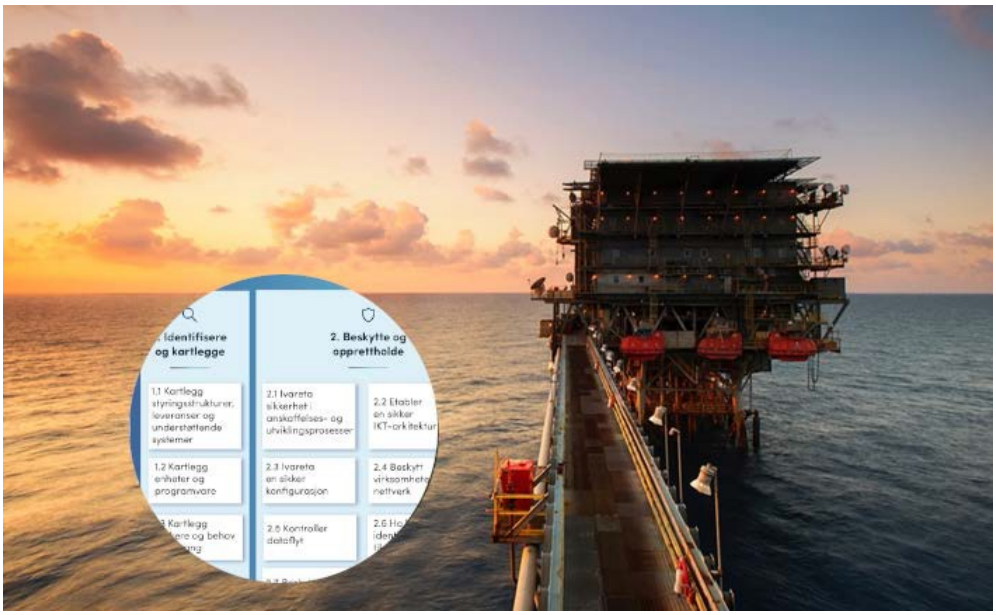
2021:00055 - Åpen

Rapport

Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

Forfattere
Martin Gilje Jaatun, Egil Wille, Karin Bernsmed, Stine Skaufel Kilskar



SINTEF Digital
2021-01-29

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim
Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer

IKT-sikkerhet – Robusthet i petroleumssektoren 2020

EMNEORD:
Cybersikkerhet
OT-system
Regelverk

VERSJON
1.0

DATO
2021-01-29

FORFATTERE,
Martin Gilje Jaatun, Egil Wille, Karin Bernsmed, Stine Skaufel Kilskar

OPPDRAGSGIVER(E)
Petroleumstilsynet

OPPDRAGSGIVERS REF.
Arne Halvor Embergsrud

PROSJEKTNR
102022556

ANTALL SIDER OG VEDLEGG:
48 (3 vedlegg)

SAMMENDRAG
Formålet med denne rapporten er å gi økt forståelse for grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer (OT-systemer) i norsk petroleumsvirksomhet basert på NSMs grunnprinsipper for IKT-sikkerhet. Vi har også vurdert i hvilken grad elementer i NVEs kraftberedskapsforskrift og NIST CyberSecurity Framework (CSF) er relevante for industrielle IKT-systemer i petroleumsvirksomheten.

Denne rapporten er en av seks SINTEF-rapporter fra prosjektet: "IKT-sikkerhet – Robusthet i petroleumssektoren 2020". Prosjektet har innhentet kunnskap om risiko, sårbarheter og IKT-sikkerhet for industrielle IKT-systemer

UTARBEIDET AV
Martin Gilje Jaatun

SIGNATUR
Martin G. Jaatun
Martin G. Jaatun (29. Jan. 2021 10:21 GMT+1)

KONTROLLERT AV
Tor Onshus

SIGNATUR
Tor Onshus
Tor Onshus (29. Jan. 2021 13:28 GMT+1)

GODKJENT AV
Maria Bartnes

SIGNATUR
Maria Bartnes

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
2021:00055	978-82-14-06479-7	Åpen	Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2021-01-29	Endelig versjon

Innholdsfortegnelse

Sammendrag

Formålet med denne rapporten er å vurdere i hvilken grad tiltakene i NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0 er relevante for industrielle IKT-systemer (OT-systemer) i petroleumsvirksomheten, samt å vurdere om det finnes komplementære tiltak i Kraftberedskapsforskriften og NIST CyberSecurity Framework (CSF).

I figuren over illustreres i hvilken grad vi vurderer at tiltakene i de enkelte prinsippene er relevante for operasjonsteknologi (OT). Prinsipper merket med ☑ vurderes til å være full ut relevante for OT, mens prinsipper merket [!] inneholder ett eller flere tiltak som krever ytterligere vurdering/tillempning i OT-miljøer. Bare ett prinsipp er merket ☒, som indikerer at vi mener at det ikke er relevant for OT. Av totalt 118 tiltak er 96 ☑, 18 [!] og 4 ☒.

Vi mener at NSMs Grunnprinsipper for IKT-sikkerhet (versjon 2.0) i stor grad er relevante for OT-systemer, men at det finnes relevante enkelttiltak i NIST CSF som ikke er dekket av Grunnprinsippene. Noen av disse dekkes av andre publikasjoner fra NSM, men vi har identifisert 27 forslag til tiltak fra NIST CSF som vi anbefaler som tillegg til Grunnprinsippene. Vi har også vurdert § 6-9 "Digitale informasjonssystemer" i Kraftberedskapsforskriften, og finner at dette dekkes av tiltakene i Grunnprinsippene, med unntak av at vi savner rettledning (eller referanse(r) til rettledning) for risikovurdering i tiltakene i Grunnprinsippene, som i versjon 2.0 kun refererer til retningslinjer som en del av "utdypende informasjon". Vi anbefaler derfor å enten peke på en slik rettledning, eller utarbeide en detaljert rettledning for risikovurdering som en del av Grunnprinsippene.

Executive summary

The purpose of this report is to assess to what extent the controls in the NSM basic principles for ICT security (version 2.0) are relevant for industrial ICT systems (OT systems) in the petroleum sector, and to assess whether there are complementary controls in Kraftberedskapsforskriften and the NIST CyberSecurity Framework.

Our assessment is that the NSM basic principles to a great extent are relevant for OT systems, provided special care is taken with selected controls, as indicated in this report. Out of 118 NSM controls, we find that 96 are fully relevant (☑); 18 are relevant, but require special care ([!]); and 4 controls are not relevant for OT systems (☒).

The NIST CSF does contain certain controls which are not covered by the NSM basic principles for ICT security, but these gaps are largely covered by other NSM publications. We have suggested 27 new controls for security in OT systems based on the identified gaps in NIST CSF. We find that § 6-9, "Digital information systems" in Kraftberedskapsforskriften is covered by the NSM basic principles, but recommend that a more detailed guideline in performing ICT security risk assessments is either explicitly referred to, or added as a new component of the basic principles.

1 Innledning

Denne rapporten presenterer en vurdering av i hvilken grad de enkelte tiltak i Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet versjon 2.0 [1] er relevante for industrielle IKT-systemer (OT-systemer) i petroleumsvirksomheten, samt om det er tilleggselementer i NVE Forskrift om sikkerhet og beredskap i kraftforsyningen (Kraftberedskapsforskriften) [2] eller i NIST CyberSecurity Framework (CSF) [3] som er relevante for OT-systemer.

1.1 Bakgrunn

Petroleumstilsynet har gitt SINTEF i oppdrag å undersøke ulike sider av IKT-sikkerhet og robusthet i petroleumssektoren. Hovedmålet er å innhente kunnskap om risiko, trusler, sårbarheter, samt viktighet av IKT-sikkerhet for industrielle systemer. Prosjektet skal bidra til å øke forståelsen for IKT-sikkerhet i petroleums-virksomheten og slik være med å øke robustheten mot uønskede hendelser. SINTEF skal også gi innspill til oppdatering av Petroleumstilsynets regelverk for oppfølging av IKT-sikkerhet.

Vedlegg A gir en beskrivelse av de seks delprosjektene.

Dette prosjektet er en del av en større satsing innenfor IKT-sikkerhet i Petroleumstilsynet. Sentrale problemstillinger for Ptil er:

- Hvordan håndterer industrien endringsprosesser knyttet til innføring av ny teknologi?
- Hvordan vil digitalisering påvirke HMS-forhold og risikostyring?

SINTEFs arbeid i dette prosjektet er i stor grad en videreføring av tidligere prosjekter gjennomført av DNV GL og SINTEF innen samme temaområde [4].

1.2 Mål og hensikt

Hovedmålet for denne leveransen er å gi næringen økt forståelse av hvordan de kan bruke NSMs Grunn-prinsipper for IKT-sikkerhet (versjon 2.0) i industrielle IKT-systemer i petroleumsvirksomheten. Vi har også vurdert relevante elementer i NVEs beredskapsforskrift, og i tillegg identifiserer vi enkelttiltak i NIST CyberSecurity Framework (CSF) som ikke dekkes av disse grunnprinsippene, men som vi mener er relevante for OT-systemer.

1.3 Begrensninger

Vurdering av grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer er basert på dagens OT-løsninger i petroleumsvirksomheten fremfor nye trender.

1.4 Begreper, definisjoner og forkortelser

Følgende definisjoner er brukt for sentrale begreper:

Begrep	Definisjon/beskrivelse
Attributtbasert aksesskontroll (ABAC)	Tilgangsstyring hvor tillatelser bestemmes ut ifra attributter knyttet til bruker, ressurs og/eller omgivelser. Hvilke attributter som kreves for forskjellige handlinger defineres i et sett med kriterier (policies) som styres sentralt.
Endringskonsekvensanalyse	Analyse av konsekvensene ved å utføre en endring (f.eks. å installere en sikkerhetsoppdatering)
Herding	Øke en komponents motstandsdyktighet mot angrep ved f.eks.: å fjerne unødvendig programvare, tjenester, etc.; ved å lukke ubrukte TCP-porter; ved å oppgradere/bytte ut programvare til versjoner som er mer motstandsdyktige mot angrep
Hvitlisting	Begrensning av hvilke programmer som kan kjøre på et system, hvilke porter det aksepteres trafikk fra, hvilke typer data som aksepteres. Fungerer etter prinsippet "alt som ikke er tillatt er forbudt".
IKT-hendelse	Normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (Ptil SF §29 [5])
Industrial Internet of things (IIoT)	Industriell anvendelse av IoT, f.eks. ved å samle inn driftsdata for prosessoptimalisering ved hjelp av internett-tilkoblede sensorer. Underkategori av IoT.
Industrielle IKT-systemer	Systemer som støtter, kontrollerer og overvåker industriell produksjon
Inntrengingstest / Pentest	En planlagt og forhåndsbestilt operasjon for å avdekke fysiske, logiske, tekniske, menneskelige og administrative sårbarheter ved et informasjonssystem og for å teste sikkerheten i systemet.
Internet of things (IoT)	Et nettverk av fysiske enheter med innebygd funksjonalitet for å samle data (sensorer) og/eller påvirke prosesser (aktuatorer). Enhetene har innebygd programvare og kan utveksle informasjon med hverandre via internett, ofte ved hjelp av skytjenester.
Operasjonell teknologi (OT)	Teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner
Rollebasert aksesskontroll (RBAC)	Tilgangsstyring hvor tillatelser bestemmes basert på brukergrupper og roller. RBAC fungerer ved at brukere og brukergrupper gis et sett med roller, mens det for hver enkelt rolle defineres et sett med tillatelser.
Sikring	Sørge for at konfidensialitet, integritet, og/eller tilgjengelighet av informasjon ivaretas
Tjenesteutsetting	Å anskaffe varer eller tjenester fra ekstern leverandør i stedet for å levere dem selv. Tjenesteutsetting gjør det mulig for en virksomhet å fokusere mer på sin kjernevirksomhet og mindre på "støttefunksjoner".

Følgende forkortelser er brukt i rapporten:

Forkortelse	Beskrivelse
ABAC	Attribute Based Access Control
BIA	Business Impact Analysis
CERT	Computer Emergency Response Team
CAIC	Control, Availability, Integrity, Confidentiality
CIA	Confidentiality, Integrity, Availability
CSF	Cybersecurity Framework
DAC	Discretionary Access Control
DMZ	Demilitarized Zone
DNS	Domain Name System
HMI	Human Machine Interface
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIoT	Industrial internet of things
IKT	Informasjons- og kommunikasjonsteknologi
IMS	Information Management System
IoT	Internet of things
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISAC	Incident Sharing and Analysis Center
IT	Informasjonsteknologi
NIST	National Institute of Standards and Technology
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OS	Operatørstasjon
OT	Operasjonell teknologi
PLS	Programmerbar logisk styring
RBAC	Role Based Access Control

1.5 Metode og gjennomføring

Rapporten er utarbeidet ved dokumentgjennomgang og innspill fra aktører både i og utenfor petroleums-virksomheten, samt prosjektgruppens kompetanse innenfor IKT-sikkerhet og OT-systemer.

1.6 Rapportstruktur

Kapittel 2 presenterer en overordnet beskrivelse av hvordan OT skiller seg fra IT, og hvilke tilleggshensyn man må ta i OT.

I kapittel 3 presenteres og vurderes i hvilken grad tiltakene i NSMs grunnprinsipper for IKT-sikkerhet er relevante for OT-systemer i petroleumsvirksomheten.

Kapittel 3 er delt inn etter samme mal som grunnprinsippene, dvs. at nummereringen starter på nytt med "NSM 1, NSM 1.1". I tillegg inkluderer kapittelet forslag til tilleggskrav basert på en gjennomgang av henholdsvis Kraftberedskapsforskriften og NIST Cybersecurity Framework.

Kapittel 4 oppsummerer SINTEFs vurderinger og konklusjoner.

Vedlegg A gir en kort oppsummering av de øvrige delprosjektene som denne rapporten er skrevet i sammenheng med.

I vedlegg B beskrives bakgrunnen for foreslåtte tilleggstiltak basert på gap mellom NSMs grunnprinsipper for IKT-sikkerhet og Kraftberedskapsforskriften.

I vedlegg C presenteres en analyse av i hvilken grad grunnprinsippene dekker elementer i NIST CSF, samt forslag til tilleggstiltak basert på denne analysen.

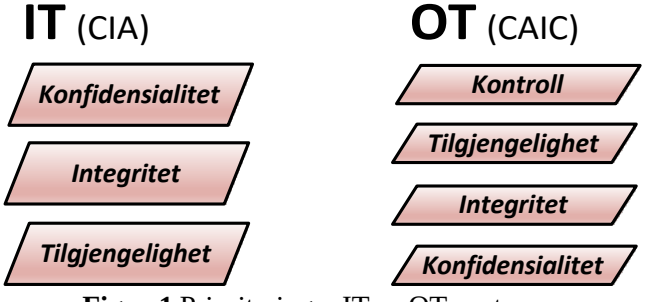
2 Hvordan er OT forskjellig fra IT?

Informasjonsteknologi (IT) er et nokså velkjent fagområde som de fleste har et forhold til. IT-systemer håndterer primært informasjon, og består av programvare og maskinvare som lagrer, prosesserer og overfører data. Operasjonell teknologi (OT) er et mindre kjent begrep, men spiller en vel så viktig rolle som IT og er en viktig del av de fleste industrielle systemer og kritisk infrastruktur. I likhet med IT håndterer OT også data, men i motsetning til IT-systemer har OT-systemer et betydelig fysisk grensesnitt i form av forskjellige *sensorer* (trykksensor, temperatursensor, hastighetsmåler, etc.) og *aktuatorer* (ventil, pumpe, bryter, motor, etc.) for å overvåke og styre fysiske tilstander. IT brukes primært til å ha kontroll over informasjon, mens OT primært brukes til å ha kontroll over fysiske prosesser.

