NVE

EKSTERN RAPPORT NR. 5 / 2025

Cyber-øvelser for virksomheter i kraftforsyningen

SKREVET AV Safetec

NVE Ekstern rapport nr. 5/2025
Cyber-øvelser for virksomheter i kraftforsyningen

Utgitt av:	Norges vassdrags- og enenrgidirektorat
Redaktør:	Linn Barstad
Forfattere:	Håkon Olsen, Annette Andersen og Jakob Stendahl v/Safetec
Omslagsbilde:	Tavle for 220 volt fordeling i Nore kraftanlegg. Foto: Statnett

ISBN:	978-82-410-2460-3
ISSN:	2535-8235
Saksnummer:	202420651

Sammendrag:	Denne rapporten presenterer en overordnet samling på 20 øvingsscenarier for IT- og OT-hendelser i kraftsektoren. Rapporten beskriver innlednngsvis relevante forhold knyttet til øvelsene, inkludert kartlegging av krav, systembeskrivelser, og roller og ansvar i hendelseshåndtering. Rapporten fokuserer på digital beredskap i små og mellomstore virksomheter. NVE har publisert en digital veileder der virksomhetene kan laste ned alle scenariene med brukerveiledning.
Emneord:	Øvelser, IT-hendelser, OT-hendelser, scenario, hendelseshåndtering, øvingsmateriale, spilløvelse, diskusjonsøvelse, evaluering.

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

Mars 2025

Forord

Kraftberedskapsforskriftens § 2-7 stiller krav til at KBO-enhetene skal gjennomføre øvelser med slikt innhold og omfang at enheten vedlikeholder og utvikler sin kompetanse til å håndtere alle aktuelle ekstraordinære situasjoner. Virksomheten skal ha en flerårig øvelsesplan, og gjennomføre minimum én årlig øvelse. Sommeren 2023 gjennomførte NVE en studie av kraftforsyningens beredskap mot digitale angrep. Resultatene fra studien viste at kraftforsyningen øver lite på å håndtere digitale angrep, og at læring fra øvelser fortsatt trenger et løft.

Hensikten med rapporten er å gjøre det enklere for virksomheter å øve på digitale angrep. Det er laget 20 øvelsesscenarier for IT- og OT-hendelser, i hovedsak tilpasset små- og mellomstore virksomheter. Øvelsene er også tilpasset ulike modenhetsnivå på digital sikkerhet. Det er bredde og kompleksitet i øvelsene slik at ulike deler av organisasjonen blir berørt, og det er ulike øvelsesformer. For å tilgjengeliggjøre scenariene på best mulig måte har NVE laget en digital veileder, *Temaveileder: Øvelsesscenario for digitale hendelser i kraftforsyningen*, hvor alt øvelsesmateriell ligger tilgjengelig for virksomhetene. Dette inkluderer også veiledning på hva en bør tenke på før, under og etter øvelsene.

Vi vil takke Safetec for deres grundige arbeid med utarbeidelsen av disse scenariene, og vi håper at disse scenariene vil inspirere virksomhetene til å øve mer.

Oslo, februar 2025

Christian Damslora
fungerende seksjonssjef
Seksjon for digital sikkerhet i kraftforsyningen
Tilsyns- og beredskapsavdelingen

Dokumentet sendes uten underskrift. Det er godkjent i henhold til interne rutiner.

Cyber-øvelser for virksomheter i kraftforsyningen

NVE

Hovedrapport

Type dokument:

Hovedrapport

Rapport-tittel:

Cyber-øvelser for virksomheter i kraftforsyningen

Kunde:

NVE

Oppsummering

Denne rapporten, utarbeidet av Safetec på oppdrag fra NVE, presenterer en samling øvingsscenarier for IT- og OT-hendelser i kraftsektoren. Rapporten beskriver innledningsvis relevante forhold knyttet til øvelsene, inkludert kartlegging av krav, systembeskrivelser, og roller og ansvar i hendelseshåndtering. Rapporten fokuserer på å forbedre digital beredskap i små og mellomstore virksomheter gjennom realistiske og relevante øvingsscenarier.

Dokument nr.
ST-001588-5

Forfatter(e)
Håkon Olsen, Annette Andersen, Jakob Stendahl

Revisjon	Dato	Grunn for revisjon	Kontrollert	Godkjent
2	05.12.2024	Endelig	C. Thingvold	Sigve Oltedal
1	26.11.2024	Utkast	C. Thingvold	Sigve Oltedal

Innholdsfortegnelse

1 Bakgrunn

Safetec har på oppdrag for NVE utarbeidet en samling med øvingsscenarier for IT- og OT-hendelser i kraftsektoren. Dette dokumentet beskriver forhold som er relevante for øvelsene og planlegging av dem, samt veiledning til gjennomføring av øvelsene. Dokumentet inkluderer kartlegging av relevante krav med hensyn på øvingsaktiviteten, overordnede systembeskrivelser av typiske nettverk og IKT-tjenester, roller og ansvar med betydning for hendelseshåndtering og beredskapsarbeid, samt oversikt over scenariene og veiledninger for bruken av disse.

Offentlig tilgjengelige data har blitt brukt for å si noe om potensielle hendelser, typiske sårbarheter og eventuelle læringsbehov. Læringsbehovene har i det videre arbeidet blitt innarbeidet i øvingsmålene for de forskjellige øvelsene.

De utarbeidede scenariene (se oversikt i avsnitt 8.3) er avklart med NVE i arbeidsmøter og retter seg mot små virksomheter med lav modenhet i det digitale beredskapsarbeidet, så vel som litt større virksomheter eller virksomheter med et noe høyere modenhetsnivå. Øvelsene retter seg ikke i utgangspunktet mot virksomheter som har avansert kapasitet og høy digital beredskapsevne.

2 Begreper

Angrepsflate
: De delene av et system en angriper kan utnytte for å komme seg inn i systemet

KBO-enheter
: Alle virksomheter som eier eller driver anlegg med vesentlig betydning for driften av hele den norske kraftforsyningen

AMS
: Avansert måle- og styringssystemer, dette er de såkalte «smarte strømmålerne».

IT
: Informasjonsteknologi

IKT
: Informasjons- og kommunikasjonsteknologi

OT
: Operasjonell teknologi, dette er typisk driftkontrollsystemer.

IoT
: «Internet of Things», dette er enheter som gjerne har sensorer og/eller styring av fysiske objekter, som sender og/eller mottar data fra typisk skyløsninger

ERP
: «Enterprise resource planning»-systemer, dette er typisk et system som forenkler oppgaver for økonomistyring, HR, prosjekt-ledelse, Lønn, osv.

Flerfaktor
: I konteksten av disse øvelsene refererer flerfaktor typisk til autentiseringsløsninger (innlogging), der en ikke har kun ett passord som kontroll, men flere faktorer.
Et eksempel er et passord (noe du vet) og en app på telefonen (noe du har).

PLS
: Programerbar logisk styring, enheter som eksisterer i OT-miljøet, som direkte styrer fysiske systemer.

SIEM
: «Security information and event management”, er typisk en del av styringssystemet, men med spesifikke fokus på cybersikkerhets-aspekter.

SOC-tjenester
: «Security operations center»-tjenester som kan ta imot blant annet logger fra nettverk, og gjør overvåking for å oppdage uønskede hendelser.

Skytjenester
: Tjenester som typisk driftes av en tredjepart, i ett eller flere datasenter (SaaS).

3 Relevante krav fra regelverk

Kraftberedskapsforskriften stiller krav til virksomheter i kraftforsyningen om å opprettholde god beredskap. Kravet innebærer at det skal gjennomføres øvelser, også for digitale hendelser. Det er også foreslått i høringsutkast til Digitalsikkerhetsforskriften at Digitalsikkerhetsloven skal være gjeldende også for KBO-enheter. Kravene der er i hovedsak i overensstemmelse med eksisterende krav i Kraftberedskapsforskriften.

Forskriften stiller krav til at KBO-enheter har etablert et planverk, og at planverket øves jevnlig. Planverket skal være tilpasset virksomhetene, hvilket betyr at detaljeringsgrad vil variere mellom virksomhetene.

Ved alvorlige hendelser er virksomhetene pålagt å varsle beredskapsmyndigheten. Forsøk på inntrengning i driftskontrollsystemer eller AMS-systemer er rapporteringspliktige. Det samme gjelder kompromittert konfidensialitet for kraftsensitiv informasjon.

Det er krav til at virksomhetene har en flerårig øvingsplan, og at det gjennomføres minst én øvelse hvert år. Det er ikke krav om at øvelsen spesifikt skal gjelde digitale angrep eller hendelser, men slike hendelser er innenfor rammene av hva det skal øves på. Det synes fornuftig å legge opp til minst én digital øvelse hvert år, der omfanget av denne kan varieres fra år til år. Det er også mulig å ta inn digitale komponenter i en øvelse med et annet fokus, for eksempel driftsforstyrrelse eller utilgjengelighet av digitale systemer under håndtering av en annen ekstraordinær situasjon, for eksempel grunnet ekstremvær.

Beredskapsmyndigheten fungerer som sektorvis responsmiljø for IKT-hendelser i kraftsektoren.

Kapittel 6 i kraftberedskapsforskriften stiller krav til informasjonssikkerhet. Her er det også inkludert krav til responsevne for uønskede hendelser i digitale systemer. Tilsvarende er det i kapittel 7 krav til evne til å kunne håndtere sikkerhetsbrudd i driftskontrollsystemer.

De nevnte kravene legges til grunn ved planlegging av øvingsscenariene, og gir grunnlag for fordeling mellom scenarier tilpasset forskjellige virksomhetsstørrelser og modenhet i digital beredskapsevne.

