

Kapittel 14:

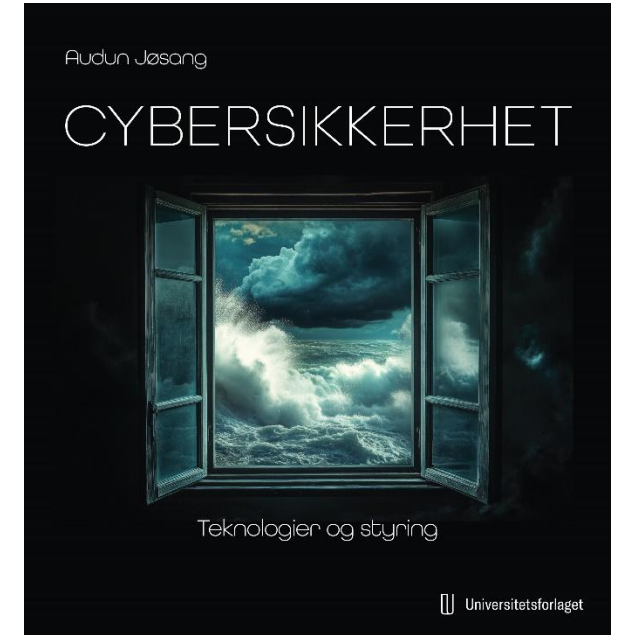
Beredskap og hendelseshåndtering

Cybersikkerhet: Teknologier og styring

Audun Jøsang

3. utg. 2025

Universitetsforlaget



Oversikt: Beredskap og hendelsesrespons

- a. Samfunnets kritiske funksjoner
- b. Beredskap
- c. Hendelsesrespons



Nasjonalt beredskapssystem

- Nasjonalt beredskapssystem består av
 - Sivilt beredskapssystem
 - Beredskapssystem for forsvarssektoren
- Dette systemet er bygd opp etter samme struktur som NATO Crisis Response System.
 - Et sentralt element i dette systemet er NATO Crisis Management Process.
- Det nasjonale beredskapssystemet gir grunnlag for underliggende beredskapsplaner for alvorlige kriser i fredstid, ved sikkerhetspolitiske kriser og i væpnede konflikter.
 - Nasjonal helseberedskapsplan er et eksempel på en underliggende plan.

Samfunnets kritiske funksjoner



Befolkningens og samfunnets grunnleggende behov

Vern om befolkningens sikkerhet og trygghet

Kategorier av kritiske samfunnsfunksjoner

Styringsevne og suverenitet

Territoriell og styringsmessig integritet. Opprettholde styringsaktiviteter og evne til å møte ekstraordinære Situasjoner.

Befolkningens sikkerhet

Vern mot død, fysisk skade eller sykdom, tap av demokratiske rettigheter og personlig integritet, tap av eller skade på livsmiljøet, eiendom, eller materielle verdier.

Samfunnets funksjonalitet

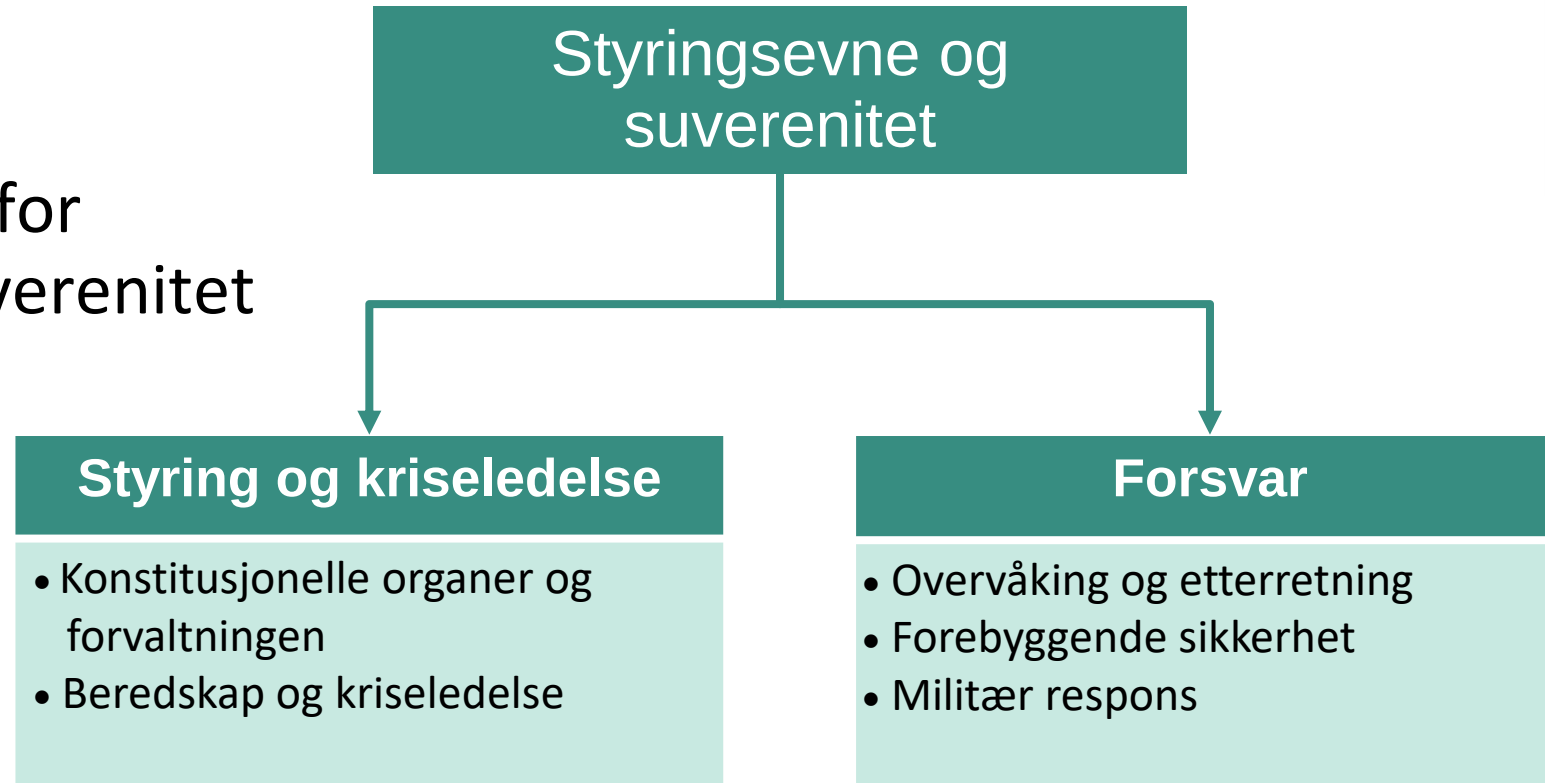
Kontinuitet i forsyninger og infrastrukturbaserte tjenester.