Moderne kraftverk, strømnett, transportsystemer, prosessanlegg og fabrikker er alle avhengige av at OT-systemer sørger for trygg og effektiv drift. Dette gjøres ved at programvare (i kombinasjon med sensorer, ventiler, pumper, brytere, motorer osv.) regulerer fysiske variabler/tilstander ved hjelp av relevante sensorer og aktuatorer. Større avvik fra ønskede verdier kan føre til store ødeleggelser – i verste fall tap av liv, og det er derfor avgjørende at OT-systemene som styrer slike prosesser er robuste mot feil og forblir operative.

OT-systemer er ikke hyllevare. De blir spesialtilpasset for en gitt anvendelse, og inneholder ofte egenutviklet (proprietær) programvare og/eller maskinvare. Selv om enkelte OT-systemer kan ha de samme grunnleggende funksjonene og fremstå som veldig like, vil det som regel være små, men viktige forskjeller mellom dem, både fysisk (hvilke komponenter som utgjør systemet og hvordan disse samhandler) og digitalt (hvordan hver enkelt komponent er konfigurert og hvilken programvare som kjører). Selv såkalte søsterinnretninger, som i utgangspunktet skal være identiske, vil ofte ha små forskjeller mellom sine tilsvarende OT-systemer, f.eks. fordi enkelte komponenter som blir brukt på skip A ikke er tilgjengelig ved bygging av skip B og må erstattes med "tilsvarende" komponenter, eller fordi det blir besluttet å gjøre små endringer mellom A og B for å bedre ytelse eller redusere kostnad. OT-systemenes "unikhet" gjør at de må vedlikeholdes og oppdateres individuelt, og det er avgjørende at vedlikeholdsansvarlig har høy OT-kompetanse og forstår hvordan endringer kan påvirke systemets funksjoner, slik at uønskede effekter unngås. Vanligvis er det leverandøren av et OT-system som har best kjennskap til hvordan det fungerer og hvordan det bør vedlikeholdes, og OT-systemer administreres og vedlikeholdes derfor ofte av leverandøren.

Innen IT-sikkerhet refereres det ofte til de tre "hovedmålene", som i prioritert rekkefølge er *konfidensialitet*, *integritet* og *tilgjengelighet* (populært kalt CIA, av de engelske begrepene *confidentiality*, *integrity* og *availability*). Konfidensialitet er altså høyt prioritert, fordi behovet for å unngå at uvedkommende får tilgang til sensitive data veier tyngre enn andre hensyn. Tilgjengelighet er mindre kritisk, og IT-brukere har oftest en viss toleranse for kortere perioder med nedetid. For OT-systemer er det også viktig å ivareta CIA, men fordi hovedoppgaven er å styre fysiske prosesser, er prioriteringsrekkefølgen forskjellig. Tilgjengelighet (A) og integritet (I) prioriteres fremfor konfidensialitet (C), slik at rekkefølgen blir "motsatt" (AIC). I tillegg til AIC kan vi si at kontroll er et eget hovedmål, som prioriteres over de tre andre, slik at vi innen OT snakker om CAIC (*control*, *availability*, *integrity* og *confidentiality*) istedenfor CIA. [6][7]



Figur 1 Prioriteringer IT vs OT-systemer

Tradisjonelt har man sikret konfidensialitet og integritet i IT-systemer ved å sørge for tilgangskontroll (også kjent som aksesskontroll), hvor man sørger for at bare de som skal ha tilgang har muligheten til å lese hhv. skrive til en bestemt fil. Den vanligste aksesskontrollmodellen har vært Diskresjonær aksesskontroll (DAC), hvor man i praksis oppretter en matrise som angir hvilken bruker skal ha hvilken rettighet (lese, skrive, kjøre, …) til hver enkelt fil. Senere ble konseptet med rollebasert aksesskontroll (RBAC [8]) introdusert; her gir man rettigheter til bestemte roller (operatør, skipselektriker, plattformsjef, etc.), og tilordner brukere bestemte roller for et kortere eller lengre tidsrom. Når en person bytter stilling, skal personen fratas den tilsvarende rollen, og gis en ny; det er følgelig ikke nødvendig å gå gjennom alle mulige filer for å fjerne tilgang for enkeltbrukere. En nyere variant er attributt-basert aksesskontroll (ABAC [9]) som tar utgangspunkt i bestemte (gjerne temporale) attributter til en bruker, f.eks. hvor vedkommende fysisk er plassert i øyeblikket. På denne måten er det mulig f.eks. å gi en operatør tilgang til HMI for prosesskontrollsystemet uten bruk av tofaktor autentisering, men kun når vedkommende befinner seg fysisk i kontrollrommet.

OT-systemer styrer ofte prosesser med høyt skadepotensiale, slik at tap av kontroll grunnet feil og nedetid må unngås for enhver pris. Værkreftene ved en oljeplattform kan for eksempel ikke settes på vent mens et forsyningsskip gjenoppretter evnen til å ligge i ro etter et strømbrudd (black-out). Fysikkens lover vil nådeløst sørge for at vind, bølger og strøm skyver fartøyet bort fra ønsket posisjon, frem til OT-systemene igjen er operative og kan gjenvinne kontrollen over fartøyets bevegelser. Ved kritiske prosesser kan toleransen for avvik være så liten at selv korte perioder med bortfall eller feil kan føre til kritiske eller katastrofale situasjoner. OT-systemer er derfor designet med hovedfokus på sikkerhet og pålitelighet, med diverse sikkerhetsbarrierer for å unngå at enkeltfeil forårsaker større hendelser. Tradisjonelt sett har ikke OT-systemer vært utsatt for betydelige cybertrusler, så sikkerhetsbarrierene har primært vært designet for å gjøre systemene robuste mot *tilfeldige* feil og påkjenninger. Cyberrisiko har hovedsakelig blitt håndtert ved å isolere OT-nettverkene fra omverden slik at hackere og skadevare ikke kommer til. På den måten har man kunnet prioritere OT-systemenes funksjonelle ytelse og pålitelighet fremfor robusthet mot cybertrusler.

I senere år har det blitt mer og mer vanlig å etablere datatrafikk mellom OT-systemer og andre nettverk, blant annet for å få bedre oversikt over drift/produksjon, forenkle prosessoptimalisering og muliggjøre fjernstøtte. Slike tiltak kan øke effektivitet og redusere kostnad, men medfører også økt cyberrisiko fordi de fører til at OT-systemene i større grad blir eksponert for trusler fra internett og andre usikre nettverk.

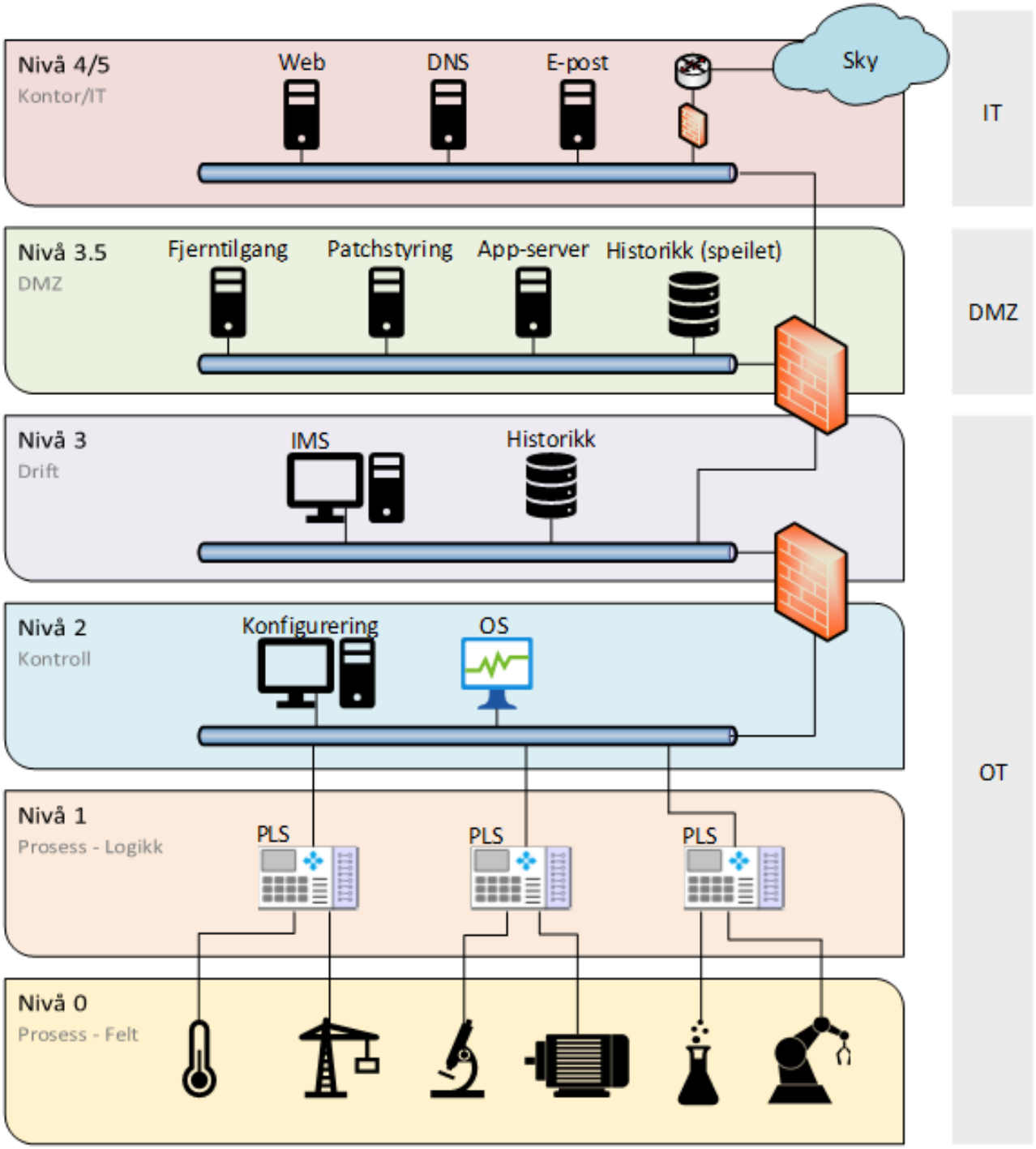
I motsetning til IT-utstyr, som kan sikkerhetsoppdateres hyppig, er OT-systemer mye mindre fleksible, fordi de inneholder komponenter som ikke kan eller ikke bør oppdateres. OT-systemer har mye lengre forventet levetid enn IT-systemer; det er ikke uvanlig at OT-systemer passerer 15 år i drift. Noen OT-komponenter styrer viktige fysiske prosesser og bør jobbe dedikert med sine hovedoppgaver uten å bli "forstyrret" av oppdateringer, mens andre kan kjøre spesiallaget (proprietær) programvare som det ikke finnes oppdateringer til. I tilfellene hvor OT-komponenter kan sikkerhetsoppdateres vil det likevel være nødvendig å verifisere oppdateringene før de installeres, for å unngå at ukjente "bivirkninger" av oppdateringene skaper problemer i OT-systemet. På grunn av slike driftskritiske hensyn er det altså vanskelig å beskytte OT-systemer mot cybertrusler på samme måte som IT-systemer, og OT-systemer er derfor generelt mye mer sårbare enn IT-systemer når tilkoblingsgraden øker. I tillegg medfører det lange livsløpet til OT-systemer at det potensielt kan være mange oppdateringer med betydelige endringer i funksjonalitet i systemets levetid.

Ettersom OT-systemer ikke alltid kan beskyttes med "vanlige" IT-barrierer som kryptering og inntrengningsdeteksjon, er det behov for en OT-tilpasset tilnærming til cybersikkerhet. En serie standarder som i den forbindelse har fått stor oppslutning og anvendelse er ISA/IEC 62443-serien [10], hvis primære formål er å inkludere OT-systemene i arbeidet med cybersikkerhet. Innholdet i IEC 62443-serien diskuteres ikke i detalj i denne veilederen, men en av de grunnleggende filosofiene som beskrives er å dele OT-systemer inn i fornuftige "soner", og "segregere" disse fra hverandre ved å kontrollere dataflyten mellom dem. Slik kan man oppnå nødvendig beskyttelse av sårbare enheter, ved at de skjermes fra usikre nettverk av nettverksutstyr som brannmurer og svitsjer. En vanlig "beste praksis", som også anbefales av ISA [11], er å beskytte hele OT-

miljøet på overordnet nivå ved hjelp av et såkalt DMZ-nettverk, slik at all kommunikasjon inn og ut av OT-systemet går via noder i DMZ. DMZ isoleres fra både OT-systemet og eksterne nettverk ved hjelp av en eller flere brannmurer.

Figur 2 viser et eksempel på overordnet nettverkstopologi for et tenkt OT-system, inkludert DMZ som skiller OT fra IT. Figuren viser forskjellige "nivåer" som svarer til Purdue/ISA-95 referansearkitektur [12] og i dette prosjektet er definert på følgende måte:

- **Nivå 4/5:** Enterprise zone kontornettverk. Dette kan eksistere både offshore/på plattform og på land, og vil ha tilkobling mot eksterne systemer utenfor selskapet via brannmur. Dette kan inkludere applikasjoner i et nettverk hos leverandøren for å aksessere utstyr som står i OT-systemet. Det kan også gjelde skyløsninger som samler inn, analyserer og gir tilbake data og informasjon for beslutningsstøtte.
- **Nivå 3.5 (DMZ):** Demilitarisert sone som styrer datatrafikk mellom nivå 4 og nivå 3. Komponenter som inngår er brannmur(er) som styrer trafikk mellom nivå 4 (IT-nettverk) og nivå 3 (del av OT-nettverk) og utstyr som er nødvendig for å mellom-håndtere denne trafikken, slik at nivå 4 ikke må aksessere direkte utstyr i nivå 3 og lavere. Også utstyr som er dedikert for å ivareta IKT-sikkerhet, slik som applikasjoner og servere for overvåkning av skadevare, sertifikater for utstyr som forespør eller sender data til nivå 3 og lavere, hendelsesrapportering, etc., plasseres i sonen.
- **Nivå 3:** Applikasjoner som ekspertsystemer, vedlikeholdssystemer og servere for lagring av historiske/aggregerte data, inkludert tilhørende nettverk.
- **Nivå 2:** Nettverk med operatørstasjoner, «engineering stasjoner», IMS (Information Management System) og servere for utveksling og presentasjon av data. En ES kan også være plassert i nivå 2 som et alternativ (eller tillegg) til ES plassert på nivå 1.
- **Nivå 1:** Nettverk med kontrollere for prosesskontroll og sikkerhetssystemer og tilhørende servere for datautveksling. Engineering stasjon (ES) kan være plassert her eller på nivå 2.
- **Nivå 0:** Den fysiske prosessen og feltutstyret som inngår i styring og overvåkning. I noen kilder beskrives feltutstyr som nivå 1, men siden ISA TR 00.00.09 og DNV-GL RP G108 ganske entydig definerer feltutstyr som del av nivå 0, så velges dette.



Figur 2 Forenklet oversikt over forskjellige nivåer i OT og IT, basert på Purdue/ISA-95 referansearkitektur.

