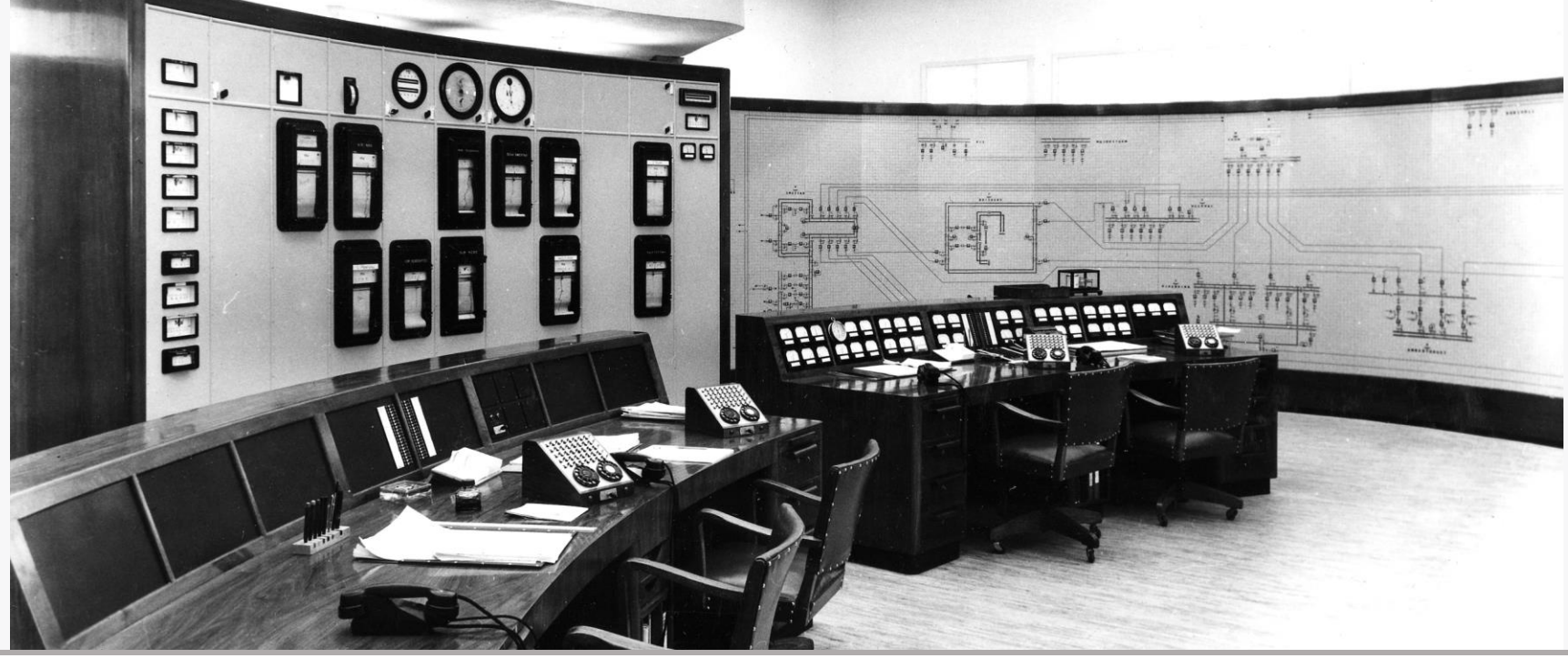
NVE
Norges vassdrags- og energidirektorat



VEILEDER NR. 2/2024

NVE

Veiledning for risikovurdering av IT og OT

SKREVET AV: KPMG

NVE Veileder nr. 2/2024
Veiledning for risikovurdering av IT og OT

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktører:	Linn Barstad og Jon-Martin Storm
Forfatter:	KPMG
Omslagsbilde:	Fra kontrollrommet i Smestad transformatorstasjon. Foto: NVE
ISBN:	978-82-410-2368-2
ISSN:	2704-0356
Saksnummer:	202317408

Sammendrag: Denne veiledningen for risikovurdering av informasjonsteknologi (IT) og operasjonell teknologi (OT) har bakgrunn i et behov for en oppdatert veiledning rettet spesifikt mot informasjonssikkerhet og digital sikkerhet. Formålet med veiledningen er å hjelpe små og mellomstore virksomheter i kraftbransjen til effektiv og god gjennomføring av risikovurderinger av IT og OT. Selv om fokuset er på IT og OT og SMB egner risikovurderingsmetoden i veiledningen også for andre typer risikovurderinger og selskaper av alle størrelser.

Emneord: Risikovurdering, IT-sikkerhet, OT-sikkerhet, Små og mellomstore virksomheter, Kraftbransjen, Grunnsikring for IT og OT

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 2024

Forord

Digitalisering og informasjonssikkerhet er av økende viktighet for alle sektorer i samfunnet. For kraftforsyningen er digitaliseringen særlig viktig for å møte utfordringene i fremtidens kraftsystem. Det er samtidig mer utfordrende å gjøre gode vurderinger av verdier, sårbarheter og trusler og ta riktige valg basert på disse. For kritisk infrastruktur som påvirker både samfunnssikkerhet og hverdagsliv, er det spesielt viktig at risikostyring håndteres godt av kraftsektoren og leverandører til denne.

NVE har lenge sett behovet for en veileder i risikovurderinger generelt og informasjonssikkerhet og digital sikkerhet i IT- og OT-systemer spesielt. Behovet for en veileder, som er tilpasset små og mellomstore virksomheter i kraftforsyningen, oppfatter vi som størst. Erfaringer viser at det er et mangfold av metoder, rammeverk, og verktøy som benyttes i sektoren. Dette kan føre til inkonsistens og varierende sikkerhetsnivå. Vi ønsker å legge til rette for en mer enhetlig tilnærming som kan styrke sektorens samlede digitale risikostyringskapasitet.

i er veldig fornøyde med å kunne dele denne nye veilederen. Den er resultatet av et grundig arbeid med å vurdere og anbefale de mest egnede risikoanalysemetodene, rammeverkene, og verktøyene for vår sektor. Vi mener at denne veilederen representerer en viktig milepæl i arbeidet med å styrke kraftforsyningens evne til å håndtere de digitale truslene, som stadig blir mer sofistikerte og omfattende. Risikovurderingsmetoden i denne veilederen egner seg også godt til risikovurderinger generelt, selv om eksemplene er hentet fra informasjonssikkerhet og digital sikkerhet i IT- og OT-systemer. Virksomhetene vil få best nytte av denne veilederen for risikovurderinger ved å bruke den sammen med den generelle veilederen for kraftberedskapsforskriften.

Veilederen er utarbeidet av KPMG på oppdrag fra NVE. Vi vil takke alle virksomhetene som stilte opp i intervjuer og spørreundersøkelser. De har bidratt med uvurderlig kunnskap om utfordringer og mulige løsninger. Rapporten som hører til veilederen er ikke delt som NVE-rapport, men er tilgjengeliggjort på eInnsyn.

Oslo, 28. februar 2024

Eldri Naadland Holo
seksjonssjef
Seksjon for beredskap
Tilsyns- og beredskapsavdelingen

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

Veiledning for Risikovurdering av IT og OT

Tilpasset små og mellomstore virksomheter i kraftbransjen

Innholdsfortegnelse

Innholdsfortegnelse

Risikovurderingens trinn

Sentrale begreper

Dette er sentrale begreper som brukes i veiledningen.

Definisjonene er basert på NS 5814:2021+AC:2023

Analyseobjekt	Analyseobjektet er det systemet, enheten, aktiviteten eller lignende som risikovurderingen rettes mot
Sannsynlighet	Hvor trolig det er at en uønsket hendelse inntreffer
Barriere	Tiltak som skal påvirke et hendelsesforløp, enten for å forhindre en hendelse eller redusere konsekvensene
Tiltak	Barrierer som har til hensikt å forhindre at en hendelse inntreffer
Uønsket hendelse	Hendelse som kan medføre tap av verdier . Uønskede hendelser omfatter både tilsiktet og utilsiktet handlinger, og kan gi opphav til ekstraordinære situasjoner, jfr. §6-9
Sårbarhet	Manglende evne til å motstå uønskede hendelser. En svakhet i en verdi eller et sikkerhetstiltak kan utnyttes av trusselaktører eller føre til utilsiktede hendelser
Konsekvens	Tap av verdier som følge av en uønsket hendelse
Verdier	Verdier er systemer, komponenter, informasjon, mennesker og andre elementer som trengs for at virksomheten skal fungere og utøve sine arbeidsoppgaver
Fare	Forhold, inkludert utilsiktet handling, som kan føre til en uønsket hendelse
Trussel	Tilsiktet handling som kan føre til en uønsket hendelse

Hvordan bruke og navigere i veiledningen

Bruk av veiledningen

Veiledningen beskriver beste praksis for risikovurderinger.
Allikevel er veiledningen forsøkt tilpasset små og mellomstore virksomheter med ulik modenhet. Den inneholder derfor en del støttetekst og eksempler, samtidig som virksomhetene kan velge å kun bruke deler av veiledningen.

Det er viktig at virksomheter tilpasser risikovurderingen til sitt behov. Større virksomheter med mange ansatte kan ha en omfattende styringsstruktur med en rekke definerte prosesser på ulike nivåer og mange personer som jobber spesifikt med dette. Mindre virksomheter har ofte en enklere styringsstruktur, og mange oppgaver som skal fordeles på få personer. Mange har ikke ressurser med et dedikert ansvar for å gjøre risikovurderinger, og noen har i tillegg begrenset kompetanse internt i virksomheten om risikovurdering, eller IT- og OT-sikkerhet.

Det er likevel viktig at arbeidet med risikovurderinger prioriteres, og over tid vil modenheten i virksomheten øke. Husk at en «dårlig» risikovurdering er bedre enn ingen risikovurdering ☺

Lykke til med risikoarbeidet!

Navigere i veiledningen

For at det skal være enklere å navigere seg i veiledningen har hvert trinn en forenklet innholdsfortegnelse som kan klikkes på. Klikk på huset for å komme til toppen av veiledningen.

I veilederen vil du også bli kjent med det fiktive kraftselskapet Elvheim Kraft. De ulike aktivitetene i veilederen vil eksemplifiseres for hvert trinn.

Trinn 1 | Trinn 2 | Trinn 3 | Trinn 4 | Elvheim Kraft

A

B

Hvert deltrinn inneholder ulike aktiviteter som bør gjennomføres

I blå bokser finner man repetisjon av viktige begreper og tips.

Denne kan du bruke denne til å navigere i presentasjonen:

Om veiledningen

Formål og målgruppe

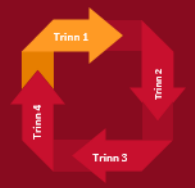
Grunnsikring

IT og OT-sikkerhet

Hva er en risikovurdering?

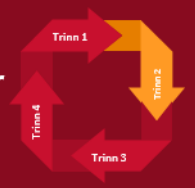
Om risiko og risikovurderinger

Rammer for risikovurderingen



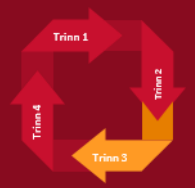
Trinn 1

Identifisere uønskede hendelser



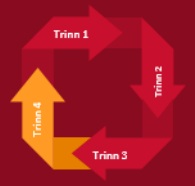
Trinn 2

Analysere risiko



Trinn 3

Håndtere risiko



Trinn 4

Videre arbeid

Hvordan bruke en risikovurdering i videre arbeid

Om veiledningen

Formål og målgruppe

Formål og målgruppe

Oppdatert veiledning for risikovurdering av IT og OT

Denne veiledningen for risikovurdering av informasjonsteknologi (IT) og operasjonell teknologi (OT) har bakgrunn i et behov for en veiledning rettet spesifikt mot informasjonssikkerhet og digital sikkerhet.

Formålet med veiledningen er å hjelpe små og mellomstore virksomheter i kraftbransjen til effektiv og god gjennomføring av risikovurderinger av IT og OT.

Risikovurderinger spiller en sentral rolle i virksomhetenes robusthet. Målet med en risikovurdering er å identifisere relevante trusler og sårbarheter, og utføre tiltak basert på disse. Gode risikovurderinger øker derfor virksomhetenes robusthet gjennom å bidra til bedre motstandsdyktighet mot uønskede hendelser.

Risikovurderinger kan være ressurskrevende, og spesielt for små virksomheter. Det er likevel et arbeid som bør prioriteres – både på kort og lang sikt. Veiledningen er en god start for å løfte kvaliteten i risikovurderinger - på sikt bidra til bedre sikkerhet i kraftbransjen. Det er også viktig at arbeidet med risikovurderingen ikke er en isolert sikkerhetsaktivitet, men en del av virksomhetens øvrige risikostyring.

Målgruppe for veiledningen

Målgruppen for veiledningen er små og mellomstore virksomheter i kraftbransjen. For å tilpasse veiledningen best mulig til målgruppens kontekst ble det i arbeidet med veiledningen hentet inn brukererfaringer gjennom spørreskjema og samtaler med virksomheter i kraftbransjen. Dette ga nyttig informasjon om utfordringer som målgruppen opplever i arbeidet med risikovurderinger, eksempelvis knyttet til begrenset tid og ressurser, varierende grad av kompetanse internt i virksomheten om IT og OT-sikkerhet og risikostyring, og bruken av driftsleverandører og ekstern kompetanse.