Samfunnets kritiske funksjoner, DSB, 2016

Styringsevne og suverenitet



Kritiske elementer for styringsevne og suverenitet



Samfunnets kritiske funksjoner, DSB, 2016

Befolkningens sikkerhet

Kritiske elementer
for befolkningens
sikkerhet

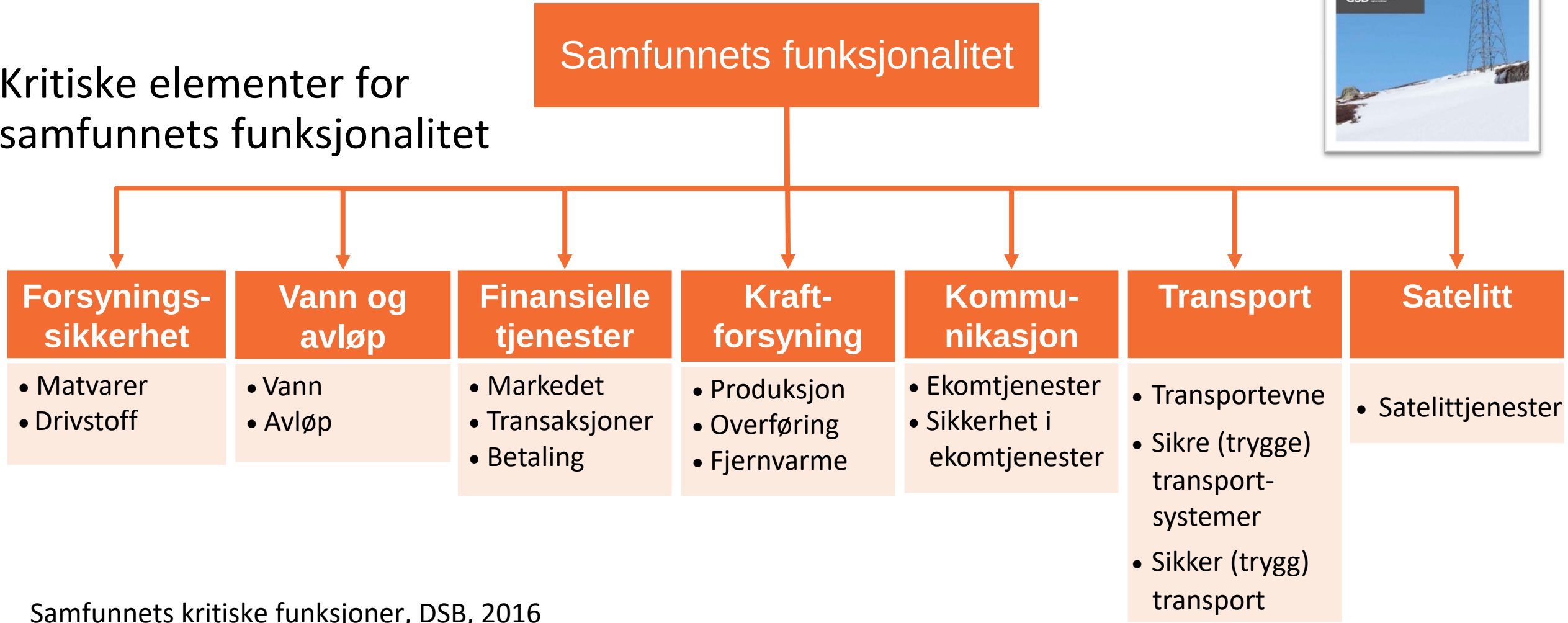


Samfunnets kritiske funksjoner, DSB, 2016

Samfunnets funksjonalitet



Kritiske elementer for samfunnets funksjonalitet

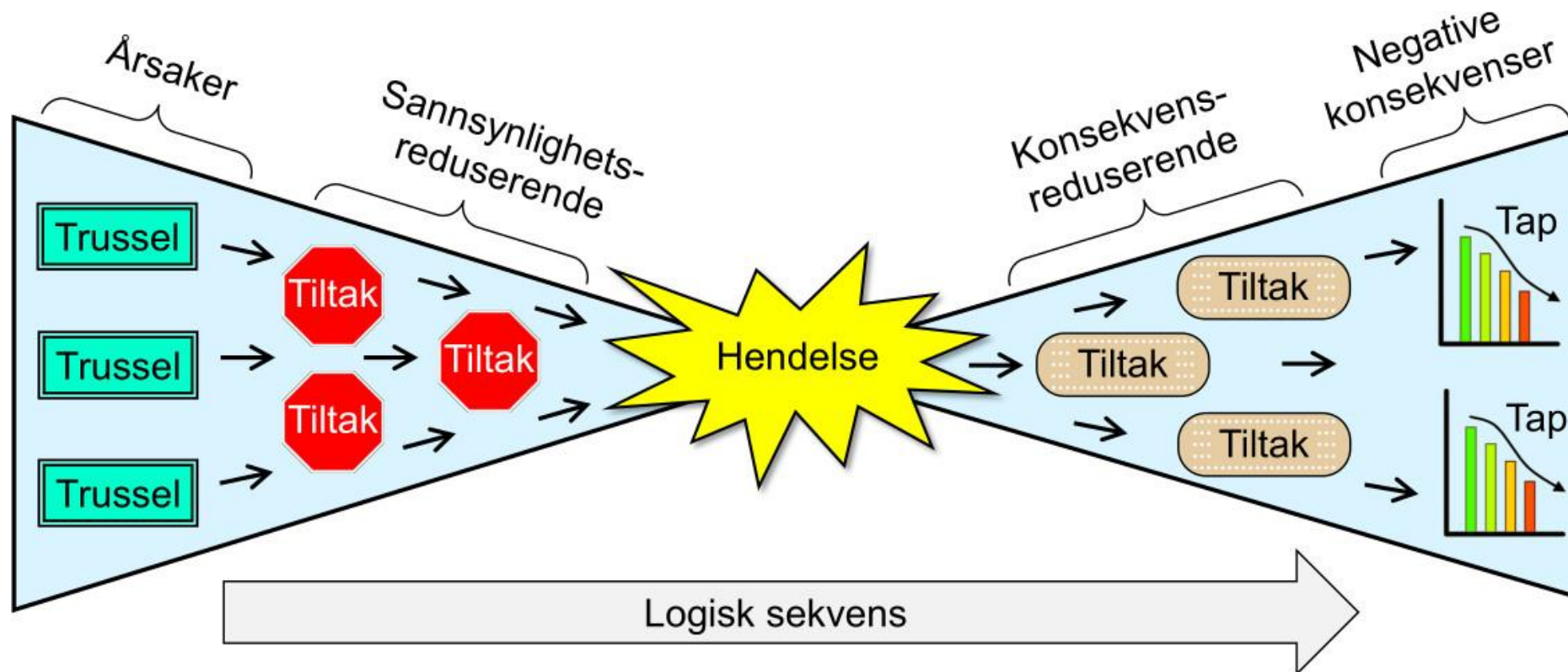


Samfunnets kritiske funksjoner, DSB, 2016

Beredskap

- Beredskap betyr å være forberedt på å aktivere *konsekvensreduserende tiltak* i tilfelle skadelige hendelser inntreffer.
- Risikovurdering danner grunnlaget for å velge konsekvensreduserende tiltak og ressurser (interne og eksterne) for å kunne håndtere relevante hendelser.
- I tilfelle av krav i lovverk, standarder eller reguleringer som krever spesifikke beredskapstiltak må disse selvsagt legges til grunn.
- Foreta øvelser som gir et realistisk bilde av den evnen virksomheten faktisk har til å håndtere relevante hendelser.
- Visdomsord:
 - Noen tror det er nok å øve til de får det til, de proffe øver til de ikke kan gjøre det feil.
 - Ikke regn med plutselig å bli god når en alvorlig hendelse inntreffer, man synker som regel ned til det nivået man har øvd på.

