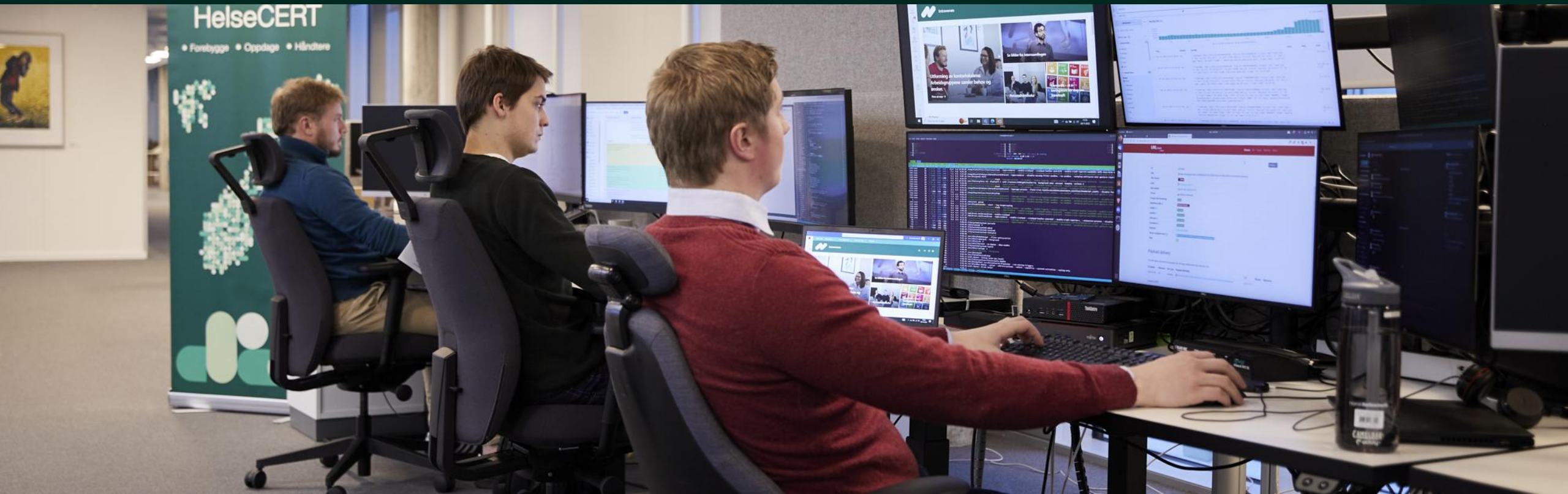
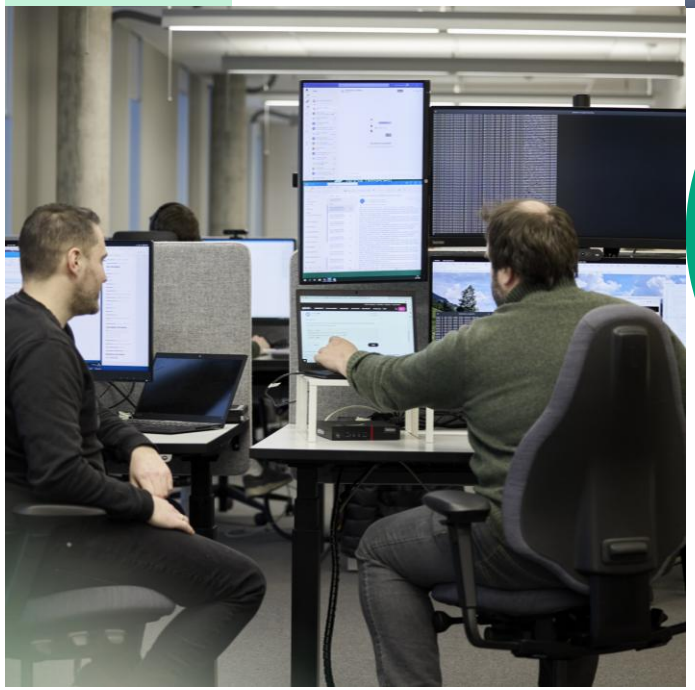
Norsk helsenett

