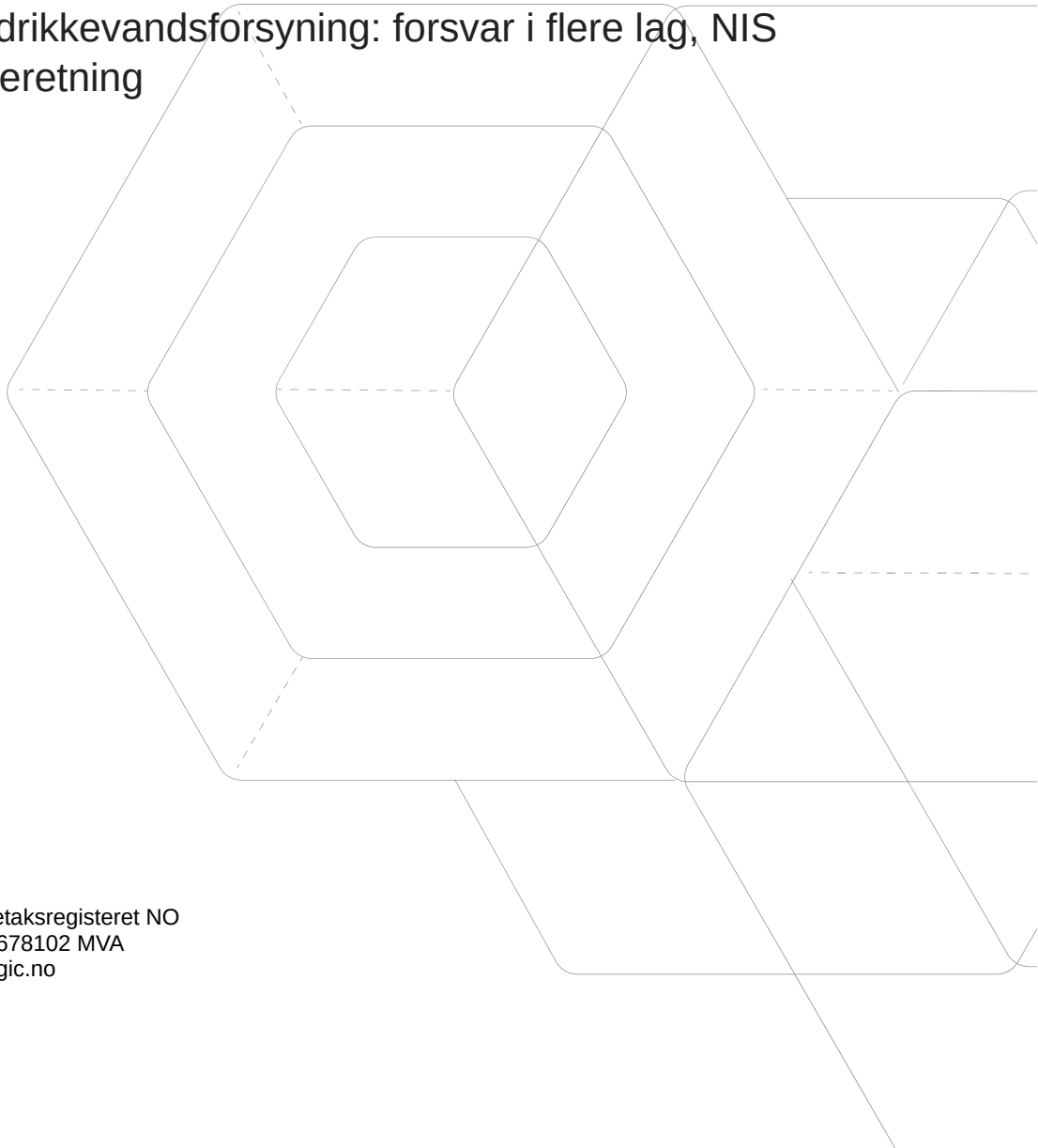
Powered by Knowledge.
Driven by Trust.