Risikovurdering med sløyfedigramm

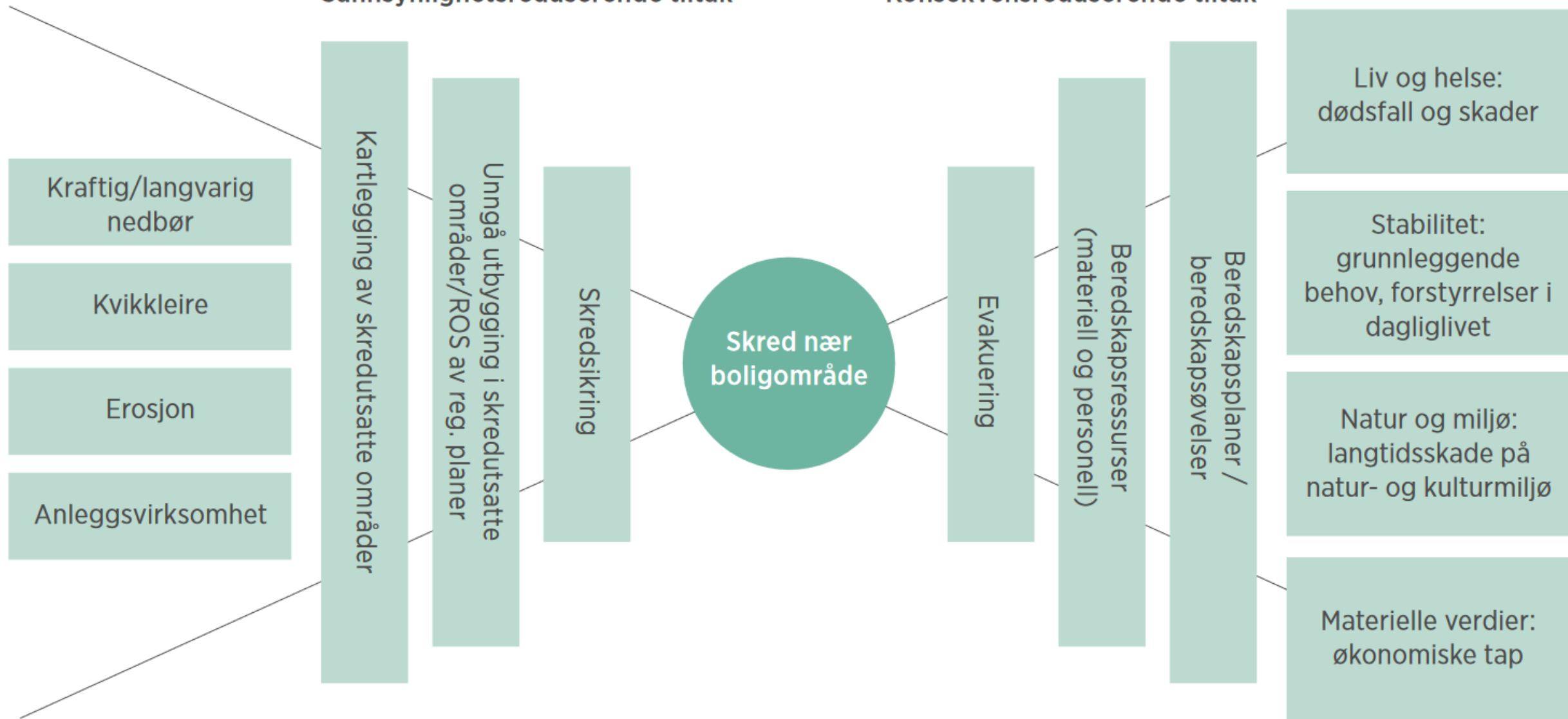


- Et sløyfedigram visualiserer kun én type hendelse, men viser sammenhengen mellom ulike årsaker og konsekvenser relatert til hendelsen, samt hvilke tiltak som er (og ikke er) blitt implementert. Sløyfedigrammet viser ikke alvorligheten av hendelsen eller konsekvensene.
- Sløyfedigram benyttes typisk for risikovurdering innen samfunnssikkerhet.
- Sløyfeanalyse betyr å lage et eller flere sløyfedigrammer.

Eksempel sløyfediagramm for jordskred

Sannsynlighetsreduserende tiltak

Konsekvensreduserende tiltak



Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen
DSB, 2014

Årsaker

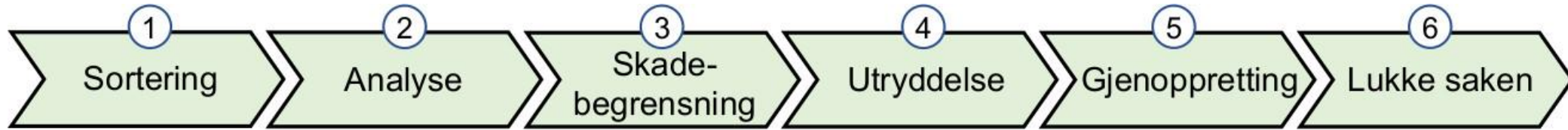
Konsekvenser

Prinsipper for krisehåndtering

