Kraftsensitivt og sårbarheter

margrete.raaum@kraftcert.no

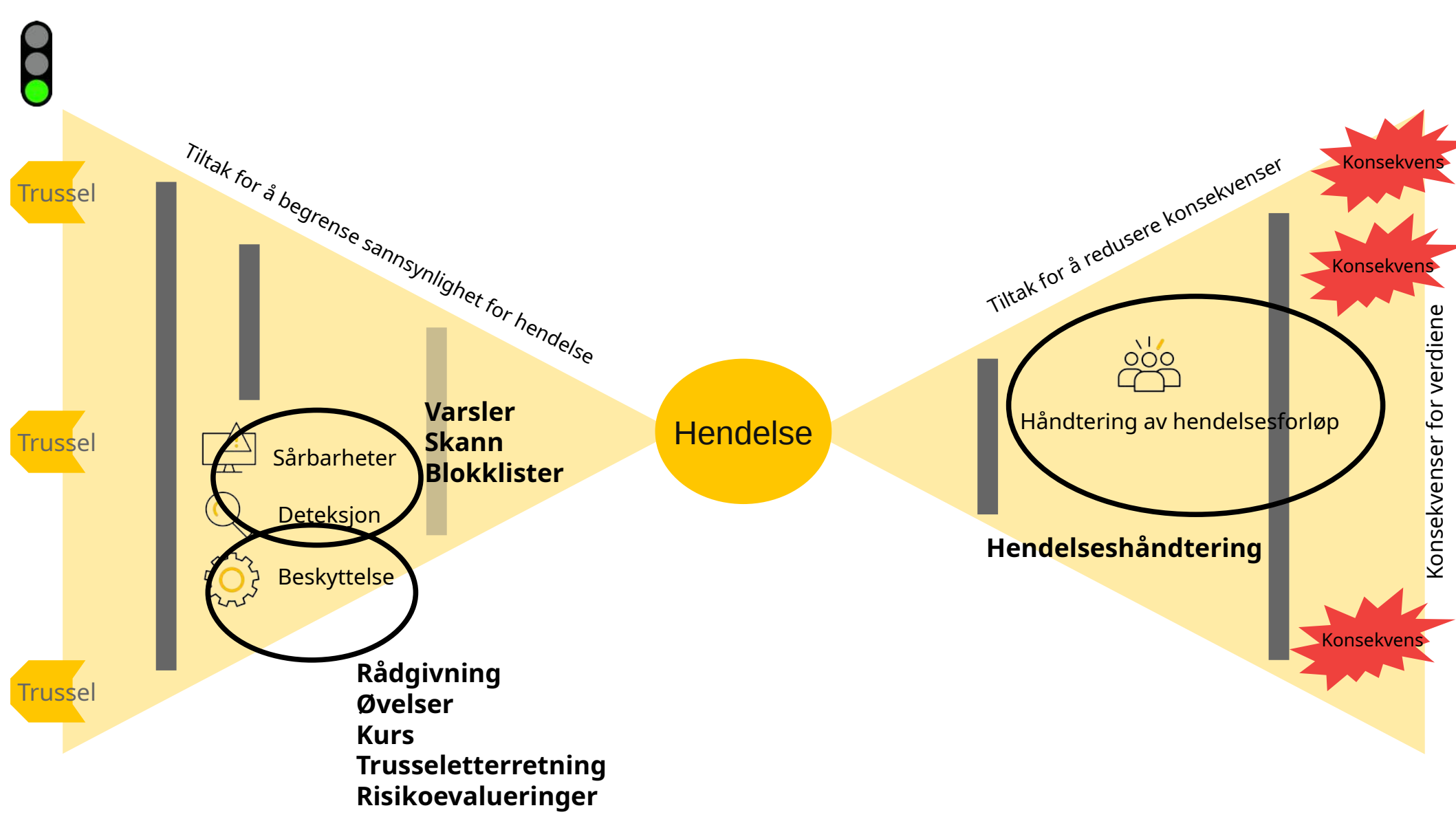
infraCERT

kraftCERT

KraftCERT/InfraCERT

(CERT=Computer Emergency Response Team)

- Initiativ for kraftbransjen fra NVE i 2013
- Sikkerhetsteam på 13 personer
- Sektor-CERT for kraftbransjen og petroleum
- V&A, fjernvarme, avfall, industri
- Er er del av KBO (kraftbransjens beredskapsorganisasjon), Nasjonalt BeskyttelsesProgram, SRM (sektor-responsmiljøet) og er NSM-partner.
- Mål: å beskytte operasjonell teknologi (OT) og omliggende teknologi i selskapene.
- KraftCERT=InfraCERT. For oljå, vann, industri