Helse- og kommuneCERT
Forebygge, oppdage og håndtere



Agenda

- Om Helse- og kommuneCERT
- Operasjonell teknologi(OT) og vann- og avløp (VA)
- Operasjonell teknologi på internett
- Oppsummering og spørsmål



Om Helse- og kommuneCERT

- Skal øke motstandsdyktigheten til helse- og kommunesektoren
- 30 ansatte
- HelseCERT opprettet i 2011
- KommuneCERT fra 1. desember 2023
- Forebygge, oppdage og håndtere alvorlige cyberangrep
- Leverer en rekke tjenester til våre medlemmer
- Gjennomfører for eksempel sårbarhetsskanninger fra internett, sikkerhetstester og webinarer til våre medlemmer

Operasjonell Teknologi (OT)

Om operasjonell teknologi (OT)

- OT styrer fysiske enheter
  - Kan være alt i fra ventilasjonsanlegg, styring av prosesser i fabrikker, styring av kritisk infrastruktur som vannforsyning, avløpspumper og strømforsyning
- Oppetid er alltid kritisk i OT. Høyt fokus på tilgjengelighet

Bakgrunn for OT/VA-satsing

- Digitalsikkerhetsloven
- KommuneCERT fra 2023
- Hacktivisme
- Økt fokus på operasjonell teknologi

Økt fokus på sikkerhet i operasjonell teknologi

NSM oppfordrer virksomheter til å styrke egen sikkerhet

Publisert: 21.05.2025 Oppdatert: 22.05.2025

NSM har sett aktivitet rettet mot digital infrastruktur knyttet til vannindustri, demningsanlegg og liknende i Norge. NSM har en klar oppfordring til norske virksomheter: Ha tydelige beredskapsplaner og øv på disse.

Kilde: nsm.no

Alvorlige hendelser rundt OT

Åtvarar mot sårbarheit: Hackarar opna damventil i Bremanger

Hackarar tok kontroll over lukkesystemet i ein dam ved Risevatnet i Bremanger i Vestland. Nasjonal sikkerhetsmyndighet har sett trusselaktivitet mot vassindustri. – Må jobbe med tiltak.

Kari Nygard Tvilde
Journalist

Per Vidar Raunholm
Journalist

Kjelde: NTB / NRK

Publisert 10. juni 2025 kl. 20:03
Oppdatert 10. juni 2025 kl. 22:02

Norge | PST

PST kobler prorussisk gruppe til nytt dataangrep på Østlandet

Politiets sikkerhetstjeneste (PST) bekrefter at de etterforsker nok et datainnbrudd, der fremgangsmåten var lik som i angrepet mot damanlegget i Bremanger i april.

Pause 01:13 / 03:41 1X

Alvorlige hendelser rundt OT

- Prorussisk aktør som fikk fjerntilgang til anlegg i Danmark
- Ønsker å skape frykt og usikkerhet
- Økte pumpene til 100% hastighet
- Vannrørene var ikke dimensjonert for trykket

Denmark says Russia was behind two 'destructive and disruptive' cyber-attacks

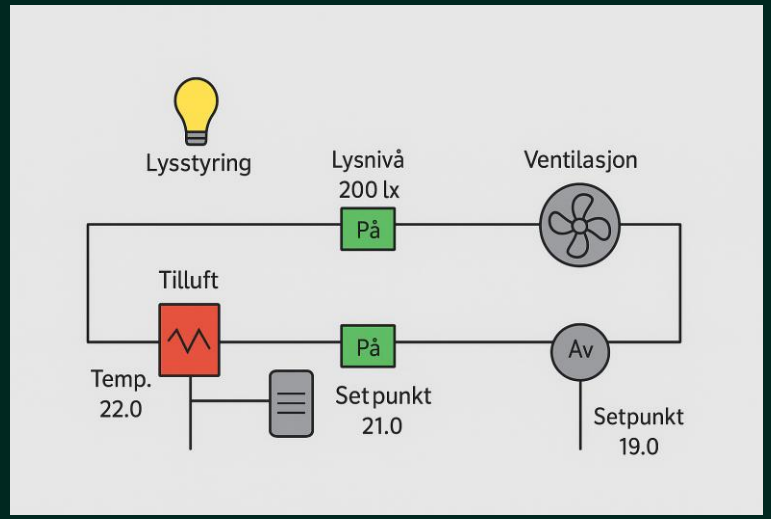
Intelligence service says attacks were work of groups connected to Russian state in 'clear evidence' of hybrid war

