Trusselvurdering 2024 – KC/IC

13092024 Espen Nodeland

Kommentar digital publisering:

Denne briefen tar utgangspunkt i vår åpne trusselvurdering:

https://www.kraftcert.no/filer/KraftCERT-ThreatAssessment2024.pdf
https://www.kraftcert.no/filer/KraftCERT-Trusselvurdering2024.pdf

Send mail til cert@kraftcert.no om du har spørsmål til våre vurderinger.

kraftCERT

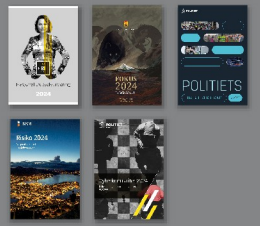
infraCERT

KraftCERT/ InfraCERT

- Ideelt selskap (non-profit)
- SRM for kraft- og petroleumsbransjene («energy») i Norge og på Island
- Årlig trusselvurdering basert på kontinuerlig innhenting og analyse
- Årlig tiltakspakke basert på trusselvurdering
- Rådgiving, øvelser, hendelseshåndtering, varsling
- **Mål:** Å beskytte operasjonell teknologi (OT) og omliggende teknologi i selskapene.

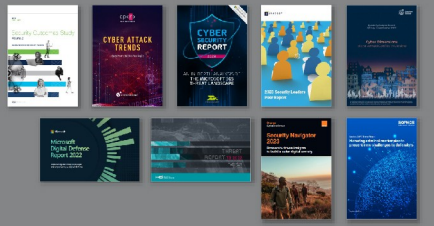
National assessments

- Actors (Russia, China, etc.)
- Insider threats
- Supply chains
- Phishing, DDoS
- Generic measures



Other sources

- ENISA, CISA, etc.
- Intelligence
- SOC-providers
- Software companies
- Trends and developments



KraftCERT's Threat Assessment

Relevant to KraftCERT members

Context
International, national, technology, OT

Relevant techniques

Supply chain sources

Relevant scenarios

KraftCERT's analysis

Local assessment

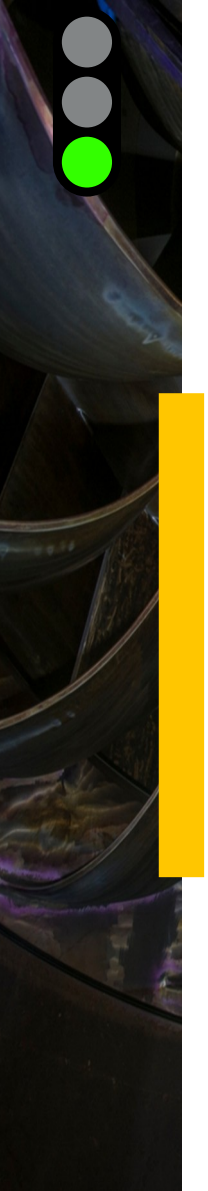
Context
Operation, location, size, staff, etc.

Company employees,
customers, technology

Technology and systems
IT/OT, dependencies

Supply chains
External system dependencies, service providers

Next step
Risk assessment, exercises, etc.