Trussel
Trussel
Trussel
Tiltak for å begrense sannsynlighet for hendelse
Sårbarheter
Deteksjon
Beskyttelse
Varsler
Skann
Blokklister
Rådgivning
Øvelser
Kurs
Trusseletterretning
Risikoevalueringer
Hendelse
Tiltak for å redusere konsekvenser
Håndtering av hendelsesforløp
Hendelseshåndtering
Konsekvens
Konsekvens
Konsekvens
Konsekvenser for verdiene

Hotbild mot hela Norden utreds: ”Kan slå till i närtid”

Främmande makt pekas ut • FRA bekräftar ökad vaksamhet

Igår 11:26 • Uppdaterad: Igår 16:58

En allvarlig hotbild mot energiinfrastrukturen i samtliga nordiska länder utreds, enligt uppgifter till TV4 Nyheterna.
Svenska myndigheter har gått upp i beredskap – och polisen bevakar samhällskritiska anläggningar.
– Det stämmer att vi har uppmanat energisektorn till ökad vaksamhet i Sverige, säger Ola Billger på FRA.

- Hva er OT og hva er IT?
  - Hva er motiv for å definere dette?
  - Mer kunder, penger eller makt
  - Hva gjør at IKT også er viktig? OT-planlegging, OT-nær, pengenær og må skrus av
  - Og hvem er egentlig ute etter dette?
- Leverandører i OT-landskapet
  - Arkitektur, planlegging, feilsøking og hendelseshåndtering
- Sårbarheter: data eller stepping stone
- NIS2
- Trusselvurderinger og risikoanalyser

Hva er OT-nær IT

- Planlegging
- Produksjon
- Kundesystemer
- Kart
- Flåtestyring
- Målinger

Trusselaktører i dag

- Kost-nyttesamarbeid
- Leverer tjenester til hverandre
- Tilgangsmeglere står for de aller fleste førsteangrep
- Informasjonsstjelende skadevare danner grunnlag for mange salg
- Stor kvalitetsforskjell på data
- De mest profesjonelle trusselaktørene har faste leverandører

Microsoft Møter Crowdstrike

MSFT	CRWD
AMETHYST RAIN	VOLCANIC TIMBER
AQUA BLIZZARD	PRIMITIVE BEAR
BRASS TYPHOON	WICKED PANDA
BROCADE TYPHOON	GOTHIC PANDA
BURGUNDY SANDSTORM	REMIX KITTEN
CADET BLIZZARD	EMBER BEAR
CANARY TYPHOON	CIRCUIT PANDA
CANVAS CYCLONE	OCEAN BUFFALO
CHARCOAL TYPHOON	AQUATIC PANDA
CHECKERED TYPHOON	DEEP PANDA
CINNAMON TEMPEST	HIGHGROUND
CIRCLE TYPHOON	EMISSARY PANDA


DRAGO
New Threat Group:
AZURITE
SINCE 2021
Az
New Threat Group:
PYROXENE
SINCE 2017
Py
New Threat Group:
SYLVANITE
SINCE 2023
Sy