4 Trusselbildet for kraftsektoren

Øvingsscenariene er utarbeidet for å være relevante og realistiske med hensyn på det eksisterende trusselbildet. I det følgende gis derfor en overordnet beskrivelse av de viktigste aspektene ved trusselbildet for kraftsektoren. Trusselbildet er i stor grad preget av geopolitiske trekk som høyt spenningsnivå mellom Russland og vesten/NATO. Kort oppsummert legges følgende til grunn om trusselaktører og forventede handlemåter:

- Etterretningstrusselen fra Russland er høy. Det er sannsynlig at statlige aktører vil benytte dataangrep både mot IKT-systemer og driftskontrollsystemer. Hensikten kan eksempelvis være spionasje for å skaffe tilgang på kraftsensitiv informasjon og kartlegge kritisk infrastruktur. Det er også sannsynlig at russiske trusselaktører har interesse av å skaffe seg vedvarende tilgang i driftskontrollsystemer for å eventuelt kunne utføre koordinerte dataangrep mot kraftforsyningen som kan medføre strømbrudd ved et ytterligere tilspisset konfliktnivå.
- Spionasje mot kraftsektoren fra andre statelig aktører kan ikke utelukkes. Dette vil mest sannsynlig omhandle kraftsensitiv informasjon, inkludert informasjon om kraftmarkedet, i tillegg til kartlegging av kritisk infrastruktur.
- Det er en høy trussel fra nettbasert kriminalitet. Dette rammer samfunnet generelt og er dominert av løsepengevirus og kompromittering av brukerkontoer for videresalg.
- Hacktivisme kan ikke utelukkes. Det er sannsynlig at trusselaktører med sympatier for Russland kan utføre tjenestenektangrep mot nettsider og offentlig tilgjengelig tjenester for å skape uro i befolkningen og redusere tiltroen til norsk infrastruktur og evne til å beskytte samfunnskritiske funksjoner.

Denne oppsummeringen er basert på myndighetenes åpne trusselvurderinger[1,2,3] og vurderinger fra KraftCERT[4].

[1] https://www.pst.no/globalassets/2024/nasjonal-trusselvurdering-2024/nasjonal-trusselvurdering-2024_uuweb.pdf
[2] https://www.etterretningstjenesten.no/publikasjoner/fokus
[3] https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2024
[4] https://www.kraftcert.no/filer/KraftCERT-Trusselvurdering2024.pdf

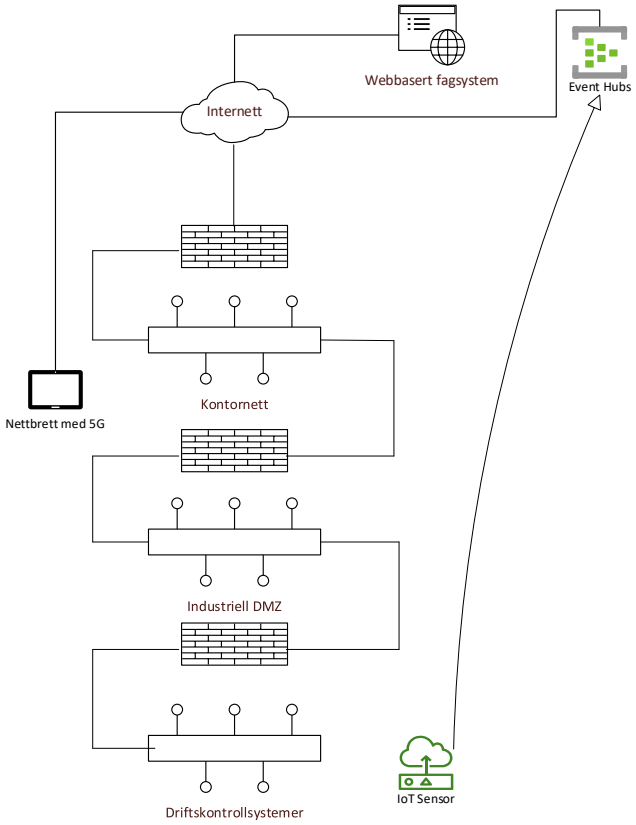
5 Relevante systembeskrivelser

I dette kapittelet gis en overordnet beskrivelse av den typiske tekniske angrepsflaten (de delene av et system en angriper kan utnytte for å komme seg inn i systemet) for IT- og OT-systemer i kraftsektoren. Hensikten med dette er å gi et overordnet bilde av hvilken type systemer som typisk er i bruk, og hvordan disse kan rammes under cyberhendelser.

5.1 Overordnet nettverksbeskrivelse

De fleste virksomheter har IT- og OT-systemer som grovt sett kan ses på som 4 miljøer:

1. Skytjenester: dette inkluderer programvare levert over nett (SaaS – software as a service-løsninger) som Microsoft 365-tjenester og webbaserte fagsystemer, så vel som infrastrukturtjenester som Microsoft Azure eller Amazon Web Services.
2. Lokale IKT-tjenester: dette er de lokale nettverkene til virksomheten som brukes til IKT-tjenester. Dette inkluderer klienter (for eksempel arbeidsstasjoner og bærbare PC-er for ansatte, eller mobiltelefoner og nettbrett), nettverksutstyr og servere. Private skyløsninger driftet av selskapet selv i eget datasenter vurderes å tilhøre denne kategorien.
3. OT-systemer: dette er nettverksbaserte tjenester som inngår i driftskontrollsystemer eller som på annen måte understøtter drift av kraftsystemene, og som er adskilt fra IKT-tjenestene.
4. IoT-tjenester: dette er fysiske systemer som har direkte kommunikasjon mot internett, og typisk består av sensorer, nettverkstilkobling og et analyselag, som typisk ligger i et skymiljø.



Figur 1: Konseptuell figur som viser typiske nettverkslag hos et kraftselskap

5.2 Forretningssystemer

Forretningssystemer kan både være driftet som lokale IKT-tjenester og som skytjenester, eventuelt som en hybridløsning. Dette kan være ERP-systemer, regnskapssystemer, analysesystemer eller andre fagløsninger som brukes til å utføre bestemte oppgaver innen virksomhetsstyring eller virksomhetens forretningsprosesser.

Slike systemer vil normalt sett:

- Ha en ekstern leverandør som også yter driftsstøtte og brukerstøtte
- Ha lokal eller sentralisert pålogging og tilgangsstyring. Ofte vil slike applikasjoner være integrert med Active Directory eller Entra ID for dette, men de kan også ha lokale brukere. Systemene bør støtte flerfaktorautentisering, men det finnes også mange eksempler der dette ikke er støttet, eller der virksomhetene ikke har valgt å ta dette i bruk..
- Systemene kan ha varierende grad av logging og integrasjon med systemer for sikkerhetsovervåkning.
- Systemene vil typisk ha velfungerende løsninger for sikkerhetskopiering og gjenoppretting, ofte støttet av leverandøren.

5.3 Vanlige kontorstøttesystemer og kommunikasjonssystemer

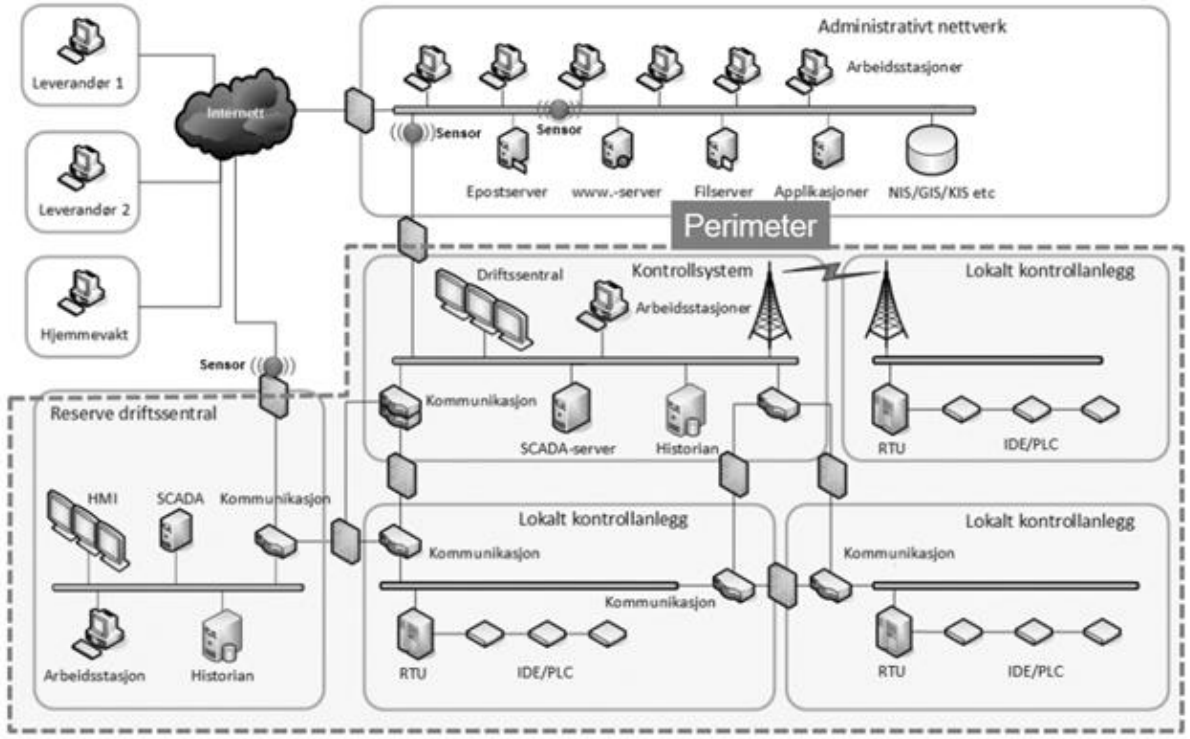
De fleste kraftselskaper benytter skybaserte kontorstøtteverktøy og kommunikasjonssystemer. Microsoft 365 eller Office 365-baserte løsninger er vanlige, med tilgang til skylagring, men også med lokale applikasjoner som kjører på Windows PC-er.

De fleste virksomheter i dag bruker Exchange Online for e-post. De vanligste samhandlingsplattformene er Microsoft Teams, og Slack/Zoom i mer tekniske miljøer som for eksempel utviklingsavdelinger.

Øvelsene vil ta utgangspunkt i Microsoft-produkter fordi disse er dominerende, men konseptene kan brukes tilsvarende på andre plattformer.

5.4 Driftskontrollsystemer

Driftskontrollsystemene er de systemene som brukes til å drifte kraftproduksjon og nettanlegg. Disse systemene består av vanlige IKT-komponenter som servere, nettverkskomponenter som svitsjer og brannmurer, men også av spesialiserte OT-komponenter som PLSer (programmerbar logisk styring) og sikkerhetskritiske systemer som skal stoppe ulykkeshendelser.



Figur 2: Figur hentet fra NVEs veiledning til Kraftberedskapsforskriften[5]

[5] Kraftberedskapsforskriften: Kapittel 7: Beskyttelse av driftskontrollsystem (nve.no)

5.5 Driftskritiske eksterne IKT- og OT-tjenester

De fleste virksomheter i dag har IKT-systemer som er nødvendige for beslutningsstøtte og samhandling. Bortfall av disse systemene kan skape et beslutningsvakuum uten at det direkte setter kraftproduksjonen i fare. Dette kan for eksempel være:

- Sensorbaserte systemer for miljøovervåkning
- Sikkerhetsovervåkning for IKT (SIEM, SOC-tjenester)
- Kommersielle analysesystemer

Slike systemer vil typisk være skybaserte, eller hybridløsninger som delvis er lokalt driftet og delvis tilgjengelig via en skyløsning. Det er også vanlig at disse systemene brukes av tredjeparter som del av en tjenesteleveranse. Forstyrrelse av slike systemer kan gå ut over leverandørenes evne til å levere tjenester, hvilket vil være driftskritisk over tid.