Mest sannsynlige trussel mot kontrollsystem

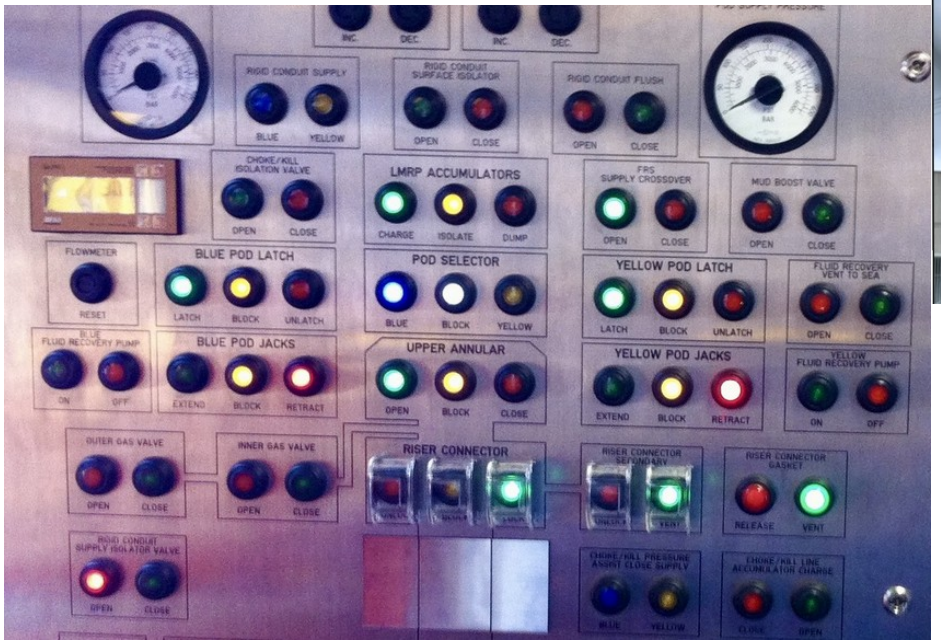
Det er **sannsynlig (60-90%)** at virksomheter i våre sektorer utsettes for angrep som har driftsforstyrrende effekt.

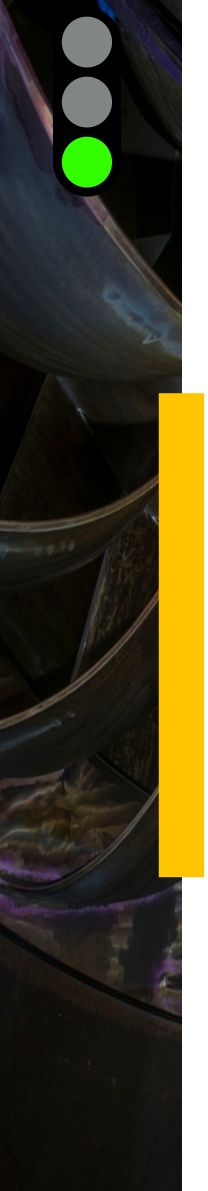
Mest alvorlige trussel mot kontrollsystem

Det er **meget lite sannsynlig (10%>)** at det på kort sikt skjer vellykkede destruktive angrep mot våre sektorer.

Det er **meget sannsynlig (90%<)** at oppdragsstyrte aktører som nasjonalstater jobber kontinuerlig for å utvikle destruktive angrep.