I tillegg til grunnleggende tekniske forskjeller mellom OT og IT, er det også noen viktige forskjeller når det gjelder brukernes interaksjon med systemene. Det er viktig at operatører av OT-systemer har god situasjonsforståelse til enhver tid, og at vedkommende kan reagere raskt og effektivt ved behov. I bemannede operatørrom er det derfor vanlig at klienter forblir ulåste slik at de kan vise relevant informasjon kontinuerlig og gi operatørene mulighet til å handle umiddelbart uten å måtte logge inn. Det er derfor vanlig at klienter i

operatørrom har generelle brukerkontoer (f.eks. "operatør") som brukes av flere personer. For visse handlinger kan det kreves personlig bekreftelse eller at man logger inn som en bruker med flere rettigheter (f.eks. "administrator"), men slike barrierer brukes primært for å unngå operatørfeil (ved å kreve aktiv bekreftelse) og har begrenset effekt som IKT-barrierer. Kontinuerlig påloggede klienter brukes kun i bemannede operatørrom, mens OT-klienter på andre lokasjoner låses/sikres med passord. Passordstyrke og -levetid varierer fra system til system, men ut ifra egne erfaringer og intervjudiskusjoner oppfatter vi at passordkultur er generelt svakere i OT enn i IT.

Til slutt i dette kapittelet oppsummeres noen viktige forskjeller mellom OT og IT, som bør hensyntas ved "OT-anvendelse" av NSMs grunnprinsipper for IKT-sikkerhet:

- **I OT prioriteres kontroll og tilgjengelighet:** Med prosesstyring som hovedformål er systemenes oppetid høyeste prioritet, og prioriteringsrekkefølgen blir CAIC (kontroll, tilgjengelighet, integritet, konfidensialitet) istedenfor CIA (konfidensialitet, integritet, tilgjengelighet).
- **OT oppdateres sjeldnere:** OT-systemer spesialtilpasset for spesifikke oppgaver og endres lite i løpet av levetiden, fordi velutprøvd maskin- og programvare er mer pålitelig enn systemer som oppdateres hyppig. Vedlikehold og oppdateringer foregår riktignok innen OT også (spesielt på nivå 2 og 3), men ikke like hyppig som innen IT. Lav oppdateringstakt kan medføre utdaterte sikkerhetsfunksjoner, og systemene må derfor skjermes mot cybertrusler.
- **OT er segregert fra Internett og andre usikre nett:** For å skjerme OT-systemer fra cybertrusler og andre uønskede forstyrrelser, plasseres de i avgrensede nettverk med streng kontroll av datatrafikken som går inn og ut. Antall eksterne tilkoblinger (for fjernstøtte, optimalisering, etc.) er økende og det er viktig å unngå at disse skaper angrepsmuligheter.
- **Lengre levetid på OT-komponenter:** IT-komponenter har relativt kort levetid (ca. 3 til 5 år) på grunn av rask teknologiutvikling, mens tilsvarende OT-komponenter kan ha like lang levetid som OT-systemet de tilhører (ca. 10 til 15 år) [13]. Særlig i de lavere nivåene (nivå 0 og nivå 1) er det lite utskifting og oppdatering.

3 Vurdering av NSMs Grunnprinsipper for IKT-sikkerhet for bruk i OT

I det følgende går vi gjennom NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0 [1] tiltak for tiltak, og angir i hvilken grad de er relevante for OT. Prinsippene, som er utarbeidet i samarbeid med virksomheter som forvalter kritiske samfunnsfunksjoner og/eller kritisk infrastruktur, ble først utgitt i 2017 og har siden blitt videreutviklet. Versjon 2.0 består av totalt 21 prinsipper fordelt mellom fire kategorier (1: Identifisere og kartlegge, 2: Beskytte og opprettholde, 3: Oppdage og 4: Håndtere og gjenopprette). Til hvert prinsipp hører et sett med konkrete tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. I tillegg er det en del viktige elementer som nevnes i den generelle teksten, men som ikke dekkes av konkrete tiltak.

I tillegg til Grunnprinsipper for IKT-sikkerhet, publiserte NSM høsten 2020 tre øvrige dokumenter som gir en rekke anbefalinger om hvordan virksomheter kan beskytte sine verdier mot fysiske trusler, innsidetrusler og digitale trusler. Disse er henholdsvis Grunnprinsipper for fysisk sikkerhet [14], Grunnprinsipper for personell-sikkerhet [15] og Grunnprinsipper for sikkerhetsstyring [16]. Når vi i dette dokumentet snakker om grunnprinsippene, er det Grunnprinsipper for IKT-sikkerhet det vises til. NSM har også andre veiledningsdokumenter som kan være relevant å referere til (f.eks. om tjenesteutsetting [17], fysisk sikkerhet [18] og personellsikkerhet [19]).

I denne gjennomgangen følger vi den samme strukturen som i Grunnprinsipper for IKT-sikkerhet, og nummererer dem "NSM X" eller "NSM X.Y", der X angir kategori og Y angir prinsipp. For hvert prinsipp X.Y presenterer vi en tabell med tiltaksoverskrifter hvor vi angir om tiltaket er relevant for OT på følgende måte:

ID		Beskrivelse	
x.y.1	☑	Tiltak 1	Tiltaket er i sin helhet relevant for OT.
x.y.2	[!]	Tiltak 2	Tiltaket er delvis relevant for OT, eller krever ytterligere tiltak.
x.y.3	☒	Tiltak 3	Tiltaket er ikke relevant for OT.

For tiltakene merket med [!], angir vi hva som kan være problematisk eller utfordrende i OT-øyemed under overskriften "Mulige problemtiltak". Legg merke til at det ofte er detaljene eller spesifikke undertiltak som kan være utfordrende, selv der den korte beskrivelsen av tiltaket ser fullt ut relevant ut. Der dette er relevant kommer vi med ytterligere diskusjon og detaljer under overskriften "Utdypende informasjon", også for prinsipper som vurderes som fullt ut relevante for OT.

For hver av de fire kategoriene har vi basert på gjennomgangen av henholdsvis Kraftberedskapsforskriften (vedlegg B) og NIST CSF (vedlegg C) lagt inn forslag til mulige tilleggstiltak som er vurdert som relevante for IKT-sikkerhet i industrielle IKT-systemer. Merk at enkelte av disse kan være helt eller delvis dekt av de øvrige Grunnprinsippene fra NSM (Grunnprinsipper for fysisk sikkerhet [14], Grunnprinsipper for personell-sikkerhet [15] og/eller Grunnprinsipper for sikkerhetsstyring [16]).

NSM 1 Identifisere og kartlegge

NSM 1.1. Kartlegg styringsstrukturer, leveranser og understøttende systemer

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
1.1.1	☑	Identifiser virksomhetens strategi og prioriterte mål.
1.1.2	☑	Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.
1.1.3	☑	Identifiser virksomhetens prosesser for risikostyring knyttet til IKT.
1.1.4	☑	Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT.
1.1.5	☑	Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner.
1.1.6	☑	Kartlegg informasjonsbehandling og dataflyt i virksomheten.

Utdypende informasjon

- Det er opp til ledelsen å legge føringer for strategi og mål.
- Ledelsen må sørge for at strukturer og prosesser også omfatter OT-systemer.
- Styrings- og støttesystemer blir en del av den kritiske driften.

NSM 1.1. Kartlegg enheter og programvare

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
1.2.1	☑	Etabler en prosess for å kartlegge enheter og programvare som er i bruk i virksomheten.
1.2.2	☑	Fastsett retningslinjer for godkjente enheter og programvare i virksomheten.
1.2.3	☑	Kartlegg enheter i bruk i virksomheten.
1.2.4	☑	Kartlegg programvare i bruk i virksomheten.

Utdypende informasjon

- OT-systemer kan ofte inneholde sårbare enheter, og det er derfor spesielt viktig å ha god oversikt over hvilke enheter som inngår og hvilke sårbarheter disse har. Disse tiltakene er også viktige for å avdekke eventuelle enheter som IKKE bør være i OT-nettverkene.

NSM 1.3. Kartlegg brukere og behov for tilgang

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
1.3.1	☑	Kartlegg brukere i informasjonssystemene.
1.3.2	☑	Kartlegg og definer de ulike brukerkategoriene.
1.3.3	☑	Kartlegg ansvar og roller spesielt knyttet til IKT-sikkerhet.

Utdypende informasjon

- På grunn av høyt tilgjengelighetsbehov i kontrollrom brukes her ofte "felleskontoer" istedenfor personlige brukerkontoer i OT-systemer. Dette gjør at en gitt brukerkonto kan forbli pålogget selv om mannskap rullerer. Man ser derfor ofte kun en brukerkonto pr. brukerkategori (f.eks. "operatør", "kaptein", "administrator" etc.), men bruk av disse begrenses vanligvis til gitte fysiske plasseringer. Ved fjerntilgang kreves det personlige brukerkontoer og autentisering.
- Utenfor kontinuerlig bemannet kontrollrom på innretningen anbefales bruk av rollebasert aksesskontroll (RBAC) og/eller attributtbasert aksesskontroll (ABAC).

Relevante tilleggstiltak

Følgende tiltak er foreslått i tillegg til de øvrige tiltakene i denne kategorien (Identifisere og kartlegge). Se vedlegg B og vedlegg C for begrunnelse og/eller utdypende informasjon.

ID	Tiltak/beskrivelse	Referanse
1.a	Identifiser og kommuniser virksomhetens rolle kontra andre aktører i industrien, for å forstå hvordan hendelser i andre virksomheter kan virke inn på egen drift/sikkerhet.	NIST CSF: ID.BE-2
1.b	Gjennomfør jevnlige risikovurderinger for å opprettholde oversikt over relevante risikoer. Dette inkluderer normalt a) Kartlegg sårbarheter og trusler, b) Identifiser potensielle konsekvenser og sannsynligheter for hendelser som kan forårsakes av avdekkede sårbarheter og trusler, c) Anslå risiko basert på trusler, sårbarheter, sannsynligheter og konsekvenser, d) Identifiser og prioriter risikotiltak.	NIST CSF: ID.RA-4, ID.RA-5, ID.RA-6 Kraftberedskaps-forskriften §6-9 bokstav b
1.c	Sørg for at virksomhetens rolle i bransjen og sektorspesifikke forhold blir hensyntatt ved fastsettelse av risikotoleranse.	NIST CSF: ID.RM-3

NSM 2 Beskytte og opprettholde

NSM 1.3. Ivareta sikkerhet i anskaffelses- og utviklingsprosesser

Tiltakene i dette prinsippet er for det meste relevante for OT. Tiltakene som omhandler egen programvareutvikling er trolig mest relevante for leverandører av OT-systemer.

ID		Beskrivelse
Anskaffelse av IKT-produkter		
2.1.1	☑	Integrer sikkerhet i virksomhetens prosess for anskaffelser.
2.1.2	[!]	Kjøp moderne og oppdatert maskin- og programvare.
2.1.3	☑	Foretrekk IKT-produkter som er sertifiserte og evaluert av en tiltrodd tredjepart.
2.1.4	☑	Reduser risiko for målrettet manipulasjon av IKT-produkter i leverandørkjeden.
Utvikling og test mht. egen programvareutvikling		
2.1.5	[!]	Benytt en metode for sikker utvikling av programvare.
2.1.6	[!]	Benytt separate miljøer for utvikling, test og produksjon.
2.1.7	[!]	Gjennomfør tilstrekkelig med testing gjennom hele utviklingsprosessen.
2.1.8	[!]	Vedlikehold programvarekode som utvikles/benyttes i virksomheten.
Tjenesteutsetting – herunder bruk av skytjenester.		
2.1.9	☑	Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
2.1.10	☑	Undersøk sikkerheten hos tjenesteleverandør ved tjenesteutsetting.

Mulige problemtiltak

- 2.1.2: Selv nyere OT-systemer kan inneholde komponenter med utdatert programvare som har relativt kritiske sårbarheter. Dette skyldes blant annet at pålitelig drift prioriteres høyt, slik at enkelte komponenter som har vist seg å være meget pålitelige gjennom tusenvis av driftstimer foretrekkes fremfor nyere (og i IT-sammenheng sikrere) alternativer som gjerne er mer kostbare og mindre utprøvd.
- 2.1.5 – 2.1.8: Disse tiltakene er relevante for OT, og er relevante både for programvareutvikling og konfigurering/drift. Selv om det hovedsakelig er leverandører som driver med programvareutvikling, er disse tiltakene også viktige for eiere/operatører, fordi driftsrelaterte konfigurasjonsendringer kan påvirke både sikkerhet og funksjon. En metode for sikker utvikling av programvare (tiltak 2.1.5) omfatter mye mer enn bare sikkerhetstesting (tiltak 2.1.7), og kontinuerlige analyser og IKT-sikkerhetsvurderinger (trusselmodellering, kodegjennomgang, etc.) er nødvendige i hele utviklingsløpet.

Utdypende informasjon

- OT-systemer oppdateres/endres sjeldnere enn typiske IT-systemer og har vesentlig lengre levetid, så det er viktig å tenke langsiktig når sikkerhetskrav til OT-systemer defineres.

NSM 1.3. Etabler en sikker IKT-arkitektur

Tiltakene i dette prinsippet er for det meste like relevante for OT som for IT.

ID		Beskrivelse
2.2.1	[!]	Etabler og vedlikehold en helhetlig sikkerhetsarkitektur.
2.2.2	☑	Bygg IKT-systemet med IKT-produkter som fungerer godt sammen sikkerhetsmessig.
2.2.3	☑	Del opp virksomhetens nettverk etter virksomhetens risikoprofil.
2.2.4	☑	Skill fysisk de mest kritiske del-nettverkene.
2.2.5	☑	Del opp domenearkitekturen iht. virksomhetens behov.
2.2.6	☑	Reguler tilgang til tjenester basert på kjennskap til både brukere og enhet.
2.2.7	☑	Etabler en robust og motstandsdyktig IKT-arkitektur.

Mulige problemtiltak

- 2.2.1: Noen av funksjonene som listes opp i tiltaket håndteres litt annerledes i OT-systemer enn i IT-systemer:
  - *Operativsystemer* er ikke alltid oppdatert, fordi oppdateringer (patcher) må testes og godkjennes (herdes) før de tas i bruk. I noen tilfeller brukes utdaterte (men velutprøvde) operativsystemer som ikke lenger støttes av leverandør.
  - *Krypteringsverktøy* er lite brukt internt i OT-systemer, men er mer relevant ved eventuelle koblinger til eksterne nettverk, som f.eks. ved dataeksport til skyløsninger.

Utdypende informasjon

- Det er relativt få klienter og brukerkontoer i OT-miljøer sammenlignet med IT-miljøer.
- Ansvaret for å drifte de forskjellige funksjonene listet opp i tiltak 2.2.1 vil havne delvis på OT-leverandør og delvis på eier/operatør, så det bør avklares med OT-leverandør hvem som har ansvar for hva.
- Noen OT-systemer opererer isolert fra IT-nettverk og andre systemer, og for slike isolerte systemer vil tiltak 2.2.2 være mindre relevant.
- OT-systemer kan være sårbare for ukjent/uventet/unødvendig nettverkstrafikk, herunder både angrep og "støy". Det er derfor spesielt viktig å unngå fremmede/ukjente enheter og trafikk i OT-nettverk.

NSM 1.3. Ivareta en sikker konfigurasjon

De fleste tiltakene her er like relevante for OT som for IT.