6 Relevante sårbarheter og hendelsestyper

Dette kapittelet omhandler de potensielle sårbarhetene og truslene som kraftsektoren står overfor. Det er avgjørende å forstå disse aspektene for å kunne planlegge og gjennomføre effektive øvelser. Ved å identifisere de mest kritiske elementene og truslene, kan øvelsene forberede kraftsektoren på ulike scenarioer som kan påvirke driften av vitale systemer. Forberedelser bidrar til å sikre kontinuitet, redusere risikoen for alvorlige hendelser, og fremme en robust og motstandsdyktig infrastruktur. Øvelser som er basert på en solid forståelse av trusselbildet og sårbarhetene vil være mer realistiske og nyttige, noe som igjen styrker sikkerheten og beredskapen i kraftsektoren.

Sårbarheter (Safetecs oppsummering av funn fra Riksrevisjonens rapport etter tilsyn med NVE's arbeid med IKT-sikkerhet i 2020-2021[6])	
Få ansatte med IKT-sikkerhetskompetanse	Innebærer sårbarhet ved fravær og uforutsette hendelser
Selskapenes evne til å oppdage IKT-hendelser	Mange selskaper mangler kriterier for varsling av hendelser, og det har vært uklart hvilke type IKT-hendelser de skal varsle om til NVE og KraftCERT.
Uklare varslingsrutiner	Det er avdekket svakheter i systemene selskapene har for å overvåke og logge IKT-sikkerhetshendelser.
Svak kultur for å varsle	Undersøkelsen viser at selskapene gjerne avventer å varsle om hendelser fordi de ønsker å løse problemet internt før de deler informasjonen med andre. Dersom selskapene klarer å få situasjonen under kontroll, er det heller ikke sikkert at de rapporterer om hendelsen i ettertid.
Læringsbehov	
En erfaring er at risikoanalysene bidrar til å få et overordnet blikk, men de spesifikke problemstillingene for IKT-sikkerhet får man ikke like godt fram via analysene. Mange har fokus på å gjennomføre risikoanalyse, men det er vel så viktig å bruke den også som grunnlag for å lage en beredskapsplan	

[6] Dokument 3:7 (2020−2021) (riksrevisjonen.no)

7 Beredskapsorganisasjonen

Beredskapsorganisasjonen vil se forskjellig ut i forskjellige virksomheter. Dette gjelder både størrelse, rapporteringslinjer og benevnelser på roller. I utforming av øvelsen har vi lagt til grunn følgende om beredskapsorganisasjonen.

- **Beredskapssjef:** det finnes en beredskapssjef som har overordnet ansvar for planverk, øving og styringssystem. Vedkommende kan være del av operativ beredskapsorgansasjon, men kan også være en mer overordnet rolle.
- **Innsatsleder**: dette er personen som leder den operative delen av hendelseshåndteringen. Vedkommende er ansvarlig for ledelse under hendelseshåndteringen og har et begrenset mandat til å ta beslutninger. Vedkommende rapporterer til beredskapssjef og selskapsledelsen (daglig leder).
- **Loggfører**: en person har rollen som loggfører og skal sikre at all relevant informasjon logges, og at innsatsledelsen og bidragsytere har god nok situasjonsforståelse underveis i håndteringsarbeidet.
- **Tekniske eksperter:** personell med dybdekompetanse på tekniske systemer eller utførelse av tekniske oppgaver, som digital etterforskning, isolering av systemer og annet. Vedkommende har oppgaveansvar og rapporterer til innsatsleder.
- **Eksterne bidragsytere**: det kan være konsulenter og andre som bistår i innsatsen. De kan inkluderes i øvelser ved samøving, eller ved at en representant fra spillstab tar denne rollen i spilløvelser.
- **Kommunikasjon**: En person som er ansvarlig for å planlegge og gjennomføre kommunikasjon i henhold til planlagte tilganger, kanaler og interessentbehov.

8 Scenarier

Det er utviklet 20 øvingsscenarier for cyberangrep tilpasset kraftselskaper og nettoperatører.

Scenariene er utviklet i samarbeid med NVE. Scenariene skal være realistiske og dekke hendelser både innen IT- og OT-systemer. Øvelsene skal dekke et bredt spekter av mulige øvingsmål, og passe for både mindre modne og mer modne virksomheter når det gjelder beredskap for cyberhendelser.

Scenariene er tilpasset to forskjellige øvingsformer: diskusjonsøvelse og spilløvelse.

8.1 Utvalg av scenarier

Scenariene er valgt for å gi bredde i tilgjengelige øvinger, og kunne passe både for virksomheter som har lite erfaring med øvingsvirksomhet, og mer modne virksomheter som ønsker større utfordringer.

Øvingene er basert på det rådende trusselbildet for kraftsektoren og inneholder scenarier som regnes som realistiske ut fra kjent tilstand på sikkerhetsnivå i bransjen og kjente handlemåter fra trusselaktører vi kan forvente utfører angrep mot virksomhetene. Scenariene er tilpasset at sammensatt trusselbilde der angrep både fra statlige aktører med betydelige kapasiteter og kriminelle som først og fremst søker økonomisk vinning, kan forventes.

Øvelsene er fordelt mellom scenarier som påvirker operasjonell teknologi (OT), og informasjonsteknologi (IT). I tillegg er det tatt med ett enkeltscenario med spesifikt fokus på skytjenester, og ett scenario som omhandler IoT-teknologi.

8.2 Øvingsformer

Det er mulig å utføre øvelser på forskjellige nivåer og med forskjellige grad av forberedelse og tid til gjennomføring. Direktoratet for samfunnssikkerhet og beredskap (DSB) har utviklet veiledere for gjennomføring av beredskapsøvelser. Disse bruker følgende øvingsformer:

- Funksjonsøvelser
- Diskusjonsøvelser (også kjent som refleksjonsøvelser)
- Spilløvelser
- Fullskalaøvelser

Funksjonsøvelser fokuserer på spesifikke funksjoner eller prosesser innen en organisasjon, og involverer roller og ansvar som utfører sine oppgaver i en simulert hendelse. Disse øvelsene tar for seg konkrete oppgaver og tester de tekniske og operative aspektene ved responsen.

Diskusjonsøvelser, også kjent som refleksjonsøvelser, innebærer at deltakerne diskuterer og reflekterer over scenarier og mulige løsninger. Disse øvelsene legger vekt på diskusjon og samarbeid for å avdekke utfordringer og muligheter til forbedring uten å gjennomføre praktiske handlinger.

Spilløvelser simulerer hendelser der deltakerne tar beslutninger og utfører aktiviteter i en oppdiktet, men realistisk situasjon. Disse øvelsene gir en dynamisk og interaktiv form for trening der beslutningstaking og koordinering er sentrale elementer.

Fullskalaøvelser er de mest omfattende og realistiske øvelsene, der både interne og eksterne ressurser mobiliseres for å håndtere en simulert krisesituasjon. Disse øvelsene tester hele organisasjonens beredskap og evne til å respondere på en krise på alle nivåer.

For mer detaljert innføring om øvingsformer på generelt grunnlag, vises det til DSB's veiledere som er tilgjengelig på internett[7].

[7] Veileder i planlegging, gjennomføring og evaluering av øvelser - grunnbok | Direktoratet for samfunnssikkerhet og beredskap

8.3 Øvingscenarier

Følgende øvingsscenarier er utviklet:

ID	Tittel	Domene	Øvingsform
1	Dataangrep på automasjonssystem	OT	Spill
2	Avansert vedvarende trussel (APT)	OT	Diskusjon
3	Brudd på integritet i sanntidsdata	OT	Diskusjon
4	Fjernaksesskompromittering	OT	Spill
5	Forsyningskjedeangrep	OT	Spill
6	Kritisk systemnedetid	OT	Diskusjon
7	Løsepengevirus	OT	Spill
8	Feil i segmentering av nettverk	OT	Spill
9	Teknologisk innovasjon	OT	Diskusjon
10	Utnyttelse av nulldagssårbarhet	OT	Diskusjon
11	Angrep på mobilapplikasjoner	IT	Spill
12	Konfigurasjonsfeil på brannmur	IT	Diskusjon
13	Brudd på autentiseringsmekanismer	IT	Spill
14	Brudd på personvern	IT	Diskusjon
15	DDoS-angrep	IT	Spill
16	Man-in-the-Middle-angrep	IT	Diskusjon
17	Sosial manipulasjon	IT	Diskusjon
18	Tyveri av legitimasjon	IT	Spill
19	Kompromittering av skytjeneste	Sky	Diskusjon
20	IoT-angrep	IoT	Spill

I tillegg til disse øvelsene har vi inkludert beskrivelse av hvordan flere av scenariene kan settes sammen til en Fullskalaøvelse (se seksjon 8.7).

Se vedlegg A for en beskrivelse av hvert scenario.
Resten av øvingsmaterialet for hvert scenario er tilgjengelig på NVE sine nettsider.

8.4 Struktur på øvingsmaterialer

Øvingsmaterialene består av 2-3 støtte-dokumenter for hvert øvingsscenario.

8.5 Direktiv

Alle scenariene er beskrevet i et direktiv på ca. 1 A4-side. Direktivet skal hjelpe virksomheten i valg av øvingsscenarier, og forberedelse til øvelsen. Direktivet inneholder:

- Øvingsform:
  - Spilløvelse
  - Diskusjonsøvelse
- Modenhetskrav:
  - lav modenhet kan brukes av alle virksomheter
  - middels modenhet er øvelser som gir mer utbytte for virksomheter med noe erfaring med eget planverk og øving)
- Forventet tidsbruk:
  En indikasjon på hvor mye tid gjennomføring antas å ta. Dette vil variere fra virksomhet til virksomhet, både etter hvor dypt man går inn i problemstillingene og hvor mye erfaring man har med øving og hendelseshåndtering.
- Beskrivelse av scenario:
  En overordnet beskrivelse av scenariet.
- Egnede øvingsmål:
  Forslag til øvingsmål som scenariet passer til. Virksomheten kan ha andre mål enn dette.
- Egnede roller for øvende:
  Roller som anses som hensiktsmessige deltar som øvende.
- Roller i spillstab:
  Kun aktuelt for spilløvelser. Roller som spillstaben må forventes å dekke.
- Øvingsmomenter:
  En kort oppsummering av innspill og hendelser i scenariet.