- **Ansvarsprinsippet**, som innebærer at den organisasjon som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området.
- **Likhetsprinsippet**, som betyr at den organisasjon man opererer med under kriser i utgangspunktet skal være mest mulig lik den organisasjon man har til daglig.
- **Nærhetsprinsippet**, som betyr at kriser organisatorisk skal håndteres på lavest mulig nivå.
- **Samvirkeprinsippet**, som betyr at myndigheter, virksomheter eller etater har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.
- Stortingsmelding 10 (2016-17) *Risiko i et trygt samfunn - Samfunnssikkerhet*

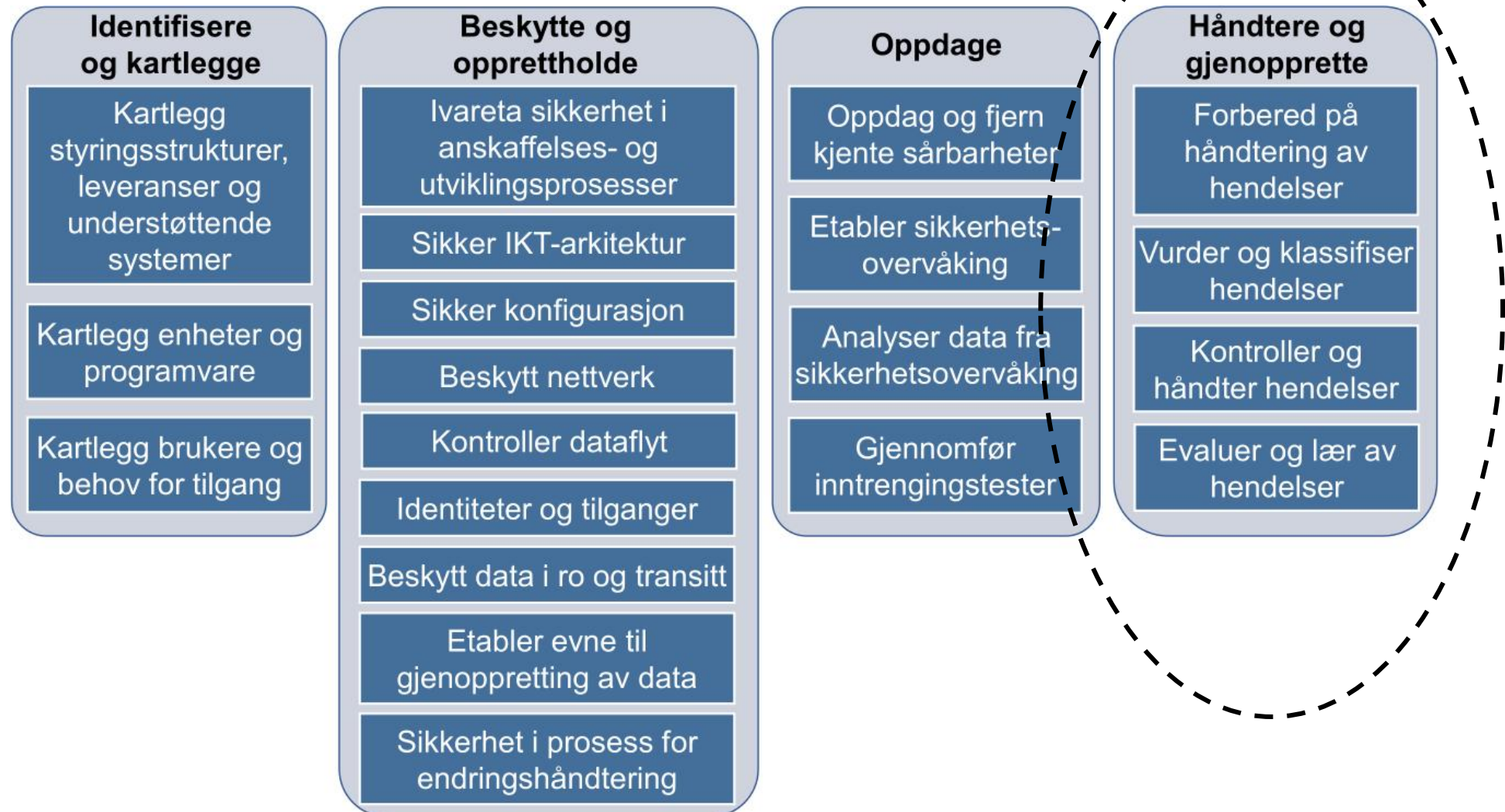
Hendelsesrespons

- Hendelsesrespons omfatter de tekniske aspektene ved håndtering av en cyberhendelse.
- Hendelseshåndtering omfatter i tillegg f.eks. kontakt med media/myndigheter og juridiske aspekter.