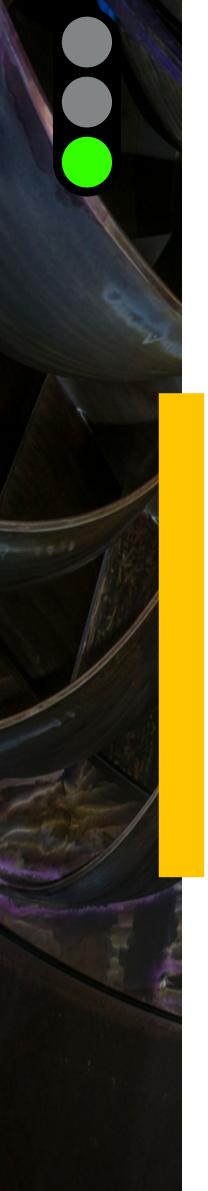
Trusselbildet
Aktører og angrepsformer





Nøkkelpunkter

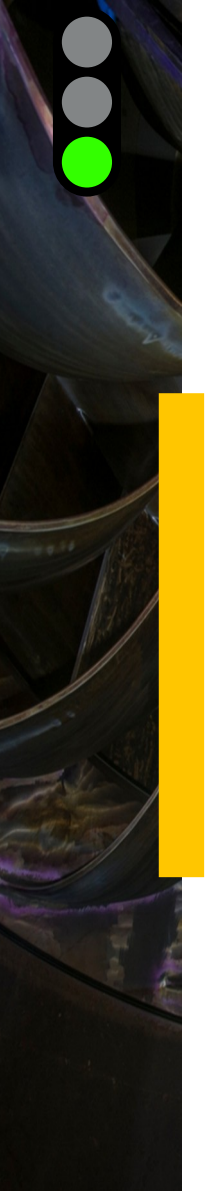
- Stadig spesialisering blant trusselaktører
- Ransomware utvikler seg, men sakte
- KI dukker opp i phishing og etter hvert andre angrep
- QR-koder er høyrisiko
- LOTL: Sannsynlig at filoverføring, fjerntiglang og VPN hos leverandører vil bli mer utsatt.



Utnyttelse av ansatte/ personell med tilgang

Utnyttelse av menneskelige feil er ikke det samme som innsidetrussel.

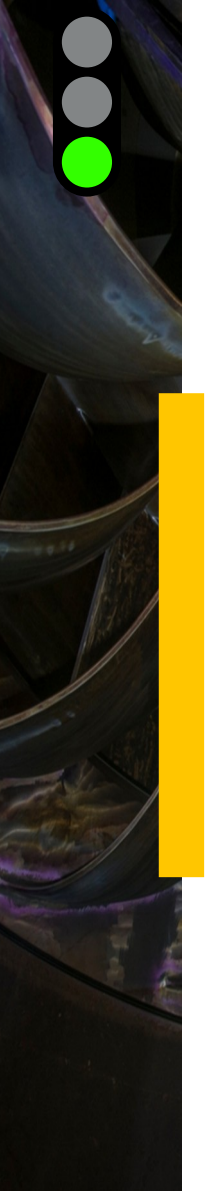
- Phishing er ikke en innsidetrussel, selv om det utnytter en person på innsiden og kan være rettet mot denne personens tilganger.
- Sikkerhetsklarering eller autorisasjonsamtaler vil ikke redusere mengden feil begått av ansatte.



Illojale innsidere, innsidetrussel

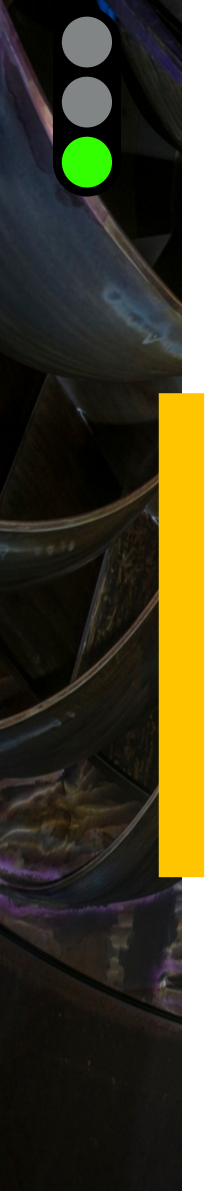
- Myndigheter hevder økning, uklart grunnlag og begrepsapparat
  - NSM sier over halvparten er «ubevisste innsidere», inkluderer folk som åpner vedlegg.
- KraftCERT ser innsidetrussel som en serie spesifikke trusler, ikke en generisk.
  - Forskning og utvikling, særlig teknologisk
  - Ukrainatilknytninger
  - Nord-områdene

Trusler mot kontrollsystemer



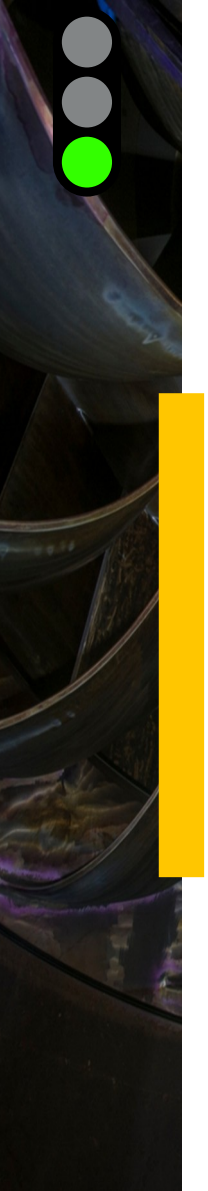
Følgeskader fra utpressingsangrep er den mest sannsynlige trusselen mot kontrollsystemer

- Angriper kan finne kontrollsystemet under angrep på noe annet.
- Usikkerhet under en hendelse kan føre til nedstenginger eller separasjoner av nettverk med konsekvenser for funksjoner med avhengigheter mellom soner.
- En perfekt preventiv nedstenging er en PR-persons mareritt om strømutfall.