I utarbeidelsen av veiledningen har det blitt lagt vekt på beste praksis som rettesnor. Ulike rammeverk og standarder ble innledningsvis sammenlignet og vurdert ut ifra kriteriene brukervennlighet og ressursbruk, kompetanseterskel, kvalitet, kompatibilitet og egnethet for små og mellomstore virksomheter i kraftbransjen.

På bakgrunn av dette falt valget på Norsk Standard 5814:2021+AC:2023.

Denne standarden er tilgjengelig på norsk, noe som bidrar til å senke kompetanseterskelen. Videre er den nylig oppdatert, skalerbar og tverrfaglig. Dette er en fordel i kraftbransjen hvor det er stort spenn i både fag, størrelse og risikokompetanse.

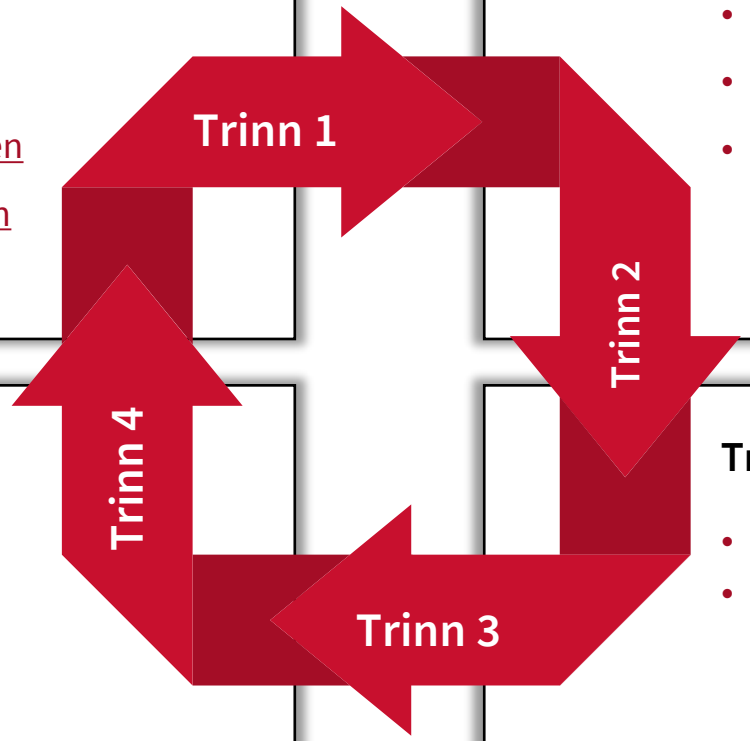
Oversikt over trinn og aktiviteter

Trinn 1 – Rammer for risikovurderingen

- Forberede, forankre og avgrense risikovurderingen
- Beskrivelse av analyseobjektet
- Vurdere sikkerhetsmål
- Gjennomføring av risikovurderingen
- Roller og ansvar i risikovurderingen

Trinn 2 – Indentifisere ønskede hendelser

- Identifisering av verdier
- Identifisering av trusler og farer
- Identifisering av uønskede hendelser
- Identifisering av sårbarheter



Trinn 4 – Håndtere risiko

- Identifisere tiltak
- Utforme anbefaling og tiltaksplan

Trinn 3 – Analysere risiko

- Vurdere konsekvens
- Vurdere sannsynlighet og usikkerhet

Grunnsikring

IT og OT-sikkerhet

Om IT og OT

Samspillet mellom IT og OT

IT og OT har tradisjonelt vært separerte domener som har snakket lite sammen. Innen sikkerhet og risiko for IT er konfidensialitet og integritet vært viktige prinsipper, mens tilgjengelighet og kontroll er særlig viktig for OT. I tillegg brukes typisk «security» og «safety» som begreper for å skille betydningen av sikkerhet i henholdsvis IT og OT. Safety er et begrep som også dekker sikring av personer og skal ha høy prioritet.

Videre har OT-komponenter lengre levetid, oppdateres sjeldnere, og er ofte segregert fra Internett. I motsetning til IT har det tidligere vært lav risiko for angrep fra utenforstående på OT, både fordi OT-systemer har befunnet seg på fysisk utilgjengelige plasser, men også fordi de ikke har vært tilkoblet nett.

Dette bildet er imidlertid i endring og det foregår økende integrasjon mellom IT og OT. Integrasjon mellom IT og OT kan kort beskrives som økt dataflyt og sammenkobling mellom de to domenene. I dag er mange systemer delvis integrert, der data primært flyter fra OT til IT. Den viktigste driveren for denne sammenkoblingen er digitalisering av OT.

Når IT og OT kobles tettere sammen, øker kompleksiteten hos virksomhetene. Det stiller strengere krav til digital sikkerhet.

Økt kompleksitet stiller strengere krav

Digitalisering kan gi store gevinster for virksomhetene i form av sanntidsbaserte produksjonsdata, effektivisering av prosesser, og bruk av smarte sensorer, men introduserer samtidig nye problemstillinger.

Økt integrasjon mellom IT og OT gjør infrastrukturen mer kompleks, det blir vanskeligere å holde oversikt og trusselbildet endrer seg. Dette stiller strengere krav til kontroll og oversikt. Det gjør også at man ikke kan håndtere IT og OT som to separerte domener.

Det er derfor behov for at fagpersoner fra både IT og OT samarbeider om risikovurderinger og øvrig sikkerhetsarbeid. Veilederen skal støtte opp under samarbeidet mellom IT og OT for å legge til rette for at risikovurderinger ser de to domene i sammenheng.

At man ser de to domene i sammenheng under en risikovurdering betyr ikke nødvendigvis at man skal risikovurdere IT og OT under ett. Formålet med veiledningen er å hjelpe virksomheter med å løfte blikket og peke ut hvilke retninger virksomheten bør se når man utarbeider en risikovurdering.

Grunnsikring for IT & OT

Få oversikt over virksomhetens verdier, avhengigheter og krav

Å skaffe seg oversikt over virksomhetens viktigste verdier, avhengigheter og krav til IT og OT-sikkerhet er en essensiell del av grunnsikringen for en virksomhet. Oversikt og kontroll er også et premiss for arbeidet med risikovurderinger.

Alle virksomheter bør prioritere å etablere følgende:

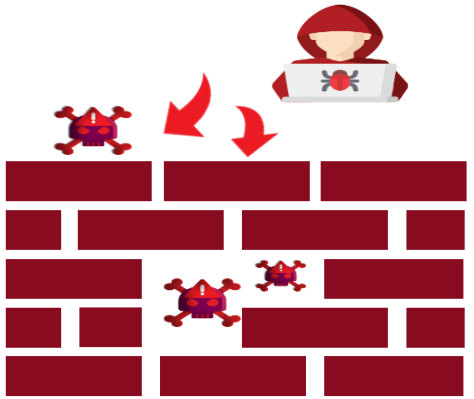
A Oversikt over virksomhetens IT og OT-systemer, og som et minimum de mest kritiske systemene. Dette er en forutsetning for å kunne sikre IT/OT-miljøet på en god nok måte. Oversikten bør dokumenteres og holder oppdatert.

B Oversikt over kraftsensitiv informasjon og annen virksomhetskritisk informasjon, og hvor dette lagres. Virksomheten bør gjøre en vurdering av hvilke systemer man kan lagre sensitiv informasjon, eksempelvis om skytjenester kan benyttes til dette formålet.

C Oversikt over alle leverandører, samt hvilke sikkerhetskrav som har blitt stilt til disse. For virksomheter med driftsleverandør bør det gjøres en undersøkelse av sikkerheten, hvis dette ikke ble gjort under anskaffelsen. Det er viktig å inkludere skyleverandører, også de store aktørene.

D Oversikt over interne og eksterne krav til IT og OT-sikkerhet. Virksomheter i kraftbransjen er blant annet underlagt Kraftberedskapsforskriften, og i tillegg har virksomheter ofte interne krav til sikkerhet som skal etterleves. Det er viktig å få oversikt over disse.

E Oversikt over avhengigheter til IT og OT, samt til leverandører. Virksomheten bør vurdere hva som er toleransegrensene dersom IT og/eller OT-systemer er utilgjengelige. Dess lavere toleransegrense, dess høyere sikkerhet er nødvendig.



Grunnsikring for IT & OT

NSMs grunnprinsipper for IKT-sikkerhet

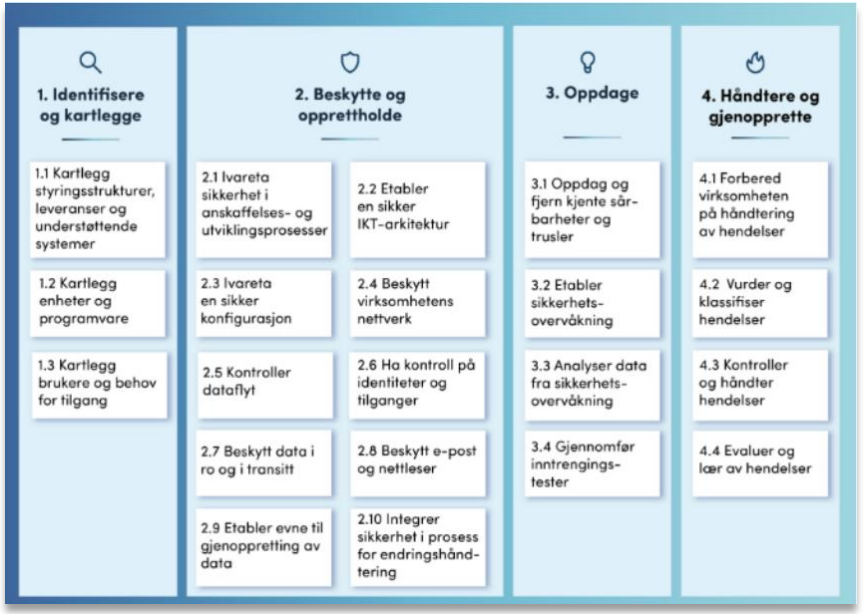
NSMs Grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Mange virksomheter i kraftbransjen har tatt i bruk grunnprinsippene som en del av den forebyggende sikkerheten, og bruker det aktivt i sikkerhetsarbeidet.

I denne veiledningen brukes NSMs grunnprinsipper for IKT-sikkerhet både som en del av grunnsikringen, og som en del av sårbarhetsvurderingen i trinn 2. Begrunnelsen for dette er at grunnprinsippene kan bidra til å gjøre virksomheter mer motstandsdyktige mot uønskede hendelser, og dermed redusere sårbarheter både for virksomheten og for kraftbransjen som helhet.

Det er viktig at virksomheter som bruker NSMs grunnprinsipper jevnlig tester effektiviteten av tiltakene for å kontrollere at tiltakene fungerer i praksis. Det er også viktig at virksomhetene prioriterer tiltak som gir størst verdi for virksomheten. En risikovurdering basert på denne veiledningen kan gi informasjon om nettopp dette.

Det er anbefalt at alle virksomheter implementerer grunnprinsippene i kategori 1 og kategori 2. Det bør i tillegg vurderes om noen grunnprinsipper fra prioritet 3 bør implementeres.

Se NVEs anbefalinger og veiledninger for mer informasjon.



Kilder og anbefalt lesing:

- NSMs grunnprinsipper for IKT-sikkerhet
- Risikovurdering av IKT-systemer
- Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer (rapport fra SINTEF)

Hva er en risikovurdering?

Om risiko og risikovurderinger

Hva er en risikovurdering?

Hva er en risiko?

Forståelse av risiko er viktig for at virksomheter skal kunne utforme og håndtere gode risikovurderinger. Risiko kan defineres som «usikkerhet knyttet til om en uønsket hendelse vil inntreffe og hvilke konsekvenser den kan få». Usikkerhet blir ofte uttrykt ved sannsynlighet.

Resultatet av risikovurderinger er ofte en rekke sikkerhetstiltak som virksomheten skal implementere. Her er det viktig at virksomheter har en risikobasert tilnærming til sikkerhetsarbeidet gjennom å prioritere tiltak som beskytter av de viktigste verdiene, samt å sørge for at effekten av tiltakene blir testet etter implementering.

Ledelsen i virksomheter har en viktig rolle i risikoarbeidet som premissgiver, og som beslutningstaker. Det er ledelsens ansvar å etablere en risikobasert tilnærming til sikkerhetsarbeidet. Dette er viktig for å sikre at virksomhetens midler blir brukt til å implementere de riktige tiltakene på rett sted, og sikre at virksomheten har de nødvendige ressursene i arbeidet med IT/OT-sikkerhet og risikovurderinger.

Hvorfor er risikovurderinger viktig?

Kraftbransjen forvalter store samfunnskritiske verdier og infrastruktur, og dekker en kritisk funksjon for samfunnet. Både tilsiktende og utilsiktede uønskede hendelser kan få store konsekvenser både for virksomhetene og for samfunnet.