8.5.1 Dreiebok (kun spilløvelser)

Dreieboken inneholder to tidslinjer. Denne er tiltenkt brukt i forberedelse og som støtte til spillstab i spilløvelser.

- Tidslinje 1: Tidslinje – hendelser. Dette er en oversikt over det simulerte dataangrepet sett fra trusselaktørens ståsted. Dette inneholder tidspunkt, beskrivelse av hendelsen, forventede spor som ville finnes i et teknisk system, og kommentarer til øvingsleder.
- Tidslinje 2: Dreiebok: dette er en kortfattet oversikt over innspillene som sendes fra spillstab til de øvende i spilløvelsen. Dette inneholder tidspunkt (kan fravikes, men er samordnet med tidslinjen), beskrivelse av innspillet, en kommentar til øvingsleder om forventet respons eller annen nyttig informasjon, hvem som er den simulerte avsenderen, hvem som er mottakeren, og hvlken kanal som er planlagt for innspillet.

Øvingsleder og spillstab bør før øvelsens start være godt kjent med dreieboken og tidslinjen. Spillstaben må forvente å svare på forespørsler fra de spillende på en hensiktsmessig måte, for eksempel med tanke på kjent informasjon om hendelsene til IT-avdelingen, vurdering av personvernpåvirkning og liknende. Da må spillstaben kunne svare ut dette på en måte som er konsistent med scenariet.

8.5.2 PowerPoint-presentasjon:

Den siste delen av støttematerialet gis i form av en PowerPoint. Denne har en felles del for både diskusjons- og spilløvelser med en introduksjon til øvelsen. Dette er beregnet presentert til de øvende i starten av øvelsen. Deretter skiller man mellom spilløvelser og diskusjonsøvelser.

- Diskusjonsøvelser: PowerPoint-slides inneholder spørsmål til diskusjon, og hint for å styre diskusjonen videre. Spørsmålene kan vises til de øvende underveis. Om øvingsleder ønsker å vise hintene i presentasjonen eller kun bruke disse muntlig er opp til øvingsleder. Om man ikke ønsker å vise hintene, kan aktuelle lysbilder skjules i PowerPoint før øvelsen.
- Spilløvelser: PowerPoint-slides inneholder maler med tekst til innspill på e-post, chat og liknende, eller manus for telefonbeskjeder. Disse brukes av spillstaben til å sende forberedte innspill.
- I noen av øvelsene (hovedsakelig diskusjonsøvelser) ligger det også hint i «Speaker-notes», disse er ment som ytterligere tips til øvingsleder for innspill som kan gis for å drive diskusjonen.
  Noen av disse har «alternative spørsmål» basert på hva spillerne har svart på det som står på sliden.

8.6 Tilpasning av øvingsscenarier til den enkelte virksomhet

Øvingsscenariene er beskrevet for fiktive systemer. De fleste deltakere i øvelser vil oppleve større øvingsutbytte dersom øvingsscenariene ligger tett opp mot systemene de jobber med til daglig. Det kan derfor være behov for å tilpasse øvelsene til egen organisasjonsstruktur, teknisk infrastruktur eller relevante leverandører.

Tilpasning av øvelser til den virkelige hverdagen til deltakerne øker realismen og relevansen, noe som resulterer i bedre læring og beredskap. Nedenfor gir vi råd til øvingsleder om aspekter som kan vurderes for god tilpasning.

8.6.1 Før øvelsen

- Tilpass materialet til din virksomhet og ønsket øvingsmåte: Kartlegg virksomhetens spesifikke behov, risikoer og teknologier. Juster scenarioene slik at de reflekterer realistiske utfordringer virksomheten kan møte.
    - Anse de vedlagte PowerPoint-presentasjonene for scenarioene som veiledere for hvordan scenarioet kan gjøres.
    - Det kan være hensiktsmessig å endre språket i innspillene slik at det ligner mer det som ville vært realistisk i din virksomhet.
    - Det kan også være hensiktsmessig å bytte ut skjermbilder med bilder som er fra virksomhetens systemer og infrastruktur, for å gjøre det mer realistisk, og ikke så generelt.
- Identifiser de viktigste interessentene tidlig, da det ofte er utfordrende å finne tid der alle nødvendige ressurser er tilgjengelige.
    - Sørg for å ha forankring i ledelsen og blant andre ledere for øvelsen, så det er tydelig at øvelsen er en prioritet.
- Skriv ut materiell som er nyttig for de øvende under øvelsen: Inkluder nettverkstopologier, diagrammer, og scenariobeskrivelser fra PowerPoint-presentasjonen.
- Eventuelle innspill, hint eller annet som spillerne skal få under øvelsen: Forbered innspill og hint basert på virksomhetens reelle operasjonelle miljø og trusler.
- Dreiebok for øvingsleders forberedelsesarbeid: Bruk dreieboken til å planlegge øvelsen, men vis den ikke til de øvende før eller under øvelsen.
- Samle kontaktinformasjon: Skaff alle nødvendige e-post-adresser og telefonnumre for gjennomføring av øvelsen.
- Forbered e-poster og telefoner: Ha alt kommunikasjonsutstyr klart, inkludert forhånds-skrevet kommunikasjon som kan brukes under øvelsen.
- Dersom virksomheten normalt bruker programvare til å støtte håndtering av alvorlige hendelser, bør man vurdere om denne skal brukes også i øvelsen.
- Det er viktig å gjøre deltakerne kjent med spillereglene (avsnitt 8.6.3), samt å informere alle som kan bli berørt av øvelsen om at det er planlagt en øvelse.
- For virksomheter med begrenset øvingskompetanse eller kapasitet til å planlegge øvelsene, kan det være hensiktsmessig å engasjere en erfaren øvingsleder fra et eksternt selskap til å bistå i planlegging og gjennomføring.

8.6.2 Under øvelsen

- Start med en runde rundt bordet:
  - Etter at scenariet er beskrevet, gå rundt bordet og be deltakerne dele sine umiddelbare tanker. Dette bidrar til å oppklare usikkerheter.
- Teknisk forklaring: Be en teknisk ressurs blant de øvende om å forklare tekniske aspekter og status ved start av øvelsen.
- Bruk av hint: Bruk hint fra PowerPoint hvis samtalen stopper opp, men hopp over dem hvis øvelsen flyter godt.
- Rolle til innsatsleder: Hjelp innsatslederen med å ta styring på diskusjoner og beslutninger for å sikre realistisk ledelsestrening.

8.6.3 Spilleregler

Det er hensiktsmessig å avtale spilleregler i starten av en øvelse. Følgende regler er ofte brukt, og bidrar til å unngå misforståelser.

- Kommunikasjonsprotokoll: Start alle meldinger/telefoner/e-post med «ØVELSE ØVELSE» for å tydeliggjøre at det er en øvelse.
- Timeouts underveis er lov.
- NO-PLAY brukes for å avbryte øvelsen hvis en reell hendelse oppstår. Øvingsleder beslutter håndtering av NO-PLAY, om øvelsen avbrytes som helhet eller om det gjøres tilpasninger.

8.6.4 Tilpasning til virksomhetens trusselbilde

Tilpasning til virksomhetens trusselbilde kan bidra til å øke beredskapsevnen der det trengs mest:

- Analyser og integrer nylige sikkerhetshendelser spesifikke for selskapet i øvelsesscenarioene for å reflektere aktuelle trusler.
- Involver avdelinger som ofte står overfor spesifikke trusler, slik som IT-sikkerhet, drift og kundeinformasjon, for en mer målrettet øvelse. Bruk gjerne innspill fra interne interessenter i utvalg og planlegging av øvelsen.

8.6.5 Struktur på øvingsmateriale

- Bruk diagrammer og nettverkstopologier som reflekterer virksomhetens faktiske infrastruktur.
- Inkluder trinnvise scenariobeskrivelser som kan tilpasses ulike avdelinger innen virksomheten, for å sikre at øvelsen er relevant for alle deltagere.

8.7 Fullskalaøvelse

Det kan også lages en mer omfattende øvelse, ved å sette sammen flere av scenariene til en større øvelse. En større øvelse kan egne seg å gjennomføre også med reell infrastruktur. Dette kan gjøres på forskjellige nivåer:

- Simulering av deler av infrastrukturen, for eksempel med bruk av en virtuell maskin (VM) som en server det skal utføres analyse av
- En mer komplett simulering av infrastrukturen med nettverk, OT-komponenter o.l, enten i et virtuelt miljø eller et fysisk labmiljø. Simulatorer kan brukes til å simulere respons fra fysiske systemer.
- Øving på reell infrastruktur med tydelige rammer for tillatte handlinger.

Øvelsen kan utvides med at det genereres logiske bevis gjennom simulerte angrep, som deretter skal granskes og håndteres. Det er også mulig å sette opp en “cyber range”-øvelse med “live fire”-elementer, hvor et lag utfører angrep, og forsvarere skal i sanntid håndtere hendelsen. Dette blir den mest realistiske øvingen, men krever også betydelige ressurser for gjennomføring. Slike store øvelser egner seg godt for samarbeid mellom flere virksomheter.

Under er et forslag på hvordan en begrenset fullskalaøvelse kan se ut, for en generell virksomhet. For at det skal fungere godt, og gi godt utbytte vil det være en fordel å tilpasse scenariet til din virksomhet. Slik at dere kan øve på de systemene og prosedyrene som gjelder hos dere.

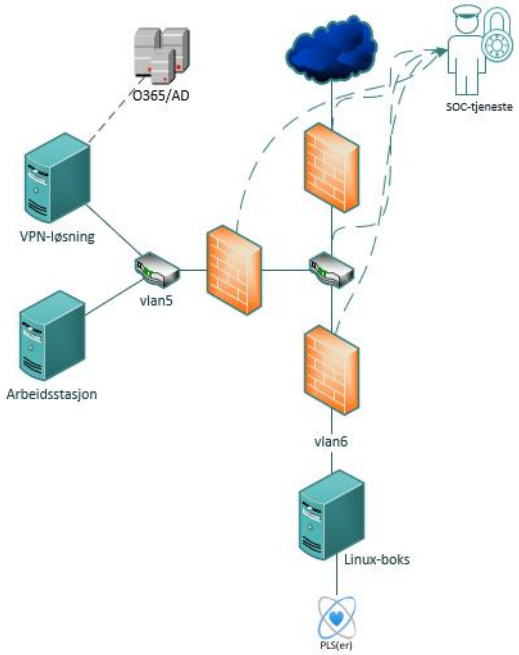
8.7.1 Medvirkende i øvelsen

- **Øvingsstab**
- **Rødt lag**
  I øvelsen vil disse være angriperne, som gjennomfører handlingene dere skal øve på å unngå/rydde opp i.
- **Beredskapsledelse**
  Beredskapsledelsen må være med, og består typisk av de rollene som er beskrevet i spill/diskusjons-scenariene.
- **Blått lag**
  Det blå laget er alle andre som skal øve på å respondere på en hendelse, som i spill- og diskusjonsøvelsene blir representert gjennom øvingsstaben.
  Det er de som skal gjennomføre teknisk respons i øvelsen.