Torsten Schack Pedersen, the minister for resilience and preparedness, said Denmark is not sufficiently equipped to withstand such attacks from Russia. Photograph: Nils Meilvang/Ritzau Scanpix/AFP/Getty Images

The Danish government has accused Russia of being behind two "destructive and disruptive" cyber-attacks in what it describes as "very clear evidence" of a hybrid war.

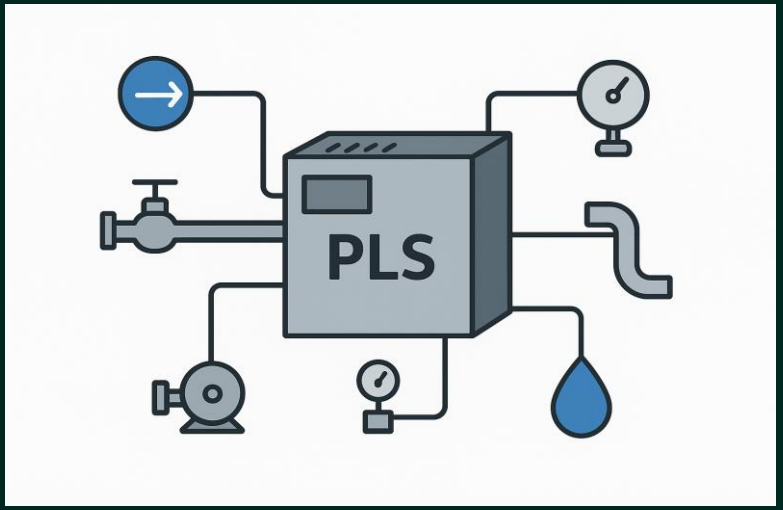
Eksempler på OT-anlegg hos offentlige virksomheter

- Flere kommuner benytter seg av Sentralt Driftskontrollanlegg (SD)
- Vi har kompromittert flere SD-anlegg under kommunetester
- Ikke uvanlig å finne IT-utstyr som benyttes i OT-installasjoner. Ofte er dette Windows-maskiner levert av en tredjepartsleverandør og er utdaterte
  - Utdaterte operativsystem har flere kjente sårbarheter
- Standard sikkerhetsoppdateringer kan potensielt knekke anleggene grunnet skreddersydd løsning og programvare
- Ofte utfordringer vedrørende samspill mellom IT og OT