Nasjonal sikkerhetsmyndighet (NSM), E-tjenesten og Politiets sikkerhetstjeneste (PST) har identifisert kraftbransjen som spesielt utsatt i sine åpne risiko- og trusselvurderinger. Trusselaktører kan ha motiver som for eksempel økonomisk vinning, politiske interesser og sabotasje. Dette fremhever behovet for et økt fokus på IKT-sikkerhet, inkludert arbeidet med risikovurderinger av IT og OT som gir et viktig kunnskapsgrunnlag for å kunne gjøre prioriteringer i sikkerhetsarbeidet.

Videre er det krav i Kraftberedskapsforskriften om at det skal gjennomføres risikovurderinger, og at disse skal holdes oppdatert.

Vil du lære mer om risiko?

- Vurdering av risiko | Digdir

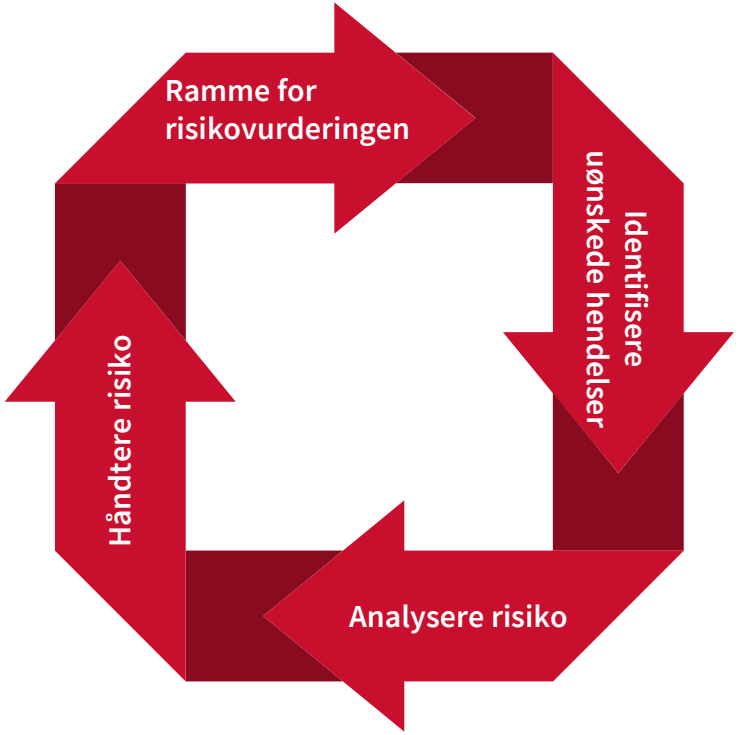
Hva er en risikovurdering?

Innholdet i en risikovurdering

En risikovurdering er en systematisk prosess der man identifiserer, analyserer og evaluerer potensielle uønskede hendelser. Prosessen bidrar til en dypere forståelse av risikoene og legger grunnlaget for hvilke tiltak som bør implementeres. Det finnes flere ulike måter som en virksomhet kan tilnærme seg og gjennomføre risikovurderinger på.

Denne veiledningen er basert på NS 5814:2021+AC:2023, og har følgende fire trinn:

1. Rammer for risikovurderingen
2. Identifisere uønskede hendelser
3. Analysere risiko
4. Håndtere risiko



Hva er en risikovurdering?

Når skal virksomheter gjennomføre risikovurderinger?

Kraftberedskapsforskriften stiller krav til KBO-enheter om når risikovurderinger skal gjennomføres. Dette inkluderer:

- KBO-enheter skal gjennomføre risikovurderinger knyttet til ekstraordinære forhold som skal vurderes minimum årlig og oppdateres ved behov, jf. § 2-3
- Virksomheter skal også gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert, jf. § 6-9

Virksomheten bør sette seg inn i og forstå hvordan kravene som er fastsatt i kraftberedskapsforskriften kan oppfylles.

Mer informasjon finnes i NVEs veiledning til kraftberedskapsforskriften.

I tillegg bør virksomheten også vurdere behovet for risikovurderinger i blant annet følgende tilfeller:

- Ved endringer i IT og/eller OT-miljøet
- Ved anskaffelser av nye systemer eller ved tjenesteutsetting til for eksempel en driftsleverandør eller en leverandør av skytjenester
- Ved endringer hos leverandører som kan påvirke virksomheten
- Ved endringer i trusselbildet

Verktøy i risikovurderingen

Bruk av verktøy

Verktøy for risikovurderinger strekker seg fra enkle regneark til interaktive verktøy fra ulike leverandører. Akkurat hvilket verktøy som passer virksomheten best vil avhenge av virksomhetens størrelse, kompetanse, hvilket verktøy som brukes i virksomheten i dag.

Det er anbefalt at virksomheten velger seg *et* verktøy for risikovurderinger. Bruk av samme verktøy standardiserer arbeidet og gjør det enklere for ulike ansatte å gjenkjenne metodikken som er brukt. Over tid vil det også være enklere å sammenligne resultatene fra ulike risikovurderinger.

Samtidig kan det være utfordrende for virksomheter å vite hvilket verktøy som er best egnet. På høyre side er en sjekkliste for kjennetegn på et godt verktøy for å dokumentere risikovurderinger. Dette kan virksomheten bruke for å navigere i utvalget av verktøy. Ved valg av verktøy bør virksomheten tenke langsiktig – dersom verktøyet for eksempel ikke lenger blir oppdatert fra leverandør er det på tide å tenke nytt.

For mange små og mellomstore virksomheter tilfredsstiller regneark/Excel de viktigste kriteriene, og kan fungere som et godt verktøy i risikovurderingen.

Sjekkliste for verktøy

- ❑ Verktøyet har mulighet for å etablere en endringslogg
- ❑ Verktøyet har mulighet for å etablere tilgangsstyring
- ❑ Leverandør av verktøyet har god nok innebygd sikkerhet til å behandle konfidensiell informasjon (for eksempel kraftsensitiv)
- ❑ Verktøyet gjør det mulig å lage og gjenbruke maler
- ❑ Verktøyet er brukervennlig og har en lav kompetanseterskel
- ❑ Ulike roller i en risikovurdering kan få tilgang til verktøyet
- ❑ Det er sannsynlig at verktøyet kan brukes flere år frem i tid
- ❑ Verktøyet gjør det enkelt å visualisere resultatet av risikovurderingen
- ❑ Verktøyet er egnet til oppfølging av tiltak.

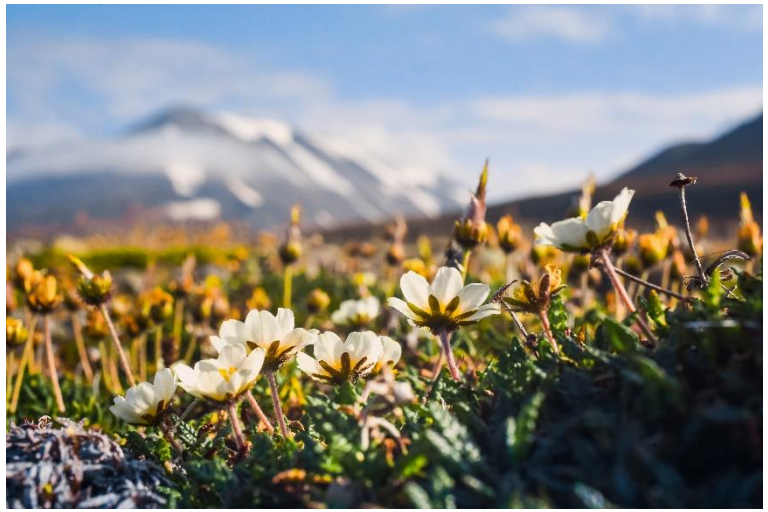
Denne sjekklisten er ikke utfyllende, og det kan være prioriteringer som er viktig for akkurat deres virksomhet. Endringslogg, tilgangsstyring og innebygd sikkerhet er viktig i alle systemer og verktøy hos virksomhet og leverandør som behandler kraftsensitiv informasjon. Dette bør stå høyt på prioriteringslisten.

Verktøy
Et hjelpemiddel for å systematisere risikovurderinger

Elvheim Kraft

Elvheim Kraft gjennomfører en risikovurdering

I løpet av veiledningen vil det fiktive kraftselskapet *Elvheim Kraft* bli brukt som eksempel. Formålet med å bruke et fiktivt kraftselskap er å gi håndfaste eksempler som virksomhetene som bruker veiledningen kan relatere til.



Kort om Elvheim
Elvheim er en liten, fiktiv by. Byen ligger i et geografisk område som ligner på Innlandsnatur, og er derfor omringet av fjell og skog. Ned fra fjellet renner det en elv, som renner gjennom byen, derav navnet. Elven varierer i størrelse etter årstidene, da blant annet smeltet snø øker vannstanden. En hjørnestein i samfunnet i Elvheim, er Elvheim kraft.

Elvheims Kraft sin risikovurdering:
Elvheim Kraft har et virksomhetskritisk IT-system som heter *ELV*. Dette systemet er integrert både med andre IT-systemer og med OT-sensorer. Det er lenge siden *ELV* ble risikovurdert, og det har blitt gjort en del endringer i den tekniske infrastrukturen og en fysiske sikkerheten de siste månedene. Driftsleder i Elvheim har derfor meldt inn et behov for å gjøre en risikovurdering av *ELV*, samt grensesnittet mot OT.

Elvheim Kraft beskrives nærmere på neste side. Underveis i veiledningen vil den fiktive virksomheten brukes for å vise hvordan de ulike trinnene i risikovurderingen kan gjennomføres.

Elvheim Kraft

Om Elvheim Kraft

Elvheim kraft er en vannkraftprodusent. Selskapet har to produksjonsanlegg, som er plassert på to ulike punkter i elva. Fordelt på disse anleggene har selskapet 12 ansatte, inkludert ingeniører, driftspersonell og administrasjon. Selskapet produserer og selger vannkraft. Normal årlig produksjon er 478GWh.

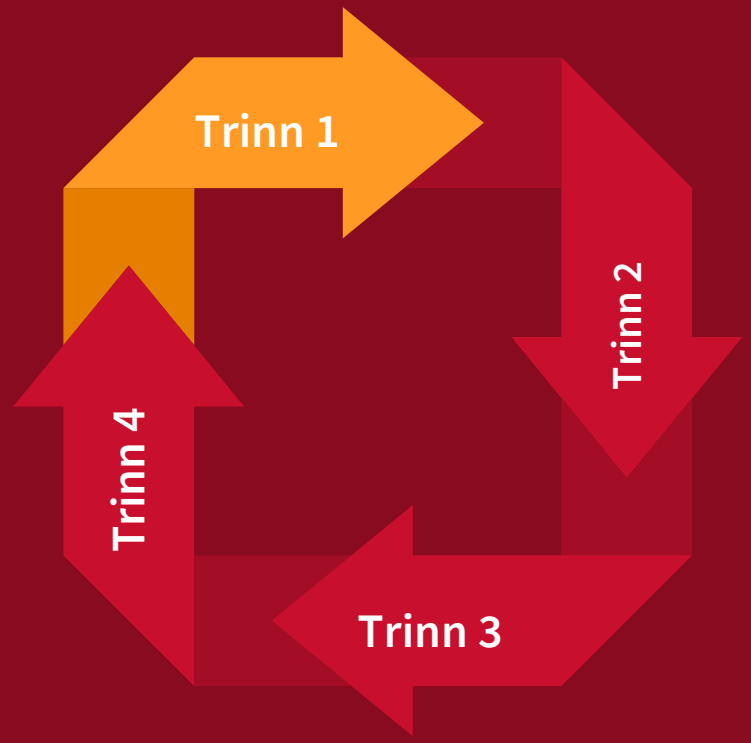
Selv om selskapet har en stabil posisjon som kraftprodusent, erkjenner Elvheim kraft behovet for modernisering i møte med en stadig mer digitalisert verden og ønsker i større grad å fremme selskapet som en produsent av grønn energi. I møte med digitaliseringen har selskapet derfor begynt å utforske integreringen av operasjonell teknologi (OT) og informasjonsteknologi (IT) for å optimalisere driften. Knyttet til dette fokuset har selskapet identifisert en mangel på IKT- og risikovurderingskompetanse blant de ansatte, og de ser behovet for å styrke denne kompetansen. Selskapet gjennomfører risikovurderinger også i dag, men det er mest for å kvittere ut lovpålagte krav. De ansatte har derfor en begrenset praktisk forståelse for risiko.

Med et økende fokus på å forbedre kompetansen innen IT, OT og IoT blant de ansatte, ønsker Elvheim kraft å modernisere driften og styrke sin evne til å håndtere potensielle digitale risikoer.