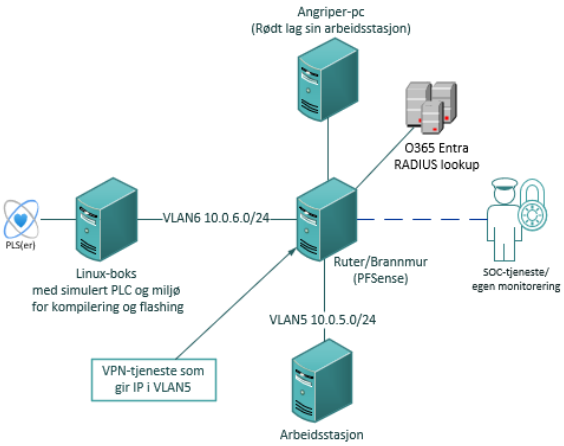
8.7.2 Overordnet scenario-eksempel

- Spearphising mot en ansatt har ført til et kontoinnbrudd i Office365.
- VPN-løsning i IT-nett, bruker samme brukerdatabase, men ikke 2FA.
- Trusselaktøren bruker VPN-løsning, og åpner en RDP-kobling til Hans Petrus arbeidsstasjon i IT-nettet.
- Det er en feilkonfigurasjon i interne brannmurer som tillater all SSH-trafikk fra IT-nett til OT-nett.
- Trusselaktøren kjører nmap og finner port 22 på en adresse i OT-nett.
- På ingeniørens arbeidsstasjon ligger det ssh-nøkler uten passhphrase, trusselaktøren bruker disse for å koble til maskinen i OT-nettet.
- Trusselaktøren laster ned ny firmware til ingeniørens arbeidsstasjon.
- Trusselaktøren kopierer fra ingeniørens arbeidsstasjon til linux-server i OT-nett med scp/rsync.
- Trusselaktøren flasher ny firmware til embedded-system fra linux-boks i OT-nett.
- Det blir mørkt.

8.7.3 Infrastruktur



Figur 3 Simulert nettverksarkitektur



Figur 4 Eksempel på fysisk oppsett

I Figur 4 er det et eksempel på en fysisk arkitektur som kan brukes for å simulere et miljø som ligner på Figur 3. Dette kan gjøres med VM-er, kontainere, eller fysiske maskiner. Nettverksarkitekturen i Figur 3. er en enkel variant av det som finnes i mange virksomheter, men det beste vil alltid være å sette opp et miljø med en arkitektur som ligner på den reelle arkitekturen i din virksomhet.

Uansett om en velger å sette opp dette miljøet i sky, vm-er eller fysiske maskiner. Vil det kreve en del konfigurasjon og planlegging. Brannmurene kan simuleres med en enkelt vm/ruter som støtter VLANS og brannmurregler, f.eks. pfsense. Her kan en også sette opp VPN-løsning med bruker-lookup via for eksempel RADIUS mot Active Directory/Entra ID.

Det bør lages en ny konto i AD/Entra for ingeniøren som blir spearphishet, som tydelig er del av øvelsen. Eventuelt kan det settes opp et nytt minimalt miljø for AD/Entra ID også. I så fall kan det settes opp flere brukere, uten at det er tydelig hvilken som er kompromittert.

Ved gjennomføring av en “live fire”-øvelse bør det være mulig å bruke eksisterende planverk og playbooks for håndtering av hendelsene. Det er hensiktsmessig å bruke tilsvarende teknologier for sikring som man har i sine reelle nettverk, for eksempel EDR-løsninger, SIEM, SOAR-verktøy og andre operasjonelle løsninger.

For beslutningslaget vil det her også være hensiktsmessig å bruke de systemene man vanligvis gjør under hendelseshåndtering, for eksempel programvare til støtte i krisehåndtering.

9 Evaluering

Evaluering av øvelser er hensiktsmessig for å få så godt utbytte som mulig.

Planlegging av evaluering bør starte samtidig som planlegging av øvelsen. Ta utgangspunkt i foreslåtte læringsmål, og mens øvelsen tilpasses, tilpass også læringsmål ut ifra behovene i din virksomhet.

9.1 SMART-mål

Det kan være nyttig å sette SMART-mål for evalueringen av en øvelse. SMART står for Spesifikke, Målbare, Oppnåelige, Relevante og Tidsbundne mål. Slike mål kan tilpasses fra de foreslåtte læringsmålene for øvelsen. Spesifikke mål bør være tydelige og konkrete, beskrive hva som forventes, og hvem som er involvert.

Målbare: mål bør kunne vurderes med indikatorer eller måleenheter.
Oppnåelige: mål bør være realistiske innenfor øvelsens rammer og tilgjengelige ressurser.
Relevante: mål bør knyttes direkte til øvelsens overordnede mål og virksomhetens behov.
Tidsbundne: mål bør ha klare tidsrammer for når de skal nås.

Å bruke SMART-rammeverket hjelper med å strukturere og fokusere evalueringen, slik at styrker og forbedringsområder lettere kan identifiseres. Det kan gjerne tas utgangspunkt i de øvingsmålene som står i direktivet, men de kan tilpasses til virksomheten som et SMART-mål.

9.2 Gjennomføring av evaluering

I et referat fra evaluering, kan det være lurt å kort oppsummere scenariet, hensikt og mål for øvelsen. Dette kan godt forberedes på forhånd eller gjøres i ettertid, det trenger ikke å være en del av evaluerings-sesjonen.

Når gjennomføringen av øvelsen er ferdig, er det gjerne hensiktsmessig å ta en evaluerings-runde med spillerne, og spillstaben, ganske kort tid etter. Målet her er å få frem refleksjoner, både for gjennomføringen av øvelsen, men hovedsakelig for tiltak virksomheten kan gjøre for å forbedre seg mot læringsmålene.

9.2.1 Runde rundt bordet

Alle de involverte i øvelsen må få muligheten til å fortelle om sine erfaringer og observasjoner før og under øvelsen. Under er noen spørsmål alle deltakerne bør få mulighet til å dele sine refleksjoner og observasjoner rundt.

- Hva forventet vi skulle skje?
- Hva fungerte godt, og hvorfor?
- Hvilke utfordringer møtte vi på?
- Hva kan forbedres, og hvordan?

9.2.2 Generelle diskusjonspunkter for øvelsene

Under er en del spørsmål som kan være relevante for flere av scenariene, disse kan brukes for å trigge flere refleksjoner rundt spesifikke aspekter av læringsmålene og øvelsene.

- Hvordan kunne dette angrepet vært forhindret?
- Diskuter mulige forebyggende tiltak som bedre autentisering, strengere tilgangskontroll, og regelmessige sikkerhetsrevisjoner hos leverandøren.
- Hvilke sikkerhetstiltak kan implementeres for å beskytte mot slike angrep?
- Utforsk tiltak som multifaktorautentisering, overvåking av nettverkstrafikk, og bruk av sikkerhetsprotokoller.
- Hvordan bør samhandlingen med leverandøren foregå når et innbrudd oppdages?
- Diskuter prosedyrer for kommunikasjon, samarbeid om å identifisere og fjerne trusler, og tiltak for å forhindre fremtidige angrep.
- Hva er de langsiktige konsekvensene av slike angrep på tilliten til leverandører og sanntidsdata?
- Diskuter hvordan slike hendelser kan påvirke tilliten til leverandører og sanntidsdata, og hvilke tiltak som kan gjenopprette denne tilliten.
- Hvordan bør kraftverket reagere på slike hendelser i fremtiden?
- Vurder beredskapsplaner, opplæring av ansatte, og etablering av en responsprotokoll for å håndtere lignende situasjoner.
- Hva er de økonomiske og operasjonelle konsekvensene av slike angrep?
- Analyser de økonomiske tapene og operasjonelle utfordringene som følge av manipulerte data og nødvendige utbedringer.

9.3 Ressurser for evaluering

Direktoratet for samfunnssikkerhet og beredskap (DSB) har en god veileder for evalueringer *Metodehefte: Evaluering av øvelser*[8]. Veilederne til DSB er noe omfattende for øvinger på cyber-hendelser, men det er mye godt innhold og mange gode tips. For evalueringer, er *Vedlegg 4: Erfaringslæring etter hendelser og øvelser* et skjema som gjerne kan brukes som utgangspunkt i evaluering av øvelser.

[8] https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/metodehefte---evaluering-av-ovelser/

Type dokument:
Vedlegg A - Direktiver

Rapport-tittel:
Cyber-øvelser for virksomheter i kraftforsyningen

Kunde:
NVE

Dokument nr. ST-001588-7				
Forfatter(e) Håkon Olsen, Annette Andersen, Jakob Stendahl				
Referanse til deler/utdrag av dette dokumentet som kan føre til feiltolkning, er ikke tillatt.				
Revisjon	Dato	Grunn for revisjon	Kontrollert	Godkjent
1	06.12.2024	Endelig	C. Thingvold	Sigve Oltedal

Scenario	**1 – Dataangrep på automasjonssystemer**
Øvingsform	Spilløvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• En målrettet angriper med vilje og evne til å utføre avanserte angrep mot OT-systemer har skaffet seg tilgang ved å utnytte svakheter i internetteksponerte systemer. • Angriperen har utført intern rekognosering og har klart å få kontroll over en datamaskin som brukes til å konfigurere regulatorer (en engineering workstation). • Angrepet oppdages gjennom et varsel fra nettverksbasert overvåkning som rapporterer om mistenkelig nettverkstrafikk
Egnede øvingsmål	• Etablere felles situasjonsforståelse i beredskapsteam • Øve på samhandling med leverandører • Øke virksomhetens evne til å bruke etablert planverk • Bevisstgjøring rundt eksisterende tiltak
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Scenarioleder • IT- og OT-sikkerhet • KraftCert • Automasjonsavdeling • OT-leverandør • Beredskapsmyndighet
Øvingsmomenter	1. Leder for IT-avdelingen får varsel fra en nettverkssensor i driftkontrollsystemet om «mulig uautorisert opplasting av prosjektfil til PLS» og varsler videre beredskapsleder på e-post 2. Beredskapsteamet kalles inn og erklærer at vi har en pågående sikkerhetshendelse. Ber automasjon rapportere inn. 3. IT-avdelingen har mottatt et varsel fra IT-sikkerhetspartner om utnyttelse av kjent sårbarhet i brannmur FIREX, som er merket som benyttes i virksomheten. IT-avdelingen har iverksatt undersøkelser og har flere tekniske funn, blant annet fra brannmur i OT-nettet. 4. Det er grunn til å tro at angriperen har reprogrammert flere regulatorer basert på nettverksdata. Det må tas en beslutning om veien videre. 5. Leverandøren stiler med personell på stedet for å bistå med gjenoppretting. Kan man stole på at personen som er sendt kommer fra leverandøren?