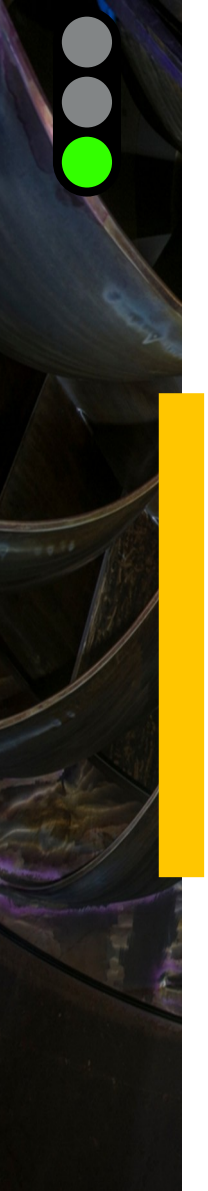
Angrep med driftsforstyrrende effekt er sannsynlig

- Angriper vil meget sannsynlig utnytte avhengigheter i funksjonalitet mellom kontrollsystemsonene og IT-sonene eller eksterne tjenester og skytjenester.
- Angriper kan utnytte at funksjoner for drift er spredt ut av kontrollsystemsonen



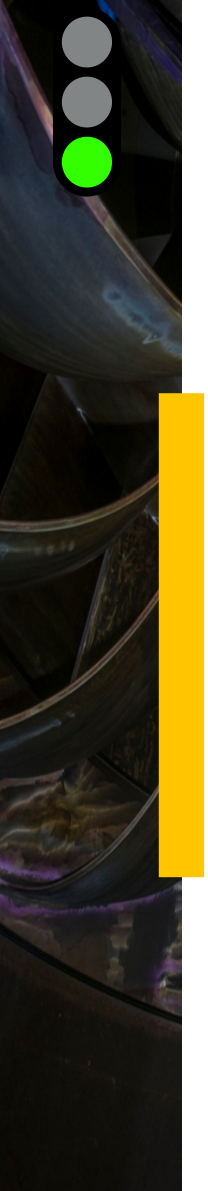
Det er meget lite sannsynlig at vi på kort sikt får se vellykkede ødeleggende angrep

- Intensjon, evne og mulighet
- NSMs påstand i Risiko 24 om strømutfall i Ukraina pga digitalt angrep er trukket tilbake. (Kudos til NSM)
- Danske myndigheter har i år hevet trusselnivå for destruktive angrep, men inkluderer wipere og massive ddos-angrep.



Det er meget sannsynlig at statlige og oppdragsstyrte aktører jobber kontinuerlig for å utvikle destruktive angrep

- Flere nasjoner og aktører bygger evne til destruktive angrep, og flere aktører utvikler slik skadevare.
- Det er sannsynlig at virksomhetenes sårbarheter gir muligheter for gjennomføring.
- Det er dermed et spørsmål om målretting, planlegging, kapasitet, tidspunkt og ikke minst informasjon om målet.



Sluttpunkter

- Angrepsmetoder og teknikker utvikler seg stadig. KI vil støtte både angrep og forsvar.
- Innsiderisiko/ innsidetrussel er komplekst og usikkert
- Krigen i Ukraina viser hvor enormt vanskelig det er å gjennomføre et destruktivt angrep på kontrollsystemer.
- Den kortsiktige trusselen for destruktive angrep mot kontrollsystemer er ikke kritisk.
- Den langsiktige trusselen er svært alvorlig.