Nøkkelinformasjon

- ❑ Vannkraftprodusent
- ❑ Innlandet
- ❑ To produksjonsanlegg
- ❑ 12 ansatte
- ❑ Normal årlig produksjon: 478GWh

Rammer for risikovurderingen

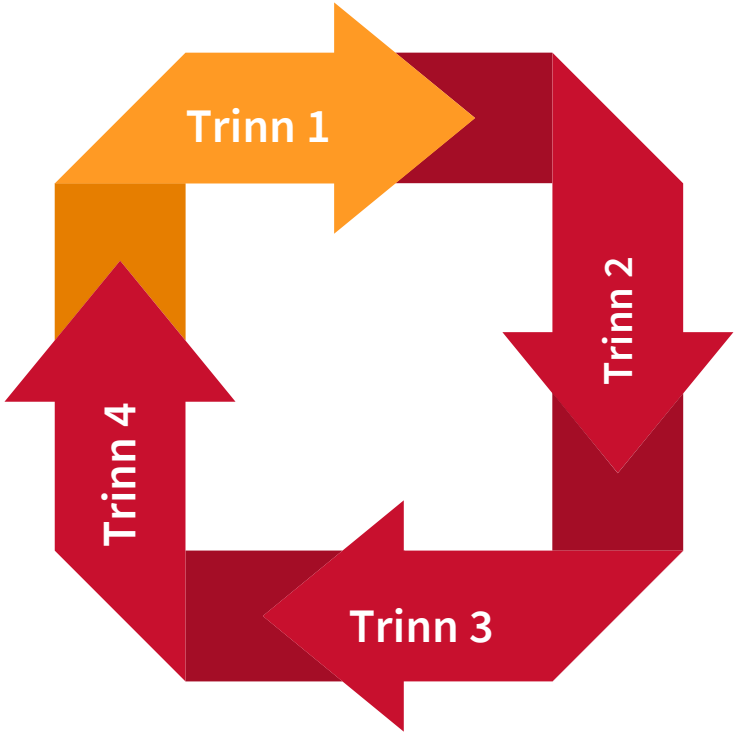


Trinn 1

Trinn 1 – Rammer for risikovurderingen

Organisering av risikovurderingen

Formålet med det første trinnet i veiledningen er å settes rammene for det videre arbeidet med risikovurderingen. Her dekkes aktiviteter og avklaringer som er viktige for at selve risikovurderingen skal bli så god og konkret som mulig.



Aktiviteter i trinn 1:

- Forberede, forankre og avgrense risikovurderingen
- Beskrivelse av analyseobjektet
- Vurdere sikkerhetsmål
- Gjennomføring av risikovurderingen
- Roller og ansvar i risikovurderingen

De neste sidene beskriver hver av aktivitetene mer i detalj.

Rammer for risikovurderingen

Forberede og forankre risikovurderingen

Det er enklere å utarbeide en god og presis risikovurdering om man har tydelig forankring i organisasjonen og klare rammer for det som skal risikovurderes.

Hvorfor er det viktig?

Risikovurderingen bør alltid forankres hos ledelsen før arbeidet settes i gang. I sammenheng med dette bør risikovurderingens formål og avgrensninger fastsettes.

Risikovurderingens formål skal belyse hva risikovurderingen skal brukes til, og svare på spørsmålet «hvorfor skal analysen gjennomføres?» For eksempel om risikovurderingen skal danne grunnlag for beslutningen om innkjøp av et nytt system, hvordan nye løsninger skal utvikles eller om det er behov for oppgraderinger.

Dokumentasjon handler både om å bruke eksisterende dokumenter og kontinuerlig dokumentere arbeidet i risikovurderingen. Dokumentasjon er viktig for å kunne se tilbake på hvilke vurderinger og beslutninger som ble lagt til grunn underveis.

Risikovurderingen bør ha et klart definert omfang og avgrensninger mot andre systemer. Mer informasjon om avgrensning og analyseobjektet på neste side.

Aktiviteter:

A Beskrive formålet med risikovurderingen, inkludert hvilke behov risikovurderingen skal dekke.

B Forankre risikovurderingen hos ledelsen. Avklar hvem som er beslutningstaker og eventuelle beslutningspunkter, samt rammer for tid og omfang.

C Avklar i hvilket format risikovurderingen skal dokumenteres, og hvor den skal lagres. Dokumenter også ledelsesforankringen og rammene som settes.

Eksempler på dokumentasjon

- Styrende dokumenter: Eksterne og interne føringer for risikovurderinger
- Utførende dokumenter: Hvordan aktivitetene i risikovurderingen skal gjennomføres, prosedyrebeskrivelser og arbeidsinstrukser

Rammer for risikovurderingen

Beskrivelse av analyseobjektet

Det er viktig å innhente mest mulig informasjon om analyseobjektet for å sikre at alle som bidrar i risikovurderingen har en felles forståelse.

Hvorfor er det viktig?

Et godt kunnskapsgrunnlag og en felles forståelse for analyseobjektet blant alle som deltar i risikovurderingsarbeidet bidrar til et godt resultat. Relevante informasjonskilder kan være tidligere risikovurderinger, tekniske tegninger og systembeskrivelser, arkitekturskisser, dataflyter, og lignende.

Risikovurderingens omfang og avgrensninger vil avhenge av formålet med risikovurderingen. For eksempel vil en årlig oppdatering av en risikovurdering som dekker hele virksomheten ha et større omgang enn risikovurderinger som gjøres i forbindelse med mindre endinger i IT-miljøet.

Analyseobjektet
Analyseobjektet er det risikovurderingen rettes mot. For eksempel et enkelt IT-system, eller hele virksomhetens IT og OT-miljø.

Aktiviteter:

A Innhent informasjon om analyseobjektet. Relevante kilder kan være tidligere risikovurderinger, tekniske tegninger og systembeskrivelser, arkitekturskisser, dataflyter, m.m.

B Sett avgrensninger for risikovurderingen og beskriv analyseobjektet.

C Vurder om det er nødvendig med en avsjekk med ledelsen eller andre relevante personer om beskrivelse og avgrensningen av analyseobjektet.

Rammer for risikovurderingen

Vurdere bruk av sikkerhetsmål

Sikkerhetsmål er en bekrivelse av sikkerheten som må være på plass for å kunne levere på virksomhetens mest kritiske tjenester. Dette kan for eksempel være ambisjonsnivå, funksjonskrav eller tekniske krav. Dersom virksomheten har definert sikkerhetsmål kan dette inkluderes i risikovurderingen.

Hvorfor er det viktig?

Sikkerhetsmål er fastsatte, overordnede mål som virksomheten har satt for å kunne ivareta virksomhetens verdier på en best mulig måte. Hva som er et relevant og konkret sikkerhetsmål avhenger av blant annet hvor kritiske tjenester virksomheten leverer, hvilke interne og eksterne krav som stilles til sikkerhet, og omfanget av verdier som skal beskyttes.

Ukjente begreper?
Sikkerhetsmål og evalueringskriterier erstatter risikoakseptkriterier i NS 5814:2021.

Hvordan sette sikkerhetsmål?

A Identifisering av de mest kritiske funksjonene til virksomheten.

B Identifiser interne og eksterne krav til IKT-sikkerhet

C Sikkerhetsmål formuleres basert på aktivitet A og B

D For virksomheter med driftsleverandør: Gi føringer om sikkerhetsmålet, og følg opp at kravene blir fulgt.

Rammer for risikovurderingen

Gjennomføring av risikovurderingen

En risikovurdering kan organiseres på ulike måter. Det er vanlig å organisere arbeidsmøter hvor man samler personer som har relevant kompetanse om analyseobjektet.

Hvorfor er det viktig?

Arbeidsmøter kan være en god arbeidsmåte for risikovurderinger fordi det sikrer at personer med relevant kunnskap og kompetanse om analyseobjektet er tilgjengelige og involvert i arbeidet. I tillegg gir det tid og rom for drøfting, samt muligheten til tverrfaglige diskusjoner som kan belyse ulike perspektiver.

For å sikre en helhetlig vurdering, bør man inkludere personer som har kompetanse om avhengigheter mellom systemene også, for eksempel dataflyten mellom IT og OT.

Neste side viser eksempler på typiske roller som kan involveres i et arbeidsmøte.

Aktiviteter:

A Identifiser personer i virksomheten med relevant kompetanse om analyseobjektet.

B Send gjerne ut kunnskapsgrunnlaget, samt en beskrivelse av hvorfor risikovurderingen gjennomføres og hvilke avgrensninger som har blitt gjort på forhånd.

C Sett av nok tid til risikovurderingen. Et alternativ kan være å ha to separate arbeidsmøter:

Del 1: Utforme uønskede hendelser og vurdere sannsynlighet og konsekvens (1-2 timer)

Del 2: Identifisere tiltak og utforme anbefaling (1-2 timer)

Tips til gjennomføring:
Det er ofte en fordel at en person er ansvarlig for å fasilitere arbeidsmøtene, og at en dedikert person til tar notater underveis.

Rammer for risikovurderingen

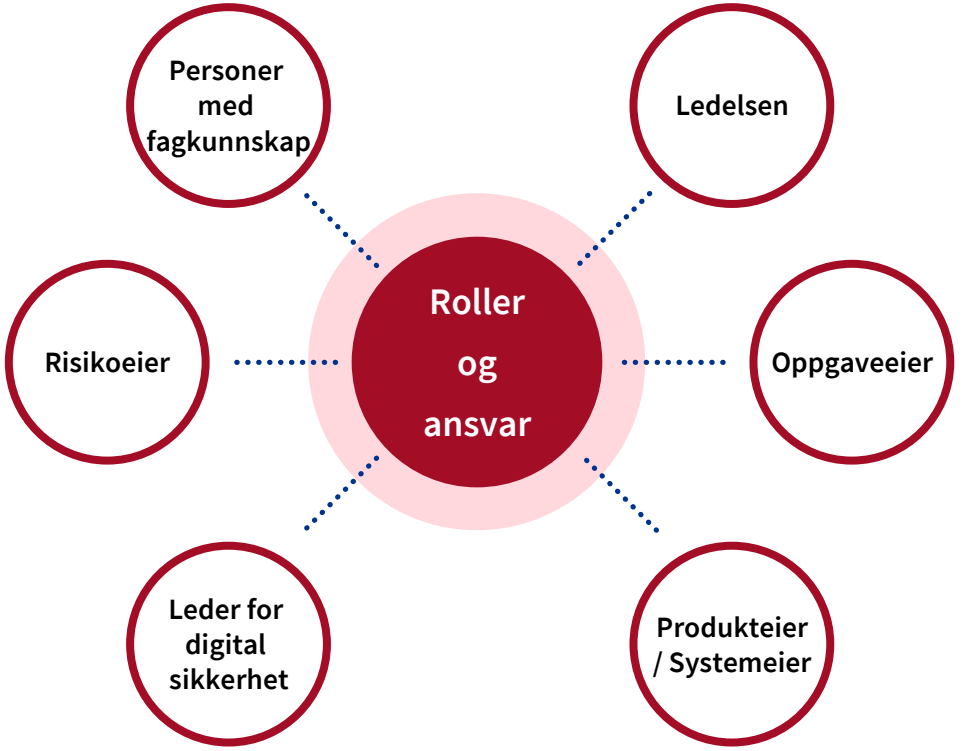
Roller og ansvar i risikovurderingen

Hvem som involveres i risikovurderingen vil være avhengig av risikovurderingens omfang og avgrensning samt hvilke fagområder som skal dekkes av risikovurderingen.

Hvem skal involveres?
Dette er eksempler på typiske roller som kan involveres i en risikovurdering. Navnet på rollene kan variere, og for mindre virksomheter kan rollene ofte overlappe. Alle rollene beskrives ikke her, men det er noen roller som spesielt bør trekkes frem.

Ledelsen bør alltid involveres slik at risikovurderingen får ledelsens aksept. **Risikoeier**, også kalt prosesseier, har oversikt over sitt område og er gjerne ansvarlig for at risikovurderinger gjennomføres. **Oppgaveeier** eller prosesseier er ofte den som har særlig ansvar for gjennomføring av risikovurderingen.

I tillegg er personer med relevant fagkunnskap ofte nyttige å involvere, selv om de ikke har et formelt ansvar i gjennomføring av risikovurderingen. Gjerne inviter disse med på arbeidsmøtene slik at de kan komme med sine perspektiver. Dette med på å sikre en helhetlig vurdering.



Elvheim kraft gjennomfører Trinn 1

Trinn 1 | Trinn 2 | Trinn 3 | Trinn 4 | Elvheim Kraft

Forberede og forankre

Elvheim Kraft har gjort en del endringer i sin IT- og OT-infrastruktur, og trenger en ny risikovurdering av det virksomhetskritiske IT-systemet *ELV*. Dette systemet er integrert med OT-sensorer, samt med andre IT-systemer.

Beredskapskoordinator i Elvheim melder inn et behov for å gjøre en risikovurdering av *ELV.*

Beredskapskoordinator beskriver **formålet med risikovurderingen** slik**:**

Risikovurderingen skal undersøke om ELV er godt nok sikret mot uønskede hendelser, og avdekke om det må implementeres nye tiltak som følge av endringer i infrastrukturen og fysisk sikring.

Beredskapskoordinator beskriver også hvor mye tid og ressurser risikovurderingen vil kreve, og lager en tidsplan.

