Havtil
Havindustritilsynet

Sikkerhetsforum 30.04.26

Ved Ingvild Klaveness og Kristian S. Teigen

Agenda

- Trussel og risikobilde; konsekvenser av angrepet på Iran
- Totalforsvarsåret 2026

Havtil
Havindustritilsynet

Trussel og risikobilde

Konsekvenser av angrep på Iran

- Trusselbildet for petroleumssektoren
  - Fysisk
  - Digitalt

- Drivstoff situasjon
  - Kunnskapsdeling: FFI rapport Nasjonal forsyningssikkerhet i krise og krig

Havtil
Havindustritilsynet

Trussel og risikobilde

Konsekvenser av angrep på Iran

- Trusselbildet for petroleumssektoren
  - Fysisk
  - Digitalt

- Drivstoff situasjon
  - Kunnskapsdeling: FFI rapport Nasjonal forsyningssikkerhet i krise og krig

Havtil
Havindustritilsynet

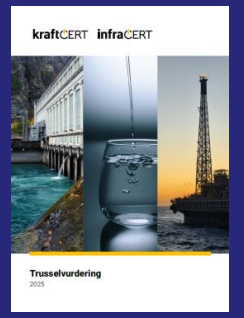
Det digitale trusselbildet – nasjonalt og sektoriellt.



*Sårbarheter i **usikrede** OT systemer, trekkes særlig frem.*

Lykkede destruktive** cyberangrep mot industrielle controls systemer er **svært lite sansynlig på kort sikt.

Operasjonelle forstyrrelser** som et resultat av **angrep på IT er sansynlig..





*Det er **lite sansynlig** at hacktivister alene **uten støtte fra statlig aktør**, er i stand til å gjennomføre destruktive angrep mot norsk infrastruktur. Det er sansynlig at et eventual cyberangrep mot norske virksomheter elle kritisk infrastruktur vil bli utført av en aktør med **innsideinformasjon eller betrodd systemtilgang.***

*…kinesiske cyberaktører **har posisjonert seg** i vestlig infrastruktur, en tilgang som potensielt kan utnyttes til å påføre skade **i en sikkerhetspolitisk tilspisset situasjon.***



Havtil

Globale hendelser:

The CISA advisory on Iranian attacks on US critical infrastructure is clear about the threat actor, less clear about the methods.

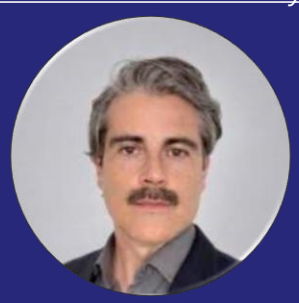
The advisory say the result was extraction of device project files, and manipulation of data on HMI. Then, was this just disruption for publicity or are we looking at a campaign that that's exposing something systematic?

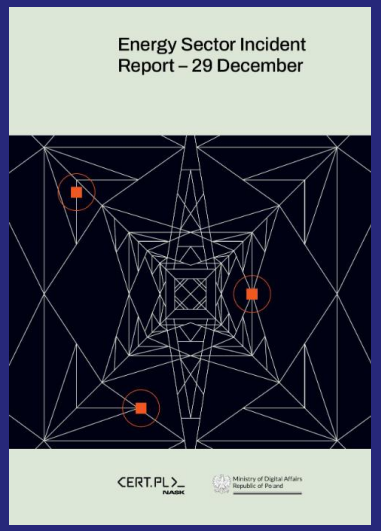
The advisory describes disruption through malicious interaction, with PLC project files, manipulation and exfiltration of HMI/Scada displays. Which is serious, but also suggests the attackers may not (have needed) complex access paths.

My assumption is that these ***cases are likely to involve smaller or resource-constrained municipal environments where limited budget and operational pressure making security improvement harder than it should be.***

The practitioners angle: I need more intel,
This can range from couch based-based cyberattacks to cyberwar.

