet automatisk blokkere enheten og varsle om dette.
- **Uautoriserte konfigurasjonsendringer:** Loggføring av enhver endring i sikkerhetsinnstillinger. Hvis TLS deaktiveres eller en ny administrator legges til lokalt på maskinen, er dette et kritisk varsel.
- **Endepunkt-sondering:** Oppdagelse av printere som plutselig utfører port-skanning av det interne nettverket (et klassisk tegn på at printeren brukes som brohode for lateral bevegelse).

Praktisk sjekkliste for NSM Kategori 3:

- **SIEM-integrasjon:** Sender alle printere sikkerhetslogger til virksomhetens SIEM-plattform?
- **Sanntidsvarsling:** Mottar SOC automatisk varsler ved kritiske hendelser?
- **Autentiseringslogging:** Logges både vellykkede og mislykkede innloggingsforsøk?
- **Konfigurasjonsendringer:** Oppdages og varsles endringer i sikkerhetsinnstillinger automatisk?
- **Firmware-overvåking:** Varsles uautoriserte firmwareoppdateringer eller integritetsbrudd?
- **Dataeksport:** Overvåkes store eller unormale skanne- og utskriftsjobber?
- **Nettverksatferd:** Oppdages portskanning eller annen mistenkelig trafikk fra printere?
- **Loggkvalitet:** Inneholder logger tilstrekkelig informasjon til etterforskning uten å lagre dokumentinnhold?
- **Korrelering:** Kan hendelser fra printere sammenstilles med andre sikkerhetshendelser i virksomheten?
- **Rapportering:** Mottar ledelsen regelmessige rapporter om sikkerhetsstatus i printermiljøet?

" En printer som ikke er synlig i sikkerhetsovervåkingen, er i praksis usynlig for virksomheten. Det du ikke kan se, kan du heller ikke beskytte."

DEL 7. HÅNDTERE OG GJENOPPRETTE (NSM KATEGORI 4)

For å gjøre denne delen av CISO-guiden enda mer operasjonell, må vi se på de skjulte farene ved en printer-sentrisk krise. Hvis 500 enheter går ned samtidig, er det ikke bare et IT-problem, det er et logistikk- og sikkerhetsmareritt.

Den menneskelige faktoren og tilgangsstyring

NSM påpeker at mange av dagens sårbarheter skyldes svikt i det helt grunnleggende. Ved en hendelse vil angripere utnytte nettopp dette:

- **Rettighets-sanering:** Under gjenoppretting må man fjerne "overflødige" tilganger. Rapporten viser at ansatte ofte har tilganger de aldri skulle hatt. En infisert printer kan ha bufret påloggingsdetaljer til høyt privilegerte brukere.
- **Administrator-hygiene:** Svake administrator-passord er en gjenganger i sikkerhetssvikt. Gjenopprettingsplanen må inkludere å sjekke at man ikke bruker et standard administratorpassord.

Digital avhengighet

Dersom utskrifts- eller administrasjonstjenester blir utilgjengelige, kan dette påvirke virksomhetens evne til å opprettholde normal drift.

- **Resiliens og beredskap:** Virksomheten bør sikre at kritiske utskriftstjenester kan opprettholdes også ved bortfall av skytjenester, Internett-forbindelse eller andre eksterne avhengigheter. Dette kan oppnås gjennom lokale eller hybride løsninger, redundans og alternative driftsmoduser.
- **Alternative driftsmoduser:** Ved bortfall av sky- eller nettverkstjenester bør løsningen kunne gå over i en lokal eller hybrid driftsmodus som opprettholder kritiske funksjoner. Dette reduserer sårbarheten knyttet til enkeltkomponenter og bidrar til kontinuitet i virksomhetens arbeidsprosesser.
- **Kontinuitetsplanlegging:** Virksomheten bør jevnlig vurdere sine avhengigheter til eksterne tjenester og sikre at det finnes dokumenterte tiltak for å opprettholde drift ved lengre avbrudd eller endrede risikobilder.

KI-akselererte angrep krever KI-akselerert respons

Med tanke på at angrep forventes å være nesten fullstendig orkestret av kunstig intelligens (KI), vil 500 printere kunne infiseres på sekunder.

Automatisert identitetskontroll: Man kan ikke manuelt sjekke 500 maskiner. Bruk av PKI-løsningen må automatiseres slik at nettverket kaster ut enheter som ikke kan fremvise gyldig, unikt maskinsertifikat i sanntid.

Mønster-gjenkjenning: Gjenopprettingen må overvåkes av verktøy som ser etter tegn på at viruset forsøker å re-etablere seg via rest-data i printer-minnet.

Den fysiske risikoen (OT-perspektivet)

Vi lærte av hendelsen ved damanlegget i Bremanger i 2025 at digitale inntrengninger kan få fysiske konsekvenser.