Beredskapskoordinator får ledelsens godkjenning for gjennomføringen**,** samt en avklaring på at det er ledergruppen som skal beslutte hvilke tiltak som eventuelt skal implementeres basert på en anbefaling fra risikovurderingen.

Beskriv analyseobjektet

Etter forankringen hos ledelsen begynner Beredskapskoordinator arbeidet med å innhente all relevant informasjon om analyseobjektet, blant annet fra tidligere risikovurderinger og teknisk dokumentasjon. Dette kombineres til et kunnskapsgrunnlag.

Beredskapskoordinator beskriver avgrensingene for risikovurderingen, og visualiserer dette i en arkitekturtegning som viser hvilke systemer som kan påvirkes av endringen.

Beredskapskoordinator involverer relevante personer i dette arbeidet for å sørge for en god forståelse av det som skal risikovurderes.

Når kunnskapsgrunnlaget og beskrivelsen av avgrensingene er ferdig, gir risikoeier en kort oppdatering om eventuelle endringer i tidsplanen til ledelsen.

Elvheim har ikke definert sikkerhetsmål enda, og tar derfor ikke dette med i risikovurderingen.

Gjennomføring

Elvheim Kraft har god erfaring med å organisere risikovurderinger i arbeidsmøter hvor alle relevante personer deltar.

Beredskapskoordinator identifiserer hvilke personer som bør delta, og sender møteinnkalling til disse sammen med kunnskapsgrunnlaget.

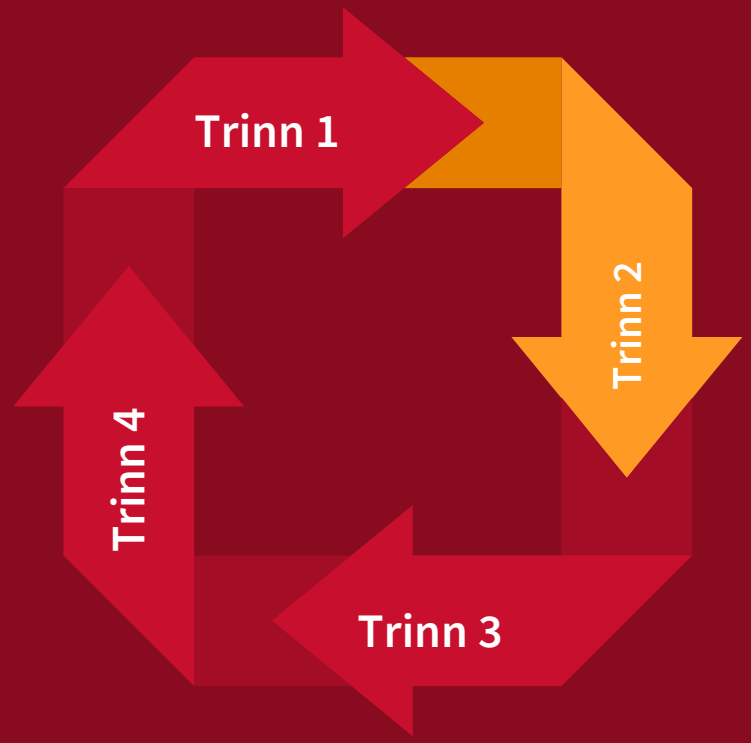
Beredskapskoordinator vurderer at det er nødvendig med to arbeidsmøter, hver på to timer:

Del 1: Utforme uønskede hendelser og vurdere sannsynlighet og konsekvens (trinn 2 og 3)

Del 2: Identifisere tiltak og utforme anbefaling (trinn 4).

Beredskapskoordinator ønsker å fasilitere risikovurderingen selv, og utpeker en dedikert person skal vil ta notater underveis.

Identifisere uønskede hendelser



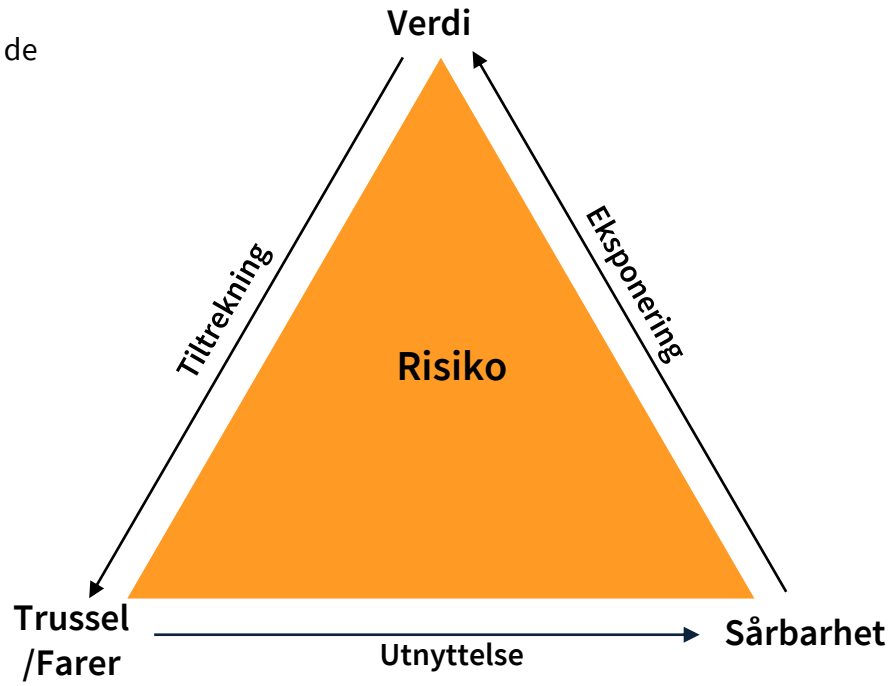
Trinn 2

Trinn 2 – Identifisere uønskede hendelser

Identifisering av uønskede hendelser

Formålet med dette trinnet er å identifisere uønskede hendelser som kan skade virksomhetens verdier. Dette gjøres ved å vise hvordan virksomhetens verdier kan bli påvirket av trusler, farer og sårbarheter. Ved å betrakte uønskede hendelser som et samspill mellom disse faktorene, kan virksomheten få en bedre forståelse av risikoene de står overfor.

Identifisering av uønskede hendelser gir grunnlaget for det neste trinnet i risikovurderingen, nemlig analysere risikoer.



Aktiviteter i trinn 2:

- Identifisering av verdier
- Identifisering av trusler og farer
- Identifisering av uønskede hendelser
- Identifisering av sårbarheter

De neste sidene beskriver hver av aktivitetene mer i detalj.

Trinn 2 – Identifisere uønskede hendelser

Identifisering av verdier

Her skal virksomheten identifisere verdier innenfor de avgrensingene som er satt for risikovurderingen. Kartleggingen gir viktig informasjon om hva en potensiell trusselaktør kan være ute etter og hvilke verdier som må beskyttes.

Virksomheten bør i tillegg rangere verdiene etter kritikalitet, slik at deltakerne i risikovurderingen har en felles forståelse for hvilke verdier som er de viktigste.

Oversikt over verdier er en viktig forutsetning for å kunne beskrive uønskede hendelser og hvordan man kan forhindre dem ved å innføre nødvendige tiltak.

Hvordan identifisere verdier

A Identifiser alle relevante verdier innenfor risikovurderingens avgrensning. Dette kan være systemer, komponenter, tilganger, informasjon osv.

B Prioriter verdiene etter kritikalitet.

C Kartlegg avhengigheter i verdiene. For eksempel kan et kritisk IT-system være avhengig av flere mindre viktige systemer for å fungere. Da bør også disse systemene prioriteres.

Verdier
Verdier er systemer, komponenter, informasjon, mennesker og andre elementer som trengs for at virksomheten skal fungere og utøve sine arbeidsoppgaver.

Trinn 2 – Identifisere uønskede hendelser

Trusler og farer

Når virksomhetens verdier er identifisert er neste aktivitet å undersøke mulige trusler og farer som er relevante for analyseobjektet. Dette kan oppnås ved å bruke åpne og sikre informasjonskilder. I kraftbransjen kan man finne informasjon om potensielle trusselaktører ved å bruke åpne rapporter som er utgitt av offentlige myndigheter som NSM og PST, og KraftCERT.

Trusselaktører kan beskrives ofte ut ifra motivasjon og ressurser. Nedenfor er noen eksempler på trusselaktører som virksomheten kan vurdere å benytte i sin risikovurdering:

- **Cyberkriminelle:** Enkeltpersoner eller mindre grupper som motiveres av en finansiell gevinst.
- **Statlige aktører:** Grupper som er velfinansierte, gjerne av en stat, og begår avanserte, målrettede angrep med formål om spionasje og finansiell gevinst.
- **Hackere:** Profesjonaliserte hackere som leies inn, gjerne av State-Nexus-grupper for å utføre angrep som løsepengeangrep.
- **«Hacktivister»:** Enkeltpersoner eller grupper med lite ressurser, men sterk motivasjon. De ønsker typisk å belyse sosiale eller politiske forhold.

Hvordan identifisere trusler og farer

A Gjennomgå eventuelle tidligere identifiserte trusler og farer, for eksempel fra risikovurderinger eller lignende.

B Innhent informasjon om trusselbildet ved bruk av åpne, sikre informasjonskilder.

C Lag en oversikt over relevante trusler og farer. Både tilsiktede og utilsiktede trusler bør inkluderes.

D Hold oversikten oppdatert, og del gjerne informasjon og erfaringer på tvers av virksomheten hvis relevant.

Farer
Forhold som kan føre til en uønsket hendelse
Trusler
Tilsiktet handling som kan føre til en uønsket hendelse

Trinn 2 – Identifisere uønskede hendelser

Identifisere uønskede hendelser

Uønskede hendelser gir tap av eller skade på verdier innenfor analyseobjektet. En uønsket hendelse kan være utilsiktet (for eksempel menneskelig feil) eller tilsiktet (for eksempel sabotasje). Både utilsiktede og tilsiktede hendelser kan gi stor skade på virksomheten.

Virksomheten bør definere uønskede hendelser basert på egne behov. En hendelse kan beskrives ved å vurdere hvordan farer og trusselaktører kan ha en negativ påvirkning på virksomhetens verdier, og hvilke konsekvensen den uønskede hendelsen kan få.

Ved å knytte farer og trusler til virksomhetens verdier, legges grunnlaget for beskrivelsene av uønskede hendelser. Generelle beskrivelser av uønskede hendelser kan, om hensiktsmessig, konkretiseres for å oppnå en mer detaljert beskrivelse og økt forståelse av hendelsesforløpet.

Til høyre er det definert seks generelle, uønskede hendelser . Det anbefales at virksomheten vurderer relevansen av å benytte disse i sine egne risikovurderinger.

I tillegg er det ofte nyttig med en «idedugnad» i arbeidsmøtet for å komme frem til potensielle uønskede hendelser, samt en detaljert gjennomgang av analyseobjektet (for eksempel arkitekturtegninger).

Eksempler på uønskede hendelser

A En ansatt gjør urettmessige endringer i et virksomhetskritisk system. Det er uklart om hendelsen er tilsiktet eller utilsiktet, men hendelsen fører til at noen systemer er utilgjengelige.

B En ekstern trusselaktør skaffer seg tilgang til virksomhetens kraftsensitive informasjon, og laster ned store mengder data på en ekstern harddisk.

C Strømbrudd fører til utfall av viktige produksjonssystemer. Dette fører til midlertidig stans i kraftproduksjonen.

D Virksomheten utsettes for et løsepengeangrep. Dette fører til en kompromittering av alle IT-systemer. All data er også utilgjengelig for virksomheten.

E En trusselaktør skaffer seg tilgang til IT-nettverket i virksomheten, og etter en tid lykkes med å traversere til OT-nettverket.

F En viktig driftsleverandør/leverandør går konkurs. Dette påvirker driften i virksomheten.

Uønsket hendelse
En hendelse som kan medføre tap eller skade på verdier

Trinn 2 – Identifisere uønskede hendelser

Identifisere sårbarheter

Når virksomheten har identifisert uønskede hendelser er neste aktivitet å identifisere sårbarheter knyttet til disse hendelsene. Sårbarhet er en manglende evne til å motstå uønskede hendelser, og er en svakhet som kan utnyttes av trusselaktører eller føre til utilsiktede hendelser. Sårbarhet kan sees på som det motsatte av robusthet.

For å vurdere sårbarhet bør virksomheten begynne med å undersøke kjente sårbarheter i analyseobjektet. Potensielle informasjonskilder er tidligere risikovurderinger, *Business Impact Assessments* (BIA), beredskapsplaner eller lignende. Deretter skal det vurderes om uønskede hendelsene kan oppstå som følge av en kjent sårbarhet og få uønskede konsekvenser.

Til slutt skal det vurderes om virksomheten har implementert barrierer som kan hindre at en uønsket hendelse oppstår, eller redusere konsekvensene (eksempelvis hvorvidt et OT-system kan gjenoppta sin funksjon etter en hendelse). Slike barrierer kan kartlegges ved å ta utgangspunkt i NSMs grunnprinsipper for å identifisere tiltak som virksomheten har implementert. Dette fordi tiltakene fra NSMs grunnprinsipper kan bidra til å gjøre virksomheter mer motstandsdyktige mot uønskede hendelser og slik redusere sårbarheter.