Scenario	**2 – Avansert vedvarende trussel (APT)**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• En trusselaktør har kompromittert IKT-systemene til virksomheten, og ønsker å bruke dette til å kartlegge robustheten i det norske kraftsystemet over tid. • Trusselaktøren har samtidig kompromittert mange aktører, og har også skaffet seg fotfeste i driftskontrollsystemene for overvåkning av produksjonsdata over tid. • Angrepet oppdages av en annen KBO-enhet, som deler indikatorer som gjør at aktiviteten kan verifiseres basert på brannmurlogger.
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Utvikle samhandling mellom IT og OT • Utvikle evne til å samhandle med andre KBO-enheter og sektorens sentrale responsmiljø
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Beskjed om pågående angrep mot sektoren bekreftet fra IT/SOC 2. Ny informasjon oppdaget om angrep/trusselaktør. Hvordan og hva skal deles? 3. Media viser interesse for angrepet og kontakter informasjonsavdelingen. Hva skal deles eksternt? 4. Nasjonal sikkerhetsmyndighet ber om statusrapport, med vurdering av potensialet for at trusselaktøren kan forstyrre kraftleveranser til sluttbruker 5. Skal virksomheten gå i øydrift inntil videre? 6. Hvordan prioriterer vi ressursbruken? 7. Er digital etterforskning og sikring av bevis viktig? 8. Hvordan sørger vi for at responsen hele tiden har et oppdatert lokalt og eksternt trusselbilde?

Scenario	**3 – Brudd på integritet i sanntidsdata**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• En bruker er kompromittert hos en leverandør som fyller ut en arbeidsordre og får denne godkjent. • Den kompromitterte brukere får åpnet for fjerntilgang til driftskontrollsystemet og installerer en skadevare som bruker en DNS-tunnel ut til internett for å nå angriperens infrastruktur. • Angrepet fører til manipulasjon av rapporterte produksjonsdata, som er grunnlag for offentlige statistikker.
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Utvikle samhandling mellom IT og OT • Utvikle evne til å samhandle med andre KBO-enheter og sektorens sentrale responsmiljø
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. En falsk arbeidsordre blir utfylt og sendt. 2. Arbeidsordren godkjennes, og skadevare installeres med ved bruk av den påfølgende autoriseringen av BjørneKraft. 3. Manipulasjon av sanntidsdata blir iverksatt av skadevaren Hvordan kan integriteten av produksjonsdata verifiseres? Hva er våre første tiltak? Husk kommunikasjon med relevante aktører. 4. Beskjed fra Bjørnekraft om mulig datainnbrudd, og at det er gjort forsøk på å komme inn i deres tjenester. 5. En operatør oppdager at interne målinger ikke samsvarer med data fra Historian. 6. Aktivering av beredskapsplan, men hendelsen kan ikke bare løses internt. 7. Media får nyss om hendelsen, og det begynner å spre seg rykter om sabotasje i organisasjonen. Hvordan skal dette håndteres, og av hvem?

Scenario	**4 – Fjernaksesskompromittering**
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• Kraftselskapet bruker en brannmurløsning som støtter SSLVPN. • En sårbarhet i brannmuren gjør at angriperen får tilgang i nettverket og beveger seg lateralt til interne servere i driftskontrollsystemet. • Aktiviteten oppdages når virksomheten får et varsel fra NVE/NSM om at det er sårbarheter I SSLVPN-løsning X som blir masseutnyttet på internett.
Egnede øvingsmål	• Etablere felles situasjonsforståelse i beredskapsteam • Øve på virksomhetens evne til å bruke etablert planverk • Bevissthet rundt eksisterende tiltak og sårbarheter
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • IT-sjef / Teknisk personell (IT og OT)
Roller i spillstab	• Scenarioleder • KraftCert • Teknisk personell (IT) • Brannmurleverandør • Journalist
Øvingsmomenter	1. IT-sjef får et varsel fra NSM om massiv utnyttelse av en sårbarhet i en SSLVPN-løsning som er bygd inn i mange brannmurer. 2. Uvanlig aktivitet blir oppdaget på interne servere. 3. Beredskapsteam kalles inn. 4. IT starter dypere undersøkelser, de finner flere ting på interne servere og brannmur. 5. Det virker som et rekognoserings-angrep, men det er umulig å være sikker på at det ikke kan påvirke driften.

Scenario	**5 - Forsyningskjede-angrep**
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• En systemleverandør er fysisk til stede og skal oppdatere firmware på regulatorer i driftskontrollsystemet. Leverandøren benytter virksomhetens service-laptop, og kobler først til nettverket for å laste ned den nye programvaren. • Ny firmware flashes til regulatorer under en planlagt kort driftsstans. Ved oppstart etterpå tripper systemet ved tilsynelatende jevne mellomrom og det blir brudd i strømproduksjonen.
Egnede øvingsmål	• Etablere felles situasjonsforståelse i beredskapsteam • Øve på samhandling med leverandører • Øke virksomhetens evne til å bruke etablert planverk
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller i spillstab	• Scenarioleder • IT og IT-sikkerhet • Automasjonsavdeling • OT-leverandør • Kundeservice • KraftCert
Øvingsmomenter	1. Oppdatering av fastvare i regulatorer installeres. 2. Regulatorer begynner å feile regelmessig. 3. KraftCERT melder at leverandøren har blitt kompromittert. 4. Leverandøren har ikke nok teknikere. 5. Virksomhetens tekniker har mange gode ideer.

Scenario	**6 – Kritisk systemnedetid**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• Et datavirus har blitt oppdaget i driftskontrollsystemet og systemene må gjenopprettes fra sikkerhetskopier før produksjon kan iverksettes igjen. Dette krever involvering fra flere leverandører. • En kritisk leverandør blir kraftig forsinket fordi det er oppstått sykdom, og de må sende en annen tekniker. Denne teknikeren er på et oppdrag i utlandet og det vil ta flere dager før vedkommende er på plass
Egnede øvingsmål	• Øve på bruk av planverk • Øve på dokumentering av hendelsesforløp, og sikring av spor
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Aktivering av beredskapsplan 2. Kommunikasjon med leverandør 3. Prioriteringer av oppgaver 4. Sikkerhetskopier 5. Håndtering av forsinkelser 6. Kommunikasjon med kunder og brukere 7. Etterforskning av viruset

Scenario	**7 - Løsepengevirus-angrep**
Øvingsform	Spilløvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse : 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• Både IT og OT-systemene er blitt rammet av Lockbit3 løsepengevirus. Alle Windows-maskiner er krypterte og viser bare et løsepengekrav når man logger på.
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Utvikle samhandling mellom IT og OT • Øve på bruk av planverk
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT) • Minst én tekniker
Roller i spillstab	• Scenarioleder • IT og IT-sikkerhet • Automasjonsavdeling • Journalist • Kunde
Øvingsmomenter	1. Driftsutfordringer mens ferieavvikling pågår 2. Godt timet phising gjør at skadevare blir installert 3. Kryptovirus sprer seg i IT og OT nettverk 4. Kunder og media tar kontakt om strømbrudd

Scenario	**8 – Nettverkssegmenteringsfeil**
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• I brannmuren mellom IT og OT-nettverkene hos en kraftprodusent er det en feilkonfigurasjon som tillater uhindret trafikk for enkelte protokoller, inkludert RPC og SMB. • En angriper har fått fotfeste i IT-nettet og beveger seg lateral over til OT ved hjelp av PsExec og får et cmd.exe-shell på en SCADA-server. • Dette oppdages når angriperen kjører flere rekognoseringskommandoer fra SCADA-serveren, og dette trigger en antivirus-alert som sendes på e-post til IT Helpdesk. Helpdesk varsler varsler driftskontroll 3 timer etter ticket ble laget.
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Utvikle samhandling mellom IT og OT • Øve på bruk av planverk • Etablere felles situasjonsforståelse
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller i spillstab	• Scenarioleder • IT og IT-sikkerhet • Automasjonsavdeling • OT-leverandør
Øvingsmomenter	1. Alert om mistenkelig aktivitet 2. Avblåses først som støy 3. Tydelige indikatorer på kompromitterte systemer 4. Årsak viser seg å være feilkonfigurasjon

Scenario	**9 - Teknologisk innovasjon**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• Et kraftselskap ønsker å effektivisere vedlikeholdsarbeidet på turbiner, og tar i bruk et nytt KI-verktøy for dette. KI-verktøyet samler data fra eksisterende prosessmålinger og egne IoT-sensorer som strømmes til leverandørens skyløsning. • Tanken er at man ved hjelp av maskinlæring skal kunne oppdage der det er risiko for feiltilstander tidlig, og derfor kunne gå over til tilstandsbasert vedlikehold i stedet for periodebasert. • Analysesleder blir gjort oppmerksom på nyhetssak hvor samme KI-leverandør har blitt hacket, og dette har ført til feilbehandling på flere sykehus i utlandet som har brukt systemet til å planlegge operasjoner. Leder for Helsedirektoratet sier på TV-nyhetene at de ikke er bekymret for liknende problemer I Norge på grunn av det strenge lovverket om risikovurdering ved innføring av KI-systemer.
Egnede øvingsmål	• Vurdere risikoer ved bruk av et KI-verktøy levert av en leverandør som har vært utsatt for et cyberangrep. • Diskutere hvordan slike risikoer kan overføres til kraftsektoren. • Utforske tiltak for å sikre KI-verktøyets pålitelighet og minimere risiko for kritiske feil. • Øke forståelsen for krav om sikkerhet og overholdelse av regelverk ved innføring av KI-løsninger.
Egnede roller for øvende	• Beredskapsleder / Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Risikoforståelse 2. Tillitt til leverandør 3. Mulige konsekvenser 4. Regulatoriske krav og lovverk 5. Beredskap 6. Data- og systemintegrasjon