Alternative motiver

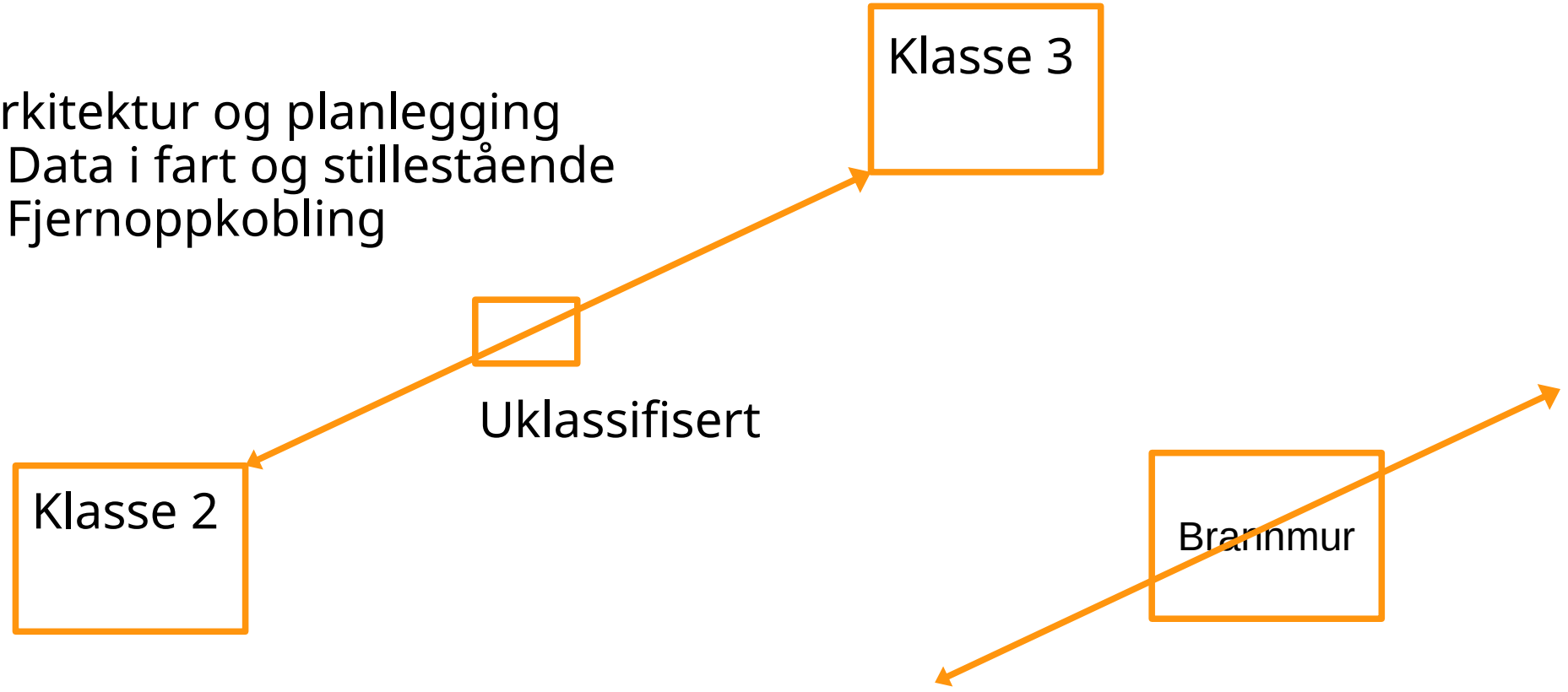
- Sikkerhetsforskere: viktig å være først
  - Ingen beskyttet tittel
  - Gamle sårbarheter
  - Utdaterte protokoller
  - Er penetrasjonstestere sikkerhetsforskere?
  - Kan man stole på dem?
    - De som banker på eller de som leies inn?
- Hvorfor er AI en trussel mot sikkerhetsforskere?
- Statens samarbeidsparner (stortinget eller kongressen)
  - Konkurransefortrinn

ALLE HAR ET MOTIV FOR Å PUBLISERE!

Sårbarheter hos leverandører

- Arkitektur
- Planlegging
- Feilsøking
- Hendelseshåndtering

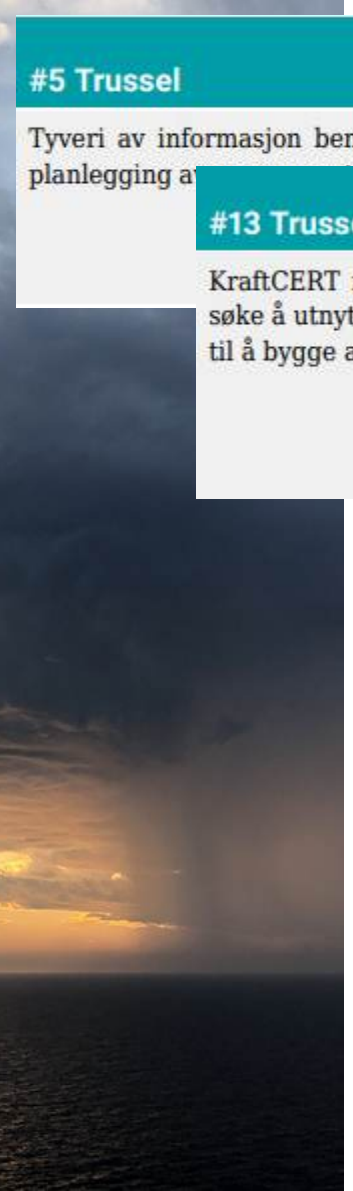
- Arkitektur og planlegging
  - Data i fart og stillestående
  - Fjernoppkobling



Inntrengning via utstyr

- Som stepping stone eller brohode
- Kan skje via en gammel database eller et kamera
- Avvikling av gamle tjenester
- Feilsegregering

Hvorfor er informasjon så viktig



#5 Trussel	Tiltak
Tyveri av informasjon benyttes i langsiktig strategisk planlegging a	Identifiser og beskytt sikkerhetssensitiv in-

#13 Trussel	Tiltak
KraftCERT mener at oppdragsstyrte trusselaktører vil søke å utnytte topologidata og adresseringsinformasjon til å bygge angrepsteknikk og skadevare.	Klassifisere topologidata og adresseringsinformasjon som sikkerhetssensitiv informasjon og beskytt dem deretter (4805).

#14 Trussel	Tiltak
KraftCERT mener at trusselaktører vil søke å utnytte metadata i datasett fra IoT-enheter i kontrollsystemet til å bygge angrepsteknikk og skadevare.	Disse metadataene er beskyttelsesverdige og Internet of Things (IoT)-enheter må beskyttes som sikkerhetssensitiv informasjon (4805). Forsvars-, håndterings- og gjenopprettingsplaner (7410) må skrives innenfor rammene av at dette er informasjon som er på avveie.

st

e mindre

KJENT!