ID		Beskrivelse
2.3.1	☑	Etabler et sentralt styrt regime for sikkerhetsoppdatering.
2.3.2	[!]	Konfigurer klienter slik at kun kjent programvare kjører på dem.
2.3.3	☑	Deaktiver unødvendig funksjonalitet.
2.3.4	☑	Etabler og vedlikehold standard sikkerhetskonfigurasjoner.
2.3.5	☑	Verifiser at aktivert sikkerhetskonfigurasjon er i henhold til virksomhetens godkjente sikkerhetskonfigurasjon.
2.3.6	☑	Utfør all konfigurasjon, installasjon, og drift for øvrig på en trygg måte.

2.3.7	☑	Endre alle standardpassord på IKT-produktene før produksjonssetting.
2.3.8	[!]	Ikke deaktiver kodebeskyttelsesfunksjoner.
2.3.9	☑	Etabler sikker tid i virksomheten.
2.3.10	☑	Reduser risiko med IoT-enheter.

Mulige problemtiltak

- 2.3.2: Tiltaket er relevant for OT, men det kan tenkes at enkelte enheter i OT-systemet ikke har støtte for begrensning av hvilke programmer som kan kjøre på enheten (hvitlisting).
- 2.3.8: Tiltaket er relevant for OT, men det kan være tilfeller hvor kodebeskyttelse ikke er tilgjengelig eller ikke tillates.

Utdypende informasjon

- Regime for sikkerhetsoppdatering er relevant for OT, men med ekstra fokus på i hvilken grad sårbarhetene representerer en aktuell fare i den aktuelle konfigurasjonen, og der kompenserende tiltak vurderes i forhold til hvor fort oppdateringen bør gjennomføres. Det er avgjørende å gjennomføre en endringskonsekvensanalyse, hvor testregime for oppdateringer vil være sentralt.
- Logisk/fysisk isolasjon av servere og andre enheter som ikke lett lar seg oppdatere må kombineres med ekstra overvåking og andre avbøtende tiltak.
- Alle OT-komponenter er kritiske, og derfor bør alle OT-komponenter herdes gitt at det ikke går ut over ytelse/pålitelighet.
- Det vil være viktig å involvere OT-leverandørene for å sørge for sikker konfigurasjon. Både OT-kompetanse og kompetanse om IKT-sikkerhet vil være nødvendig for å finne riktige tiltak.
- Bruk av IoT/IIoT er sikkerhetsmessig utfordrende ettersom slike enheter vil være internett-eksponerte, og det er derfor særlig viktig å vurdere risiko nøye før IoT-/IIoT-enheter tas i bruk i OT-systemer.

NSM 1.1. Beskytt virksomhetens nettverk

De fleste tiltakene her er like relevante for OT som for IT.

ID		Beskrivelse
2.4.1	☑	Etabler tilgangskontroll på flest mulige nettverksporter.
2.4.2	[!]	Krypter alle trådløse og kablede forbindelser.
2.4.3	☑	Kartlegg fysisk tilgjengelighet for svitsjer og kabler.
2.4.4	☑	Aktiver brannmur på alle klienter og servere.

Mulige problemtiltak

- 2.4.2: Kryptering kan i noen tilfeller føre til avbrudd eller forsinkelser i kommunikasjonen, og unngås derfor ofte i kritiske forbindelser i OT-systemer (fordi tilgjengelighet er viktigere enn konfidensialitet). Kryptering kan også bidra til mindre mulighet for å oppdage uønsket trafikk. Det er derfor viktig å gjennomføre en risikovurdering før man avgjør om forbindelser skal krypteres eller ei.

Utdypende informasjon

- Det er viktig å ha kontroll på patchingen i patcheskap for å unngå at porter som skal være inaktive eller begrenset har bredere tilgang i nettverket enn tiltenkt.
- Dagens OT-komponenter lavt nede i hierarkiet har som grunnregel ikke tilstrekkelig ytelse til å kryptere all trafikk.

NSM 1.1. Kontroller dataflyt

De fleste tiltakene her er like relevante for OT som for IT.

ID		Beskrivelse
2.5.1	☑	Styr dataflyt mellom nettverks-soner.
2.5.2	☑	Begrens tilgangen til interne tjenester fra eksterne lokasjoner.
2.5.3	☑	Sperr all direkte-trafikk mellom klienter.
2.5.4	☑	Isoler utstyr som er sårbart og har lav tillitt.
2.5.5	[!]	Styr dataflyten til spesielt eksponerte tjenester.
2.5.6	☑	Beskytt spesielt kritiske tjenester med egen dataflyt.
2.5.7	☑	Ha kontroll på trafikk mellom virksomheten og samarbeidspartnere/ tjenesteleverandører.
2.5.8	☑	Styr all trafikk (ikke bare interne tjenester) til og fra forvaltede mobile klienter via virksomhetens nett.

Mulige problemtiltak

- 2.5.5: Det er ikke vanlig å ha dataflyt mellom OT-systemer og eksponerte tjenester som web og epost, så dette tiltaket er lite/ikke relevant for OT. Men i eventuelle tilfeller hvor OT likevel tilkobles eksponerte tjenester, vil det være høyst relevant å ha kontroll på slik dataflyt, f.eks. ved å bruke gateway-løsninger som skiller OT-nettet fra de eksponerte tjenestene.

Utdypende informasjon

- Å kontrollere dataflyt er vel så viktig innen OT som IT, og det har for lengst blitt en "bransjestandard" å holde OT nokså isolert fra omverden. Selv om det er økende behov/ønske om å etablere trafikk inn/ut av OT-systemer er det fortsatt avgjørende å skjerme OT fra trusler i usikrede nettverk. Datatrafikk ut av et OT-system medfører generelt mindre risiko enn datatrafikk inn.
- Tekniske sikkerhetsbarrierer krever regnekraft og vil i noen tilfeller kunne føre til OT-systemets ytelse svekkes (f.eks. p.g.a. forsinkede datapakker). Innen OT er ytelse og tilgjengelighet ofte prioritert såpass høyt at enkelte sikkerhetsbarrierer må vike (og evt. erstattes av kompenserende tiltak, f.eks. isolasjon).
- OT-leverandører kan ha egne løsninger for fjerntilkobling, for å ha bedre kontroll på eget system og for å unngå avhengighet til andre parters løsninger.
- Tiltak for mobile klienter er lite relevante i dag, men vil være aktuelle dersom mobile klienter (nettbrett, e.l.) benyttes i OT.

NSM 1.3. Ha kontroll på identiteter og tilganger

De fleste tiltakene her er like relevante for OT som for IT.

ID		Beskrivelse
2.6.1	☑	Etabler retningslinjer for tilgangskontroll.
2.6.2	☑	Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter.
2.6.3	[!]	Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter.
2.6.4	☑	Minimer rettigheter til sluttbrukere og spesialbrukere.
2.6.5	[!]	Minimer rettigheter på drifts-kontoer.
2.6.6	☑	Styr tilganger til enheter.
2.6.7	[!]	Bruk multi-faktor autentisering.

Mulige problemtiltak

- 2.6.3: Det kan være vanskelig å finne et verktøy som er egnet for å administrere både IT og OT, så å ha en egen løsning for OT er relativt sannsynlig.
- 2.6.5: Det er viktig å unngå at operatør/bruker av OT-systemet har unødvendige rettigheter, men det er også viktig at ikke mangel på rettigheter blir et hinder i kritiske situasjoner.
- 2.6.7: Trolig mest relevant for eventuell fjerntilgang eller for operatørstasjoner som er tilgjengelige i utstyrsrom o.l.

Utdypende informasjon

- OT-systemer har en "stabil konfigurasjon" som sjelden endres/oppdateres, så behovet for sentraliserte konfigureringsverktøy er mindre enn i IT.
- Innen OT er det ofte en mer fysisk tilnærming til tilgangskontroll, ved at utstyr kun er tilgjengelig i områder med begrenset fysisk tilgang. Logisk tilgangsbegrensning er relevant for terminaler i utstyrsrom eller ved fjerntilgang.

NSM 1.1. Beskytt data i ro og i transitt

Tiltakene i dette prinsippet er for det meste like relevante for OT som for IT.

ID		Beskrivelse
2.7.1	☑	Etabler en strategi for håndtering av kryptografi i virksomheten.
2.7.2	[!]	Aktiver kryptering i de tjenestene som tilbyr slik funksjonalitet.
2.7.3	☑	Krypter lagringsmedier som holder konfidensiell data og som lett kan mistes eller kompromitteres.
2.7.4	☑	Benytt kryptering når konfidensiell informasjon overføres eller når tilliten til informasjonskanalen er lav.
2.7.5	☑	Definer krav til sikringsnivå for ulike typer informasjon.

Mulige problemtiltak

- 2.7.2: Enkelte tjenester innen OT kan tenkes å ha krypteringsmuligheter, men hvorvidt slike verktøy skal brukes må bestemmes ut ifra risikovurderinger. I noen tilfeller vil det være ønskelig å unngå kryptering.

Utdypende informasjon

- Generelt er kravene til konfidensialitet underordnet integritet og tilgjengelighet i OT-nettverk, og det er ikke gitt at krypteringsverktøy er tilgjengelig i alle sammenhenger.
- I den grad OT-systemer håndterer konfidensielle data er det selvsagt relevant med kryptering, men da gjerne på et høyere nivå enn selve prosesstyringen.

NSM 1.3. Beskytt e-post og nettleser

Disse tiltakene er lite relevante for OT, ettersom det i utgangspunktet ikke benyttes epost og nettlesere i OT-nettverk.

ID		Beskrivelse
2.8.1	☒	Verifiser at innkommende e-post er fra en legitim avsender-adresse.
2.8.2	☒	Aktiver STARTTLS på virksomhetens e-postserver.
2.8.3	☒	Bruk kun støttede e-postklienter, nettlesere og programtillegg.
2.8.4	☒	Tillat kun virksomhetsgodkjente programtillegg.

Utdypende informasjon

- Enkelte OT-systemer har brukergrensesnitt (GUI) som kjøres i nettleser, men da kun med lokal nettverkstrafikk (internt i OT-systemet). Hensiktsmessig soneinndeling og brannmurer med god/riktig konfigurering er også viktige barrierer for å hindre uønsket trafikk til og fra nettleser.

NSM 1.1. Etabler evne til gjenoppretting av data

Disse tiltakene gjelder i stor grad på samme måte for OT som for IT.

ID		Beskrivelse
2.9.1	☑	Legg en plan for regelmessig sikkerhetskopiering av alle *virksomhetsdata*.
2.9.2	☑	Inkluder sikkerhetskopier av programvare.
2.9.3	☑	Test sikkerhetskopier regelmessig.
2.9.4	☑	Beskytt sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning.

Utdypende informasjon

- Konfigurasjon og programvare for selve prosesstyringen blir sjelden endret, slik at behovet for regelmessig sikkerhetskopiering er beskjedent. Det er altså avgjørende å ha nødvendige sikkerhetskopier slik at systemene kan reetableres effektivt (f.eks. etter en ransomwarehendelse), men selve sikkerhetskopieringen trenger ikke skje hyppig.
- Loggdata fra den generelle aktiviteten ("event logging") overføres vanligvis til IT-systemer og håndteres der, men de ferskeste loggene lagres også i OT for eventuell granskning og feilsøking, eller for optimalisering.
- Informasjon om produksjonsvolum og andre ting som danner grunnlag for fakturering/transaksjoner vil også være kandidater for regelmessig sikkerhetskopiering, både i og utenfor OT-systemet.

NSM 2.10. Integrer sikkerhet i prosess for endringshåndtering

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
2.10.1	☑	Integrer sikkerhet i virksomhetens prosess for endringshåndtering.
2.10.2	☑	Involver nødvendig IKT-sikkerhetspersonell i forbindelse med endringer.
2.10.3	☑	Gjennomfør nødvendig endring, konfigurering og testing av påvirkede sikkerhetsfunksjoner.
2.10.4	[!]	Integrer sikkerhet i virksomhetens prosess for hasteendringer.

Mulige problemtiltak

- 2.10.4: Viktig å sikre at endringer ikke får uønskede konsekvenser for OT-prosesser. Endrings-konsekvensanalyse må gjennomføres.

Utdypende informasjon

- OT-sikkerhetspersonell (med ansvar for funksjonell sikkerhet) må også involveres i forbindelse med endringer.

Relevante tilleggstiltak

Følgende tiltak er foreslått i tillegg til de øvrige tiltakene i denne kategorien (Beskytte og opprettholde). Se vedlegg B og vedlegg C for begrunnelse og/eller utdypende informasjon.

ID	Tiltak/beskrivelse	Referanse
2.a	Prioriter ressurser på basis av kritikalitet og forretningsverdi.	NIST CSF: ID.AM-5
2.b	Identifiser kritiske funksjoner og avgjør hvilken grad av robusthet som kreves av disse i forskjellige driftstilstander (under normal drift, under kritiske operasjoner, under angrep etc.)	NIST CSF: ID.BE-5
2.c	Etabler en prosess for styring av IKT-sikkerhetsrisiko i hele leverandørkjeden.	NIST CSF: ID.SC-1
2.d	Identifiser og prioriter alle involverte aktører for å forstå IKT-sikkerhetsrisikoen i hele leverandørkjeden.	NIST CSF: ID.SC-2
2.e	Inkluder krav til IKT-sikkerhet i kontrakter med leverandører.	NIST CSF: ID.SC-3
2.f	Rutinemessig følg opp leverandørers etterlevelse av kontraktfestede krav til IKT-sikkerhet.	NIST CSF: ID.SC-4
2.g	Vurder behovet for å involvere mer enn en person for bestemte handlinger (*separation of duties*).	NIST CSF: PR.AC-4
2.h	Påse nødvendig opplæring og trening i IKT-sikkerhet for å sikre god risiko- og sikkerhetsforståelse blant alle brukere (ansatte så vel som leverandører, underleverandører og andre oppdragstakere).	NIST CSF: PR.AT-1
2.i	Påse at alle som utfører aktiviteter med betydning for IKT-sikkerhet forstår hvordan egen rolle og ansvar påvirker sikkerheten.	NIST CSF: PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5
2.j	Etabler rutiner for håndtering av aktiva ved fjerning, overføring og avhending.	NIST CSF: PR.DS-3, (PR.IP-2), PR.IP-6
2.k	Opprettholde tilstrekkelig kapasitet for å sikre tilgjengelighet.	NIST CSF: PR.DS-4

2.l	Sikre etterlevelse av regler og forskrifter knyttet til fysisk driftsmiljø for organisasjonens aktiva.	NIST CSF: PR.IP-5
2.m	Etabler rutiner for (kontinuerlig) forbedring av prosesser for sikring/beskyttelse.	NIST CSF: PR.IP-7
2.n	Del informasjon vedrørende effektivitet av teknologi for sikring/beskyttelse med relevante interessenter.	NIST CSF: PR.IP-8
2.o	Inkluder IKT-sikkerhet i personal-praksis (f.eks. i forbindelse med ansettelse og ansettelsesforhold).	NIST CSF: PR.IP-11
2.p	Utfør og loggfør vedlikehold og reparasjoner av organisasjonens aktiva ved hjelp av godkjente verktøy.	NIST CSF: PR.MA-1
2.q	Godkjenn, utfør og loggfør fjernvedlikehold på en måte som forhindrer uautorisert tilgang.	NIST CSF: PR.MA-2
2.r	Implementer nødvendige mekanismer for å sikre tilstrekkelig robusthet i forskjellige driftstilstander (under normal drift, under kritiske operasjoner, under angrep etc.)	NIST CSF: PR.PT-5

NSM 3 Oppdage

NSM 1.3. Oppdag og fjern kjente sårbarheter og trusler

Disse tiltakene gjelder i stor grad på samme måte for OT som for IT.