1. Sortering er å klassifisere alarmer for å luke ut falske positive, kategorisere hendelsen i henhold til type og alvorlighetsgrad, prioritere ressurser og angi retningen for videre håndtering.
2. Analyse er å opparbeide størst mulig forståelse av hva som har skjedd og hva som bør gjøres videre.
3. Skadebegrensning søker å minimere konsekvens og sørge for at angrepet ikke sprer seg videre.
4. Utryddelse (utkastelse) er å fjerne sårbarheter som ble utnyttet, oppgradere/patche systemer, fjerne skadevare og korrigere systemkonfigurasjoner slik at angriper er ute og ikke kan komme tilbake.
5. Gjenoppretting er å reinstallere sikkerhetskopier fra backup, gjenopprett tjenester, fortsette logging og monitorering, og hvis nødvendig å samle og overlevere bevis til politi.
6. Lukke saken gjøres ved at team for hendelsesrespons og andre involverte overleverer sluttrapport med samlet og avsluttende informasjon.

Hendelsesrespons i NSMs grunnprinsipper for IKT sikkerhet



NSMs grunnprinsipper

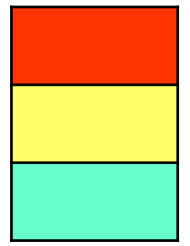
4.1 Forbered virksomheten på håndtering av hendelser

Beredskapsplanlegging

Nr	Beskrivelse
4.1.1	Etabler et planverk for hendelseshåndtering som ivaretar behovet for virksomhetskontinuitet ved beredskap og krise.
4.1.2	Gjennomfør en analyse av virksomhetskritiske effekter, og gjennomfør en konsekvensanalyse: BIA (Business Impact Analysis).
4.1.3	Utarbeid rolle- og ansvarsbeskrivelse for personell som skal involveres i hendelseshåndtering.
4.1.4	Utarbeid avtaler med relevante tredjeparter slik at disse er klare til å yte støtte dersom det kreves ved en hendelse.
4.1.5	Fastsett hvilke kommunikasjonskanaler som skal benyttes i forbindelse med hendelser.
4.1.6	Test og øv på planer jevnlig slik at disse er godt innøvd.