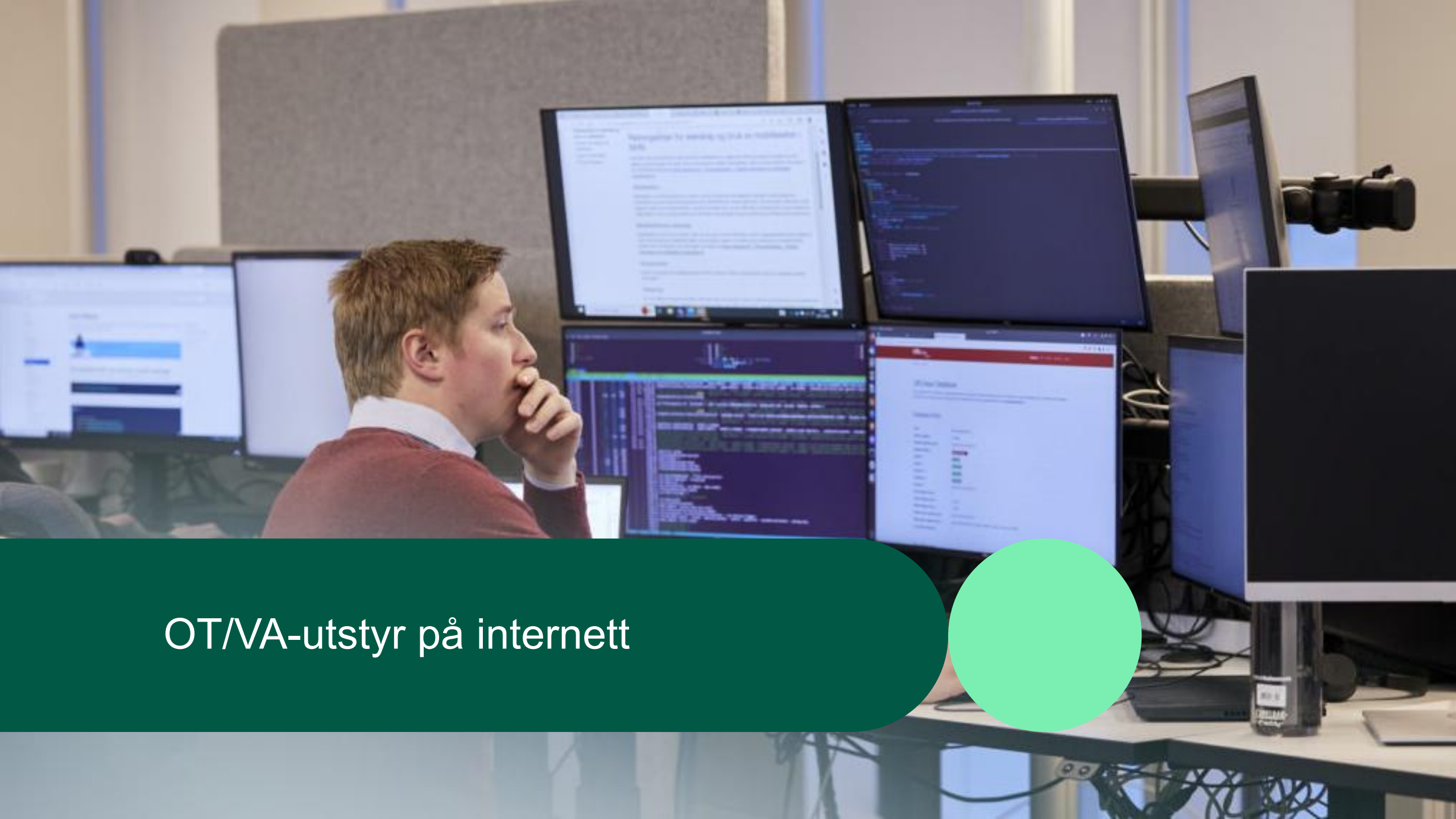
Vann- og avløpsanlegg (VA)

- Noen offentlige virksomheter benytter seg av et IKS
- Flere virksomheter drifter vann- og avløpsanlegg selv. Noen pumper vannet videre ferdig renset, andre renser selv
- Igjen, ofte tungt avhengig av tredjepartsleverandører. Systemeier har ofte lite innsikt og kontroll over anleggene
- Windows operativsystem ofte benyttet med spesialisert/skreddersydd software. Oppdateringer kan knekke anlegget



Sårbarheter i både IT og OT-systemer

- Manglende sikkerhetsoppdateringer
- Svake passord og gjenbruk av passord
  - Ser ofte samme passord blir benyttet flere steder, også på tvers av virksomheter
  - Fra vår erfaring er dette en av hovedårsakene til full kompromittering
- Feilkonfigurasjoner og manglende herding
- Observerer ofte nøkkelferdige løsninger med begrenset kompetanse hos systemeier
  - Systemeier eier risikoen og er ansvarlig, men bruker ofte eksterne til utførelse/drift
  - I mange tilfeller tungt avhengig av leverandør(er)
- Lite samspill mellom IT- og OT-miljøer