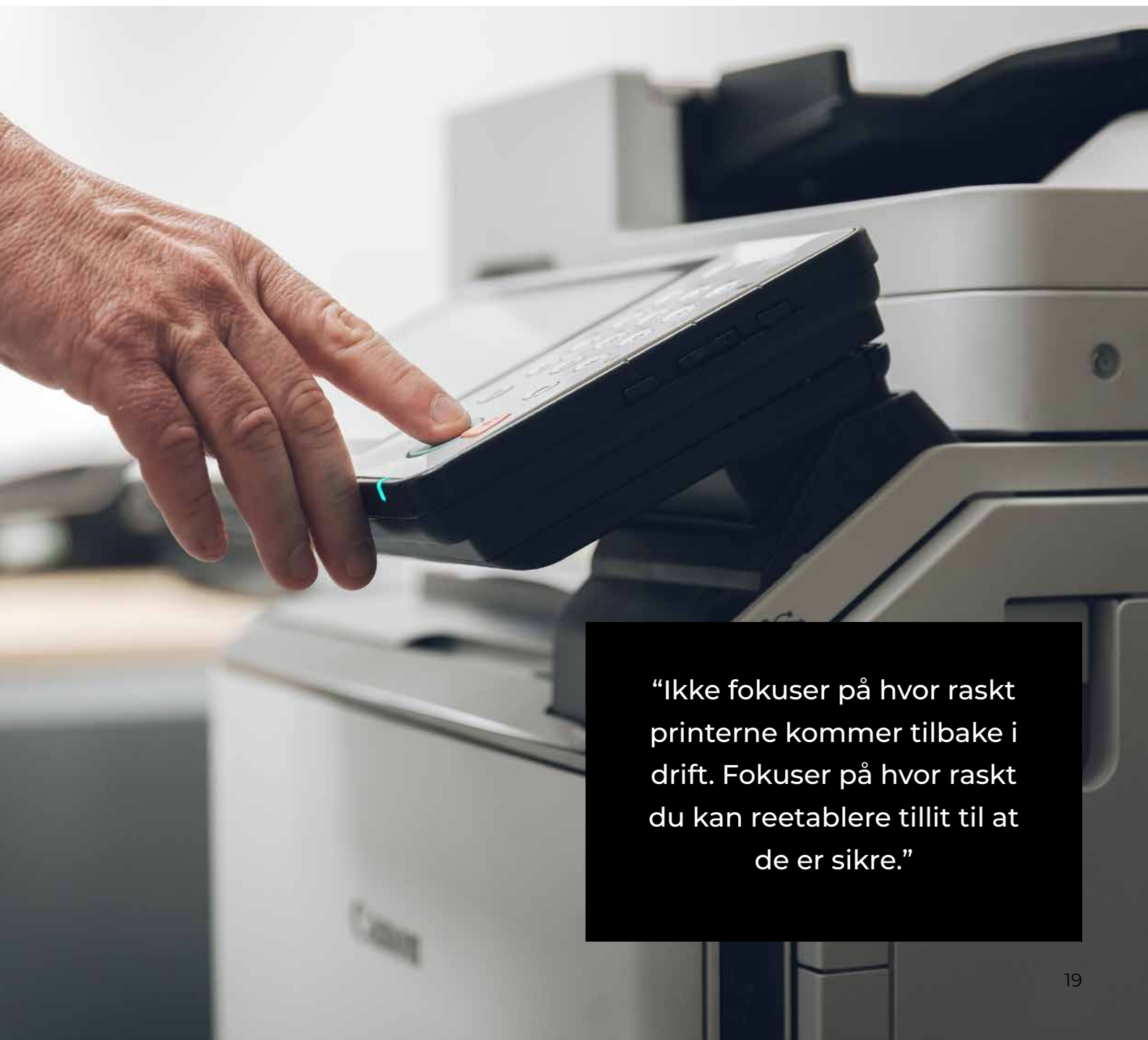
Fysisk sikring: En printerflåte på 500 enheter fungerer som 500 fysiske sensorer og noder i bygningsmassen. Ved et løsepengevirus-angrep må man vurdere om printere koblet mot sensitive soner (som arkiv eller kontrollrom) må prioriteres for fysisk isolering for å hindre sabotasje.

Oppsummert sjekkliste for gjenoppretting av printerflåten:

1. Isolering: Klipp forbindelsen mellom printer-VLAN og resten av bedriftsnettverket umiddelbart.
2. Identitets-revidering: Trekk tilbake alle eksisterende sertifikater i PKI-løsningen for å hindre spoofing.
3. Grunnleggende herding: Oppdater fastvare og bytt ut alle svake passord før enhetene tas inn i varmen igjen.
4. Kontinuitetssjekk: Vurder om dere er for avhengige av én enkelt skyleverandør for utskriftstjenester.

Praktisk sjekkliste for NSM Kategori 4:

- **Beredskapsplan:** Er printermiljøet inkludert i virksomhetens Incident Response-plan?
- **Isoleringsrutiner:** Kan berørte printere raskt kobles fra nettverket ved en hendelse?
- **Gjenoppretting:** Finnes det dokumenterte prosedyrer for reinstallasjon og re-herding av printere?
- **Passordhygiene:** Inngår bytte av administrator-passord som del av gjenopprettingsprosessen?
- **Tilgangsrevisjon:** Gjennomgås bruker- og administratortilganger etter sikkerhetshendelser?
- **Kontinuitet:** Kan kritiske utskriftstjenester opprettholdes ved bortfall av sky- eller nettverkstjenester?
- **Alternative driftsmoduser:** Er lokale eller hybride utskriftsløsninger tilgjengelige ved kriser?
- **Automatisert respons:** Kan kompromitterte enheter automatisk blokkeres eller isoleres?
- **Fysisk sikring:** Er det etablert rutiner for fysisk isolering av printere i sensitive soner?
- **Erfaringslæring:** Gjennomføres evaluering og forbedring etter hendelser?
- **Øvelser:** Testes printerrelaterte sikkerhetshendelser gjennom jevnlig beredskapsøvelser?