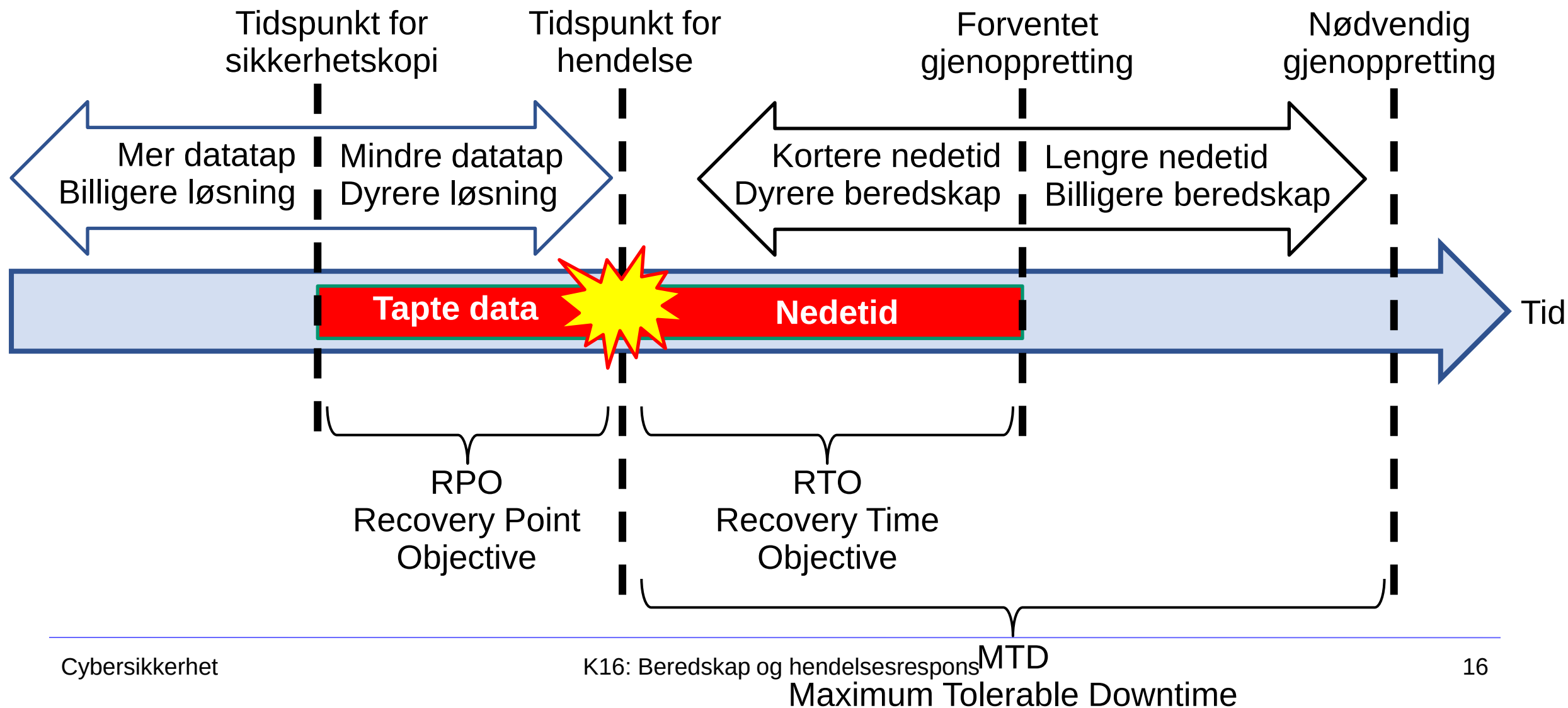
Konsekvensanalyse

BIA – Business Impact Analysis



- En konsekvensanalyse (BIA: Business Impact Analysis) utføres som en del av beredskapsplanleggingen for å identifisere kritiske funksjoner som i tilfelle av et avbrudd vil forårsake størst økonomisk eller operasjonelt tap.
- Spesifisering av gjenopprettingstidsmål (RTO: Recovery Time Objective) som er målsetting for hurtighet av gjenoppretting etter avbrudd (dvs. maksimal akseptabel tidsperiode for avbrudd) for hver kritiske funksjon.
- Spesifisering av gjenopprettingspunktmål (RPO: Recovery Point Objective) som er høyeste akseptabel alder på sikkerhetskopier som må gjenopprettes. Hvis en organisasjon har en kort RPO på noen få timer eller minutter, må sikkerhetskopiering gjøres tilsvarende ofte.
- Det skilles mellom (begrensede) krisehendelser og katastrofehendelser for spesifisering av RTO og RPO. Ved katastrofehendelser er det akseptabelt med lengre RTO og RPO fordi gjenoppretting forventes å være vanskeligere.

RPO og RTO



Eksempel RTO og RPO

- Tabellen nedenfor gir eksempel på RTO (gjenopprettingstidsmål) og RPO (gjenopprettingspunktmål) som kan spesifiseres for ulike kritiske funksjoner.
- Det skilles mellom krise- og katastrofehendelser for spesifisering av RTO og RPO.

Kritikalitet av funksjon	Farge		RTO og RPO ved krisehendelser	RTO og RPO ved katastrofehendelser
Høy		Rød	RTO Innen 2 timer med full funksjonalitet og kapasite. RPO: 2 timer.	RTO Redusert drift innen 1 dag, 100% drift innen 7 dager. RPO: 2 timer.
Medium		Gul	RTO Inntil 8 timer med full funksjonalitet og kapasitet. RPO: 1 døgn.	RTO Innen 7 dager med full funksjonalitet og kapasitet. RPO: 1 døgn.
Lav		Grønn	RTO Inntil 1 uke med full funksjonalitet. RPO: 1 uke.	RTO Innen 3 uker med redusert drift innen 4 uker med full funksjonalitet og kapasitet. RPO: 1 uke.

Øvelse på håndtering av cyberangrep

- Øvelsesformer
 - Papirøvelse (tabletop): Personell som har ansvar for å håndtere hendelser setter seg sammen for å gå gjennom håndtering av spesifikke angrepsscenarioer
 - Hybrid: Papirøvelse kombinert med elementer av simulerte angrep
 - TIBER (Threat Intelligence-based Ethical Red Teaming) simulerte realistiske angrep mot systemer som er i produksjon
- Øvelsesdirektiv skal spesifisere:
 - Hensikt: 1) øve noe virksomheten er forberedt på, 2) teste evne til å håndtere hendelser som virksomheten ikke er forberedt på
 - Fokusnivå: 1) enkeltfunksjoner, 2) hele virksomheten, 3) en hel sektor, 4) nasjonal øvelse
 - Øvelseselementer, dvs. typer angrep og hvordan de skal gjennomføres
- Planlegge beredskapsøvelsen og produsere dokumentasjon for øvelsen
- Evaluering og oppfølging etter øvelser
 - Hvordan erfaring fra øvelsen skal innlemmes i planverk for hendelseshåndtering

Team for cyberøvelser

- Blue Team (BT):
 - Gruppe (forsvarsteam) som under cyberøvelser jobber med forsvar mot cyberangrep, og som utfører hendelsesrespons i tilfelle cyberhendelser. Under vanlig drift (utenfor testsituasjoner) er den samme gruppen typisk organisert som SOC (Security Operations Centre) og CERT/CSIRT (Computer Emergency Response Team eller Computer Security Incident Response Team).
- Pen-tester (penetrasjonstester)
 - Etske hackere som prøver å bryte seg inn i et datasystem med hensikt å avdekke sårbarheter. BT er informert om at pen-testingen foregår.
- Read Team (RT)
 - Gruppe (angrepsteam) som går lengre enn pen-testing, og legger til fysisk pen-testing, sosial manipulering og et element av villedning og overraskelse. BT er ikke informert om at RT gjennomfører simulerte angrep, og vil derfor håndtere det som et ekte angrep.
- White Team (WT)
 - Liten gruppe mennesker som er informert om at et RT utfører simulerte angrep.
- Purple Team
 - Kombinasjon av BT og RT.

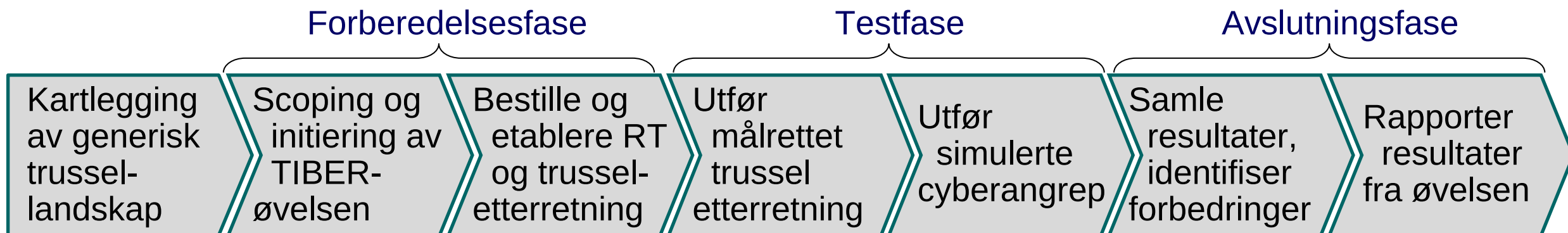
TIBER (Threat Intelligence-based Ethical Red Teaming)