Oktober 2026

# Fra gættet adgangskode til sprængte rør

OT-sikkerhed i drikkevandsforsyning: forsvar i flere lag, NIS 2-loven og indberetning



nLogic AS

Foretaksregisteret NO
821678102 MVA
nLogic.no

**Deling:** TLP:CLEAR

**Forfatter:** Kim Hansen, Solution Architect Security, nLogic AS

**Dato:** 29. oktober 2026

**Tema:** OT-sikkerhed i drikkevandsforsyning: forsvar i flere lag, NIS 2-loven og indberetning

**Grunnlag:** Konstruert hendelse. Angrepskjeden følger et øvingsscenario (CTF) analysert av nLogic og teknikker fra dokumenterte hendelser i 2024–2025. Virksomheten, tidspunktene, adressene og loggene er fiktive.

**Målgruppe:** Ledelse samt drifts-, automations- og sikkerhedsansvarlige i danske vandværker og forsyningsselskaber

***Fiktiv hændelse.*** *Eksempel Forsyning A/S findes ikke, og tidspunkter, adresser, kontonavne og loglinjer er lavet til artiklen. Adresserne er hentet fra de blokke, der er reserveret til dokumentation. Det, der er virkeligt, er linket til kilden.*

Kl. 19:52 ringer den første borger til vagttelefonen. Der står vand i kælderen. Kl. 20:05 står vagten ved trykforøgerstationen og ser, at alle pumper kører på maksimal ydelse, mens kontrolrummet viser normalt tryk.

Hændelsen er konstrueret, men den har et forbillede. Forsvarets Efterretningstjeneste vurderede i december 2025, at »Rusland stod bag et destruktivt cyberangreb mod et dansk vandværk i 2024«, og pegede på den prorussiske gruppe Z-Pentest (FE). Ved angrebet blev trykket påvirket, så vandrør sprang (Kristeligt Dagblad).

Den 24. september hævede Styrelsen for Samfundssikkerhed trusselsniveauet for destruktive cyberangreb mod Danmark fra MIDDEL til HØJ. »Rusland fører hybridkrig mod Vesten og udviser øget risikovillighed«, sagde direktør Laila Reenberg (Ritzau). Styrelsen nævner to angrebsformer: wiperangreb og manipulation af OT, de systemer der styrer fysiske processer.

# Del 1: Til ledelsen

## Hvad der skete

Eksempel Forsyning A/S leverer drikkevand til omkring 40.000 indbyggere i Midtjylland. En PLC styrer trykforøgerpumperne ud mod ledningsnettet.

Angriberen kom ind 14 dage før. En filserver havde SSH åben mod internettet, og adgangskoden til en driftskonto blev gættet på tre sekunder. Derfra gik vejen gennem en gammel Windows-server og en vedligeholdelsesdatabase, hvor OT-adgangskoderne lå i klartekst. Med dem kom angriberen ind på jumpserveren mellem IT og OT, og jumpserveren kunne tale med PLC'en.

Hændelsesaftenen slog angriberen tre alarmer fra og hævede derefter trykindstillingen. Der var ingen trykbegrænsning uden om PLC'en. Tre ledninger sprang, og ved midnat havde kommunen udsendt en kogeanbefaling for to postnumre.