Dr. Jesus Molina
LinkedIn 8.4.2026





"In each affected facility, a FortiGate device was present, ***serving as both a VPN concentrator and a firewall****. In every case, the VPN interface was exposed to the Internet and allowed authentication to accounts defined in the configuration* ***without multi-factor authentication.***

Hitatchi RTUsThe attack was carried out by logging into the web interface ***using the "Default" account****.*

Mikronika RTUs: , the attacker used ***default credentials*** *to log in via the SSH console to an account with* ***root privileges.***

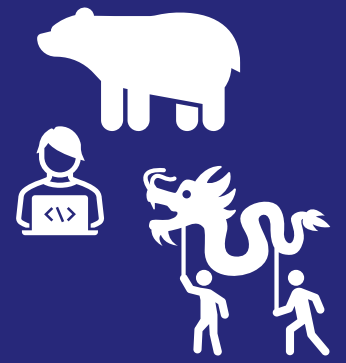
Hitachi IEDs: These devices have the ***FTP service enabled by default****, which provides access to the device's system files. The attacker used a* ***built-in account with default credentials.***

Mikronika HMI Computers: The machines were configured with a ***default password*** *set during deployment for an account with* ***local administrator privileges.***

Moxa Nport:devices had the ***web interface enabled*** *and were configured with* ***default login credentials.***

Havtil

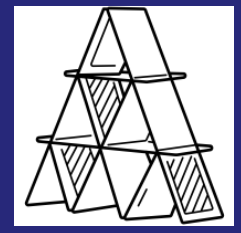
Havtils cyber budskap – to tanker i hodet samtidig



Det handler om å håndtere de mest sannsynlige og hyppigste truslene i dag (og forvente at de vil utvikle seg) ,samtidig som man forbereder seg på mer strategiske og langsiktig orienterte aktører.

Avstanden mellom robust og sårbar handler ofte om svikt i noen (få) grunnleggende tiltak.

= tid fra sårbar til -> under angrep krymper





Sterk grunnsikring reduserer hvor attraktivt skjult tilgang er.

Det handler om å løfte sikkerhetsnivået slik at trusselaktører må ta større eksponeringsrisiko, velge mer høylytte løsninger og operere med høyere kostnad.

Havtil

Totalforsvarsåret 2026

Havtil

Artikler på havtil.no

- Med beredskap i blodet
- Gründere ruster opp
- Fra barkebiller til Nato

Fagdag

- 17.06.26 «Også vi, når det blir krevet»

Øvelse

- Skal øve håndtering av digitale angrep og cyberhendelser

Nasjonalt

- **DSB**:
  - Generelt om Totalforsvarsåret 2026
  - Råd om egenberedskap for virksomheter
    - Råd
    - Veiledere

- **Webinarer**
  - Informasjonshåndtering
  - Egenberedskap og kontinuitetsplanlegging
  - Erfaringer fra Ukraina

Havtil
Havindustritilsynet

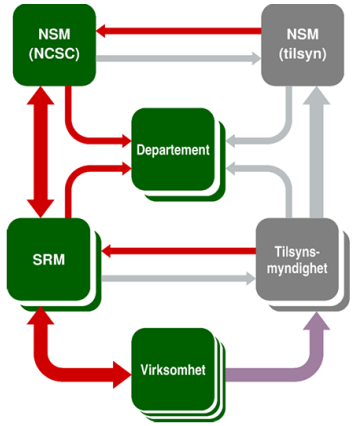
Øvelse grålysning 2026

Hovedmålet er å styrke samvirke, beslutningsevne og situasjonsforståelse på tvers av aktører involvert i hendelseshåndtering i petroleumssektoren.

Et sekundært formål er å utvikle gjensidige erfaringer med håndtering av hendelser etter den nasjonale hendelseshåndteringsmodellen (SRM rammeverket)







- Øvelsen Grålysning petroleum 2026 arrangeres i samarbeid med KraftCERT/InfraCERT.
- For operatører med topside eller landanlegg, samt tekniske tjenesteytere (Technical Service Providers (TSP) på norsk sokkel.
- Format: Tabletop (TTX), blandede bord.
- Målgruppe: ledere og fagpersoner innen digital hendelseshåndtering, beredskap og risikoeiere, samt kommunikasjon.
- Sammensatt scenario på norsk sokkel, digitale angrep, påvirkningsoperasjoner og hendelser utfordrer beredskapen.
- Gjennomføres i Stavanger 22.–23. september 2026.

Havtil
Havindustritilsynet

Tentativ agenda – fagdag «Også vi, når det blir krevet»

Onsdag 17. juni 2026 - Solastranden gård

- Innledning v/ Adm. direktør
- Energidepartementet
- Politidirektoratet
- Forsvarets liaison til sektoren
- Equinor marin
- Havtil
- Lill- Heidi Bakkerud
- FFI



Kilde: April 1940 en måned i Solabuenes liv som ikke blir glemt. - Sola Historielag

Havtil
Havindustritilsynet