ID		Beskrivelse
3.1.1	☑	Gjennomfør jevnlig sårbarhetskartlegging.
3.1.2	☑	Abonner på tjenester relatert til sårbarhetsetterretning.
3.1.3	[!]	Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare).

Mulige problemtiltak

- 3.1.3: Bruk av Intrusion Prevention System (IPS) i et OT-miljø må tilpasses nøye slik at det ikke forstyrrer normal drift.

Utdypende informasjon

- Selv om enkelte enheter ikke patches eller patches sjelden, vil det likevel være nyttig å ha oversikt over sårbarhetene. Sårbarhetsskannere (vulnerability scanners) kan generere mer trafikk enn OT-komponentene "tåler", så en vurdering av systemets tåleevne bør gjøres og holdes opp mot verdien av implementering av slike verktøy.
- Kjente sårbarheter som ikke kan fjernes må risikovurderes for å avgjøre om andre avbøtende tiltak er nødvendige.
- Medlemskap i CERT eller ISAC kan være en kilde til sårbarhetsetterretning.

NSM 1.1. Etabler sikkerhetsovervåkning

Disse tiltakene er relevante på samme måte for OT som for IT.

ID		Beskrivelse
3.2.1	☑	Fastsett virksomhetens strategi og retningslinjer for sikkerhetsovervåkning.
3.2.2	☑	Følg lover, reguleringer og virksomhetens retningslinjer for sikkerhetsovervåkning.
3.2.3	☑	Avgjør hvilke deler av IKT-systemet som skal overvåkes.
3.2.4	☑	Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn.
3.2.5	☑	Verifiser at innsamling fungerer etter hensikt.
3.2.6	☑	Påse at innsamlet data ikke kan manipuleres.
3.2.7	☑	Gjennomgå og konfigurer innhenting av sikkerhetsrelevant data og den sentrale loggdatabasen jevnlig.

Utdypende informasjon

- Ettersom OT ofte er knyttet til store maskiner og farlige omgivelser vil det (i tillegg til overvåkning av nettverkstrafikk) ofte være behov for "safety-overvåkning" i form av f.eks. CCTV.
- Det er viktig å påse at verktøyene som tas i bruk ikke forstyrrer OT-systemene.

NSM 1.3. Analyser data fra sikkerhetsovervåkning

Disse tiltakene er relevante på samme måte for OT som for IT.

ID		Beskrivelse
3.3.1	☑	Lage en plan for analyse av data fra sikkerhetsovervåkning.
3.3.2	☑	Etabler og vedlikehold kompetanse om normaltilstanden i virksomhetens informasjonssystemer.
3.3.3	☑	Ta i bruk verktøy som muliggjør manuelle og automatiske søk, samt alarmering basert på kriterier.
3.3.4	☑	Innhent og bearbeid trusselinformasjon fra relevante kilder.
3.3.5	☑	Vurder fortløpende om innhentet data er tilstrekkelig relevant og detaljert.
3.3.6	☑	Etabler rutine for eskalering av alarmer.
3.3.7	☑	Benytt analyseverktøy, teknologi og algoritmer.

Utdypende informasjon

- OT-systemer har ofte forskjellige advarsler og alarmer for å framheve viktig informasjon knyttet til prosesstyring. Det er viktig å unngå for mange falske alarmer og annen informasjonsoverbelastning. Involver gjerne OT og IKT personell for å fjerne feilkonfigurasjoner og feilalarmer som kan forstyrre og bedøve faktiske alarmer som det må responderes på.

NSM 1.3. Gjennomfør inntrengingstester

Inntrengningstesting er relevant/nyttig også innen OT, men OT-systemenes "natur" gjør at spesielle hensyn må tas.

ID		Beskrivelse
3.4.1	☑	Planlegg inntrengingstester med tydelig mål og omfang.
3.4.2	☑	Involver relevante interesseparter i forkant.
3.4.3	[!]	Benytt verktøy for sårbarhetskartlegging og angrepsverktøy.
3.4.4	☑	Gjennomfør jevnlige inntrengingstester (minst årlige) for å identifisere sårbarheter.
3.4.5	☑	Test rutiner for deteksjon og beredskap.
3.4.6	☑	Kommuniser resultater fra inntrengingstester til relevante interesseparter.

Mulige problemtiltak

- 3.4.3: Dagens OT-systemer er i liten grad designet for å håndtere uvanlig trafikk i sine nettverk og kan være sårbare for nettverksforstyrrelser og fremmede prosesser. Selv standardisert sårbarhetsskanning (som gjøres hyppig og nokså risikofritt i mange IT-systemer) kan sette kritisk OT-utstyr fullstendig ut av spill og i verste fall medføre tapt produksjon og/eller store ødeleggelser.

Utdypende informasjon

- For å gjennomføre forsvarlig inntrengningstesting av OT-systemer er det viktig å foreta grundig risikovurdering (av planlagt testaktivitet) på forhånd, hvor det avklares hvilke aktiviteter/tester som

kan gjennomføres og hvilke som må utelates grunnet uakseptabel risiko. Det bør videre være tett dialog mellom involverte parter før og under testing, for å påse at alle nødvendige hensyn blir tatt.

- Å gjøre testingen på et tidspunkt hvor anlegget ikke er i drift (ifm. vedlikehold eller annen planlagt nedetid) er vanligvis å foretrekke, fordi det medfører mindre risiko og tillater grundigere testing. Det kan likevel tenkes at enkelte tester ønskes utført under normal drift, for å få bedre svar på hva som faktisk vil skje i et gitt scenario. All testing må uansett risikovurderes og planlegges godt på forhånd.
- Som tiltak 3.4.4 sier bør inntrengingstester gjøres jevnlig, og det er lurt å ha en langsiktig plan slik at man unngår å "begynne på nytt" hver gang testing skal gjennomføres. Eget, relevant personell bør involveres, ikke bare for å påse at testingen foregår forsvarlig, men også for å lære mest mulig. Kompetanse som opparbeides ifm. slik testing bør spres i organisasjonen, spesielt til teknisk personell, innkjøpsansvarlige og ledelse.
- Definisjonen av inntrengningstest (også kjent som penetrasjonstest, pentest, etc) er noe uklar, og innholdet kan variere veldig fra tilbyder til tilbyder og fra oppdrag til oppdrag. Hvor omfattende en inntrengingstest skal være, kommer an på blant annet risikotoleranse og økonomi. Selv snille/-forsiktige inntrengingstester har betydelig verdi. For å få mest mulig hensiktsmessig testomfang (scope) er det lurt å delta aktivt i planleggingen, slik at testaktiviteter som genererer mest mulig verdifull innsikt blir valgt.

Relevante tilleggstiltak

Følgende tiltak er foreslått i tillegg til de øvrige tiltakene i denne kategorien (Oppdage). Se vedlegg C for begrunnelse og/eller utdypende informasjon.

ID	Tiltak/beskrivelse	Referanse
3.a	Overvåk systemenes fysiske driftsmiljø (ved hjelp av kameraer og andre deteksjonsmidler) for å oppdage potensielle IKT-hendelser.	NIST CSF: DE.CM-2
3.b	Overvåk trafikk til og fra eksterne tjenesteleverandører for å oppdage potensielle IKT-hendelser.	NIST CSF: DE.CM-6
3.c	Del informasjon vedrørende avviksdeteksjon med relevante interessenter.	NIST CSF: DE.DP-4
3.d	Etabler rutiner for kontinuerlig forbedring av prosesser for avviksdeteksjon.	NIST CSF: DE.DP-5

NSM 4 Håndtere og gjenopprette

NSM 1.3. Forbered virksomheten på håndtering av hendelser

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
4.1.1	☑	Etabler et planverk for hendelseshåndtering.
4.1.2	☑	Gjennomfør en analyse av virksomhetskritiske effekter.
4.1.3	☑	Utarbeid rolle- og ansvarsbeskrivelse for personell som skal involveres i hendelseshåndtering.
4.1.4	☑	Utarbeid avtaler med relevante tredjeparter.
4.1.5	☑	Fastsett hvilke kommunikasjonskanaler som skal benyttes i forbindelse med hendelser.
4.1.6	☑	Test og øv på planer jevnlig slik at disse er godt innøvd.

Utdypende informasjon

- Det er verdt å merke at hendelser som påvirker OT-systemer kan ha direkte og umiddelbare konsekvenser for produksjon og sikkerhet. Det er derfor viktig å identifisere mulige/sannsynlige fysiske konsekvenser som en del av Business Impact Analysis (BIA)

NSM 1.1. Vurder og klassifiser hendelser

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
4.2.1	☑	Gjennomgå loggdata og samle relevante data om hendelsen for å oppnå et godt beslutningsgrunnlag.
4.2.2	☑	Avgjør alvorlighetsgrad for hendelsen.
4.2.3	☑	Informer relevante interesseparter.

Utdypende informasjon

- Hendelser i OT-nettverk kan ha fysiske konsekvenser, inkludert liv og helse.
- Det vil kunne ha alvorlige konsekvenser å stenge ned et OT-system på feil tidspunkt

NSM 1.1. Kontroller og håndter hendelser

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
4.3.1	☑	Kartlegg omfang og påvirkning på forretningsprosesser.
4.3.2	[!]	Undersøk om hendelsen er under kontroll og gjennomfør nødvendige reaktive tiltak.
4.3.3	☑	Loggfør alle aktiviteter, resultater og relevante avgjørelser for senere analyse.
4.3.4	☑	Iverksett gjenopprettingsplan i løpet av, eller i etterkant av hendelsen.

4.3.5	☑	Koordiner og kommuniser med interne og eksterne interessenter underveis i hendelseshåndteringen.
4.3.6	☑	Gjennomfør nødvendige aktiviteter i etterkant av hendelsen.

Mulige problemtiltak

- 4.3.2: Terminering av prosesser må også vurderes opp mot krav til oppetid mm. Man kan ikke blindt stenge ned alt man mistenker er kompromittert.

Utdypende informasjon

- Generelt er kravene til konfidensialitet underordnet integritet og tilgjengelighet i OT-nettverk. Dette gjelder også ved håndtering av hendelser, hvor kontroll og tilgjengelighet er viktigst.

NSM 1.1. Evaluer og lær av hendelser

Tiltakene i dette prinsippet er like relevante for OT som for IT.

ID		Beskrivelse
4.4.1	☑	Identifiser erfaringer og læringspunkter («lessons learned») fra hendelser.
4.4.2	☑	Kartlegg og gjennomgå identifiserte, kompromitterte sikkerhetstiltak.
4.4.3	☑	Vurdere effektiviteten av prosesser, prosedyrer, rapporteringsformater og organisatoriske strukturer med tanke på å respondere på hendelser.
4.4.4	☑	Kommuniser og del erfaringsresultatene med (relevante) interessenter.

Utdypende informasjon

- OT-systemer berører både den digitale og den fysiske verden, og det er derfor viktig å ivareta læring i begge domener.

Relevante tilleggstiltak

Følgende tiltak er foreslått i tillegg til de øvrige tiltakene i denne kategorien (Håndtere og gjenopprette). Se vedlegg C for begrunnelse og/eller utdypende informasjon.

ID	Tiltak/beskrivelse	Referanse
4.a	Håndter risiko knyttet til nyoppdagede sårbarheter (ved å iverksette tiltak eller akseptere risiko).	NIST CSF: RS.MI-3
4.b	Etabler rutiner for å begrense omdømmetap etter en hendelse.	NIST CSF: RC.CO-2

4 Oppsummering og konklusjon

NSMs grunnprinsipper for IKT-sikkerhet (versjon 2.0) er i stor grad relevant også for OT-domenet, men enkelte tiltak krever ytterligere tillempninger sammenlignet med slik det fungerer i IT. Av totalt 118 tiltak er 96 vurdert til å være fullt ut relevante for OT (☑); 18 tiltak er relevante, men krever særlig omhu eller ytterligere tillempninger ([!]); og 4 tiltak vurderes til å være mindre relevante for OT (☒). NSM har også andre veiledningsdokumenter som det kan være relevant å referere til (f.eks. om tjenesteutsetting [17], fysisk sikkerhet [18] og personellsikkerhet [19]).

Krav i Kraftberedskapsforskriften dekkes i stor grad av NSMs grunnprinsipper for IKT-sikkerhet, men førstnevnte er mer eksplisitt på metoder for risikovurdering (se vedlegg B). Vi har funnet at det på enkelte områder er et gap mellom NIST CSF og NSMs grunnprinsipper for IKT-sikkerhet, hvor en del tiltak i førstnevnte ikke er dekket (eller bare delvis dekket) av sistnevnte (se vedlegg C). Vi har identifisert 27 forslag til tiltak som vi anbefaler som tillegg til Grunnprinsippene, basert på gapene mot NIST CSF. NSMs Grunnprinsipper for IKT-sikkerhet og NIST CSF har en ganske ulik oppbygning og gruppering av tiltak. Ifølge NSM selv er Grunnprinsippene ment å være mer konkrete og rett på sak enn det man opplever i noen av de utenlandske rammeverkene. Internasjonale rammeverk er gjerne optimalisert for store virksomheter og store IT-avdelinger, mens NSMs grunnprinsipper er mer tilpasset mindre virksomheter med mindre hierarki og mer delegert myndighet. Det er ikke forslått eksplisitte tilleggstiltak med utgangspunkt i gapene mot Kraftberedskapsforskriften, men på generelt grunnlag anbefaler vi at det utarbeides en detaljert rettledning for risikovurdering som en del av Grunnprinsippene eller at det vises til en slik rettledning annet sted.