“Ikke fokuser på hvor raskt printerne kommer tilbake i drift. Fokuser på hvor raskt du kan reetablere tillit til at de er sikre.”

DEL 8. SUPPLY CHAIN SECURITY: FIRMWARE OG LEVERANDØRSTYRING

Det er avgjørende å se på operasjonell gjennomføring som en helhetlig prosess der man sikrer hele livsløpet til printerflåten. NSM understreker at vi nå befinner oss i en tid der digitale trusler får alvorlige konsekvenser i den fysiske verden, slik vi så med sabotasjen mot damanlegget i Bremanger.

Når man skal håndtere leverandørkjeden og firmware-sikkerhet, er det ikke lenger nok å stole på at produsenten har kontroll; man må kreve full innsikt gjennom en Software Bill of Materials (SBOM). Dette dokumentet fungerer som en detaljert ingrediensliste over all programvare og alle biblioteker i enheten, slik at sikkerhetsteamet umiddelbart kan identifisere om flåten er sårbar for nye trusler uten å vente på leverandørens egen analyse.

Dette henger tett sammen med behovet for hurtig patching av Zero-Day sårbarheter. I en hverdag der kunstig intelligens gjør angrepene både raskere og mer treffsikre, er tiden fra en sårbarhet oppdages til den utnyttes i ferd med å forsvinne.

Rapporten **Risiko 2026** påpeker at det ofte er svikt i det helt grunnleggende som feller virksomheter, for eksempel mangelfull segmentering og svake passord.

Microsoft har lansert Windows Ready Print (tidligere kalt Modern Print Platform) og Windows Protected Print Mode, to teknologier som vil endre hvordan PC-er kommuniserer med skrivere. Allerede den 15. januar 2026 stoppet Microsoft publisering og sertifisering av nye skriverdrivere i Windows Update.

Dette er ikke en liten oppussing, men en full ombygging av utskriftsarkitekturen. Den tradisjonelle driverbaserte utskriftsmodellen – der hver skriver krever sin egen programvare – er på vei ut. I stedet skal Windows bruke en strømlinjeformet, sikker og



universell print-stack som bygger på industrielle standarder som IPP (Internet Printing Protocol). For å fungere i Windows Ready Print må skriveren være Mopria-sertifisert eller støtte tilsvarende IPP-basert teknologi. Mange nyere modeller gjør det allerede, men eldre enheter – særlig de med spesialfunksjoner eller proprietære drivere – vil kunne miste utskriftsfunksjonalitet når WPP slås på. Når Windows fjerner gamle drivere, vil også eksisterende utskriftskøer forsvinne og må bygges opp på nytt.

Når Windows Protected Print Mode er aktivert, blokkeres tradisjonelle leverandørspesifikke drivere, og maskinen tillater kun utskrift via moderne protokoller.

Det høres kanskje enkelt og greit ut – og det er hele poenget. Sikkerheten blir bedre, administrasjonen lettere og risikoen lavere. For IT-avdelinger som i årevis har kjempet med driverpakker og kompatibilitetsproblemer, er dette nærmest en lettelse.

Microsofts mål er tydelig: utskrift skal bli enklere, sikrere og mindre avhengig av leverandørspesifikke løsninger. Men de nærmeste årene blir en overgangsperiode som krever arbeid fra virksomhetene.



“Som CISO må man stille krav til at leverandørene ikke bare leverer maskinvare, men også støtter en moderne sikkerhetsarkitektur. Beslutningene som tas i dag ved valg av teknologi og risikohåndtering, er det som avgjør om virksomheten er i stand til å stå imot de stadig mer automatiserte og målrettede angrepene vi vil se fremover.”

DEL 9. 2027 – HVOR BÆREKRAFT MØTER SIKKERHET

I den tradisjonelle forretningsverdenen har bærekraft (ESG) og informasjonssikkerhet ofte blitt behandlet som to separate spor. I dag er dette skillet i ferd med å forsvinne helt.

Som NSM påpeker i rapporten Risiko 2026, står Norge overfor et digitalt trusselbilde som endrer karakter. De mest modne virksomhetene har beveget seg fra å se bærekraft som et rapporteringskrav til å behandle det som et spørsmål om virksomhetskritisk robusthet. Ressursbruk, energiforbruk, datalagring, leverandør-avhengighet og sikkerhetsrisiko styres nå gjennom de samme beslutningsprosessene. Virksomheter stiller i økende grad krav til både sikkerhet og bærekraft i hele leverandørkjeden. Printleverandører forventes ikke lenger bare å dokumentere lave utslipp, men også sikker programvareutvikling, sporbarhet i komponentleveranser, hendelseshåndtering og evne til å opprettholde tjenestene under kriser. De beste partnerne leverer derfor både ESG-data og dokumentert cybersikkerhet gjennom hele verdikjeden.

Fra maskinleverandør til digital transformasjonspartner

Moderne leverandører av print- og dokumentløsninger har transformert seg fra å være utstyrsprodusenter til å bli strategiske sikkerhetsarkitekter. De leder an i arbeidet med å tette det NSM beskriver som "vesentlige mangler i det forebyggende sikkerhetsarbeidet" ved å flytte fokus fra selve utskriften til den digitale reisen dokumentet tar.