- Bakgrunn

- Behov for å gjennomføre realistiske RT-øvelser for å være forberedt på ekte cyberangrep
- Risikabelt å gjøre realistiske RT-øvelser med systemer som er i produksjon
- Behov for et rammeverk for å gjennomføre RT-øvelser på en trygg måte
- Finanssektoren i EU er svært utsatt for cyberangrep, tok initiativ til TIBER-EU-rammeverket

- TIBER-EU

- Europeisk rammeverk for RT-øvelser, primært i finanssektoren, men også andre sektorer
- Krever at RT er eksternt og uavhengig av virksomheten, for mest mulig realistiske øvelser
- Simulerte angrep er basert på digital trusseletterretning, for mest mulig realistiske øvelser
- Må ta hensyn til juridiske aspekter rundt TIBER-øvelser, pga. intrusiv og sensitiv karakter



NSMs grunnprinsipper

4.2 Vurder og klassifiser hendelser

Nr	Beskrivelse
4.2.1	Gjennomgå loggdata og samle relevante data om hendelsen for å oppnå et godt beslutningsgrunnlag. Dette kan innebære innhenting og sammenstilling av data fra flere kilder, gjennomføre tester eller målinger for å verifisere eller avkrefte en hendelse. Metode og omfang vil avhenge av type hendelse som har oppstått.
4.2.2	Avgjør alvorlighetsgrad for hendelsen iht. etablert planverk, se 4.1.1. a) Vurder om hendelsen er en mulig eller bekreftet sikkerhetshendelse eller en falsk alarm. b) Klassifiser hendelsen i henhold til virksomhetens klassifiseringsregimet (4.1.1.d). c) Involver relevante roller (4.1.3). d) Iverksett beredskapsplan dersom hendelsen tilsier dette.
4.2.3	Informer relevante interesseparter. Dette kan være sektorvise responsmiljøer, IT-spesialister innen ulike fagfelt, leverandører av utstyr og programvare, ledelsen, sluttbrukere, media mm. Se 4.1.3 - 4.1.4.

Betydning av riktig klassifisering

- Riktig klassifisering og prioritering av hendelser er viktig for at ressurser kan disponere fornuftig og hendelsen skal kunne løses raskest mulig.
- Hvis det tar lang tid fra en hendelse blir oppdaget til den blir varslet, prioritert og håndtert kan skadeomfang, ressursbruk og gjenopprettingstid øke betydelig.
- Feilklassifisering av en hendelse kan føre til at en virksomhet bruker mye tid og ressurser på uvesentlige hendelser mens alvorlige hendelser går under radaren.
- En hendelse som i utgangspunktet kunne vært løst enkelt kan eskalere og spre seg hvis det ikke settes inn reaktive tiltak hurtig nok.
- Ved kompleks skadevare vil de færreste klare å se reelt skadeomfang før i etterkant av hendelsen. I slike tilfeller vil mange virksomheter ha behov for å hente kompetanse utenfor egen virksomhet.

Viktighet av kompetanse og erfaring for beslutninger

- Når en sikkerhetshendelse oppstår vil det typisk diskuteres om tjenester bør stenges ned, om det bør settes inn tiltak eller om det er best å sitte stille og bare observere for å forstå hva som skjer.
- Dette er en svært vanskelig vurdering som krever at de som vurderer hendelsen er kompetente og har erfaring.
- Skadeomfanget kan bli svært forskjellig for de ulike valgene.
 - Å stenge ned en tjeneste vil kunne medføre konsekvenser for virksomhetens leveranser, og en for tidlig nedstenging kan gjøre det vanskelig å rydde opp og komme i gang igjen.
 - Å ikke stenge ned tjenester kan medføre at disse blir kompromittert.
 - Å innføre tiltak uten å vite om angriperen er fullstendig utryddet kan medføre at angriperen legger seg i skjul mens den fremdeles har en bakdør til nettet.
- Virksomheter må tilstrebe at alle relevante ressurser sitter rundt bordet når slike beslutningen skal tas.

NSMs grunnprinsipper

4.3 Kontroller og håndter hendelser

Nr	Beskrivelse
4.3.1	Kartlegg omfang og påvirkning på forretningsprosesser. Kartlegg hendelsens påvirkning på underliggende IKT-funksjoner, IKT-tjenester og IKT-systemer. Se 4.1.2
4.3.2	Undersøk om hendelsen er under kontroll og gjennomfør nødvendige reaktive tiltak. Dersom omfanget øker og ser ut til å få alvorlige konsekvenser for virksomhetens forretningsprosesser bør kriseresponsaktiviteter iverksettes ved å eskalere til krisehåndteringsfunksjonen.
4.3.3	Loggfør alle aktiviteter, resultater og relevante avgjørelser for senere analyse.
4.3.4	Iverksett gjenopprettingsplan i løpet av, eller i etterkant av hendelsen.
4.3.5	Koordiner og kommuniser med interne og eksterne interessenter underveis i hendelseshåndteringen. Dette kan være intern drift, ledelsen, interne avdelinger og andre virksomheter som kan bli påvirket av hendelsen. Virksomheten bør også ha en klar mediestrategi ved hendelser som kan ha en interesse for medier og allmenheten.
4.3.6	Gjennomfør nødvendige aktiviteter i etterkant av hendelsen. Alvorlighetsgrad av hendelsen og virksomhetens kompetanse og kapasitet vil være styrende for hva som gjennomføres og om det skal gjøres av internt eller eksternt personell.