Hvordan identifisere sårbarheter

A Kartlegg og dokumenter kjente sårbarheter i analyseobjektet. Informasjonskilder kan være tidligere risikovurderinger, BIA, beredskapsplaner og lignende.

B Vurder om de uønskede hendelsene som har blitt identifisert tidligere kan oppstå som følge av en kjent sårbarhet, og hvilke konsekvenser det kan få. For eksempel om en trusselaktør kan utnytte en sårbarhet for å påføre virksomheten skader.

C Identifiser barrierer som er implementert i virksomheten og som kan redusere sannsynligheten for at en hendelse skjer, eller begrense konsekvensen. Ta gjerne utgangspunkt i NSMs grunnprinsipper for å identifisere tiltak som virksomheten har implementert.

Sårbarhet
Manglende evne til å motstå uønskede hendelser. En svakhet kan utnyttes av trusselaktører.

Elvheim kraft gjennomfører Trinn 2

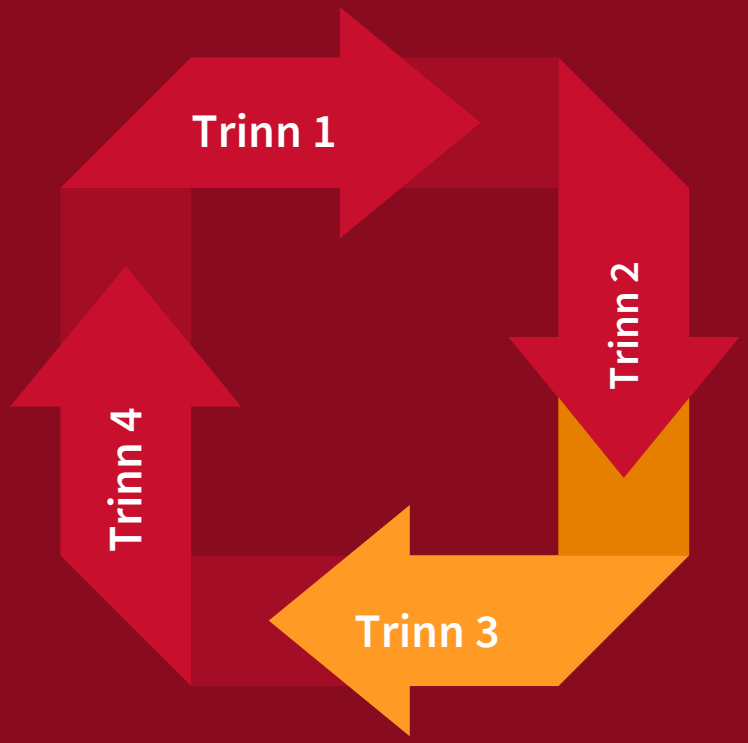
Elvheim Kraft gjennomfører det første av to arbeidsmøter. Her skal de identifisere verdier, trusler og farer, uønskede hendelser og sårbarheter.

Elvheim kraft dokumenterer følgende i arbeidsmøtet:

Verdier	Trusler og farer	Uønskede hendelser	Sårbarheter
• IT-systemet *ELV* (kritisk) • OT-sensorer (mindre kritisk) • Dataflyten mellom OT-sensorer og ELV (kritisk) • Kraftsensitiv informasjon i ELV (kritisk) • Administratortilgang i ELV (mindre kritisk) • IT-systemet *HEIM* (mindre kritisk) Elvheim registrerer i tillegg at *ELV* er har en avhengighet til dataflyten fra OT-sensorene. Dermed ansees også OT-sensorene som kritiske i denne sammenhengen, selv om sensorene i seg selv ikke er kritiske for virksomheten. Det er ingen andre kjente avhengigheter blant de andre verdiene.	• Cyberkriminelle (tilsiktet) • Hacktivister (tilsiktet) • Strømbrudd (utilsiktet) • Menneskelig feil (utilsiktet) **Informasjonskilder:** For informasjonskilder bruker Elvheim tidligere risikovurderinger og NSMs åpne risikovurdering (NSM Risiko)	• En cyberkriminell skaffer seg tilgang til kraftsensitiv informasjon i ELV, og laster ned store mengder data for å selge videre på «dark web». • En hacktivist skaffer seg tilgang til ELV via en stasjons-PC og gjør urettmessige endringer i *ELV* med mål om å forårsake skade. Dette fører til at systemet er utilgjengelig. • Strømbrudd fører til utfall av OT-sensorer som ELV er avhengig av. • En ansatt med administratortilgang gjør urettmessige endringer i *ELV* ved en feiltakelse. Dette fører til at systemet er utilgjengelig.	**Kjente sårbarheter i analyseobjektet:** • Manglende tilgangsstyring til kraftsensitiv informasjon i *ELV* • Mange ansatte har admin-tilgang til *ELV* • Manglende sikring av dataflyten mellom *ELV* og OT-sensorene • Manglende testing av gjenoppretting av fra backup **Barrierer:** Elvheim har implementert flere av NSMs grunnprinsipper som barrierer, blant annet: • Overvåking av IKT-systemer • Planverk for hendelseshåndtering • Beskyttelse av virksomhetens nettverk • Aktiver brannmur på klienter og servere • Fysisk sikring av rom med stasjons-PC

Analysere risiko

Trinn 3

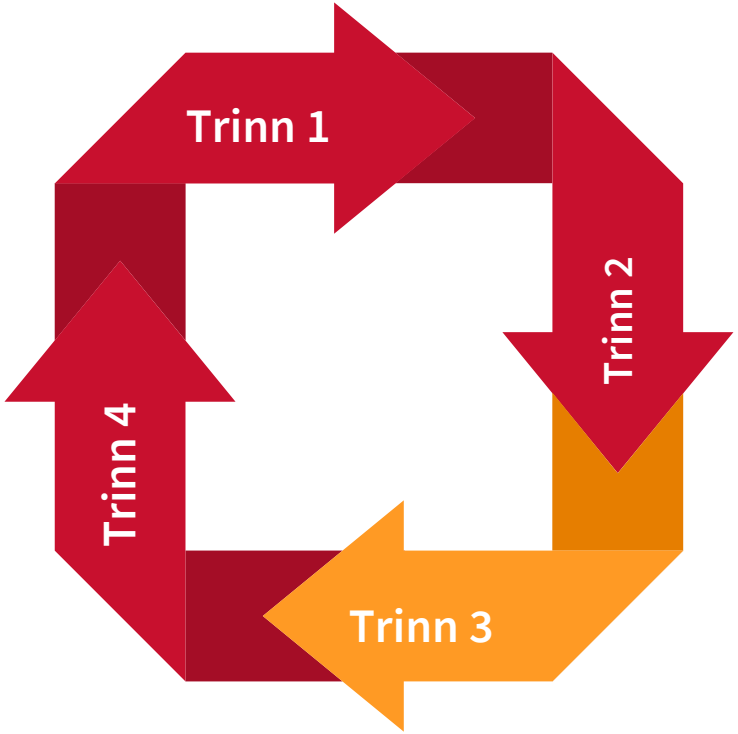


Trinn 3 – Analysere risiko

Konsekvens, sannsynlighet og usikkerhet

Formålet med det tredje trinnet i risikovurderingen er å gjøre en analyse av de uønskede hendelsene i trinn 2 for å se nærmere på hvilke konsekvenser hendelsene kan få for virksomheten, og hva som er sannsynligheten for at hendelsen inntreffer. Her kan man også gjøre en vurdering av usikkerhet.

Veilederen beskriver hvordan virksomheten kan gå frem for å vurdere sannsynlighet, konsekvens og usikkerhet, uavhengig av hvilke matriser eller kriterier som legges til grunn for vurderingen.



Aktiviteter i trinn 3:

- Vurdere konsekvenser
- Vurdere sannsynlighet og usikkerhet

De neste sidene beskriver hver av aktivitetene mer i detalj.

Analysere risiko

Vurdere konsekvens ved uønskede hendelser

I dette trinnet skal virksomheten vurdere konsekvens for hver av de uønskede hendelsene som ble identifisert i trinn 2.

Hvorfor er det viktig?

I en vurdering av konsekvens forsøker man å beskrive hvilken effekt den uønskede hendelsen kan få for verdiene i analyseobjektet og for virksomheten. Vurderingen av konsekvens er en subjektiv vurdering som gjerne gjøres av deltakerne i et arbeidsmøte. Konsekvens kan beskrives på ulike måter; ved tallverdier, gjennom ord som «lav», «moderat» eller «kritisk», eller visuelt.

Hvis mulig, er det ofte en fordel å benytte de samme matrisene som brukes ellers i virksomheten. På den måten kan man oppnå at risikovurderinger av IT og OT-sikkerhet blir en integrert del av risikostyringen i virksomheten. Det gjør også at ledelsen kan sammenligne risikoer på tvers av ulike fagområder.

Virksomheten kan benytte matrisene som er inkludert i veilederen hvis dette vurderes som relevant.

Hvordan vurdere konsekvens

A Vurder hvor stor skade en uønsket hendelse kan få for analyseobjektet. Her bør man inkludere «worst-case scenarioer» som kan føre til ekstraordinære situasjoner.

B Vurder om det er flere mulige utfall av en uønsket hendelse, og som kan ha ulike konsekvenser.

C Hvis det er nyttig for virksomheten, vurder hvilken type konsekvens en uønsket hendelse kan få. Dette kan være skade for liv og helse, økonomiske konsekvenser, eller annet.

D Hvis virksomheten har definert sine sikkerhetsmål, kan man også vurdere om disse er nådd.

Link til matriser i veilederen:

- Matriser

Analysere risiko

Vurdere sannsynligheten for uønskede hendelser

Her skal det gjøres en vurdering av sannsynligheten for hver av de uønskede hendelsene som ble identifisert i trinn 2.

Hvorfor er det viktig?

Med sannsynlighet for en hendelse forsøker man å beskrive hvor trolig det er at den uønskede hendelsen vil inntreffe. Det er alltid usikkerhet knyttet til om en hendelse vil inntreffe, og denne usikkerheten kan uttrykkes gjennom sannsynlighet.

En sannsynlighetsvurdering kan gjøres på ulike måter, og med ulike vurderingskriterier. Hvis mulig, er det ofte en fordel å benytte seg av de samme matrisene som brukes ellers i virksomheten. På den måten kan man oppnå at risikovurderinger av IT og OT-sikkerhet blir en integrert del av risikostyringen i virksomheten. Det gjør også at ledelsen kan sammenligne risikoer på tvers av ulike fagområder.

Link til matriser i veilederen:

- Matriser

Hvordan vurdere sannsynlighet og usikkerhet

A Vurder hvor stor sjanse det er for at hendelsen skjer. Her kan man eksempelvis bruke historiske data, feilstatistikk og informasjon i de åpne trussel- og risikovurderingene.

B Vurder hvilke kontroller virksomheten har implementert som kan redusere sannsynligheten for en uønsket hendelse. Dette kan være NSMs grunnprinsipper for IKT-sikkerhet eller andre tiltak.

C Vurder hvor effektive kontrollene er for å hindre en trusselaktør i å utnytte en kjent sårbarhet. Eksempelvis, drøft hvor vanskelig det er for en trusselaktør (både intern og ekstern) å omgå kontrollene.

D For usikkerhet: Vurder hvor godt kunnskapsgrunnlag virksomheten har for å kunne estimere sannsynligheten for om en uønsket hendelse inntreffer. Dette kan eksempelvis være i hvor stor grad har man testet effektiviteten av kontrollene som man har implementert, eller hvor pålitelig er historiske data som virksomheten baserer sannsynligheten på.

Analysere risiko

Konsekvens- og sannsynlighetsmatriser

Virksomheten må selv vurdere hvilke matriser som skal legges til grunn i vurderingen av konsekvens og sannsynlighet.

Matrisene på denne siden er utarbeidet på bakgrunn av prinsipper som fremheves i NS5814, og kan være et godt alternativ for virksomheter som ikke har andre egnede matriser som brukes av virksomheten.

NS 5814:2021 om konsekvenser:
Effekten av barrierer mot følgehendelser og konsekvenser skal inngå i vurderingen

NS 5814:2021 om sannsynlighet:
Sannsynlighet kan beskrives verbalt, med tall eller med definerte kategorier.