Scenario	**10 - Zero-day exploit**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• En nulldagssårbarhet i Chromium blir utnyttet av avanserte aktører i målrettede angrep mot kraftsektoren i flere NATO-land. • Dette har ført til at flere kraftselskaper har blitt kompromittert. Sårbarheten skal ha vært av typen som ikke krever brukerinteraksjon, slik at om man besøker en spesielt utformet nettside, blir man hacket. • Det kommer varsel fra KraftCERT om at kraftselskapene som har blitt hacket, har besøkt kunnskapsbasen til en leverandør av digitale vern, og at denne tilgangen til internett normalt sett er en del av det vanlige oppsettet av HMI-ene for dette systemet. Alle kraftselskaper oppfordres til å sjekke om de er rammet eller sårbare, og ta hensiktsmessige grep. Avvik skal rapporteres til beredskapsmyndigheten.
Egnede øvingsmål	• Øve på bruk av planverk • Øve på kommunikasjon med myndighets-organer • Øve på dokumentering av hendelsesforløp, og sikring av spor
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Identifisering av sårbarheter 2. Aktivering av beredskapsplan 3. Samarbeid med eksterne parter 4. Håndtering av kompromitterte systemer 5. Prioritering av tiltak 6. Gjenoppretting og normalisering 7. Rapportering og dokumentasjon

Scenario	11 - Angrep på mobile applikasjoner
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• Et kraftselskap benytter timeføringssystemet “SmartWork”. Dette har en mobilapplikasjon som gjør det enkelt å føre timer på farten, og for ledere å godkjenne dem. App’en tillater også hurtig utbetaling av utlegg fra ansatte via en Vipps-integrasjon • En regnskapsfører varsler fra til HR om at det har vært en rekke utbetalinger til en tidligere ansatt over tid, og spør om dette skal være riktig. HR sjekker sine systemer og finner ingen spor av utlegg eller årsaker til disse utbetalingene. De mistenker datainnbrudd og varsler IT.
Egnede øvingsmål	• Etablere situasjonsforståelse under et komplekst angrep hvor mye av informasjonstilgangen kommer fra tekniske analyser • Vurdere personvernkonsekvenser og finansielle konsekvenser i et angrep som berører HR-systemer • Samhandling mellom teknisk respons og HR/økonomi
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell • HR-representant • Personvernombud
Roller i spillstab	• Øvingsleder • Digital etterforsker – mobile applikasjoner • IT-avdeling • Regnskapsfører • Tillitsvalgt fra fagforening eller verneombud • Representant fra leverandør (SmartWorks) • Arne
Øvingsmomenter	1. Teknisk analyse må oversettes til felles situasjonsforståelse 2. Det oppdages at overføringer er gjort fra flere steder i verden, hvor ingen fra HR eller økonomi har oppholdt seg 3. Det oppdages at store mengder data er lastet ned av en trusselaktør, inkludert lønnsdata og timeregnskap for ansatte 4. Underveis i håndteringen oppdages det at SmarWork har sendt ut en oppdatering av app’en 2 måneder tidligere som var satt som kritisk med anbefaling om å oppdatere. Ingen har fått med seg dette. 5. Det må vurderes hvilke myndigheter som skal varsles og hvordan. Datatilsynet, Politiet, Beredskapsmyndigheten er på blokka. 6. Fagforeningen ønsker at beredskapsleder kaller inn til informasjonsmøte med alle ansatte. 7. Alle ansatte må oppdatere SmartWork før den kan tas i bruk igjen.

Scenario	**12 – Brannmurkonfigurasjonsfeil**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• Et kraftselskap har leid inn et konsulentfirma for å gjøre en sjekk av oppsett av sikkerhetssystemene for IKT. Konsulentene finner flere feilkonfigurasjoner i brannmuren, blant annet at bade RDP og SSH-trafikk fra internett er tillatt. • Eskaleringspunkt 1: man oppdager ved undersøkelse av logger at det er flere innlogginger over RDP fra en IP-adresse i Kina. • Eskaleringspunkt 2: man oppdager mystiske kortvarige ssh-tilkoblinger fra ukjente norske IP-adresser, kun på natten.
Egnede øvingsmål	• Teste evne til å håndtere tilfeldig oppdaget angrep • Teste evne til samarbeid med IT drift • Øve på å vurdere alvorlighetsgrad av et funn i henhold til planverk
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Mulige handlemåter og prioritering: blokkere først, eller analysere mulighet for utnyttelse først? 2. Kommunikasjon til ledelsen: hvem har ansvaret for gjennomføring av tiltak, og hvorfor var brannmuren feilkonfigurert? 3. Eskaleringspunkt 1: IT-avdelingen har avdekket fra logger at det er flere RDP-innlogginger fra Kina. Dette skjer daglig i en periode på 2 måneder. Det er så lenge man har logger. Hva er hensiktsmessige spørsmål å stille om dette, og hva er mulige handlemåter? 4. På serveren finner IT-teamet ZIP-filer med ukenummer i navnet. Docs_week<NO>.zip i mappen C:\Temp. De regner med disse har blitt lastet opp av hackeren. Mappene er passordbeskyttet. Hvordan håndterer vi dette? 5. Eksaleringspunkt 2: IT-avdelingen har også søkt etter andre protokoller og funnet at det har vært SSH-sesjoner på natten med varighet opp til 2 minutter. Disse har gått til to forskjellige systemer, til en dedikert server som brukes til styring av adgangskontroll. 6. Ledelsen ønsker en statusrapport. Hva har skjedd, hva er skadevirkningene, og hva er gjort for å få kontroll? 7. Undersøkelse av endringslogg på brannmuren viser at det er systemadminsitratoren Steinar Lurv som har åpnet brannmuren for innlogginger via SSH og RDP fra 0.0.0.0/0, mens oppgaven i Jira viser at den egentlig skulle åpnes fra en spesifikk IP-adresse.

Scenario	**13 - Brudd på autentiseringsmekanismer**
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• Det kommer et varsel fra sikkerhetssystemene om forhøyet risiko for Økon Onomisjef, som jobber I BjørneKraft. • Årsaken er gjentatte “impossible travel”-varsler som har blitt ignorert av IT-avdelingen • Ved nærmere undersøkelse mistenker IT-avdelingen at Økon har blitt utsatt for avansert phishing, et såkalt “skurk-i-midten”-angrep og at uvedkommende har tilgang til kontoen hans. Ved samtale med Økon har han ikke merket noe spesielt, annet enn at teksten på knapper I Outlook I nettleseren noen ganger skifter språk mellom norsk, engelsk og fransk.
Egnede øvingsmål	• Forbedre kommunikasjonen mellom beredskapsleder, IT-avdelingen og ansatte under hendelser • Øve på samhandling i et scenario som har både menneskelige og tekniske faktorer
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • IT-sjef • HR-representant
Roller i spillstab	• Øvingsleder • Den ansatte (Økon Onomisjef) • IT-avdeling/IT-sikkerhet • Styreleder Rikerud
Øvingsmomenter	1. Kompromittert konto via phishing 2. Brudd på tofaktorautentisering 3. Tyveri av sensitive dokumenter 4. Kommunikasjon med styreleder 5. Personalhåndtering

Scenario	**14 – Brudd på personvern**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• En dataanalytiker har tilgang til kundedatabasen via et API, og bruker dette til å lage analysedashbord i PowerBI. API-nøkkelen ble ved et uhell lekket i et offentlig Github-repo. • En angriper bruker nøkkelen og henter ut alle kundedata. Dataene inneholder adresser, telefonnummer, fakturaer, transaksjonsinformasjon og statistikk fra AMS-målere. Dette legges ut for salg på det mørke nettet. • Kraftselskapet blir varslet av en anonym person om at disse dataene ligger ut for salg på «DarkPower» et forum for kriminelle som handler i stjålne data fra kraftselskaper.
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Utvikle samhandling mellom IT og OT • Øve på bruk av planverk
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Anonymt tips kommer på e-post om at kundedata er lagt ut for salg på det mørke nettet. 2. Tips med lenke til kundedata dukker opp på e-post. 3. Henvendelse fra VG kommer på SMS. De har fått et anonymt tips. 4. Det har kommet en henvendelse til IT-sjefen noen dager tidligere om en lekket API-nøkkel, denne har ikke kommet frem. 5. Det viser seg at data sannsynligvis er lekket via denne API-nøkkelen. 6. Det konstateres at alle kundedata sannsynligvis er lekket. 7. Krisestab er satt, kunder begynner å etterspørre informasjon.

Scenario	**15 - DDoS-angrep**
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• En botfarm med kontroll over tusenvis av X- og instagramkontoer poster og forsterker hverandres poster om at Kraftselskapet X kommer til å øke alle prisene med 50% og øke oppsigelsestiden på alle avtaler til 24 måneder. • De utfører så et DDoS-angrep mot kundeserviceavdelingen og nettsiden til Kraftselskapet X. • Selskapet kan ikke motta kundeforespørsler på chat, e-post er nede, og nettsiden er utilgjengelig. Dette er første nyhet på alle nyhetskanaler i Nord-Europa.
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Koordinere krisehåndtering mellom avdelinger • Håndtere et teknisk angrep (DDoS) og gjenopprette systemer • Kommunikasjon med media og eksterne aktører under krise
Egnede roller for øvende	• Beredskapsleder / innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller i spillstab	• Scenarioleder • IT og OT-sikkerhet • Media • Kundeservice
Øvingsmomenter	1. En kommunikasjonsovervåker varsler om en plutselig økning i sosial aktivitet på X og Instagram. Bot-kontoer sprer falske rykter om at selskapet skal øke prisene med 50 % og øke oppsigelsestiden til 24 måneder. 2. Kundeservice opplever en kraftig økning i henvendelser om prisøkninger og endringer i avtalevilkår. Kundene uttrykker bekymring og frustrasjon. 3. Et DDoS-angrep slår til mot selskapets nettside, og systemene begynner å gå ned. Kundeserviceportalen er utilgjengelig, og kundene kan ikke komme i kontakt med selskapet. 4. IT-avdelingen begynner å få kontroll over DDoS-angrepet, men tjenestene er fortsatt nede. Offentligheten krever svar, og mediene har begynt å dekke krisen.