Fysisk papir representerer en betydelig, men ofte oversett, sårbarhet. Mens virksomheter investerer tungt i brannmurer, viser NSMs penetrasjonstest at sårbarheter ofte skyldes svikt i det helt grunnleggende. Ledende partnere hjelper nå virksomheter med å eliminere disse "analoge hullene" gjennom:

- **Sikker digitalisering:** Ved å implementere løsninger for direkte skanning til sikre skytjenester, reduseres behovet for fysisk utskrift. Dette fjerner risikoen for at sensitiv informasjon glemmes i en taxi eller havner i feil hender via en usikret printer.

- **Miljømessig synergi:** Reduksjon i papir- og strømforbruk bidrar direkte til utslippsmål, samtidig som det fjerner fysiske flater for informasjonlekkasje. I tillegg har vi ustrukturert lagring av dokumenter, dupliserte filer og unødvendig dataoppbevaring øker både energiforbruk, kostnader og angrepsflate. Moderne dokumentforvaltning bidrar til å redusere datamengder, forbedre sikkerhetskontroller og redusere ressursforbruk samtidig.

Reduksjon av papirflyt handler ikke bare om miljø. Hvert fysisk dokument representerer en ukontrollert kopi av virksomhetens informasjon. Digitale arbeidsprosesser gir sporbarhet, tilgangskontroll og revisjonsmuligheter som ikke er mulig å oppnå med papirbaserte prosesser.

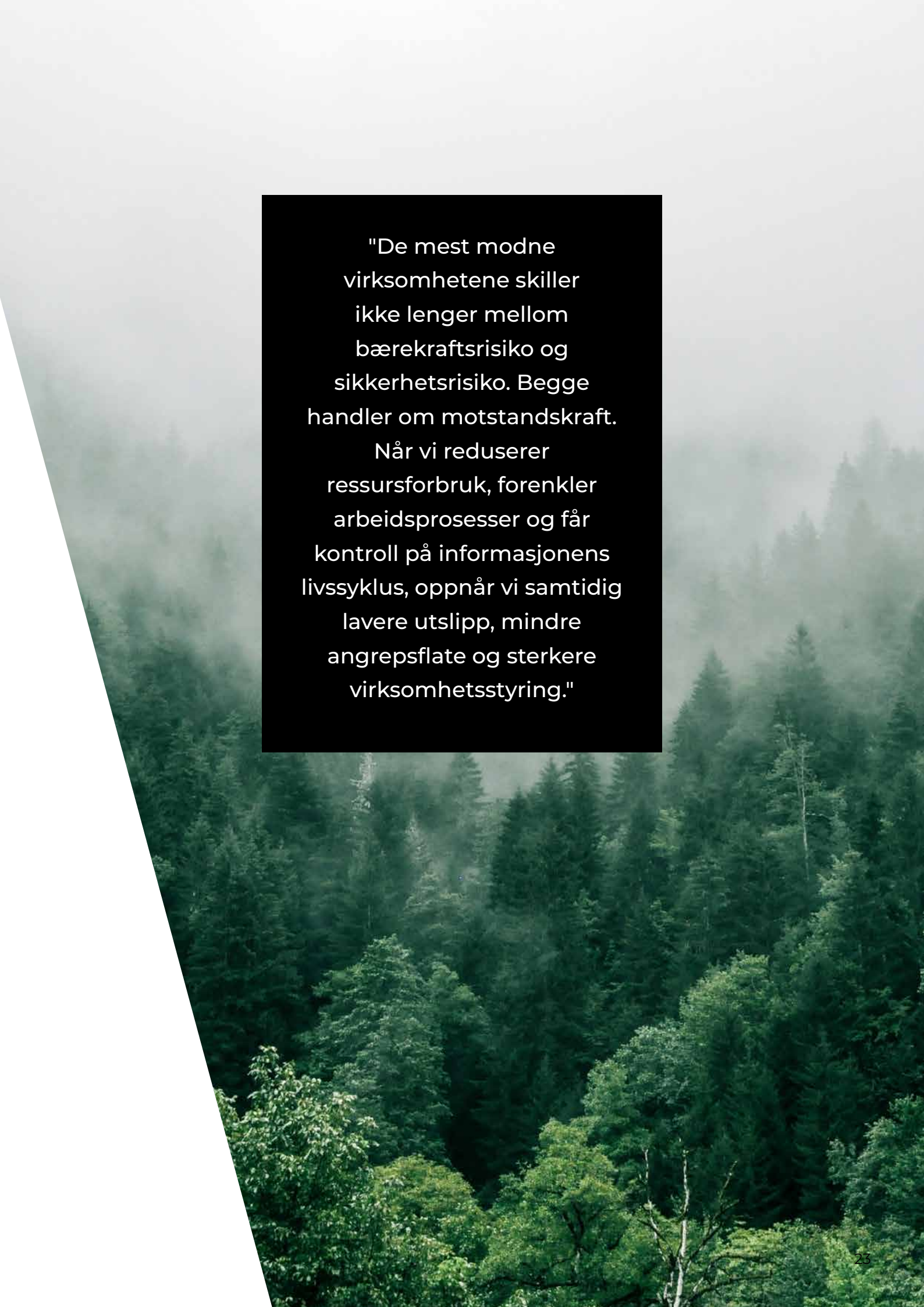
NATO, miljø og strategisk motstandskraft

Det er ikke bare sivile myndigheter som ser denne sammenhengen; NATO har også integrert klima- og miljøhensyn som en kjernekomponent i sine sikkerhetsanalyser. Resiliens krever bærekraft.