- Kan ha lekket gjennom IoT eller for eksempel backup, fagsystemer, programmeringsverktøy (som nevnt i trusselvurdering)
- Kan ha vært en innsider

Kraftsensitiv informasjon

- Informasjon om systemer som ivaretar driftskontrollfunksjoner
  - Ullent: gjelder det OT-nære systemer? Planleggingssystemer?
- Fremstilling av hele eller deler av kraftsystemet
- Detaljert informasjon
  - Og når det er satt sammen: inneholder det informasjon om deler av kraftsystemet?
- Informasjon som beskriver eller avdekker sårbarheter i «kraftforsyningen»
- ROS-analyse: risiko må legges sammen om ting blir samlet (type Elbits, Safebase)

Hvordan skal dette håndteres

- Beskyttelse
- Merking
- Men de lekker det jo likevel!
- De andre skjønner ikke hva som er sensitivt

Lov og forskrift om digitalsikkerhet (NIS1)

- Forskrift, ikrafttredelse 1.oktober 2025

  https://lovdata.no/dokument/LTI/forskrift/2025-06-20-1131

- Lov

https://lovdata.no/dokument/LTI/lov/2023-12-20-108

Forskrift om digital sikkerhet (digitalsikkerhetsforskriften)

Dato	FOR-2025-06-20-1131
Departement	Justis- og beredskapsdepartementet
Ikrafttredelse	01.10.2025
Hjemmel	LOV-2023-12-20-108-§2, LOV-2023-12-20-108-§3, LOV-2023-12-20-108-§6, LOV-2023-12-20-108-§9, LOV-2023-12-20-108-§13, LOV-2023-12-20-108-§18
Kunngjort	23.06.2025 kl. 10.50
Journalnr	2025-0734
Korttittel	Digitalsikkerhetsforskriften

Veiledning og råd NSM:

https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/digitalsikkerhetsloven-og-forskrift

IKKE I KRAFT

➡ Gå til opprinnelig kunngjort versjon

Lov om digital sikkerhet (digitalsikkerhetsloven)

Dato	LOV-2023-12-20-108
Departement	Justis- og beredskapsdepartementet
Ikrafttredelse	01.10.2025
Kunngjort	20.12.2023 kl. 11.40
Korttittel	Digitalsikkerhetsloven
EØS/EU/Schengen	EØS-avtalen vedlegg XI nr. 5cpa (direktiv (EU) 2016/1148).

Prop.109 LS (2022–2023), Innst.78 L (2023–2024), Lovvedtak 15 (2023–2024). Stortingets første og andre gangs behandling hhv. 7. og 12. desember 2023. Fremmet av Justis- og beredskapsdepartementet.

Grafikk: SNL.no

Lov om digitalsikkerhet i Norge (NIS1)

Sett fra KraftCERT/InfraCERT perspektiv

One pager-intro

1. Styringssystem for sikkerhet
- Digital sikkerhet

2. Risikovurdering
- Utføre vurdering og dokumentere risiko

3. Sikkerhetstiltak
- Organisatorisk
- Teknologisk
- Fysisk
- Personell

4. Hendelseshåndtering, beredskap og øvelse
- Hendelseshåndtering
- Beredskapsplaner
- Øvelse på hendelse og planverk

5. Oppfølgingsplikt
- Varsling ved hendelse

6. Ansvar for leverandører
- Leverandørkrav og oppfølging av lov ved avhengigheter

ikrafttredelse 1.oktober 2025

Lov om digitalsikkerhet i Norge (NIS1)

Sett fra KraftCERT/InfraCERT perspektiv

Sektor	**Vann og avløp** (*)	**Kraft** (**)
Aktuelt	**JA**	**Ja**
Terskel	Vannforsyningssystem som behandler minst 2000m3 per døgn	KBO-enheter
Sektor	**Petroleum** (***)	**Leverandører**
Aktuelt	**Nei**. Norsk sokkel, landanlegg er utenfor. (upstream, midstream) **Ja.** Tankanlegg, drivstofflangring (downstream)	**Ja**
Terskel		Avhengigheter til de som er utpekt

(*) Gjelder også Svalbard
(**) Svalbard er ikke utpekt som KBO
(***) Ingen av KraftCERTs medlemmer

ikrafttredelse 1.oktober 2025

Er dere medlem? Er det kurs eller veiledninger som du ville hatt nytte av? Konferanser?

Alle i selskapene skal ha adgang.

margrete.raaum@kraftcert.no
cert@kraftcert.no
Tlf: +47 95201798

kraftCERT

infraCERT