Konsekvens	Sannsynlighet		Ubetydelig 1	Lav 2	Moderat 3	Høy 4	Svært høy 5
	Ubetydelig skade	1	1	2	3	4	5
	Minimal skade	2	2	4	6	8	10
	Moderat skade	3	3	6	9	12	15
	Betydelig skade	4	4	8	12	16	20
	Kritisk skade	5	5	10	15	20	25

Konsekvens	Kontroller/kompenserende tiltak prioritert i henhold til konsekvens
Ubetydelig skade	Ingen kontroller eller kompenserende tiltak er nødvendige
Minimal skade	Kontroller og/eller kompenserende tiltak kan vurderes og prioriteres for implementering
Moderat skade	Kontroller og/eller implementerende tiltak bør vurderes og prioriteres for implementering
Betydelig skade	Kontroller og/eller kompenserende tiltak skal vurderes om det bør implementeres
Kritisk skade	Kontroller og/eller kompenserende tiltak skal implementeres

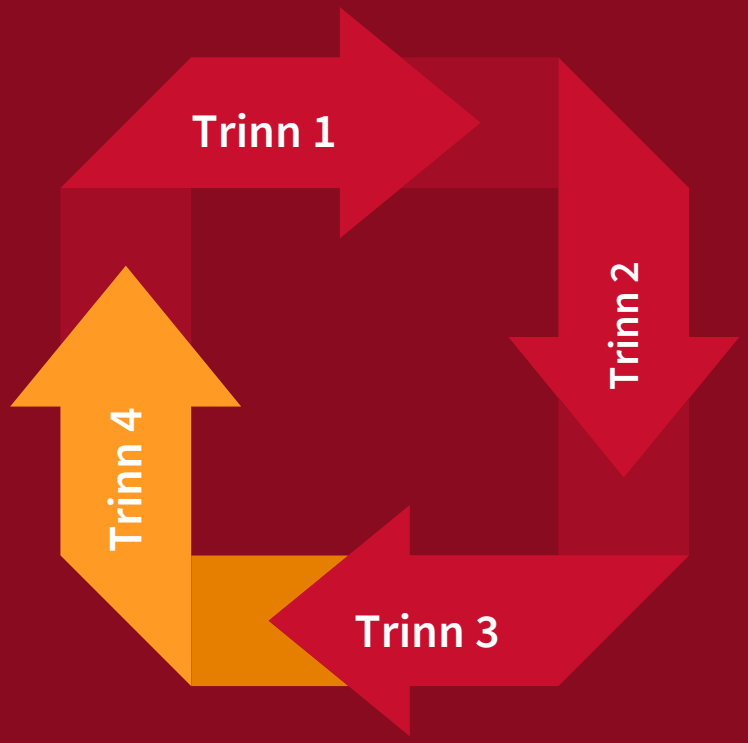
Elvheim kraft gjennomfører Trinn 3

Elvheim Kraft gjennomfører det siste arbeidsmøtet. Her vurderer de konsekvens, sannsynlighet og usikkerhet for hver av hendelsene, samt anbefale tiltak. Elvheim bruker matrisene for sannsynlighet og konsekvens fra trinn 3 i veilederen.

#	Uønskede hendelser	Konsekvens	Sannsynlighet	Usikkerhet
A	En cyberkriminell skaffer seg tilgang til kraftsensitiv informasjon i ELV, og laster ned store mengder data for å selge videre på «dark web».	Hendelsen kan føre til kraftsensitiv informasjon på avveie, og dermed gi **betydelig** skade for virksomheten.	Elvheim kjenner ikke til at hendelsen har skjedd tidligere, og det er implementert kontroller som kryptering og sikkerhetsovervåking. Dermed vurderes sannsynligheten som **lav**.	Elvheim har begrenset med historisk data for å vurdere usikkerheten, og det er over ett år siden kontrollene som skal fungere som redusere sannsynligheten har blitt testet. Det er derfor **moderat** usikkerhet.
B	En hacktivist skaffer seg tilgang til ELV via en stasjons-PC og gjør urettmessige endringer i *ELV* med mål om å forårsake skade. Dette fører til at systemet er utilgjengelig.	Hendelsen kan føre til at virksomheten ikke har tilgang til det virksomhetskritiske systemet *ELV*. I tillegg kan en ekstern aktør kan forårsake ytterligere skade. Det er etablert beredskapsplaner for ELV, men konsekvensen vurderes likevel til **kritisk skade.**	Elvheim kjenner ikke til at hendelsen har skjedd tidligere, og har implementert kontroller som sikkerhetsovervåking, beskyttelse av nettverket, og fysisk sikring av stasjons-PC'en. Sannsynligheten vurderes derfor til **lav.**	Elvheim har begrenset med historisk data for å vurdere usikkerheten, og det er over ett år siden kontrollene som skal fungere som redusere sannsynligheten har blitt testet. Det er derfor **moderat** usikkerhet.
C	Strømbrudd fører til utfall av OT-sensorer som ELV er avhengig av.	Hendelsen kan føre til at virksomheten ikke får oppdaterte produksjonsdata fra *ELV,* men dette kan innhentes manuelt. Derfor er konsekvensen **minimal skade.**	Det er mye dårlig vær i Elvheim, og feilstatistikken viser utfall flere ganger i året. Det er derfor **høy** sannsynlighet for at hendelsen kan inntreffe.	På grunn av godt kunnskapsgrunnlag fra feilstatistikken, vurderes usikkerheten til **lav.**
D	En ansatt med administratortilgang gjør urettmessige endringer i *ELV* ved en feiltakelse. Dette fører til at systemet er utilgjengelig.	Hendelsen kan føre til at virksomheten ikke har tilgang til det virksomhetskritiske systemet *ELV.* En uheldig ansatt vil raskt kunne varsle om at *ELV* utilgjengelig, og derfor vurderes konsekvensen til **moderat skade.**	Det er mange ansatte med administratortilgang, og dette øker sannsynligheten for feil. Den vurderes til **moderat.**	På grunn av godt kunnskapsgrunnlag fra feilstatistikken, vurderes usikkerheten til **lav.**

Håndtere risiko

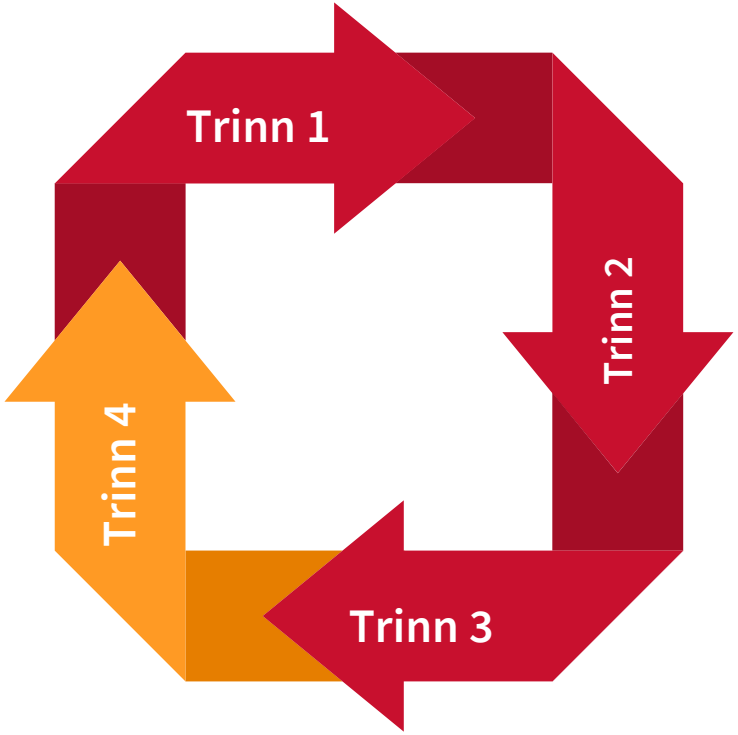
Trinn 4



Trinn 4 – Håndtere risiko

Håndtere risiko

Formålet med det fjerde trinnet er å håndtere risikoene fra trinn 3 gjennom å identifisere risikoreduserende tiltak, og utforme en anbefaling og aksjonsplan som ledelsen skal ta stilling til. Til slutt beslutter virksomhetens ledelse hvilke tiltak som skal implementeres, og hvilke risikoer som skal håndteres på en annen måte.



Aktiviteter i trinn 4:

- Identifisere tiltak
- Utforme anbefaling og tiltaksplan

De neste sidene beskriver hver av aktivitetene mer i detalj.

Håndtere risiko

Identifisere tiltak

I dette trinnet skal virksomheten identifisere risikoreduserende tiltak for de uønskede hendelsene. Det er viktig å fokusere innsatsen der risikoen er størst, og man oppnår best effekt av risikoreduserende tiltak.

Hvorfor er det viktig?

Dersom en uønsket hendelse kan føre til betydelig skade for virksomheten, bør det implementeres tiltak som enten kan redusere sannsynligheten for at en hendelse inntreffer, eller redusere konsekvensen av hendelsen. De konsekvensreduserende tiltakene er en viktig del av beredskapen.

Hvilke risikoer som skal ha tiltak avhenger av virksomhetens kriterier, men et vanlig nivå er:

- Risikoer som kan føre til kritisk eller betydelig skade («rød/oransje risikoer») skal ha risikoreduserende tiltak
- Risikoer som kan føre til moderat eller minimal skade («gule risikoer») bør vurderes om tiltak er nødvendig
- Risikoer som kan føre til ubetydelig skade («grønne risikoer» trenger typisk ikke tiltak.

Hvordan identifisere tiltak

A Identifiser tiltak som allerede er på plass, og vurder hvor effektivt disse beskytter verdiene innenfor analyseobjektet. Eksempler på eksisterende tiltak er NSMs grunnprinsipper eller tiltak fra andre risikovurderinger.

B Identifiser nye tiltak der hvor risikoen trengs å reduseres. Her er det viktig å fokusere på tiltak som beskytter de viktigste verdiene. Det bør vurderes både tekniske, fysiske, menneskelige og organisatoriske tiltak.

C Ranger og prioriter tiltakene slik at det kommer tydelig frem hvilke tiltak som er viktigst. Dette er de som reduserer risikoen mest. Her kan man også gjøre en kost-nytte vurdering, hvor man ser på effekten av tiltaket opp mot kostnaden av å implementere det.

D Vurder om beredskapsplaner må oppdateres som følge av funn i risikovurderingen. Dette kan eksempelvis være at man må gjøre endringer basert på ny kunnskap om potensielle konsekvenser ved en uønsket hendelse.

Håndtere risiko

Utforme anbefaling og tiltaksplan

I dette trinnet skal det dokumentasjonen fra risikovurderingen sammenstilles til en anbefaling til ledelsen. Det bør også utformes en tiltaksplan.

Hvorfor er det viktig?

Til sist i risikovurderingen skal ledelsen beslutte hvordan risikoen skal håndteres. Det er viktig at ledelsen mottar et godt kunnskapsgrunnlag om hvilke uønskede hendelser som er identifisert, og hvordan disse kan skade virksomheten. Vurderinger av sannsynlighet og konsekvens bør også komme tydelig frem. En risikomatrise som visualiserer resultatet av risikovurderingen kan være et nyttig virkemiddel for å kommunisere risiko til ledelsen.

I kunnskapsgrunnlaget til ledelsen bør det også utformes en anbefaling til håndtering av risikoene. Dette kan eksempelvis være å implementere prioriterte tiltak, eller å foreta flere undersøkelser for å forstå risikoen bedre – og dermed redusere usikkerheten. Til sist beslutter virksomhetens ledelse hvilke tiltak som skal implementeres.

Basert på ledelsens beslutning bør det utformes en tiltaksplan som beskriver hva som skal gjøres, av hvem, og en frist for gjennomføringen.

Hvordan utforme anbefaling og tiltaksplan

A Sammenstill dokumentasjonen fra risikovurderingen slik at det blir et godt kunnskapsgrunnlag for ledelsen. Det bør komme tydelig frem hvilke risikoer som er identifisert, og vurderingene av sannsynlighet og konsekvens.

B Utform en anbefaling til hvordan risikoene bør håndteres, eksempelvis ved å implementere tiltakene som er identifisert og prioritert som en del av risikovurderingen.

C Presentere resultatet av risikovurderingen og anbefalingen til virksomhetens ledelse for beslutning.

D Ledelsen beslutter hvilke tiltak som skal implementeres.

E Utform en tiltaksplan som beskriver hvem som er ansvarlige for gjennomføring av tiltaket, og en frist for gjennomføringen.

F Følge opp at tiltaksplanen blir implementert og lukket i henhold til tidsplanen.

Elvheim kraft gjennomfører Trinn 4 (del 1)

Elvheim Kraft gjennomfører det siste arbeidsmøtet. Her vurderer de konsekvens, sannsynlighet og usikkerhet for hver av hendelsene, samt anbefale tiltak. Elvheim bruker matrisene for sannsynlighet og konsekvens fra trinn 3 i veilederen.

Beredskapskoordinator sammenstiller risikoene i en matrise for enklere oversikt:

	Sannsynlighet		Ubetydelig 1	Lav 2	Moderat 3	Høy 4	Svært høy 5
Konsekvens	Ubetydelig skade	1					
	Minimal skade	2				C	
	Moderat skade	3			D		
	Betydelig skade	4		A			
	Kritisk skade	5		B			

I følge matrisen som Elvheim bruker, skal alle «mørkerøde» risikoer ha tiltak. For «lyserøde» risikoer skal det vurderes om tiltak bør implementeres.

For «oransje» risikoer bør det vurderes om tiltak skal implementeres.