Den sirkulære sikkerhetsmodellen

NSM-sjefen understreker at valgene vi tar i dag, avgjør morgendagens risiko. Innovative partnere svarer på dette ved å tilby en sirkulær livssyklus for teknologi:

- **Intelligent flåtestyring:** Ved å bruke KI-drevet analyse for å optimalisere utskriftsvolumet, forlenges utstyrets levetid. Dette er bra for miljøet og gir virksomheten rom til å planlegge sikre strategier for skytjenester, slik NSM anbefaler.
- **Sirkulær sikkerhet som standard:** Fremtidsrettede partnere tar ansvar for hele livsløpet. De sikrer at minnemoduler slettes korrekt før maskiner resirkuleres, slik at "glemte" printere i et hjørne aldri blir en kilde til datainnbrudd. Sirkulær sikkerhet handler om å sikre informasjon gjennom hele teknologiens livssyklus – fra anskaffelse og drift til gjenbruk og avhending. Hver fase representerer både en miljømessig og sikkerhetsmessig risiko dersom den ikke håndteres kontrollert.

The background of the page is a photograph of a dense forest. In the foreground, there are lush green deciduous trees. In the background, there are tall, dark evergreen trees shrouded in a thick mist or fog. A large, black, semi-transparent rectangular box is positioned in the upper-middle part of the image, containing white text. The text is arranged in two paragraphs. The overall mood is serene and natural.

"De mest modne
virksomhetene skiller
ikke lenger mellom
bærekraftsrisiko og
sikkerhetsrisiko. Begge
handler om motstandskraft.

Når vi reduserer
ressursforbruk, forenkler
arbeidsprosesser og får
kontroll på informasjonens
livssyklus, oppnår vi samtidig
lavere utslipp, mindre
angrepsflate og sterkere
virksomhetsstyring."

DEL 10. SJEKKLISTE FOR BEREDSKAP

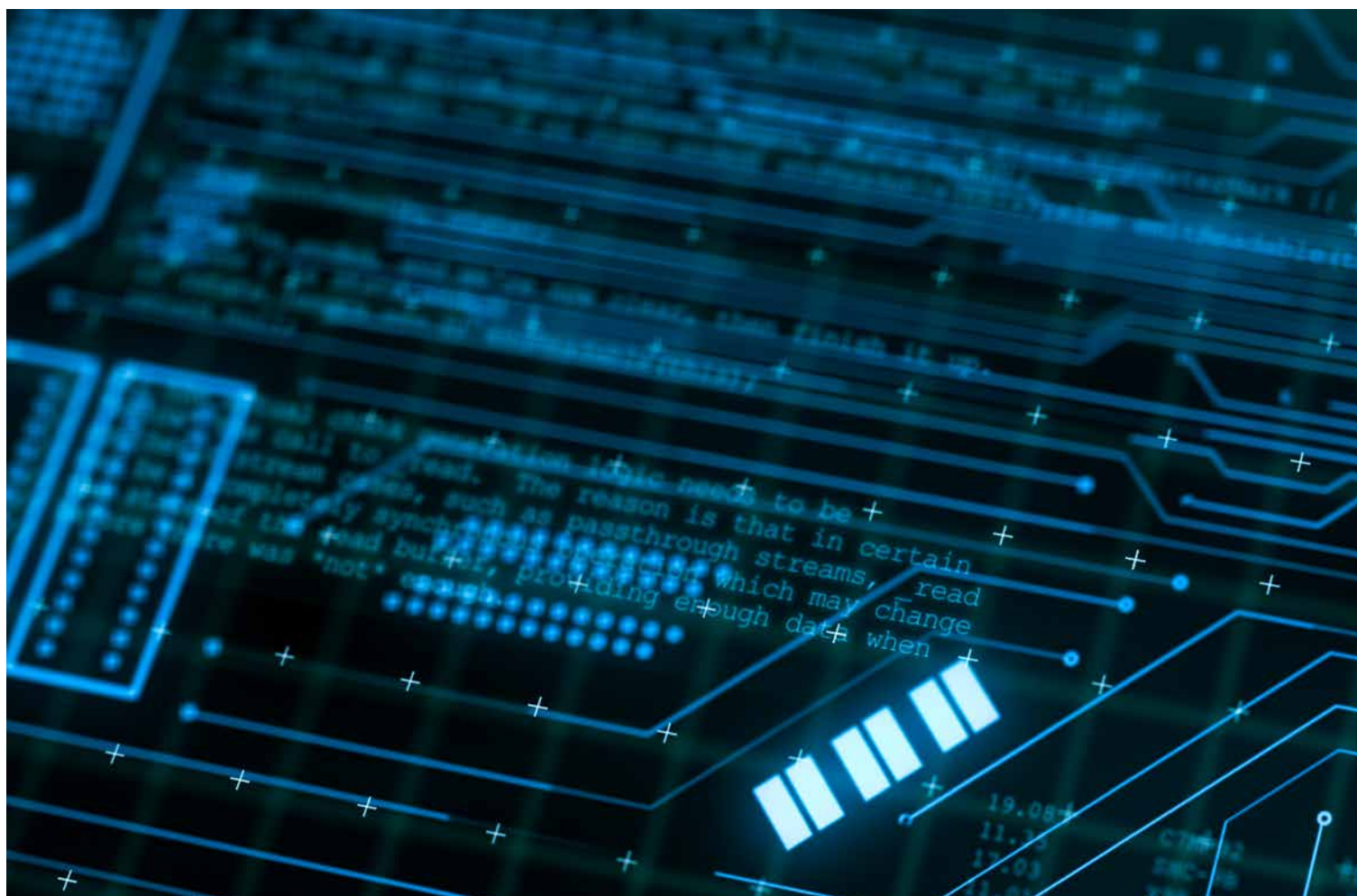
Denne handlingsplanen adresserer behovet for å våkne opp og ta valg i dag som sikrer virksomheten i morgen.