Referanser

[1] Nasjonal sikkerhetsmyndighet (NSM), 2020. NSMs grunnprinsipper for IKT-sikkerhet, versjon 2.0, https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

[2] FOR-2012-12-07-1157 Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften), https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

[3] National Institute of Standards and Technology (NIST), 2018. Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[4] Petroleumstilsynet, 2020. IKT-sikkerhet – robusthet i petroleumssektoren, https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/2020/ikt-sikkerhet--robusthet-i-petroleumssektoren/

[5] Petroleumstilsynet, Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften), https://lovdata.no/dokument/SF/forskrift/2010-04-29-611

[6] General Electric, An Executive Guide to Cyber Security for Operational Technology, https://www.ge.com/fr/sites/www.ge.com.fr/files/an-executive-guide-to-cyber-security-for-operational-technology-whitepaper.pdf

[7] Foss, G., 2018. Cyber Security Management of Industrial Automation and Control Systems (IACS), Asset Guardian, https://www.assetguardian.com/cyber-security-management-of-industrial-automation-and-control-systems-iacs/

[8] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E., 1996, Role-based access control models, *Computer*, 29, (2), 38-47, doi: 10.1109/2.485845, https://doi.org/10.1109/2.485845

[9] Hu, V., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., 2014. Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST SP 800-162, https://csrc.nist.gov/publications/detail/sp/800-162/final

[10] Salater, T., 2020. NEK IEC 62443 – en bærebjelke for cybersikkerhet, https://www.nek.no/nek-iec-62443-en-baerebjelke-for-cybersikkerhet/

[11] Wood, R., 2017. Three keys to designing and configuring secure industrial networks, https://www.isa.org/intech-home/2017/november-december/features/three-keys-designing-configuring-secure-networks

[12] Williams, T.J. (ed.), 1989. A Reference Model For Computer Integrated Manufacturing (CIM), http://www.pera.net/Pera/PurdueReferenceModel/TOC&Intro.pdf

[13] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., 2015. NIST Special Publication 800-82 Revision 2 – Guide to Industrial Control Systems (ICS) Security, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[14] Nasjonal sikkerhetsmyndighet (NSM), 2020. Grunnprinsipper for fysisk sikkerhet, versjon 1, https://nsm.no/getfile.php/134285-1601623568/Demo/Dokumenter/Grunnprinsipper%20for%20fysisk_sikkerhet.pdf

[15] Nasjonal sikkerhetsmyndighet (NSM), 2020. Grunnprinsipper for personellsikkerhet, https://nsm.no/getfile.php/134159-1598879548/Demo/Dokumenter/Grunnprinsipper%20for%20personellsikkerhet%20.pdf

[16] Nasjonal sikkerhetsmyndighet (NSM), 2020. Grunnprinsipper for sikkerhetsstyring, versjon 1, https://nsm.no/getfile.php/134493-1605693992/Demo/Dokumenter/Grunnprinsipper%20for%20sikkerhetsstyring.pdf

[17] Nasjonal sikkerhetsmyndighet (NSM), 2018. Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. En utdyping av området "Beslutt leveransemodell" i NSMs grunnprinsipper for IKT-sikkerhet, versjon 1.1, https://nsm.no/getfile.php/133666-1592829282/Demo/Dokumenter/tjenesteutsetting2018v1.1_enkelstsider.pdf

[18] Nasjonal sikkerhetsmyndighet (NSM). Veileder i fysisk sikkerhet, Versjon 1, https://nsm.no/getfile.php/133110-1591610826/Demo/Dokumenter/Veiledere/veileder-i-fysisk-sikkerhet.pdf
[19] Nasjonal sikkerhetsmyndighet (NSM). Veileder i personellsikkerhet, Versjon 1, https://nsm.no/getfile.php/132407-1590749199/Demo/Dokumenter/Veiledere/Veileder%20i%20personellsikkerhet.pdf
[20] Norges vassdrags- og energidirektorat (NVE), 2018. Foreløpig tilleggsveileder til kraftberedskapsforskriften - Oppdateringer etter revisjon, https://www.nve.no/media/7598/forel%C3%B8pig-tilleggsveileder-kraftberedskapsforskriften.pdf
[21] ISO/IEC, 2018. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, https://www.iso.org/standard/75281.html
[22] ISO/IEC, 2013. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, https://www.iso.org/standard/54533.html

Vedlegg A: Delprosjekter "IKT-sikkerhet – Robusthet i petroleumssektoren"

Denne rapporten er del av et oppdrag for Petroleumstilsynet med følgende delprosjekter:

Datakvalitet

Hensikten har vært å undersøke hvilke datakilder og data som benyttes i industrielle IKT-systemer og hvordan data behandles og prosesseres før de gjøres tilgjengelig i kontornettet. Styrker og sårbarheter knyttet til datakvalitet og sikring av data er diskutert.

Notat – IKT-sikkerhet i petroleumsindustrien

SINTEF har utarbeidet et notat som klargjør hvordan IKT-sikkerhet i petroleumsindustrien blir regulert i gjeldende regelverk. Notatet belyser også forventninger fra myndighetene, og gir en oversikt over og status på satsingen innenfor IKT-sikkerhet i petroleumsnæringen de siste årene.

Veileder IKT-sikkerhet – *denne rapporten*

Det er utarbeidet et veiledningsdokument ("veileder") for norsk petroleumsvirksomhet som skal kunne brukes som et vedlegg til NSMs grunnprinsipper for IKT-sikkerhet. Veilederen er tilpasset de løsningene som er vanlige i petroleumssektoren, samtidig som den har fleksibilitet til å kunne håndtere hovedelementene innen petroleumsindustriens satsing på digitalisering.

Modellkontrollert operasjon

Rapporten sammenfatter kunnskap og anbefalinger om sikker bruk av data fra modellkontrollerte operasjoner. Det er lagt spesiell vekt på kvalitetssikring av modeller og kommunikasjon mellom programvareløsninger i boreoperasjoner.

Premisser for digitalisering og integrasjon IT – OT

Hensikten har vært å beskrive og vurdere hvordan digitalisering og bruk av skytjenester påvirker industrielle IKT-systemer, samt hvilke sikkerhetsløsninger man må iverksette for sikker bruk av skytjenester. I Petroleumstilsynets regelverk står spesielt prinsippet om segregering og uavhengighet sentralt som strategi for å etablere sikkerhet.

Kommunikasjonsnettverk

Hensikten har vært å undersøke hvilken rolle datanettverk ivaretar for ekstern kommunikasjon ved fare- og ulykkessituasjoner. Rapporten beskriver utfordringer knyttet til risiko og sårbarhet i data-nettverkene og det er utarbeidet konkrete forslag til forbedringer.

Vedlegg B: Vurdering av mulige tilleggstiltak fra Kraftberedskapsforskriften

I denne konteksten er det særlig "§ 6-9. Digitale informasjonssystemer" i Kraftberedskapsforskriften [2] som er relevant. Kraftberedskapsforskriften henviser eksplisitt til NSMs grunnprinsipper, men lister selv opp følgende områder: a) identifisere og dokumentere, b) risikovurdering, c) sikre og oppdage, d) håndtere og gjenopprette, e) tjenesteutsetting og f) sikkerhetsrevisjon.

Det er gjennomført en kartlegging av NSMs grunnprinsipper mot Kraftberedskapsforskriften, med den hensikt å avdekke gap. I tillegg til selve forskriften, er det gjort en vurdering av grunnprinsippene mot den utdypende informasjonen som er gitt av foreløpig tilleggsveileder til Kraftberedskapsforskriften [20]. Her er det verdt å bemerke at det skilles mellom det som er myndighetspålagt (forskriften) og det som ikke er det (veilederen).

Tabellen under gir en kortfattet oversikt over vår vurdering av Grunnprinsippenes dekning av punkter i Kraftberedskapsforskriftens § 6-9.

	Dekket av Grunnprinsipper for IKT-sikkerhet?	Mulige tilleggstiltak
a. Identifisere og dokumentere	Ja	-
b. Risikovurdering	Delvis	Ønskelig med detaljert veiledning i gjennomføring av risikovurdering, dekkes i stor grad av foreslått tiltak 2.b i kapittel 3
c. Sikre og oppdage	Ja	-
d. Håndtere og gjenopprette	Ja	-
e. Tjenesteutsetting	Delvis	Dekkes av tiltak foreslått i vedlegg C
f. Sikkerhetsrevisjon	Delvis	Dekkes av NSMs Grunnprinsipper for sikkerhetsstyring [16]

Identifisere og dokumentere

Virksomheter skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert. ([2], §6-9 bokstav a)

Ifølge tilleggsveilederen inngår kravet til å identifisere og dokumentere i grunnprinsippene som omhandler kartlegging av leveranser og verdikjeder, kartlegging av enheter og programvare, samt kartlegging av brukere og behov for tilgang ([20], s. 27). Dette kravet i forskriften dekkes altså av grunnprinsippenes kapittel 1.

Risikovurdering

Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert. ([2], §6-9 bokstav b)

Tilleggsveilederen gir ikke selv noen referanser til grunnprinsipper som dekker dette kravet.

Grunnprinsippenes tiltak 1.1.3 sier at virksomhetens prosesser for risikostyring skal identifiseres, og at dette normalt inkluderer risikovurdering. Ellers er det kapittel 2 (Beskytte og opprettholde) som i størst grad berører dette kravet. Tiltak 2.1.9 sier at det må tas ansvar for virksomhetens sikkerhet også ved tjenesteutsetting. Ifølge tiltak 2.2.7 skal det etableres en robust og motstandsdyktig IKT-arkitektur, noe som innebærer gjennomføring av risikovurderinger. Tiltak 2.3.10 sier at man skal redusere risiko med IoT-enheter. Det er imidlertid ingen tiltak i grunnprinsippene som eksplisitt sier at det skal gjennomføres risikovurderinger ved systemendringer.

Ofte er tilleggsveilederen sin gjennomgang av forskriftskravene presentert i form av runde formuleringer og forslag. Det framgår samtidig en del spissere formuleringer som bruker begrepene *skal* og *må*. Eksempler på dette er: "Risikovurdering skal kartlegge trusler og fare, og systematisk beskrive forekomst og konsekvens av uønskede hendelser og handlinger." ([20], s.28), "For tilsiktede hendelser må fastsettelse av risiko bygge på kvalitativ, kunnskapsbasert (subjektiv) vurdering av usikkerhet, noe som ikke alltid kommer frem. (…)" ([20], s.28) og "Nye risikovurderinger må gjennomføres ved organisatoriske, personellmessige eller systemtekniske endringer som har betydning for informasjonssikkerheten." ([20], s.28). Grunnprinsippene dekker ikke disse detaljene, men viser i stedet til eksempler på ulike metoder/rammeverk som kan brukes for å gjennomføre risikovurdering ([1], s.12).

NSMs Grunnprinsipper for sikkerhetsstyring [16] gir imidlertid mer føringer for gjennomføring av risikovurderinger generelt, og Grunnprinsipper for personellsikkerhet [15] omhandler aspekter personellmessige endringer som kan ha betydning for informasjonssikkerheten. På den måten utfyller de ulike grunnprinsippene hverandre. Det kan også være verdt å merke seg at risikovurdering generelt hviler på en annen standard (ISO/IEC 27005 [21]) enn den NSMs Grunnprinsipper for IKT-sikkerhet tar utgangspunkt i (ISO/IEC 27002 [22]).

Sikre og oppdage

Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres. Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer. ([2], §6-9 bokstav c)

Tilleggsveilederen til forskriften lister en rekke tiltak i grunnprinsippene som dekker kranene til å sikre og oppdage. Disse tiltakene inngår i grunnprinsippenes kapittel 2 og 3.

Også for kravet om å sikre inkluderer tilleggsveilederen noen formuleringer som bruker begrepet *må*: "For å oppfylle kravet om å sikre, må virksomheten i praksis som et minimum prioritere følgende tiltak: Blokkere kjøring av ikke autoriserte programmer; Oppgradere program- og maskinvare; Installere sikkerhets-oppdateringer; Begrense tildelingen av administrasjonsrettigheter. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres." ([20], s.29). Alle disse temaene er dekket av tiltak i grunnprinsippene.

Videre står det i forbindelse med krav om å oppdage at "virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer" og at "virksomheten skal varsle uønskede hendelser som for eksempel datainnbrudd, nektelsesangrep, oppdagelse av skadevare eller sabotasje-forsøk til det sektorvise responsmiljøet." ([20], s. 29). Dette dekkes av tiltak 4.2.3, som sier relevante interesseparter skal informeres i forbindelse med en hendelse.

Håndtere og gjenopprette

Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold. ([2], §6-9 bokstav d)

Ifølge tilleggsveilederen inngår kravet til å identifisere og dokumentere i grunnprinsippene som omhandler å forberede virksomheten på håndtering av hendelser, vurdere og kategorisere hendelser, kontrollere og håndtere hendelser, samt å evaluere og lære av hendelser ([20], s. 37). Dette kravet i forskriften dekkes altså av grunnprinsippenes kapittel 4.

Tjenesteutsetting

Virksomheter skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester. ([2], §6-9 bokstav e)

Tilleggsveilederen gir ikke selv noen referanser til grunnprinsipper som dekker dette kravet. Kravet dekkes imidlertid av tiltak 2.1.9 som handler om å ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting, tiltak 2.1.10 som sier at man skal undersøke sikkerheten hos tjenesteleverandør ved tjenesteutsetting, og tiltak 2.2.7 om å etablere en robust og motstandsdyktig IKT-arkitektur, inkludert risikovurdering av tjenesteleverandørtilgjengelighet.

Tilleggsveilederen sier at "virksomheter må velge løsninger som tilbyr minst like god IKT-sikkerhet som eksisterende løsning" og at "i tillegg må løsningen tilfredsstille de andre kravene som forskriften stiller, herunder krav til dokumentasjon, risikovurdering og jevnlig revisjon." ([20], s.30). Dette er ikke eksplisitt nevnt i grunnprinsippene.

NSM har en egen temarapport om tjenesteutsetting [17] som har mer detaljer om sikkerhetsrelevante hensyn å ta ved tjenesteutsetting.

Sikkerhetsrevisjon

Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene. ([2], §6-9 bokstav f)

Heller ikke her viser tilleggsveilederen selv til tiltak i grunnprinsippene som dekker kravet.

Det er likevel en rekke ulike tiltak som er inne på denne tematikken. Blant disse er tiltak 1.1.3 som handler om å identifisere virksomhetens prosesser for risikostyring knyttet til IKT, tiltak 2.3.5 som sier at man skal verifisere at aktivert sikkerhetskonfigurasjon er i henhold til virksomhetens godkjente sikkerhetskonfigurasjon, og tiltak 2.6.2 om å etablere en formell prosess for administrasjon av kontoer, tilganger og rettigheter. Også tiltak 3.4.1 (planlegg inntrengingstester med tydelig mål og omfang), 3.4.3 (benytt verktøy for sårbarhetskartlegging og angrepsverktøy) og 3.4.4 (gjennomfør jevnlige inntrengingstester (minst årlige) for å identifisere sårbarheter) er relevante i denne konteksten.

Det er presisert i tilleggsveilederen at "revisjonsrapporter må være et tema på virksomhetens ledermøter eller andre relevante fora i virksomheten. Som minimum må revisjonen kontrollere organisering av sikkerhetsarbeidet, inkludert plassering av ansvar, og tiltak for beskyttelse av kraftsensitiv informasjon mot uautorisert tilgang." ([20], s.31). Det står også at "resultatene og konklusjonene sikkerhetsrevisjonene må dokumenteres" og at "avvik og feil må håndteres i henhold til virksomhetens internkontrollsystem jf. kbf. § 2-10." ([20], s.31). Dette er ikke eksplisitt omtalt i grunnprinsippene.

- **Oppsummerende kommentarer**Grunnprinsippene dekker i grove trekk kravene i Kraftberedskapsforskriften.
- Når det gjelder risikovurderinger, henviser ikke tilleggsveileder til Kraftberedskapsforskriften til NSMs grunnprinsipper for IKT-sikkerhet. Grunnprinsippene omfatter risikovurdering, men sier lite om hvordan disse skal eller kan gjøres. Store deler av dette gapet dekkes imidlertid av NSMs grunnprinsipper for sikkerhetsstyring.

Vedlegg C: Vurdering av mulige tilleggstiltak fra NIST CSF

Ifølge National Institute of Standards and Technology (NIST) integrerer deres Cybersecurity Framework (CSF) industristandarder og beste praksis for å hjelpe organisasjoner med å håndtere risiko knyttet til cybersikkerhet. Rammeverket er delt inn i fem funksjoner: 1) identifisere, 2) beskytte, 3) oppdage, 4) respondere og 5) gjenopprette [3]. Hver av disse inneholder ulike kategorier og delkategorier. På overordnet nivå samsvarer funksjonene i stor grad på inndelingen som er gjort i NSM sine grunnprinsipper for IKT-sikkerhet. Det er gjennomført en kartlegging av NSMs grunnprinsipper mot NIST CSF, med den hensikt å avdekke gap, samt vurdere relevansen av disse for industrielle IKT-systemer. Tabellen under oppsummerer i hvilken grad hver av delkategoriene i NIST er dekket av grunnprinsippene (Ja/Delvis/Nei). For delkategoriene som er merket *Delvis* eller *Nei*, er det antydet med en hake (✓) der vi har foreslått tilleggstiltak til grunnprinsippene. Merk at noen av hakene representerer samme tilleggstiltak.