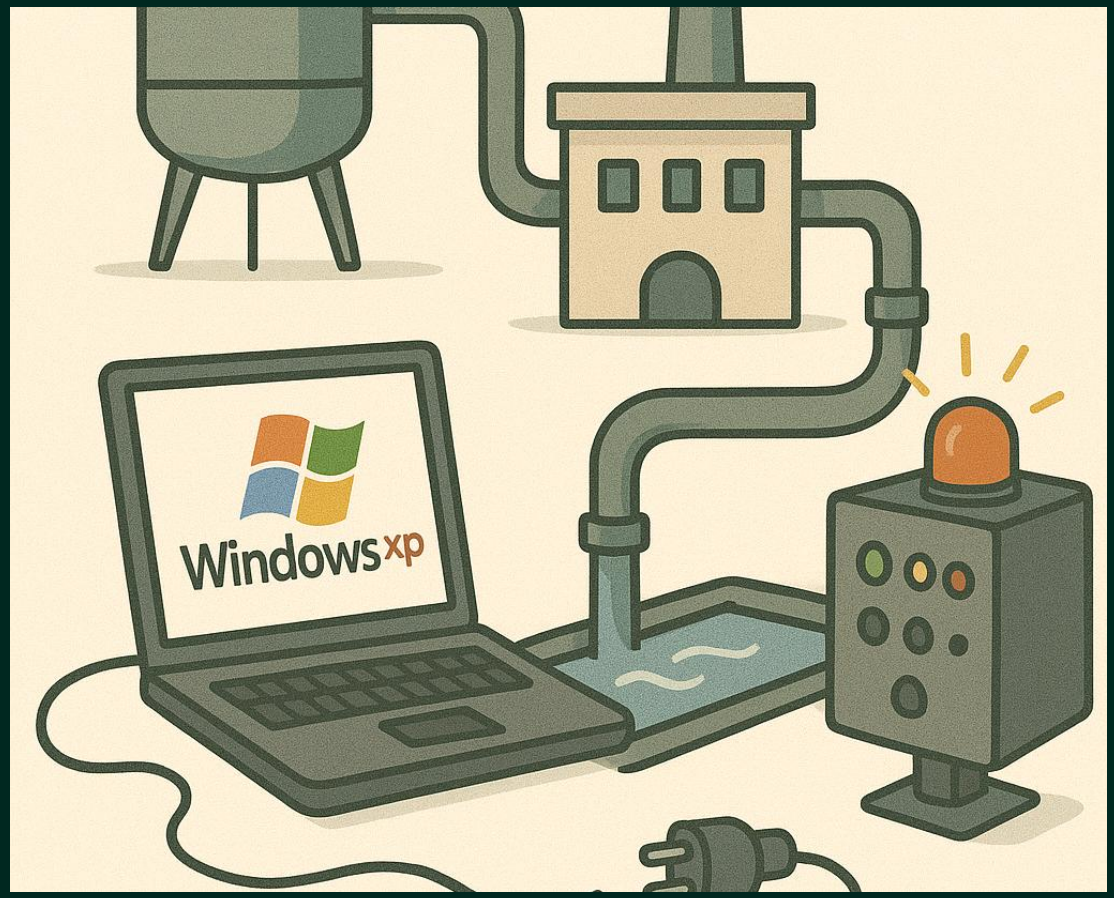
OT/VA-utstyr på internett

OT/VA-jakting av Helse- og kommuneCERT

- Vi har i perioder satt ekstra fokus på å finne utstyr
- I hovedsak bruk av åpne kilder på internett, men også vår intern database
- Omfattende søk etter kjent teknologi og produkter
- Avdekket flere hundre enheter tilhørende OT/VA
- Varslet mange medlemmer, men også andre sektorer og privat næringsliv

Resultat fra OT-jakting på internett

- Demninger
- Renseanlegg
- Kraftverk
- Høydebasseng
- PLS-er
- SD-anlegg



Hvordan finner vi disse installasjonene på internett?