Strategi og Kontroll

- 1. Etabler gode krise-planer for kritiske skytjenester:** Utarbeid konkrete planer for hvordan virksomheten effektivt kan forholde seg til kriser der nettverket går ned eller er utilgjengelig.
- 2. Gjennomfør "Back-to-Basics" revisjon:** Identifiser og fjern svake administratorpassord, rydd opp i ansattes tilganger som aldri skulle vært tildelt, og sikre korrekt segmentering av printere på nettverket.
- 3. Verifiser sikkerheten i utskriftsinfrastrukturen:** Sørg for at alle skrivere, multifunksjonseenheter og printservere er oppdatert med siste sikkerhetsoppdateringer, benytter sterk autentisering og er konfigurert i henhold til virksomhetens sikkerhetskrav. Gjennomfør regelmessige kontroller for å identifisere sårbarheter og avvik.

Operasjonell Sikkerhet (inkludert Print og IoT)

- 4. Sikre printerflåten med unike identiteter:** Implementer krav om unike maskinsertifikater utstedt av bedriftens PKI-løsning for alle nettverkstilsluttede printere for å forhindre identitetsforfalskning (spoofing).
- 5. WINDOWS READY PRINT:** Forbered deg på å aktivere Windows Protected Print. Tradisjonelle skriverdrivere fra printerleverandører er i ferd med å avvikles, og erstattes snart av IPP baserte skriverdrivere fra Microsoft.
- 6. Krev SBOM fra leverandører:** Still krav om Software Bill of Materials ved alle nye anskaffelser av fastvare og maskinvare for å ha full oversikt over sårbarheter i leverandørkjeden.