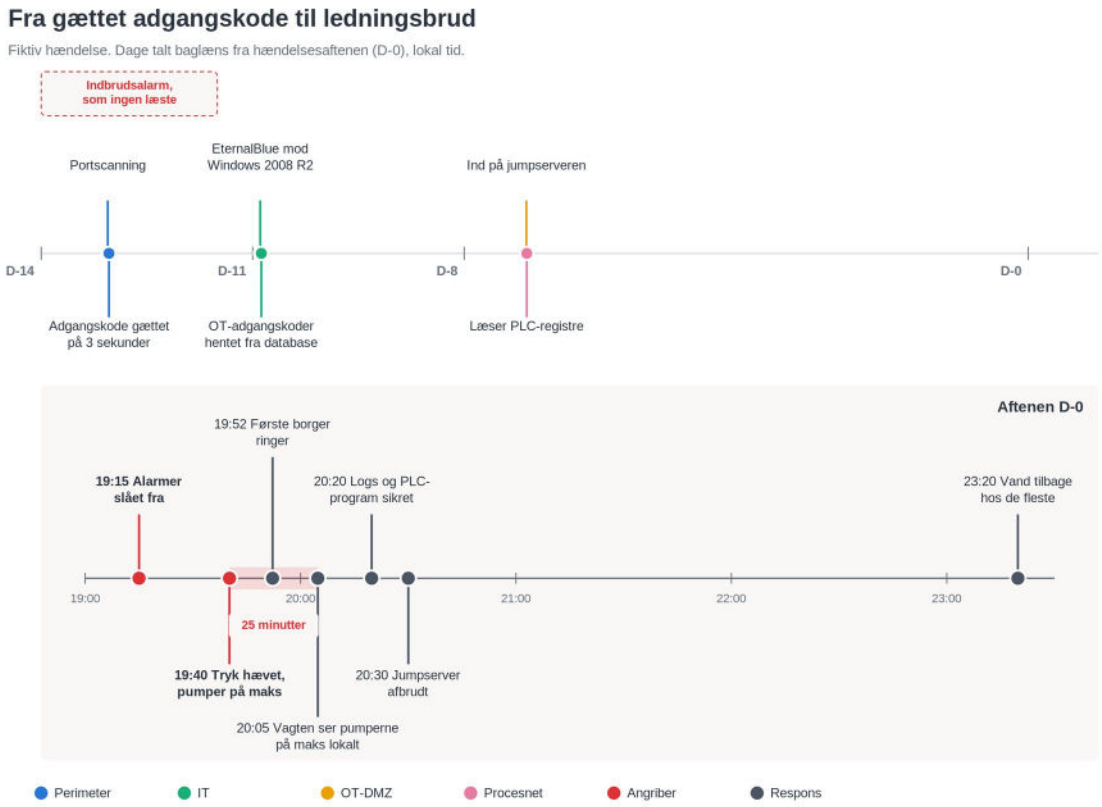
Dragos fandt svag segmentering mellem IT og OT i 81 procent af de vurderinger, firmaet lavede i 2025 (Dragos). I den her hændelse var det netop forbindelsen fra IT til PLC'en, der gjorde skaden mulig.

**Spørgsmål til ledelsen**

1. Kan vi sige med sikkerhed, at intet i IT-netværket kan sende kommandoer til vores PLC'er?
2. Hvad beskytter ledningsnettet, hvis PLC'en gør præcis det, den får besked på?
3. Hvem ringer til kommunen, og hvem taler med pressen, når borgerne mangler vand en almindelig aften?

# Del 2: Hændelsen i detaljer

## Tidslinje

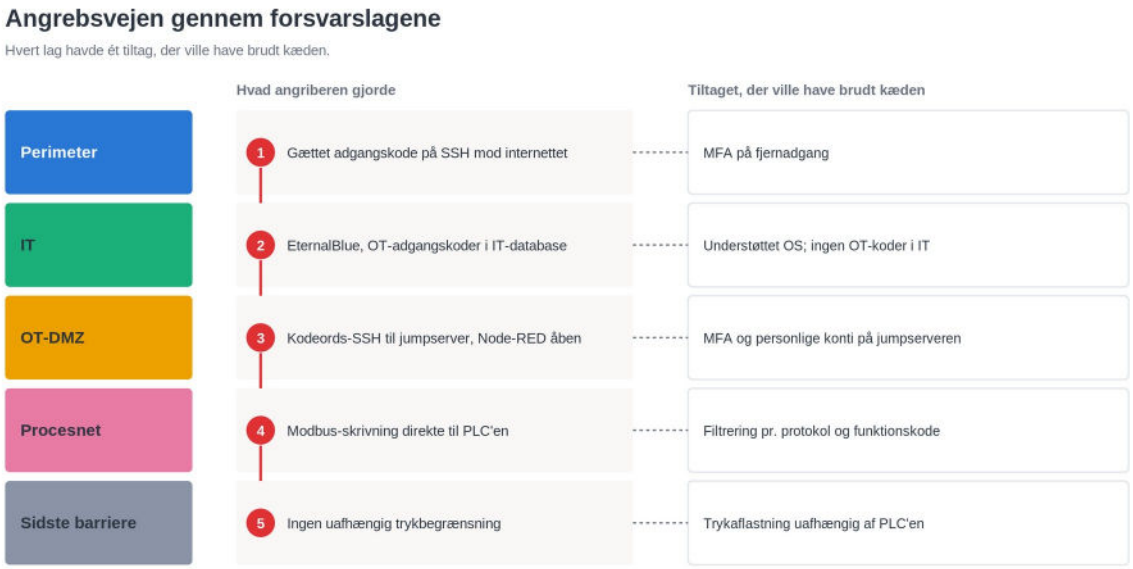



*Figur 1: Tidslinje fra D-14 til aftenen D-0. Indbruddet sker D-14, bevægelsen i IT D-11 og adgangen til jumpserveren D-8. Aftenen D-0 slås alarmerne fra 19:15, og trykket hæves 19:40. Der går 25 minutter, før vagten ser pumperne på maks kl. 20:05.*