- I hovedsak åpne kilder ved bruk av Censys og Shodan – men litt skanning selv
- Intern domenekunnskap hos oss (søke etter spesifikk type software/hardware)
- Vi vet nøyaktig hva vi skal søke etter basert på besøk fra vannverk (ulike komponenter i installasjonen)
- Vi har bedt virksomheter melde inn hvem de benytter som leverandør med tilhørende offentlige IP adresser og domener
- Søk etter OT-relaterte stikkord


PI_TANK
Trykk
Tank
UV
Dykk
Tank 1
Tank 2
Tank 3
Tømming av tank
Velg ønsket tank
Start tømming
1.246 m
0.00 L/min
22187 L
1.395 m
3.33 L/min
24944 L
1.346 m
-2.77 L/min
24088 L
Nedtapping min
19000
Hysterese fyllin
2000
Max fylling
24000

Magasin

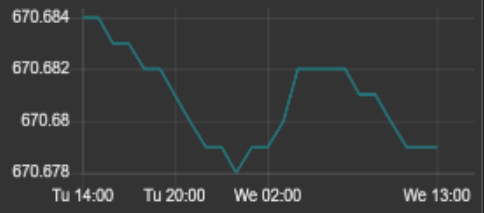
[redacted]

Oppdatert: 14/1-2026 kl 13:17

[redacted]

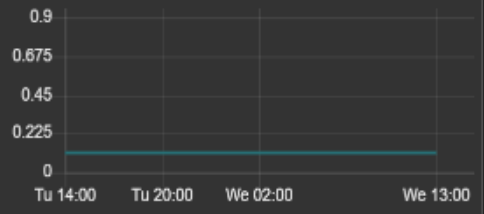
Velg periode 1 døgn

Vannstand siste periode (moh)



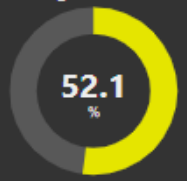
Siste døgn: -0.5 cm synkende vst

Lukeposisjon siste periode (m)



Dam-anlegg

Magasinvolum



Lukepos

Batterispenning (volt)	13.1
Batterispenning 24 (volt)	25
Lufttemperatur (C)	-2.1
Poretrykk V (m)	7.92
Poretrykk H (m)	8.449
Luke-bryter:	LOKAL
Luke lavt oljenivå:	OK
Luke kritisk lavt oljenivå:	OK
Luke kritisk avt oljetrykk:	OK
Luke motorvern:	OK
Luke endebryter åpen:	
Luke endebryter åpen:	