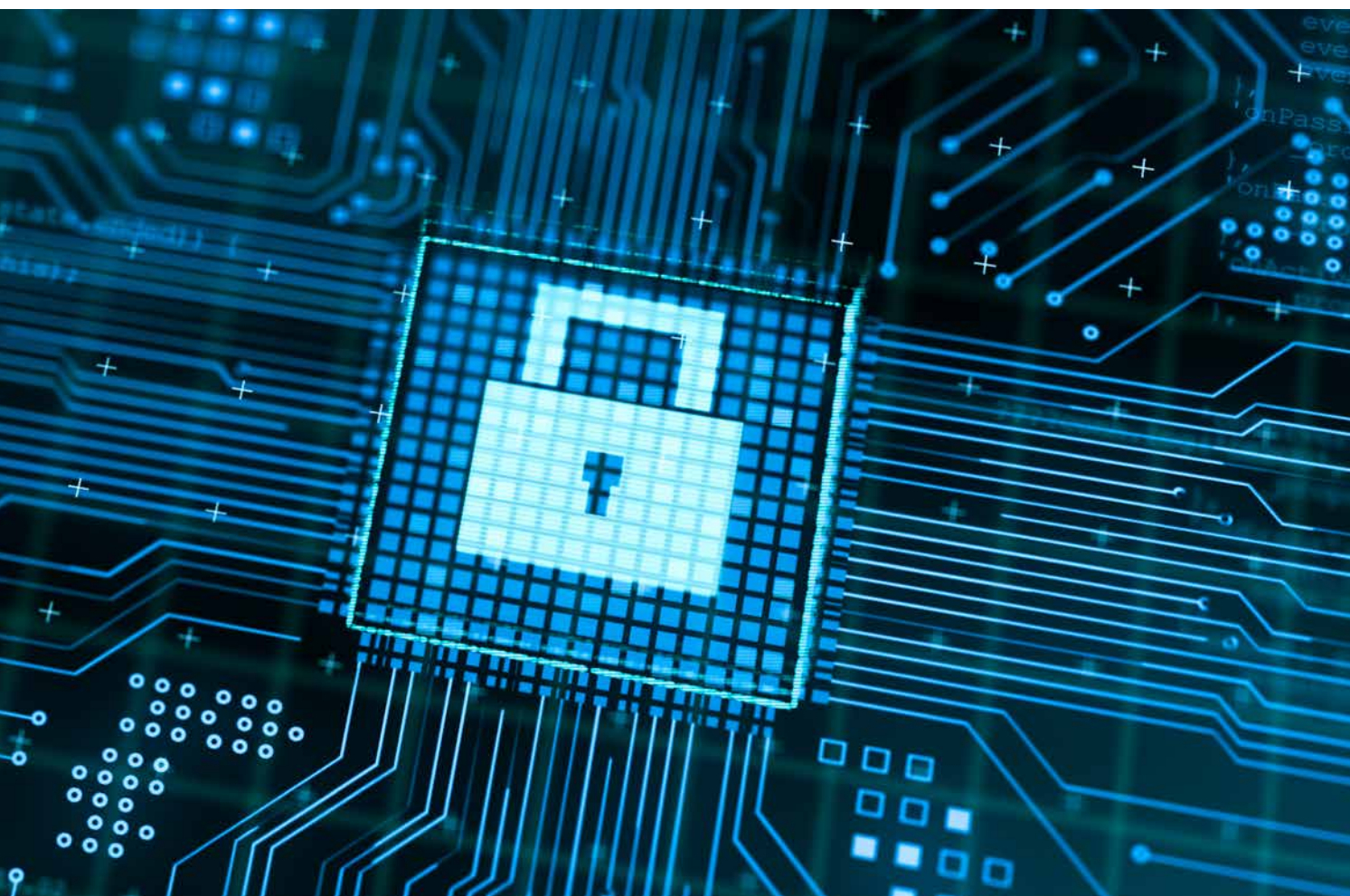


Personvern og Angrepshåndtering

- 7. Sårbarhetsanalyse av printmiljø:** Evaluer risikoen for eksponering av sensitiv informasjon gjennom skrivere, utskriftskøer og etterlatte utskrifter. Tren ansatte i sikker håndtering av utskrifter og i å gjenkjenne forsøk på sosial manipulering basert på informasjon hentet fra printmiljøet.
- 8. Oppdater Incident Response for fysiske konsekvenser:** Revider beredskapsplaner slik at de inkluderer scenarier der digitale angrep gir fysiske utslag, som sabotasje av infrastruktur eller kontrollsystemer.

Bærekraft og Fremtid

- 9. Integrer bærekraft i sikkerhetsanalysen:** Implementer NATO-inspirerte miljøhensyn i risikovurderingene og prioriter digitalisering av arbeidsflyt for å redusere mengden fysisk papir og dermed faren for informasjonslekkasje.
- 10. Gjennomfør inntrengningstesting av "glemte" noder:** Test murene ved å la eksperter forsøke å ta kontroll over systemet via perifere enheter som printere og sensorer, slik NSMs egne eksperter gjorde med nedslående resultater i fjor.



DEL 11. TOTALFORSVARSÅRET 2026

Regjeringen har gitt Direktoratet for samfunnssikkerhet og beredskap (DSB) – sammen med Forsvaret, i oppdrag å lede planleggingen og gjennomføringen av Totalforsvarsåret 2026. Målet er å styrke Norges evne til å forebygge og håndtere sikkerhetspolitiske kriser og krig.

I et moderne totalforsvar er skillet mellom sivil og militær sektor hvisket ut, fordi den digitale infrastrukturen, som eies og driftes av det sivile, er det som holder Norge i gang i krisetider.

1. Hva er Totalforsvarsåret 2026?

I 2026 er ikke lenger "forsvaret av Norge" noe som bare foregår ved grensene og av de militære. Tanken er at det foregår like mye i bedriftene. Totalforsvarskonseptet innebærer at alle virksomheter, både offentlige og private, er en del av den nasjonale beredskapen.

Digital suverenitet: NSM advarer om at vår ekstreme avhengighet av utenlandske skytjenester er en nasjonal sårbarhet.

Tverrsektoriell risiko: Svikt i én etat eller bedrift kan forplante seg til hele samfunnet.

2. Hva betyr det for CISO-en?

For en CISO betyr 2026 at ansvarsområdet utvides fra å beskytte bedriftens data til å beskytte en del av nasjonens operative evne.

- **Krav om "operasjonell resiliens":** CISO-en må kunne dokumentere hvordan virksomheten kan fortsette normal drift i en kontrollert nød modus dersom sentrale sky- eller nettverkstjenester blir utilgjengelige over lengre tid.
- **Fokus på det grunnleggende:** NSM har vist at de kan ta full kontroll over statlige etater ved hjelp av enkle feil. CISO-en må nå bevise at "murene holder" mot både statlige aktører og KI-styrte angrep.
- **NATO-tilpasning:** Sikkerhetsanalysen må nå inkludere miljø og forsyningskjeder, slik NATO krever.

3. Hvorfor er printsikkerhet en viktig del av dette?

Det hjelper lite å ha sikre servere hvis "bakdøren" står åpen. I Totalforsvarsåret 2026 er printeren (MFP-en) definert som et kritisk endepunkt av tre grunner:

- **Inngangsporten for sabotasje:** En printer er en fullverdig datamaskin på innsiden av nettverket. Hvis denne ikke er sikret, kan en angriper bruke den som et brohode for å lamme resten av virksomheten.
- **Informasjonslekkasje i en krise:** I en beredskaps-situasjon øker behovet for fysiske dokumenter og ordre. Uten kontroll på hvem som printer hva, og uten kryptering av datastrømmen, er printerflåten det svakeste leddet for informasjonslekkasje.
- **Den "glemte" noden:** NSM peker på at sårbarheter går igjen på tvers av sektorer. Printere står ofte igjen med fabrikkinnstillinger og svake passord. I et totalforsvarsperspektiv er hver eneste usikret printer en potensiell mulighet for en motstander til å drive digital sabotasje.



“Totalforsvarsåret 2026 krever at vi slutter å se på sikkerhet i siloer. Printsikkerhet er ikke lenger et "kontorproblem", det er en integrert del av virksomhetens – og dermed nasjonens – evne til å motstå og gjenopprette drift etter angrep. God printsikkerhet i 2027 handler om å fjerne anonyme enheter fra nettverket og sikre at alle noder er verifiserte og herdede.”

Del 12: Nasjonal sikkerhetsmåned 2026: Digital dømmekraft i fokus

I oktober markeres Nasjonal sikkerhetsmåned for 16. år på rad. Kampanjen er en del av en europeisk satsing på digital sikkerhet, der virksomheter, organisasjoner og privatpersoner oppfordres til å styrke sin motstandskraft mot digitale trusler.