Identify		Protect		Detect		Respond		Recover	
ID.AM-1	Ja	PR.AC-1	Ja	DE.AE-1	Ja	RS.RP-1	Ja	RC.RP-1	Ja
ID.AM-2	Ja	PR.AC-2	Nei ✓	DE.AE-2	Ja	RS.CO-1	Ja	RC.IM-1	Ja
ID.AM-3	Ja	PR.AC-3	Ja	DE.AE-3	Ja	RS.CO-2	Ja	RC.IM-2	Ja
ID.AM-4	Ja	PR.AC-4	Delvis ✓	DE.AE-4	Ja	RS.CO-3	Ja	RC.CO-1	Ja
ID.AM-5	Nei ✓	PR.AC-5	Ja	DE.AE-5	Ja	RS.CO-4	Ja	RC.CO-2	Nei ✓
ID.AM-6	Ja	PR.AC-6	Ja	DE.CM-1	Ja	RS.CO-5	Ja	RC.CO-3	Ja
ID.BE-1	Ja	PR.AC-7	Delvis ✓	DE.CM-2	Nei ✓	RS.AN-1	Ja		
ID.BE-2	Nei ✓	PR.AT-1	Nei ✓	DE.CM-3	Ja	RS.AN-2	Ja		
ID.BE-3	Ja	PR.AT-2	Nei ✓	DE.CM-4	Ja	RS.AN-3	Ja		
ID.BE-4	Ja	PR.AT-3	Nei ✓	DE.CM-5	Ja	RS.AN-4	Ja		
ID.BE-5	Delvis ✓	PR.AT-4	Nei ✓	DE.CM-6	Delvis ✓	RS.AN-5	Ja		
ID.GV-1	Ja	PR.AT-5	Nei ✓	DE.CM-7	Ja	RS.MI-1	Ja		
ID.GV-2	Ja	PR.DS-1	Ja	DE.CM-8	Ja	RS.MI-2	Ja		
ID.GV-3	Delvis ✓	PR.DS-2	Ja	DE.DP-1	Ja	RS.MI-3	Delvis ✓		
ID.GV-4	Ja	PR.DS-3	Delvis ✓	DE.DP-2	Ja	RS.IM-1	Ja		
ID.RA-1	Ja	PR.DS-4	Nei ✓	DE.DP-3	Ja	RS.IM-2	Ja		
ID.RA-2	Ja	PR.DS-5	Delvis ✓	DE.DP-4	Delvis ✓				
ID.RA-3	Ja	PR.DS-6	Ja	DE.DP-5	Delvis ✓				
ID.RA-4	Nei ✓	PR.DS-7	Ja						
ID.RA-5	Nei ✓	PR.DS-8	Delvis ✓						
ID.RA-6	Nei ✓	PR.IP-1	Ja						
ID.RM-1	Ja	PR.IP-2	Delvis ✓						
ID.RM-2	Ja	PR.IP-3	Ja						
ID.RM-3	Nei ✓	PR.IP-4	Ja						
ID.SC-1	Delvis ✓	PR.IP-5	Nei ✓						
ID.SC-2	Delvis ✓	PR.IP-6	Delvis ✓						
ID.SC-3	Delvis ✓	PR.IP-7	Nei ✓						
ID.SC-4	Delvis ✓	PR.IP-8	Nei ✓						
ID.SC-5	Ja	PR.IP-9	Ja						
		PR.IP-10	Ja						
		PR.IP-11	Nei ✓						
		PR.IP-12	Ja						
		PR.MA-1	Nei ✓						
		PR.MA-2	Nei ✓						
		PR.PT-1	Ja						
		PR.PT-2	Ja						
		PR.PT-3	Ja						
		PR.PT-4	Ja						
		PR.PT-5	Nei ✓						

Nedenfor følger en beskrivelse av de identifiserte gapene med begrunnelse for de enkelte delkategoriene som er merket med *nei* eller *delvis*, samt en vurdering av relevans for OT og om det for disse derfor foreslås tillegg til tiltakene i NSMs Grunnprinsipper for IKT-sikkerhet.

Identifisere

ID.AM-5	***Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value*** Grunnprinsippene stiller ikke krav til prioritering av ressurser. Tiltak 2.7.5 sier at det skal defineres krav til sikringsnivå for ulike typer informasjon, men sier ingenting om andre typer ressurser. Dette dekkes imidlertid delvis av NSMs Grunnprinsipper for sikkerhetsstyring som sier at "Verdivurderingen er en kartlegging av virksomhetens verdier" og at "Formålet med vurderingen er å identifisere hvilke verdier som er de viktigste for virksomhetens funksjoner" (s.9)
Tiltak 2.a	*Prioriter ressurser på basis av kritikalitet og forretningsverdi.*
ID.BE-2	***The organization's place in critical infrastructure and its industry sector is identified and communicated*** NSM påpeker at grunnprinsippene retter seg mot kritisk infrastruktur, men det er ikke utformet tiltak som går på det å identifisere egen rolle i kritisk infrastruktur.
Tiltak 1.a	*Identifiser og kommuniser virksomhetens rolle kontra andre aktører i industrien, for å forstå hvordan hendelser i andre virksomheter kan virke inn på egen drift/sikkerhet.*
ID-BE-5	***Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations*** Tiltak 2.2.7 sier at man skal gjennomføre risikovurderinger for ulike typer feil og angrep, og videre at man ut fra resultatene fra risikovurdering og kritikalitet kan gjøre deler av IT-løsningen mer robust. Grunnprinsippene spesifiserer derimot ikke at man skal stille krav basert på ulike driftstilstander (under angrep, under gjenopprettelse, samt under normal drift).
Tiltak 2.b	*Identifiser kritiske funksjoner og avgjør hvilken grad av robusthet som kreves av disse i forskjellige driftstilstander (under normal drift, under kritiske operasjoner, under angrep etc.)*
ID-GV-3	***Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed*** Grunnprinsippene omfatter kun et krav om at lover, reguleringer og virksomhetens retningslinjer for sikkerhetsovervåkning skal følges (3.2.2). Generelle lover og regler for cybersikkerhet er ikke nevnt.
-	*Ingen tiltak foreslås, ettersom dette burde dekkes av tiltak 3.2.2 samt foreslått tiltak 2.h.*

ID.RA-4	***Potential business impacts and likelihoods are identified***
	Kartlegging av mulig påvirkning av forretningsprosesser basert på sårbarheter og trusler er ikke dekket av grunnprinsippene. Tiltak 4.3.1 er eneste tiltak som omhandler kartlegging av påvirkning av forretningsprosesser, men da kun i sammenheng med enkelthendelser.
Tiltak 1.b	*Gjennomfør jevnlige risikovurderinger for å opprettholde oversikt over relevante risikoer. Dette inkluderer normalt a) Kartlegg sårbarheter og trusler, b) Identifiser potensielle konsekvenser og sannsynligheter for hendelser som kan forårsakes av avdekkede sårbarheter og trusler, c) Anslå risiko basert på trusler, sårbarheter, sannsynligheter og konsekvenser, d) Identifiser og prioriter risikotiltak.*
ID.RA-5	***Threats, vulnerabilities, likelihoods, and impacts are used to determine risk***
	Grunnprinsippenes tiltak 2.2.7 sier at man skal gjennomføre risikovurderinger, men det sies ikke noe om *hvordan* disse skal gjøres (bruk av identifiserte trusler, sårbarheter, osv.). I den utdypende informasjonen til tiltak 1.1 står det imidlertid at man må bruke riktig metode for risikovurdering i den enkelte virksomheten, og det henvises til eksempler på ulike metoder/rammeverk som kan brukes (s. 12). I grunnprinsippene for sikkerhetsstyring er det presisert at en risikovurdering "bør inneholde en vurdering av trusler, sårbarheter og avhengigheter, inkludert vurdering av sannsynlighet og konsekvens." (s.8)
-	*Se ID.RA-4 (og foreslått tiltak 1.b)*
ID.RA-6	***Risk responses are identified and prioritized***
	Grunnprinsippene dekker ikke identifisering og prioritering av risikotiltak på generelt nivå. Grunnprinsipper for sikkerhetsstyring dekker derimot dette, bl.a. gjennom følgende: "En sentral del av det forebyggende sikkerhetsarbeidet er å velge de risikoreduserende sikkerhetstiltakene som er mest hensiktsmessige og effektive for beskyttelse av virksomhetens verdier." (s.6)
-	*Se ID.RA-4 (og foreslått tiltak 1.b)*
ID.RM-3	***The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis***
	NSM nevner ikke egen plassering i kritisk infrastruktur (ref. ID.BE-2), og sier dermed heller ikke noe om at fastsettelse av risikotoleranse skal bruke denne typen av informasjon.
Tiltak 1.c	*Sørg for at virksomhetens rolle i bransjen og sektorspesifikke forhold blir hensyntatt ved fastsettelse av risikotoleranse.*
ID.SC-1	***Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders***
	Grunnprinsippene omhandler kun reduksjon av risiko for målrettet manipulasjon av IKT-produkter i leverandørkjeden (2.1.4), men sier ellers lite om risikohåndtering av leverandørkjeden på generelt nivå.
Tiltak 2.c	*Etabler en prosess for styring av IKT-sikkerhetsrisiko i hele leverandørkjeden.*

ID.SC-2	***Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process***
	Fra den generelle teksten: "Med tjenesteutsetting menes her at virksomheten velger å anskaffe «varer eller tjenester» fra en ekstern leverandør i stedet for å levere dem selv". Tiltak 2.1.10 i grunnprinsippene sier at man skal undersøke sikkerheten hos tjeneste-leverandør ved tjenesteutsetting, men det sier ikke noe om prioritering og vurdering. Dekkes av den generelle teksten, men har ikke noe eksplisitt tiltak.
Tiltak 2.d	*Identifiser og prioriter alle involverte aktører for å forstå IKT-sikkerhetsrisikoen i hele leverandørkjeden.*

ID.SC-3	***Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan***
	Tiltak 2.1.10 i grunnprinsippene sier at man skal undersøke sikkerheten hos tjeneste-leverandør ved tjenesteutsetting, men sier ikke noe om kontrakter knyttet til sikkerhetsmål.
Tiltak 2.e	*Inkluder krav til IKT-sikkerhet i kontrakter med leverandører.*

ID.SC-4	***Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations***
	Tiltak 2.1.10 i grunnprinsippene sier at man skal undersøke sikkerheten hos tjeneste-leverandør ved tjenesteutsetting, men sier ikke noe om rutinemessig vurdering.
Tiltak 2.f	*Rutinemessig følg opp leverandørers etterlevelse av kontraktfestede krav til IKT-sikkerhet.*

Beskytte

PR.AC-2	***Physical access to assets is managed and protected***
	NSMs grunnprinsipper for IKT-sikkerhet stiller ikke krav til håndtering og beskyttelse knyttet til fysisk tilgang. NSM har imidlertid utgitt et eget dokument med grunnprinsipper for fysisk sikkerhet [14] som bl.a. skal bidra til virksomheters arbeid med å beskytte verdier og funksjoner mot uautorisert adgang, og der "opprett elektronisk adgangskontroll" er et anbefalt tiltak. Bruk av adgangskort er dessuten nevnt som eksempel på organisatorisk barriere som kan understøtte fysiske sikkerhetstiltak.
-	*Ingen tiltak er foreslått, siden grunnprinsippene er spesifikt rettet mot IKT. Veiledning for fysisk sikring finnes i NSMs grunnprinsipper for fysisk sikring.*

PR.AC-4	***Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties***
	Grunnprinsippene inkluderer et tiltak om etablering av retningslinjer for tilgangskontroll (2.6.1) og spesifiserer at disse retningslinjene bør følge minste privilegiums prinsipp. Prinsippet om "separation of duties" (en form for internkontroll der mer enn én person kreves for å fullføre en oppgave for å forhindre svindel eller feil) er derimot ikke nevnt i grunnprinsippene.
Tiltak 2.g	*Vurder behovet for å involvere mer enn en person for bestemte handlinger (separation of duties).*

PR.AC-7	***Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)***
	NSM sier at man skal etablere en formell prosess for administrasjon av kontoer, tilganger og rettigheter (2.6.2), at man skal styre tilgang til enheter (2.6.6), samt at man skal bruke multi-faktor autentisering for å autentisere bruker (2.6.7). Det fremgår imidlertid ikke av grunnprinsippene at brukere, utstyr og andre verdier autentiseres (f.eks. énfaktor, flerfaktor) med basis i vurdert risiko.
-	*Ingen tiltak er foreslått, siden dette antas å bli håndtert implisitt.*
PR.AT-1	***All users are informed and trained***
	NSM sine grunnprinsipper mangler dette overordnede fokuset på bevisstgjøring og opplæring knyttet til cybersikkerhet. Kapittel 4 i dekker opplæring, men da kun av personell som skal involveres i hendelseshåndtering. Kapittelet omfatter også bevisstgjøring, men kun i form av "lessons learned" etter konkrete hendelser. NSMs Grunnprinsipper for sikkerhetsstyring sier at "Ledelsen bør sikre tilstrekkelig risiko- og sikkerhetsforståelse i hele virksomheten. Dette gjøres gjennom opplæring av egne ansatte, men vel så viktig er å sørge for at leverandører, underleverandører og andre oppdragstakere har god risiko- og sikkerhetsforståelse." (s.6) Det presiseres også at riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, trening og øvelser.
Tiltak 2.h	*Påse nødvendig opplæring og trening i IKT-sikkerhet for å sikre god risiko- og sikkerhetsforståelse blant alle brukere (ansatte så vel som leverandører, underleverandører og andre oppdragstakere).*
PR.AT-2	***Privileged users understand their roles and responsibilities***
	NSM sier ikke noe konkret om at privilegerte brukere skal forstå sine roller og sitt ansvar. Grunnprinsippene for sikkerhetsstyring inkluderer et avsnitt om øvelse, trening og opplæring der det er presisert at "Alle som utfører aktiviteter med betydning for sikkerhet bør kjenne de grunnleggende forutsetningene for egen arbeidsutførelse." (s. 17)
Tiltak 2.i	*Påse at alle som utfører aktiviteter med betydning for IKT-sikkerhet forstår hvordan egen rolle og ansvar påvirker sikkerheten.*
PR.AT-3	***Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities***
	NSM sier ikke noe om at tredjeparts interessenter skal forstå sine roller og sitt ansvar. Grunnprinsippene for sikkerhetsstyring inkluderer et avsnitt om øvelse, trening og opplæring der det er presisert at "Alle som utfører aktiviteter med betydning for sikkerhet bør kjenne de grunnleggende forutsetningene for egen arbeidsutførelse." (s. 17)
-	*Se PR.AT-2 (og forslag til tiltak 2.i)*
PR.AT-4	***Senior executives understand their roles and responsibilities***
	NSM sier ikke noe om at øverste ledelse skal forstå sine roller og sitt ansvar. Grunnprinsippene for sikkerhetsstyring inkluderer et avsnitt om øvelse, trening og opplæring der det er presisert at "Alle som utfører aktiviteter med betydning for sikkerhet bør kjenne de grunnleggende forutsetningene for egen arbeidsutførelse." (s. 17)
-	*Se PR.AT-2 (og forslag til tiltak 2.i)*