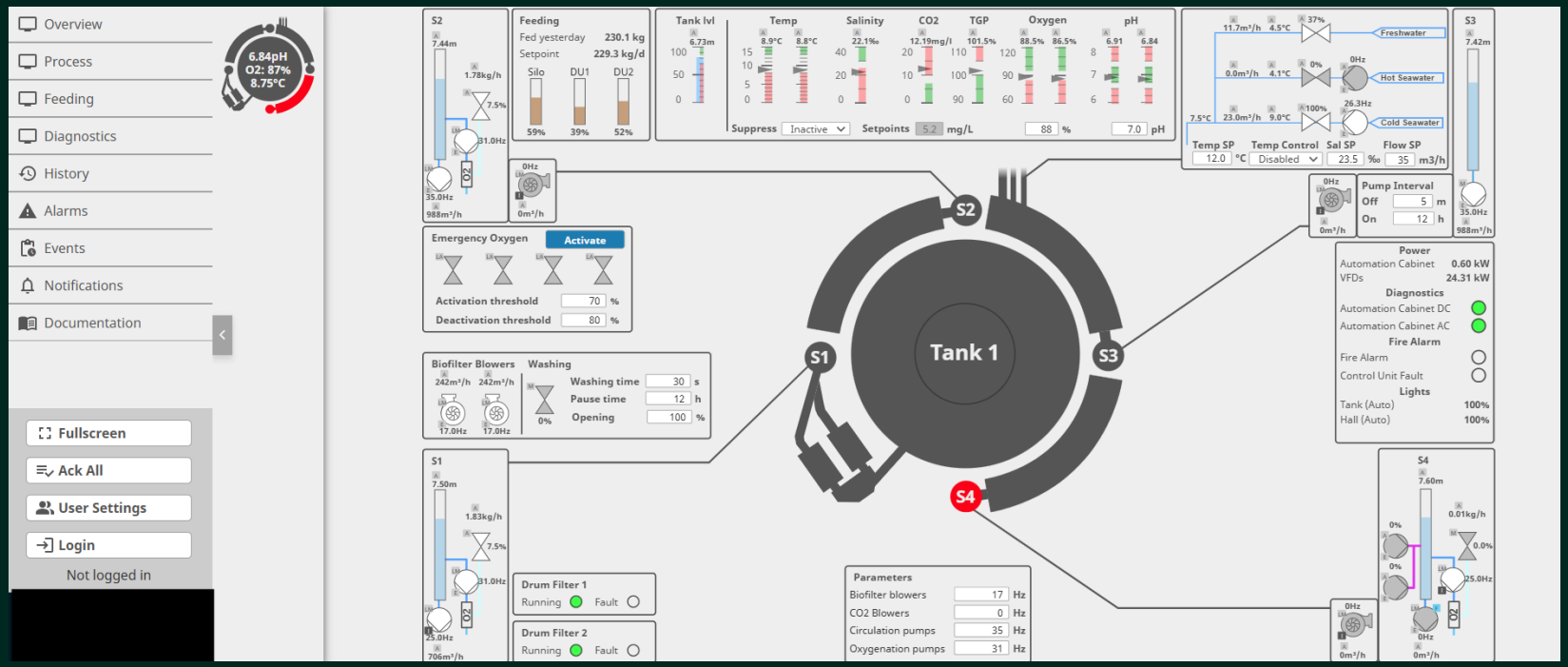
Fjernstyring

Passord for styring:

Set setpunkt (cm) :

BEKREFT TAPPELUKE STYRING

NØDSTOPP LUKE-STYRING


Overview
Process
Feeding
Diagnostics
History
Alarms
Events
Notifications
Documentation
6.84pH
O2: 87%
8.75°C
Fullscreen
Ack All
User Settings
Login
Not logged in
Tank 1
S1
S2
S3
S4
Feeding
Fed yesterday 230.1 kg
Setpoint 229.3 kg/d
Silo DU1 DU2
59% 39% 52%
Tank lvl
Temp
Salinity
CO2
TGP
Oxygen
pH
Suppress Inactive
Setpoints
Temp SP 12.0 °C
Temp Control Disabled
Sal SP 23.5 ‰
Flow SP 35 m3/h
Freshwater
Hot Seawater
Cold Seawater
Emergency Oxygen
Activate
Activation threshold 70 %
Deactivation threshold 80 %
Biofilter Blowers
Washing
Washing time 30 s
Pause time 12 h
Opening 100 %
Pump Interval
Off 5 m
On 12 h
Power
Automation Cabinet 0.60 kW
VFDs 24.31 kW
Diagnostics
Automation Cabinet DC
Automation Cabinet AC
Fire Alarm
Fire Alarm
Control Unit Fault
Lights
Tank (Auto) 100%
Hall (Auto) 100%
Drum Filter 1
Running Fault
Drum Filter 2
Running Fault
Parameters
Biofilter blowers 17 Hz
CO2 Blowers 0 Hz
Circulation pumps 35 Hz
Oxygenation pumps 31 Hz

Hva kan vi i Helse- og kommuneCERT bistå med?

- Gjennomføre sikkerhetsvurderinger av VA-anlegg
- Fortsette å jakte etter OT/VA-utstyr på internett
- Dialog med leverandører for å inkludere de som medlemmer
  - Vi har allerede flere OT-leverandører med som medlemmer
  - Målet vårt er å gjøre helse og kommune-Norge sikrere
- OT-sjekkliste
  - Gjennomført OT-webinar hvor sjekklisten ble presentert

Norsk helsenett

Helse- og KommuneCERT

for helse- og kommunesektoren

Gunnar.Johansen@nhn.no

post@helsecert.no