| Tid | Hændelse | Kilde |
|---|---|---|
| D-14 22:41 | Portscanning mod 203.0.113.46. SSH svarer | Firewall-log |
| D-14 23:05 | Login som drift efter fem forsøg på tre sekunder | auth.log på fil01 |
| D-11 02:39 | MS17-010 (EternalBlue) mod app-old, en Windows Server 2008 R2 | Flowlog |

| Tid | Hændelse | Kilde |
|---|---|---|
| D-11 02:58 | Login som sa i vedligehold-db. Tabellen ot_konti læses | Databaselog |
| D-8 21:14 | SSH fra fil01 til jumpserveren ot-jump med en adgangskode fra databasen | auth.log på ot-jump |
| D-8 21:20 | Modbus-læsning af registrene for tryk, niveau og pumper | Pcap |
| D-0 19:15 | Alarmerne for højt tryk, lavt niveau i rentvandstanken og pumpefejl slås fra | Pcap |
| D-0 19:40 | Trykindstillingen hæves over den tilladte grænse, og pumperne tvinges til maksimal ydelse | Pcap, PLC'ens hændelseslog |
| D-0 19:52 | Første borger ringer om vand i kælderen | Vagtlog |
| D-0 20:05 | Vagten ser pumperne på maks lokalt og stiller dem i håndbetjening | Vagtlog |
| D-0 20:20 | Logs fra ot-jump og PLC-programmet kopieres | Hændelseslog |
| D-0 20:30 | ot-jump afbrydes fra IT-netværket | Hændelseslog |
| D-0 23:20 | Vand tilbage hos de fleste. To ledningsbrud repareres næste dag | Vagtlog |
| D+1 00:15 | PLC-leverandøren bekræfter uautoriseret Modbus-skrivning fra jumpserveren | Hændelseslog |

## Lag for lag




*Figur 2: Angrebsvejen gennem fem lag: perimeter, IT, OT-DMZ, procesnet og sidste barriere. For hvert lag viser figuren, hvad angriberen gjorde, og hvilket tiltag der ville have brudt kæden.*

Forsvar i flere lag betyder, at ét gennembrud ikke må være nok. Her blev hvert lag brudt med en svaghed, de fleste forsyninger vil kunne genkende.

Perimeteren og IT-netværket faldt på en gættet adgangskode og et styresystem, der har været uden support siden januar 2020 og manglede en opdatering fra marts 2017 (Microsoft). Det alvorligste fund var tabellen med OT-adgangskoder i vedligeholdelsesdatabasen. Den gjorde de næste lag ligegyldige.

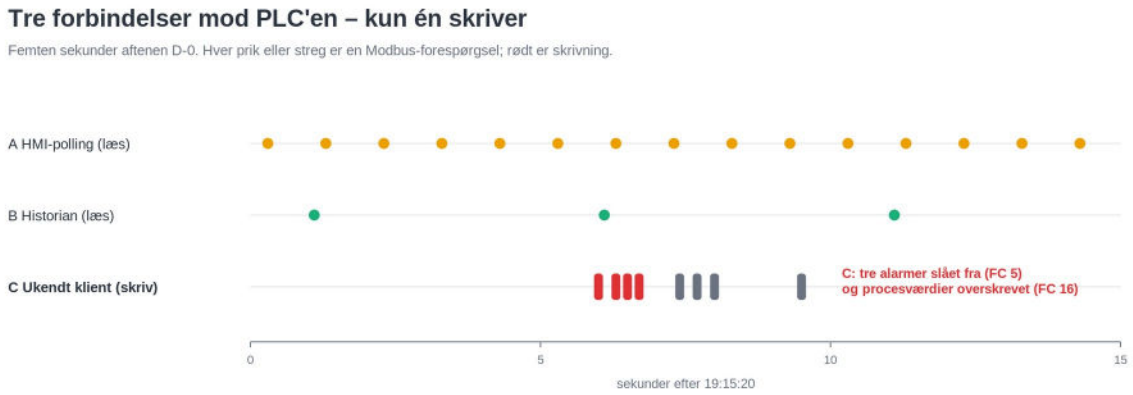
Jumpserveren lukkede alle ind, der havde den rigtige adgangskode. Node-RED på serveren havde ikke login slået til, og det er standard, indtil nogen ændrer det (Node-RED). Fra jumpserveren gik Modbus TCP direkte til PLC'en, og Modbus har ingen autentificering.