PR.AT-5	***Physical and cybersecurity personnel understand their roles and responsibilities***
	NSM sier ikke noe om at sikkerhetspersonell skal forstå sine roller og sitt ansvar. Grunnprinsippene for sikkerhetsstyring inkluderer et avsnitt om øvelse, trening og opplæring der det er presisert at "Alle som utfører aktiviteter med betydning for sikkerhet bør kjenne de grunnleggende forutsetningene for egen arbeidsutførelse." (s. 17)
-	*Se PR.AT-2 (og forslag til tiltak 2.i)*
PR.DS-3	***Assets are formally managed throughout removal, transfers, and disposition***
	Ifølge tiltak 1.2.1 skal det etableres en prosess for å kartlegge enheter og programvare som er i bruk i virksomheten. Det er imidlertid ikke presisert at aktiva formelt skal håndteres gjennom fjerning, overføring og avhending.
Tiltak 2.j	*Etabler rutiner for håndtering av aktiva ved fjerning, overføring og avhending.*
PR.DS-4	***Adequate capacity to ensure availability is maintained***
	Det er ingen tiltak som eksplisitt sier at det må opprettholdes tilstrekkelig kapasitet for å sikre tilgjengelighet. Grunnprinsippene berører tematikken i tiltak 1.1.4, men kun i konteksten "å fastsette risikogrenser".
Tiltak 2.k	*Opprettholdt tilstrekkelig kapasitet for å sikre tilgjengelighet.*
PR.DS-5	***Protections against data leaks are implemented***
	Tiltak 2.5.8 sier at man skal styre all trafikk til og fra forvaltede mobile klienter via virksomhetens nett, dette bl.a. for å hindre og detektere datalekkasje fra kompromitterte klienter. Det kan imidlertid være ytterligere relevante tiltak. Dessuten kan NIST sin delkategori omfatte mer enn bare mobile klienter.
-	*Ingen tiltak er foreslått, siden OT i liten grad krever konfidensialitetsbeskyttelse, og det er få eksterne tilkoblinger.*
PR.DS-8	***Integrity checking mechanisms are used to verify hardware integrity***
	Grunnprinsippene dekker kun maskinvareintegritet i anskaffelsesprosessen (f.eks. 2.1.4, 2.2.1 og 2.3.4), men ser ut til å ha lite fokus på denne typen integritet etter installasjon.
-	*Ingen tiltak er foreslått, siden OT-systemer generelt er lite fysisk tilgjengelig for eksterne.*
PR.IP-2	***A System Development Life Cycle to manage systems is implemented***
	Grunnprinsippene omfatter ikke et konkret tiltak om implementering av livssyklus for systemutvikling. Likevel dekker kapittel 2 i mye av det som forventes inkludert i en slik livssyklus. Blant annet er det spesifisert at man skal benytte en metode for sikker utvikling av programvare (2.1.5), gjennomføre tilstrekkelig med testing gjennom hele utviklingsprosessen (2.1.7) og vedlikeholde programvarekode som utvikles/benyttes i virksomheten (2.1.8). Videre presiseres det at det skal etableres og vedlikeholdes en helhetlig sikkerhetsarkitektur (2.2.1), etableres og vedlikeholdes standard sikkerhets-konfigurasjoner (2.3.4), samt at sikkerhet skal integreres i virksomhetens prosess for endringshåndtering (2.10.1). Det grunnprinsippene ikke adresserer er "sluttfasen" til systemer, for eksempel når det gjelder generell sletting av data.
-	*Ingen tiltak er foreslått, siden dette dekkes av summen av eksisterende tiltak, samt foreslått tiltak 2.j.*

PR.IP-5	***Policy and regulations regarding the physical operating environment for organizational assets are met***
	NSMs grunnprinsipper gir ingen referanse til retningslinjer eller lovverk for fysisk plassering og beskyttelse. NSM har utgitt et eget dokument med grunnprinsipper for fysisk sikkerhet [14], men presiserer i dette følgende: "Grunnprinsippene er ikke knyttet opp mot krav i, eller i medhold av sikkerhetsloven eller andre regelverk. For virksomheter underlagt sikkerhetsloven viser vi til NSMs Veileder i fysisk sikkerhet, der det dannes et grunnlag for virksomhetenes arbeid med å etterleve regelverket." (s. 3).
Tiltak 2.l	*Sikre etterlevelse av regler og forskrifter knyttet til fysisk driftsmiljø for organisasjonens aktiva.*
PR.IP-6	***Data is destroyed according to policy***
	NSMs tiltak 2.1.10 sier at det bør undersøkes om tjenesteleverandør ved tjenesteutsetting "har spesifisert hvilke aktiviteter som skal utføres ved terminering av kontrakten, blant annet tilbakeføring/flytting/ sletting av virksomhetens informasjon". Videre sier tiltak 3.2.1 at sletting av data skal beskrives i virksomhetens strategi og retningslinjer for sikkerhetsovervåking. Grunnprinsippene adresserer imidlertid ikke generell sletting av data for eksempel i forbindelse med "sluttfasen" til systemer.
-	*Se PR.DS-3 (og foreslått tiltak 2.j)*
PR.IP-7	***Protection processes are improved***
	Grunnprinsippenes tiltak 2.3.4 omfatter regelmessig oppdatering av konfigurasjon, samt at dette må følge virksomhetens prosess for endrings-håndtering. NSM beskriver altså langt på vei en prosess for sikring/beskyttelse, men krever ikke på samme måte som NIST CSF forbedring av prosessen.
Tiltak 2.m	*Etabler rutiner for (kontinuerlig) forbedring av prosesser for sikring/beskyttelse.*
PR.IP-8	***Effectiveness of protection technologies is shared***
	Deling av denne typen informasjon nevnes ikke eksplisitt av NSM.
Tiltak 2.n	*Del informasjon vedrørende effektivitet av teknologi for sikring/beskyttelse med relevante interessenter.*
PR.IP-11	***Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening***
	På et generelt nivå sier at NSM at det skal etableres en formell prosess for administrasjon av kontoer, tilganger og rettigheter (2.6.2): Dette tiltaket er likevel ikke veldig detaljert, og nevner heller ikke at cybersikkerhet skal inngå i HR-prosedyrer. NSMs Grunnprinsipper for personellsikkerhet [15] foreslår en rekke relevante tiltak knyttet til blant annet sikkerhetsbasert tilnærming til rekruttering (s. 6) og reduksjon av risiko under ansettelsesforhold (s. 9). Disse er imidlertid generelle og har derfor ikke et spesielt fokus på IKT-sikkerhet.
Tiltak 2.o	*Inkluder IKT-sikkerhet i personal-praksis (f.eks. i forbindelse med ansettelse og ansettelsesforhold).*

PR.MA-1 ***Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools***

Grunnprinsippene omfatter ikke konkrete tiltak knyttet til verktøy for vedlikehold og reparasjon. Tiltak 2.1.4 er eneste tiltak som omhandler vedlikehold, og dette spesifiserer at leverandørers fysiske adgang ifm. vedlikehold av IKT-produkter bør reguleres og kontrolleres.

Tiltak 2.p *Utfør og loggfør vedlikehold og reparasjoner av organisasjonens aktiva ved hjelp av godkjente verktøy.*

PR.MA-2 ***Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access***

Grunnprinsippene sier ikke noe eksplisitt om fjernstyring av vedlikehold.

Tiltak 2.q *Godkjenn, utfør og loggfør fjernvedlikehold på en måte som forhindrer uautorisert tilgang.*

PR.PT-5 ***Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations***

Tiltakene i grunnprinsippene dekker ikke mekanismer for å innfri krav til resiliens både i normalsituasjon og i avvikende situasjoner.

Tiltak 2.r *Implementer nødvendige mekanismer for å sikre tilstrekkelig robusthet i forskjellige driftstilstander (under normal drift, under kritiske operasjoner, under angrep etc.)*

Oppdage

DE.CM-2 ***The physical environment is monitored to detect potential cybersecurity events***

NSMs grunnprinsipper stiller ikke selv krav til overvåkning av det fysiske driftsmiljøet. NSMs Grunnprinsipper for fysisk sikkerhet [14] omhandler bl.a. bruk av kameraer og andre deteksjonsmidler.

Tiltak 3.a *Overvåk systemenes fysiske driftsmiljø (ved hjelp av kameraer og andre deteksjonsmidler) for å oppdage potensielle IKT-hendelser.*

DE.CM-6 ***External service provider activity is monitored to detect potential cybersecurity events***

Tiltak 2.5.7 sier at man må ha kontroll på trafikk mellom virksomheten og samarbeidspartnere/tjenesteleverandører. Det er også andre tiltak som omhandler planer for sikkerhet knyttet til tjenestetilbydere (f.eks. 2.1.1, 2.1.9 og 2.1.10). Det er imidlertid lite fokus på den faktiske overvåkningen.

Tiltak 3.b *Overvåk trafikk til og fra eksterne tjenesteleverandører for å oppdage potensielle IKT-hendelser.*

DE.DP-4 ***Event detection information is communicated***

Tiltak 3.4.6 sier at resultater fra inntrengningstester skal kommuniseres til relevante interesseparter. Det finnes også tiltak som går mer direkte på koordinering og kommunikasjon under og i etterkant av hendelser (4.3.5 og 4.3.6). Mens NIST CSF skiller mellom "event" og "incident", er ikke et tilsvarende skille like synlig i NSM. Det kan være annen informasjon enn kun resultater fra inntrengningstester som med fordel kan kommuniseres/deles.

Tiltak 3.c *Del informasjon vedrørende avviksdeteksjon med relevante interessenter.*

DE.DP-5 ***Detection processes are continuously improved***

I den utdypende informasjonen om analysering av data for sikkerhetsovervåkning i NSM står det at "virksomhetene bør kontinuerlig forbedre sitt kompetansenivå på prosessering av sikkerhetsrelevant data, herunder forståelse av egne systemer, verktøybruk, truslene og utvikling av metoder for å detektere uautoriserte hendelser." (s. 43) Intensjonen er altså dekket av den generelle teksten, men det finnes ikke noe konkret tiltak i grunnprinsippene som stiller krav til dette. NSM er inne på tematikken i tiltak 3.3.3, som sier at man skal benytte kunnskap om normaltilstanden og trusler til å forbedre kriterier for alarmering i verktøyet.

Tiltak 3.d *Etabler rutiner for kontinuerlig forbedring av prosesser for avviksdeteksjon.*

Håndtere

RS.MI-3 ***Newly identified vulnerabilities are mitigated or documented as accepted risks***

Grunnprinsippene omfatter både identifikasjon av toleransegrenser for risiko (1.1.4) og gjennomføring av sårbarhetskartlegging (3.1.1). Det er imidlertid ingen eksplisitt kobling mellom de som har ansvar for sårbarhetskartlegging og de som har ansvar for overordnet risikostyring. Det er ingen tiltak som sier noe om å dokumentere identifiserte sårbarheter som "akseptert risiko".

Tiltak 4.a *Håndter risiko knyttet til nyoppdagede sårbarheter (ved å iverksette tiltak eller akseptere risiko).*

Gjenopprette

RC.CO-2 ***Reputation is repaired after an incident***

Grunnprinsippene inkluderer ikke noen tiltak som omhandler gjenoppbygging av omdømme etter en hendelse.

Tiltak 4.b *Etabler rutiner for å begrense omdømmetap etter en hendelse.*

Oppsummerende kommentarer

- Den overordnede strukturen i NIST sitt rammeverk ligner på inndelingen som er gjort i NSM sine grunnprinsipper for IKT-sikkerhet.
- Gjennomgangen viser størst gap under de proaktive verdiene *identifisere* og *beskytte*, mens det er færre kategorier som ikke dekkes eller bare delvis dekkes under de tre øvrige verdiene. Særlig under de reaktive verdiene *respondere* og *gjenopprette* er det få gap å bemerke.
- NIST CSF dekker bredere når det gjelder risikovurderinger (ID.RA). Tiltak knyttet til identifisering av mulig påvirkning av forretningsprosesser, bruk av trusler og sårbarheter til fastsetting av risiko, samt identifisering av risikotiltak mangler i grunnprinsippene. Deler av dette dekkes imidlertid av grunnprinsippene for sikkerhetsstyring [16].
- Også risikohåndtering av leverandørkjeden (ID.SC) er grundigere dekket i NIST CSF. Mens NIST omtaler prosesser for risikohåndtering av leverandørkjeden, dekker grunnprinsippene kun målrettet manipulasjon av IKT-produkter. Videre fokuserer NSM på tjenesteleverandører ved tjenesteutsetting, mens NIST bruker bredere benevnelser som leverandører og tredjeparts partnere.

- Gjennomgangen viser at grunnprinsippene ikke inkluderer tiltak som dekker fysisk tilgang, fysisk plassering og beskyttelse eller overvåking av fysisk arbeidsmiljø. Dette presiseres imidlertid også eksplisitt i dokumentets introduksjon som sier at fokuset er på teknologiske og organisatoriske tiltak, og at tiltak som dekker fysisk sikkerhet og den menneskelige perspektiv i liten grad omtales i Grunnprinsipper for IKT-sikkerhet. Disse aspektene dekkes imidlertid av Grunnprinsipper for fysisk sikkerhet [14].
- NIST CSF har en egen kategori om bevisstgjøring og trening (PR.AT), der det sies at alle brukere skal være informert og trent. NSM sine grunnprinsipper omhandler kun opplæring av personell som skal involveres i hendelseshåndtering, samt bevisstgjøring i form av lærepunkter etter hendelser. NIST sier videre at privilegerte brukere, tredjeparts interessenter, øverste ledelse og sikkerhetspersonell skal forstå sine roller og sitt ansvar. Grunnprinsippene mangler dette generelle fokuset på bevisstgjøring og trening. Fokuset på bevisstgjøring og trening dekkes derimot i stor grad av grunnprinsippene for sikkerhetsstyring [16], som sier at "Alle som utfører aktiviteter med betydning for sikkerhet bør kjenne de grunnleggende forutsetningene for egen arbeidsutførelse" og at "riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, trening og øvelser." (s. 17)
- Både NIST CSF og NSM sine grunnprinsipper dekker viktigheten av kommunikasjon med interne og eksterne interessenter under og etter en hendelse. Det er kun i forbindelse med resultater fra inntrengningstester (3.4.6) at NSM omtaler kommunikasjon med relevante eksterne interesseparter i annen sammenheng enn i forbindelse med hendelser. Kontinuerlig kommunikasjon, med eksterne så vel som interne parter, går oftere igjen i rammeverket til NIST.
- Gjennomgangen har også avdekket noen språklige ulikheter mellom NIST CSF og grunnprinsippene til NSM som det er verdt å bemerke: 1) Mens NSM bruker formuleringer som *kartlegg* og *etabler*, er NIST ofte mer konkrete på handling i sine kategorier. For eksempel sier NSM at det skal etableres planer, uten eksplisitt å presisere at disse skal brukes. NIST går ut fra at det er etablert planer, og sier at disse skal følges. 2) NIST CSF skiller mellom *event* og *incident*. Et tilsvarende skille er ikke like synlig i grunnprinsippene, noe som kan skyldes at begge begreper ofte oversettes til *hendelse*. I foreslåtte tilleggstiltak har vi valgt å omtale det NIST kaller *anomalous event* som *avvik*.

Vi har forslått 27 tilleggstiltak basert på de avdekte gapene mellom NSM sine grunnprinsipper for IKT-sikkerhet og NIST CSF – henholdsvis 3 på kategorien Identifisere og kartlegge, 18 på kategorien Beskytte og opprettholde, 4 på kategorien Oppdage og 2 på kategorien Håndtere og gjenopprette.

Teknologi for et bedre samfunn

www.sintef.no