Årets tema er «**Digital dømmekraft – Små valg. Store konsekvenser.**» Budskapet er at sikkerhet ikke bare handler om teknologi, men om valgene vi tar hver dag. Hver gang vi klikker på en lenke, åpner et vedlegg, deler informasjon eller godkjenner en forespørsel, gjør vi sikkerhetsvalg som kan påvirke både oss selv og virksomheten vi jobber i. Et øyeblikks ettertanke kan være forskjellen mellom en trygg handling og en sikkerhetshendelse.

For ansatte er digital dømmekraft en viktig del av arbeidshverdagen. Angrep starter ofte med en e-post, en melding eller en tilsynelatende legitim forespørsel. Ved å være oppmerksom på uvanlige henvendelser, kontrollere avsenderen og melde fra om mistenkelige aktiviteter, bidrar hver enkelt til å styrke virksomhetens sikkerhet. En god sikkerhetskultur bygges gjennom små handlinger som gjentas hver dag.

Ledere har et særlig ansvar for å skape rammer som gjør det enkelt å ta gode sikkerhetsvalg. Når ledelsen prioriterer digital sikkerhet, støtter opplæring og oppmuntrer ansatte til å si fra om feil og avvik, etableres en kultur der sikkerhet blir en naturlig del av arbeidsprosessene. Sterk sikkerhetskultur er ikke et resultat av én kampanje, men av mange små beslutninger over tid.

Nasjonal sikkerhetsmåned minner oss om at cyberangrep ikke alltid lykkes på grunn av avansert teknologi, men ofte fordi noen blir lurt til å ta et feil valg. Derfor er digital dømmekraft en av de viktigste forsvarsmekanismene vi har – både på jobb og privat. Små valg kan få store konsekvenser, men de samme valgene kan også være det som stopper det neste angrepet.





Del 13: Et tilbakeblikk: Nasjonal sikkerhetsmåned 2025: Digital beredskap

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 multifunksjonseenheter er ofte en blindsoner i sikkerhetsarbeidet. Ikke overse dette i virksomhetens sikkerhetsarbeid.

Er din digitale beredskapskasse komplett – og oppdatert?

DEL 14. CYBERSIKKERHETS TRUSLER 2027

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

Agentisk KI og autonome cyberangrep

2026 handlet om KI-genererte e-poster og nettsider. 2027 vil i større grad preges av agentiske KI-systemer som kan planlegge, tilpasse og gjennomføre deler av angrepskjeden automatisk. I 2024 var gjennomsnittstid til første observerte utnyttelse om lag 5 dager, ned fra 32 dager året før. I 2026 ser vi at angripere i økende grad operasjonaliserer sårbarheter i løpet av timer eller få dager, og flere analyser peker på gjennomsnittstider på under ett døgn for aktivt utnyttede sårbarheter.

2

Hyperrealistiske deepfakes og identitetssvindel

Deepfakes blir stadig vanskeligere å oppdage. Angripere vil kombinere video, stemme, sosiale medier og lekkede data for å gjennomføre svært troverdige bedrageriforsøk mot ledere, ansatte og kunder.

3

Ransomware 3.0 og destruktive angrep

Løsepengevirus vil fortsatt være en av de største truslene, men flere aktører vil fokusere på driftstans, sabotasje og utpressing fremfor ren kryptering av data. Målet vil ofte være maksimal forretningsmessig skade.

4

Angrep via leverandørkjeder og tredjepartsleverandører

NIS2, DORA og NSMs risikovurderinger har satt søkelys på leverandørkjeden. Angripere vet at mindre leverandører ofte har svakere sikkerhet enn hovedmålet, og vil fortsette å bruke disse som inngangsport.

5

Angrep mot identitetssystemer

Identitet har blitt den nye sikkerhetsperimeteren. Tyveri av sesjonskapsler, MFA-omgåelse, token-tyveri og kompromittering av identitetsplattformer vil være blant de mest effektive angrepsmetodene i 2027.

6

IoT-, OT- og printerrelaterte angrep

Flere virksomheter får stadig flere tilkoblede enheter. Printere, kameraer, sensorer, industrielle kontrollsystemer og andre IoT-enheter vil fortsatt være attraktive mål fordi de ofte har svakere overvåking og sikkerhetskontroller enn tradisjonelle servere og klienter.

7

"Harvest Now, Decrypt Later" og overgangen til post-kvantekryptografi

Flere statlige aktører samler allerede inn krypterte data i dag med mål om å dekryptere dem når kvantedatamaskiner blir kraftige nok. Selv om en fullskala kvantebrudd ikke er sannsynlig i 2027, vil risikoen knyttet til kryptografisk gjeld og manglende PQC-strategi bli stadig viktigere.

A man with a beard, wearing a dark sweater and trousers, is walking through a server room. He is holding a light blue laptop. The room is filled with rows of server racks, and the floor has a grid pattern. The lighting is dim, with some blue light emanating from the server racks. A large black text box is overlaid on the right side of the image.

"Trusselbildet i 2027 vil i stor grad være en videreføring av 2026, men med økt bruk av kunstig intelligens, mer avanserte identitetsangrep og større søkelys på leverandørkjeder og kritisk infrastruktur. Samtidig vil overgangen til post-kvantekryptografi, nye regulatoriske krav og et mer komplekst geopolitisk landskap kreve at CISO-er tenker langsiktig om både teknologi, risiko og motstandsdyktighet. Når identitet, data og tilkoblede enheter blir stadig viktigere mål, vil virksomheter som kombinerer Zero Trust, cyber resilience og sikkerhetskultur være best rustet til å møte truslene i 2027."



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



Canon