Elvheim kraft gjennomfører Trinn 4 (del 2)

Elvheim Kraft identifiserer tiltak i henhold til kravene i matrisen, og anbefaler en prioritet for tiltakene. Disse skal aksepteres av virksomhetens ledelse før implementering.

Følgende tiltaksplan og anbefaling presenteres for ledelsen for beslutning:

#	Uønskede hendelser	Anbefalt tiltak	Anbefalt prioritet	Ansvarlig	Frist for gjennomføring
A	En cyberkriminell skaffer seg tilgang til kraftsensitiv informasjon i ELV, og laster ned store mengder data for å selge videre på «dark web».	• Implementere tilgangsstyring for kraftsensitiv informasjon i IT-systemet *ELV*	Høy prioritet	Steve C	31.12.202x
B	En hacktivist skaffer seg tilgang til ELV via en stasjons-PC og gjør urettmessige endringer i *ELV* med mål om å forårsake skade. Dette fører til at systemet er utilgjengelig.	• Sikre dataflyt mellom OT-sensorer og ELV for å hindre en trusselaktør i å traversere til OT-nettet • Installere kamera ved inngangen til stasjonsanlegg	Høy prioritet	Embla J	01.02.202x
C	Strømbrudd fører til utfall av OT-sensorer som ELV er avhengig av.	Trenger ikke tiltak.	N/A	N/A	N/A
D	En ansatt med administratortilgang gjør urettmessige endringer i *ELV* ved en feiltakelse. Dette fører til at systemet er utilgjengelig.	• Begrense antall ansatte med admistratortilganger.	Lav prioritet	Trine G	15.06.202x

Ledelsen beslutter at tiltakene med høy prioritet skal implementeres, og godkjenner både risikovurderingen og tiltaksplanen.

Videre arbeid

Hvordan bruke en risikovurdering i videre arbeid

Videre arbeid

Proaktiv bruk av risikovurderinger

Virksomhetene bør ha en proaktiv oppfølging av risikovurderingene. Resultatet av risikovurderingene er nyttige i videre arbeid og bør ikke legges i en skuff, men holdes relevant og oppdatert.

Risikovurderingen gir grunnlag for systematisk sikkerhetsarbeid. Systematisk sikkerhetsarbeid handler om å ha en kontinuerlig prosess som styrker og oppdaterer virksomhetens sikkerhet.

Risikovurderingen kan altså brukes som aktivt utgangspunkt for videre arbeid med informasjonssikkerhet og digital sikkerhet. For eksempel kan resultatet brukes til å:

- ✓ Gjennomføre beredskapsøvelser basert på de uønskede hendelsene
- ✓ Oppdatere beredskapsplaner, sjekklister og styringsdokumenter som følge av ny kunnskap om mulige konsekvenser ved en hendelse
- ✓ Prioriteringer i sikkerhetsarbeidet, eksempelvis utbedre sårbarheter som inngår i mange risikoer.
- ✓ Verifisere at barrierene som er identifisert i risikovurderingen fungerer etter hensikten. Dette kan testes ved en penetrasjonstest eller lignende.
- ✓ Definere nye sikkerhetsmål eller oppdatere sikkerhetsstrategi
- ✓ Planlegge for fremtidig vedlikehold av IT- og OT-infrastruktur

Særlig viktig i omgivelser med raske endringer

Illustrasjonen på neste side viser hvordan økt integrasjon mellom IT og OT åpner flere dører for trusselaktører. Digitalisering har og vil fortsette å ha en tilnærmet eksponentiell vekst. Dette gjelder også for kraftbransjen.

Derfor er det spesielt viktig at sikkerhetsarbeidet prioriteres og at risikovurderinger holdes oppdatert. Risikovurdering er en kontinuerlig prosess og verdien av vurderingen ligger i det videre arbeidet.

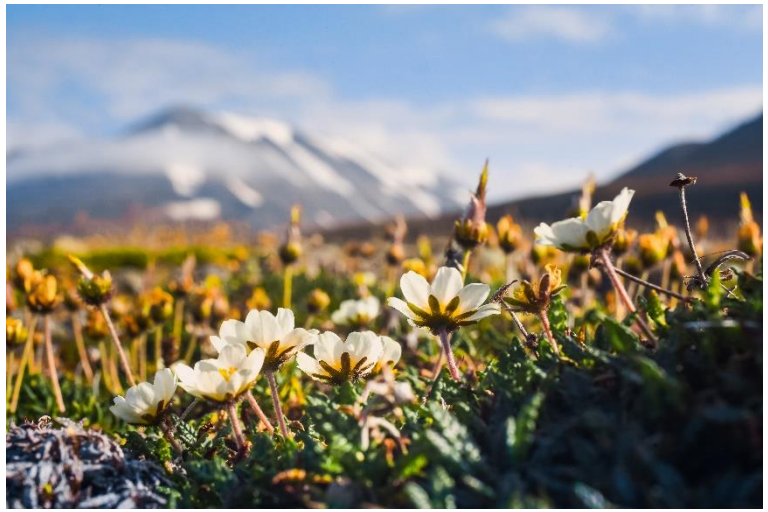
Tiltakene som er identifisert bør jevnlig testes for etterlevelse. Identifiserte tiltak som ikke implementeres, eller er ineffektive fordi de ikke blir inkludert i virksomhetens strategi vil ikke fungere som barrierer for trusselaktører. I verste fall gir det virksomhetene et falskt inntrykk av sikkerhet og realiteten er at man er enda mer sårbar enn tidligere.

Elvheim kraft sitt videre arbeid

I tiden etter risikovurderingen bruker Elvheim kraft funnene aktivt til å øke modenheten sin i sikkerhetsarbeidet.

Konkret gjør Elvheim kraft følgende aktiviteter:

- ✓ Sørger for at tiltaksplanen blir fulgt opp innen tidsfristen
- ✓ Oppdaterer beredskapsplaner og sjekklister som følge av ny kunnskap om potensielle uønskede hendelser og konsekvensen av disse.
- ✓ Definerer sikkerhetsmål for virksomheten
- ✓ Tester at kontroller som ble identifisert som barrierer mot kjente sårbarheter i risikovurderingen fungerer etter hensikten, blant annet for å verifisere at *ELV* kan gjenopprettes fra backup og at sikkerhetsovervåkingen fanger opp de uønskede hendelsene som ble identifisert.
- ✓ Iverksetter et større initiativ for å bedre identitets- og tilgangsstyringen i virksomheten for å skaffe bedre oversikt over tilgangsrettigheter og administratorrettigheter.



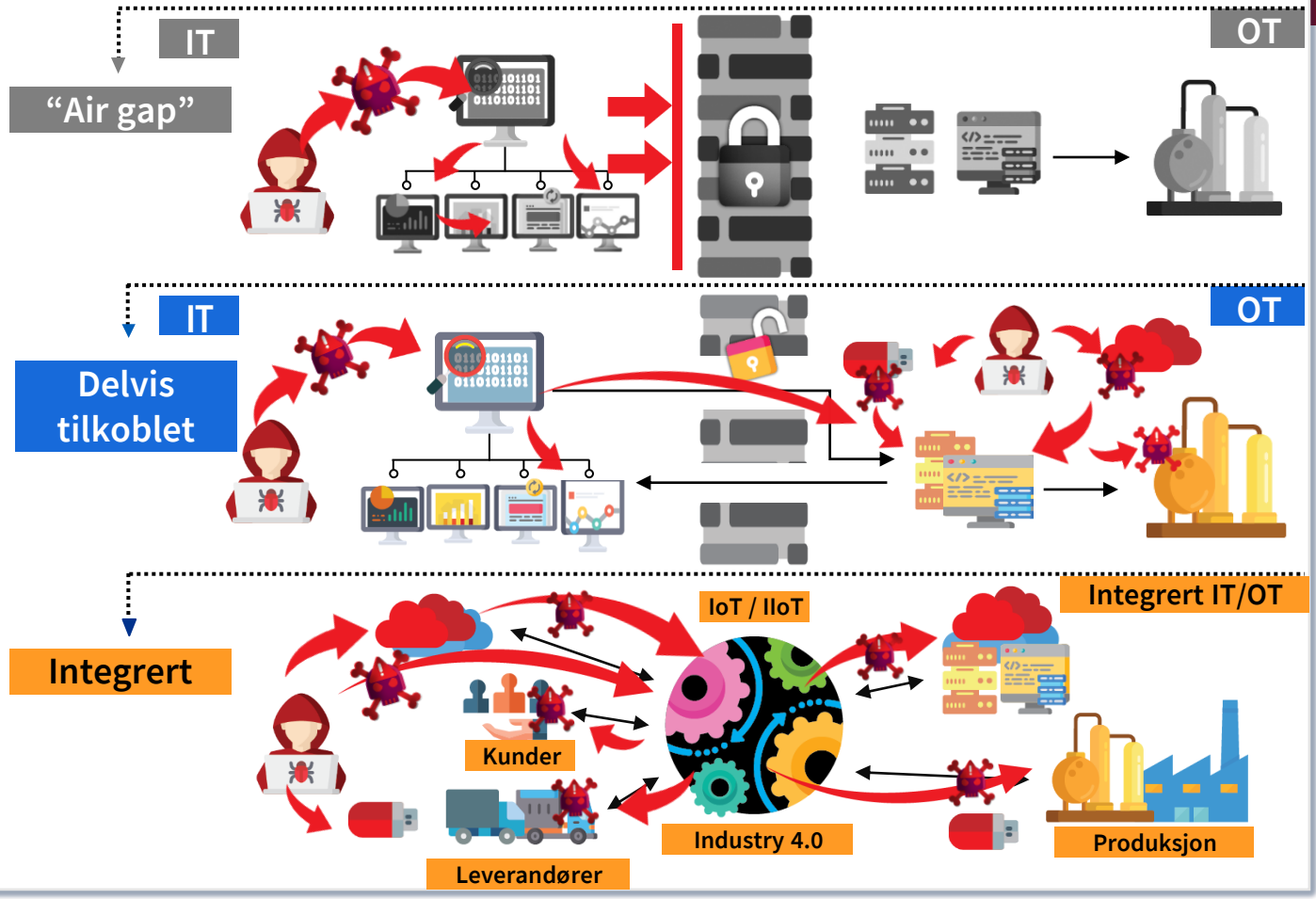
Videre arbeid

Følg med på utviklingen

Denne figuren illustrerer hvordan økt integrering mellom IT og OT gjør angrepsflaten større. Når man åpner opp mellom IT og OT, åpner man også mulighetene for trusselaktører. Der tilgang tidligere var utilgjengelig, finnes det flere veier inn.

I dag er de fleste virksomheter delvis tilkoblet, men i fremtiden vil man nærme seg full integrasjon. Med utviklinger som industri 4.0, bruk av maskinlæring og kunstig intelligens vil også sammenkoblingene bli enda mer komplekse. Dette gjør det vanskeligere å holde oversikt over trusler og sårbarheter.

Dette understreker viktigheten av at de to domene arbeider sammen i sikkerhetsarbeidet og i risikovurderinger, samt at det bør bygges kompetanse på tvers av IT og OT.



Videre arbeid

I dybden på risiko og IKT-sikkerhet

Det finnes flere gode sikkerhetsstandarder for virksomheter som ønsker å gå dypere inn i risikovurderinger og sikkerhetsarbeidet, for eksempel:

- ISO/IEC 27001 – Ledelsessystemer for informasjonssikkerhet
- ISO/IEC 27002 – Informasjonssikkerhetstiltak
- ISO/IEC 27005 – Guidance on managing information security risks
- ISO 31000 – Risk management
- NIST Cyber Security Framework
- IEC 62443 – Gruppe av internasjonale standarder for operasjonell cybersikkerhet

Annet nyttig støttemateriell er:

- NVEs veiledning i sikring av AMS, med referanser til NSMs grunnprinsipper
- SINTEF og petroleumstilsynets rapport om NSMs grunnprinsipper for OT
- Mnemonics kobling mellom grunnprinsippene og NIST Cyber Security Framework
- DNV (Det Norske Veritas) og forsikringsselskapet Gjensidiges verktøy for Cyber Modenhetsvurdering, der virksomheter kan måle sin sikkerhet opp mot NSMs grunnprinsipper.

Nyttige kilder til informasjon om trusselbildet

Det finnes mange offentlige, gode publikasjoner virksomhetene kan lese for å få en oversikt og holde seg oppdatert på dagens trusselbilde.
For eksempel publiseres årlig NSMs Nasjonalt digitalt risikobilde og ENISAs Threat Landscape. Andre kilder til relevant informasjon er:

- Offentlige myndigheters publikasjoner (NSM, E-tjenesten, PST)
- Internasjonale organisasjoners publikasjoner (EU, ENISA, NATO)
- Bransjeorganisasjoners publikasjoner (KraftCERT)
- Store konsulentselskapers, forskningsorganisasjoners og sikkerhetsleverandørers offentlige publikasjoner (SINTEF)
- Virksomhetens interne registreringer av sikkerhetsbrudd og sikkerhetstruende hendelser
- Mediebildet