Scenario	**16 - Man-in-the-Middle (MitM) angrep**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• Energitraderne i Superkraft bruker chatte-app'en "Superchat" til å snakke seg imellom om mulige kontrakter og diskutere investeringer. En angriper har laget en falsk versjon av Superchat, og lurer investeringssjefen over på denne. • Det dukker opp en "ugyldig sertifikat"-advarsel i nettleseren som investeringssjefen ignorerer. Hackerne snapper opp meldingene på den falske serveren før de blir sendt videre til den ekte Superchat-serveren. På denne måten kan de avlytte kommunikasjonen og manipulere den. • Dette oppdages først etter at det ble inngått en futures-kontrakt som investeringssjefen var sikker på var en god investering, men hvor det viste seg at han/hun burde visst mye bedre. Ved nærmere undersøkelser oppdaget investeringssjefen at det var avvik I beskjedene som var sendt og mottatt med traderne.
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Øve på samhandling mellom IT og andre • Øve på bruk av planverk
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Sikkerhetskultur i virksomheten 2. Håndtering av feilmeldinger/advarsler 3. Kommunikasjonsprotokoller 4. Etiske dilemmaer med overvåking av kommunikasjon 5. Håndtering av kritiske hendelser

Scenario	**17 – Sosial manipulasjonsangrep**
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• En trusselaktør er aktiv og kontakter administrativt personell I Superkraft på LinkedIn. De blir utsatt for smiger og oppmuntring, og får tilbud om uvanlig god betaling for å bli "intervjuet" til et fagmagasin om trender i kraftsektoren • De utvikler et vennskap over e-post, og administrativt ansatte for ofte gode tips om arrangementer eller informasjon som er interessant for lederne. • For å få enda bedre hjelp sender noen av administratorene jevnlig over en utskrift over møte- og reiseagendaen til lederne i virksomheten. • **Valgfritt***: lederen i Superkraft skal på en konferanse om KI i kraftsektoren, og får på morgenen tilsendt en PDF om akkurat det temaet han/hun skal være med i en paneldebatt om. Dette fører til at angriperen får hacket vedkommendes laptop.*
Egnede øvingsmål	• Øve på beslutninger under usikkerhet • Utvikle samhandling mellom IT og OT • Utvikle evne til å samhandle med andre KBO-enheter og sektorens sentrale responsmiljø
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. Administrativt personell blir kontaktet på LinkedIn av en trusselaktør. 2. Noen ansatte svarer på e-post, og ønsker å stille til intervju Ola foreslår noen tidspunkter langt frem i tid. 3. Vennskap blir utviklet over e-post, mellom ansatte og «Ola». 4. Ola følger opp over de neste ukene med mer ros og gode tips til arrangementer og nyttig informasjon for både administrativt personell og ledere i Superkraft. De ansatte føler de har en ressurs for Superkraft i forholdet til Ola. 5. Ola etterspør agendaen til lederne i virksomheten, for å kunne lettere filtrere ut tips som ikke er relevante. De ansatte begynner å jevnlig sende ledernes agenda til Ola.
	6. Ola spør om lederen i SuperKraft kan være interessert i å delta i en paneldebatt på en konferanse om KI i kraftsektoren. 7. Lederen i Superkraft sitter på hotellrommet på morgenen dagen paneldebatten skal være, når en e-post vedlagt en artikkel om KI i kraftbransjen tikker inn. Dette fører til at skadevare blir installert på maskinen hans.

Scenario	18 – Tyveri av legitimasjon
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• Per Bjarne jobber i IT-avdelingen hos Superkraft. En dag finner han ikke adgangskortet sitt i gangen hjemme når han skal på jobb. Han kjører til jobben og varsler om at kortet er borte, men sikkert bare er på avveie hjemme. Han får et lånekort for dagen. • I løpet av natten har uvedkommende vært inne i kontorbygget til Superkraft. De har plugget inn en RaspberryPi med mobilmodem i en ledig port konfigurert i admin-VLAN i en svitsj som ikke var låst inn. Senere undersøkelser viser at noen hadde brukt Per Bjarnes adgangskort klokken 2:15 på natten. • En uke senere varsler Per Bjarne at han fortsatt ikke kan finne adgangskortet sitt, og ber om å få et nytt et. Det gamle kortet blir sperret og man iverksetter rutinemessig en sjekk om kortet har blitt brukt i mellomtiden. Da merker man at noen brukte det klokken 2:15 på natten en uke tidligere.
Egnede øvingsmål	• Øve på samarbeid mellom fysisk sikkerhet, IT-avdeling og ledelse under en sikkerhetshendelse. • Trene på avdekking av uautorisert nettverkstilgang og håndtering av mistenkelige enheter. • Forbedre rutiner for logganalyse og monitorering av sensitive områder. • Evaluere kommunikasjon under krisesituasjoner, internt og eksternt.
Egnede roller for øvende	• Beredskapsleder/innsatsleder • IT-sjef eller IT-sikkerhet • Loggfører • Kommunikasjon
Roller i spillstab	• Adgangskontroll • IT-avdeling • Per Bjarne • Media
Øvingsmomenter	1. Adgangskontroll mottar en melding fra Per Bjarne om at han har mistet adgangskortet sitt. Han varsler om at han tror det bare er borte midlertidig. 2. En uke etter at adgangskortet ble meldt tapt, finner man ut at kortet har blitt brukt til et mistenkelig innbrudd, og selskapet står i fare for at flere systemer kan være kompromittert. Selskapets ledelse og ansatte må informeres. 3. Det blir funnet en RaspberryPi i et serverrom som det har vært jevnlig trafikk på siden den ble installert. FSHARE-1 er brukt av prosjektet «Nettutbedring ny kraftstasjon Høymarka». Alle filene derfra kopieres over til 10.10.1.2 hver natt klokken 03:00. Dette er IP-en som RaspberryPI-en hadde.

Scenario	19 – Kompromittering av skytjenester
Øvingsform	Diskusjonsøvelse
Modenhetskrav	Lav
Forventet tidsbruk	Forberedelse: 8 timer Gjennomføring: 2 timer Evaluering: 1 timer
Beskrivelse av scenario	• Minikraft har hyret inn en student som utvikler på deltid. Utvikleren deployer en webapp for testing i AWS. • Dessverre har utvikleren lekket den hemmelige nøkkelen som gir tilgang til AWS-kontoen på internet ved et uhell. Dette gir tilgang til å spinne opp virtuelle maskiner for den som har nøkkelen. • En angriper finner nøkkelen og spinner opp 10 kraftige VM-er med mye GPU-ressurser, for å kjøre kryptominere. Dette oppdages når AWS-kontoeier får et varsel om at AWS-regningen for måneden er estimert å bli over 900.000 kroner.
Egnede øvingsmål	• Øve på bruk av planverk for ekstern skytjeneste • Øve på involvering av supporttjenester fra plattformleverandør
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT)
Roller under øvelse	• Øvingsleder (diskusjonsøvelse) • Referent
Øvingsmomenter	1. **Identifisering av hendelsen**: Hvordan kan organisasjonen raskt identifisere at en skykonto er kompromittert? Hvilke indikatorer bør de se etter? 2. **Kommunikasjon med skyleverandør**: Hvordan skal organisasjonen kontakte AWS supporttjeneste? Hvilken informasjon bør de ha klar for å få raskest mulig hjelp? 3. **Tilgangshåndtering**: Hvordan kan organisasjonen sikre at hemmelige nøkler og andre sensitive opplysninger ikke lekker ut? Hvilke beste praksiser bør følges? 4. **Skadebegrensning**: Hva kan gjøres umiddelbart for å begrense skaden når en kompromittert konto oppdages? Hvordan kan man raskt stoppe de virtuelle maskinene som kjører kryptominere? 5. **Kostnadshåndtering**: Hvordan kan organisasjonen håndtere den økonomiske belastningen av en slik hendelse? Er det mulig å få refusjon fra AWS? 6. **Intern kommunikasjon**: Hvordan kan situasjonen forklares til ikke-tekniske avdelinger i organisasjonen? Hvilke nøkkelpunkter bør inkluderes for å sikre forståelse? 7. **Etterforskning av hendelsen**: Hvilke trinn bør tas for å etterforske hvordan nøkkelen ble lekket og hvem som kan stå bak angrepet? 8. **Opplæring og bevisstgjøring**: Hvordan kan organisasjonen trene sine ansatte, inkludert utviklere, på sikker håndtering av skykontoer og hemmelige nøkler?

Scenario	**20 – Kompromittering av IoT-enhet**
Øvingsform	Spilløvelse
Modenhetskrav	Middels
Forventet tidsbruk	Forberedelse: 40 timer Gjennomføring: 2-6 timer Evaluering: 2 timer
Beskrivelse av scenario	• Minikraft har kjøpt billige overvåkningskameraer fra Alibaba.com. Disse fungerer utmerket og tillater de ansatte å sjekke tilstanden rundt i anlegget via mobiltelefonen. • IT-avdelingen får et varsel fra Politiet at IP-adresser fra Minikraft er blitt brukt til å forsøke å bryte seg inn i webserverne til Diamantbanken. IT-avdelingen ser raskt at IP-adressene det gjelder er to av de billige kameraene.
Egnede øvingsmål	• Håndtere varsel om hendelse fra tredjepart (Politiet) • Samhandling mellom fysisk og digital sikkerhet
Egnede roller for øvende	• Innsatsleder • Loggfører • Kommunikasjonsansvarlig • Teknisk personell (IT og OT) • Vaktsjef (som bruker kameraer)
Roller under øvelse	• Scenarioleder • IT-sikkerhet • Teknisk personell • Kontoradministrator • Beredskapsmyndighet (politi) • Vaktpersonell • Kommunikasjonssjef i diamantbanken
Øvingsmomenter	1. Identifisere at IP-adresser gjelder billige kameraer 2. Tegne på forsøk på lateral bevegelse fra IP-kameraer til interne systemer 3. IT-avdeling oppdager at passord fra IP-kamera også er brukt på admin-panel for låsesystem 4. Trusselrapport viser at trusselaktør som målretter seg mot slike kameraer ofte bygger inn bakdører 5. Teknisk analyse av kamera finner tegn på slike bakdører 6. Diamantbanken sender IOC-er som også inkluderer andre IP-adresser fra kontornettet. Dette gjelder smarte møteromsskilt. 7. Analyse tyder på at det er et kompromittert default SSH-passord på møteromsskiltene som er misbrukt, og at det kommer innlogginger fra de billige kameraene.

NVE

Norges vassdrags- og energidirektorat

Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95