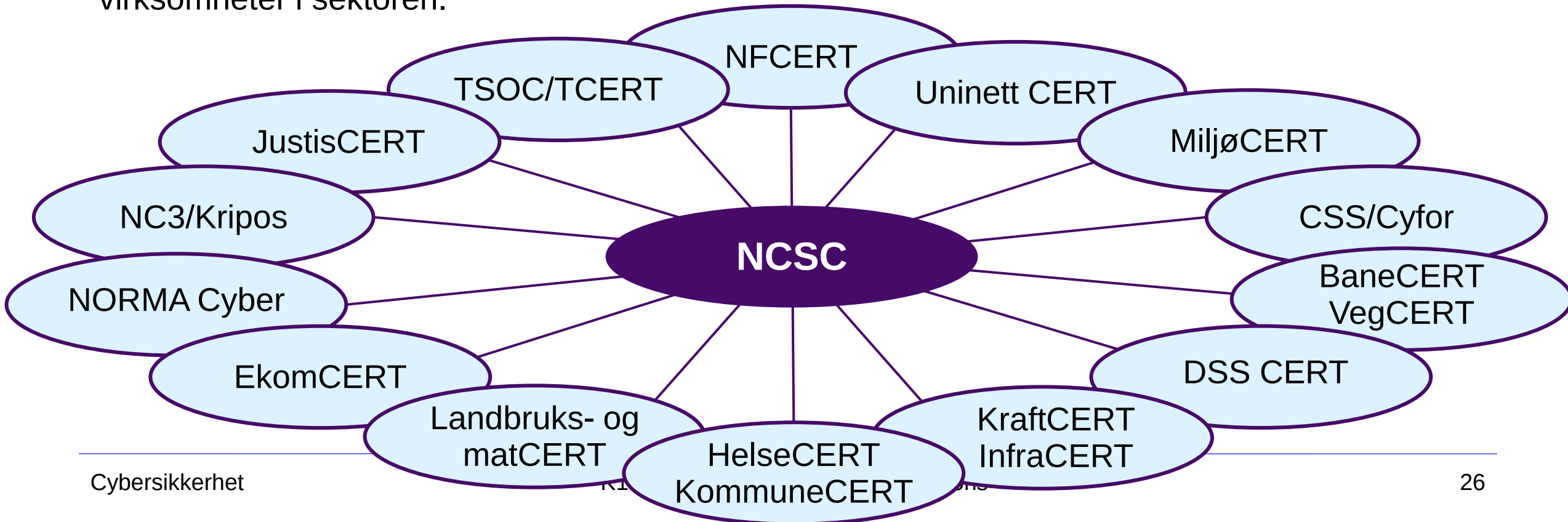
Globale trusler krever samlet respons

- Digital sikkerhet har utviklet seg fra å handle om tekniske aspekter som hver virksomhet håndterer selv, til å bli en strategisk utfordring som adresseres sektorvis, nasjonalt og globalt.
- Leveransekjedeangrepet mot IT-leverandøren SolarWinds er et kjent eksempel som førte til omfattende konsekvenser for virksomheter i hele verden. Slike globale hendelser viser at cyberoperasjoner rammer i stor skala og har et globalt nedslagsfelt.
- *Angrep på én er forsvar for de andre.* Dette prinsippet betyr at samarbeid mellom likesinnede land gjør det mulig å respondere på cyberhendelser langt mer effektivt. Globale trusler krever samlet respons.



NCSC og sektorvise responsmiljøer

- NCSC (Nasjonalt cybersikkerhetssenter), som er en del av NSM, er nasjonal koordinerende enhet for sikkerhetshendelser med hensyn til deteksjon, hendelsesrespons og koordinering.
- I tillegg til NCSC er det opprettet en rekke sektorvise responsmiljøer (SRM), som er selvstendige enheter som koordinerer sine aktiviteter med NCSC.
- Cyberangrep foregår ofte i kampanjer mot en sektor. I slike situasjoner spiller et SRM en viktig rolle for å koordinere deling av etterretning og gi råd om sikkerhetstiltak til virksomheter i sektoren.



NSMs grunnprinsipper

4.4 Evaluer og lær av hendelsen

Nr	Beskrivelse
4.4.1	Identifiser erfaringer og læringspunkter («lessons learned») fra hendelser, både det som virket og det som kan forbedres.
4.4.2	Kartlegg og gjennomgå identifiserte, kompromitterte sikkerhetstiltak og oppdater eller forny disse for å hindre at en tilsvarende hendelse gjenoppstår. Vurder om etablerte tiltak er dekkende for virksomheten risikobilde.
4.4.3	Vurdere effektiviteten av prosesser, prosedyrer, rapporteringsformater og organisatoriske strukturer med tanke på å respondere på hendelser. Gjennomgå disse regelmessig, og etter hendelser, og oppdater basert på eventuelle læringspunktene.
4.4.4	Kommuniser og del erfaringsresultatene med (relevante) interessenter og bruk reelle historier fra hendelseshåndtering i opplæring og bevisstgjøring av ansatte.

Lære av hendelsen, og ikke peke på syndebukker

1. **God forståelse av hendelsen.** For å kunne forklare en hendelse må de som rapporterer og kommuniserer selv ha en god forståelse av hendelsen.
2. **Fokus på «hva».** Det må fokuseres på *hva* som gikk galt, og ikke *hvem* som gjorde noe galt. Enkeltindivider er aldri rotårsaken til hendelse, kanskje bortsett fra tilfeller av tilsiktede hendelser.
3. **Fokus på «hvordan».** Hvordan samme type hendelse kan unngås i fremtiden.
4. **Åpen dør.** Ansatte må alltid føle seg velkommen til å snakke om hendelser og observasjoner, og til å rapportere egne eller andres avvik uten frykt for kritikk.
5. **Utelukk vurdering av individer.** Selv om enkeltindivider har vist vedvarende dårlig sikkerhetskultur skal dette ikke nevnes i hendelsesrapporten. Å korrigere slike holdninger hører kanskje bedre hjemme i HR.
6. **Fokuser på læring.** Det viktigste er å lære hvordan unngå lignende hendelser i fremtiden, og å bedre kunne håndtere hendelser hvis det likevel skjer.

<https://www.threatstack.com/blog/how-to-conduct-a-blameless-security-post-mortem>

Slutt på presentasjon