Tiltakspakke 2024

Produkt av årets trusselvurdering 2024

Fagdag sikring
Havtil 13.09.2024

Espen Seljemo

Merknad digital publisering
Dette er et utdrag av det som ble presentert på fagdag 2024
Originalmateriale er TLP Amber, og deles med våre medlemmer

kraftCERT

infraCERT

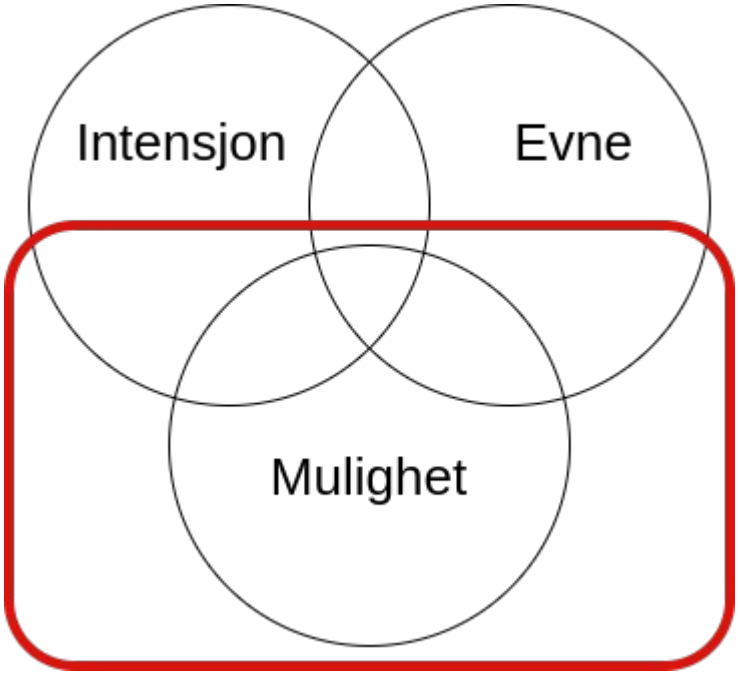
Tiltak mot trusler må tilpasses tiden, tiltak er ferskvare

Drøbaksundet 1940 - Senking av Blücher

Digitalisering i 1967

Bilder: Wikipedia og NRK

Tiltak



Det eneste du kan påvirke er angripers muligheter!

Tiltak mot trusler i sektoren

- NSMs grunnprinsipper er basis for tiltak!

- Sektorvist trusselbilde brukes til å prioritere tiltak

- Virksomhetens prioritering av tiltak må baseres på eget trusselbilde

Tiltakspakka 2024:
- Sikring av systemer og prosesser
- Styrk deteksjonevnen
- Utvid håndteringsferdigheter og -planer
- Andre tiltak

Fra trussel til tiltak

#24 Trussel	Tiltak
KraftCERT vurderer at for kontrollsystemer er følgeskader fra utpressingsangrep den mest sannsynlige trusselen	Overvåk logger i et sentralt loggrammeverk (SIEM)(6702) Sørg for fungerende offline backup (7412) Demonstrer evne til drift uten et eller flere støttesystem (7222) Planlegg for beredskapsheving med begrensninger (7410)

Ved løsepengeangrep vil de som har ansvaret for kontrollsystemer ha ansvar for å opprettholde drift og leveranse. Ofte vil man vegre seg for å stenge produksjon, og det er da viktig å ha oversikt over hvilke systemer som er kompromittert, og om angriper kan få tilgang til kontrollsystemsonene.

Hvis virksomheten har øvd på drift uten støttesystemer eller øydriftmodus, vil effekten av utpressingsangrep i IT-sonene være mindre. En plan for heving av beredskap, med begrensninger i tilganger fra f.eks. leverandør eller IT-sonen, kan gjøre det enklere å opprettholde drift, selv under angrep.

kraftCERT

KraftCERT InfraCERT
www.kraftcert.no
epost: cert@kraftcert.no

infraCERT