Selve angrebet havde to trin. Først gjorde alarmerne operatøren blind (Alarm Suppression, T0878), og derefter kom kommandoerne, der hævede trykket (Command Message, T1692.001). Ledningsnettet blev den sidste barriere, fordi ingen havde valgt en anden.

### Spørgsmål til næste driftsmøde

- Ligger der OT-adgangskoder i et IT-system, et regneark eller en delt postkasse?
- Hvad kan jumpserveren nå i procesnettet? Svaret skal være en liste, ikke »alt«.
- Hvad er det højeste tryk, pumperne kan levere, og hvad tåler de ældste dele af ledningsnettet?

## Trafikken, der skilte sig ud




*Figur 3: Femten sekunder Modbus-trafik mod PLC'en. HMI-pollingen læser hvert sekund og historian hvert femte. Den ukendte klient sender fire skrivninger på under ét sekund og derefter nogle læsninger.*

HMI'en og historian spørger PLC'en hele tiden, og ingen af dem skriver. Forbindelse C kom fra samme jumpserver, så en firewall, der kun ser på adresser, lukkede den igennem. En overvågning, der skelner mellem læsning og skrivning, ville have set den med det samme.

Der var også et tidligere signal. Et lille script på filserveren sendte en e-mail ved login med svag adgangskode:

```
D-14 23:05:03 fil01 sshd[19231]: Accepted password for drift from 198.51.100.50 port 58122 ssh2
D-14 23:05:04 fil01 loginvakt: INTRUSION DETECTED: weak-credential SSH login - user=drift from=198.51.100.50
```

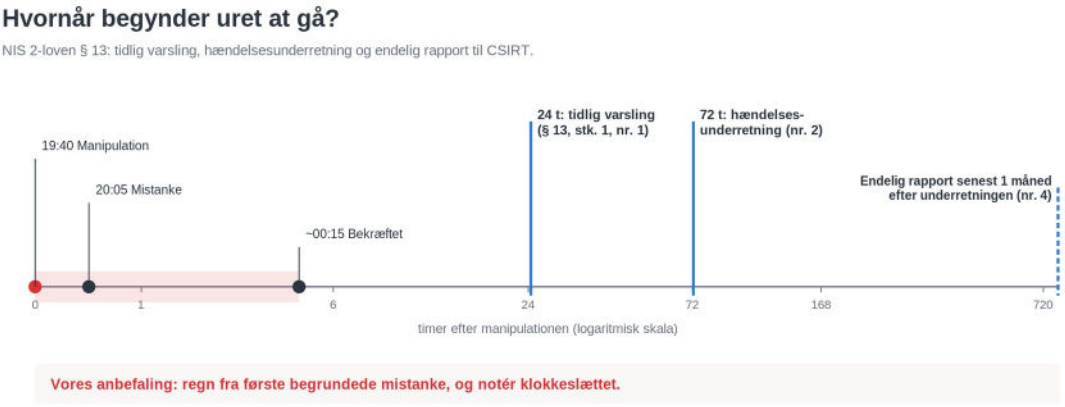
E-mailen gik til en postkasse, der blev oprettet ved installationen og aldrig læst.

## Hvad der gik godt, og hvad der ikke gjorde

Vagten stolede mere på pumperne end på skærmen og stillede dem i håndbetjening. Bagefter blev logs og PLC-program kopieret, før jumpserveren blev afbrudt, så politiet og leverandøren havde noget at arbejde med.

Det tog 25 minutter fra trykket blev hævet, til nogen så, hvad der skete, og først borgernes opkald satte gang i det. Beredskabsplanen beskrev ledningsbrud, men ikke at et ledningsbrud kunne skyldes et angreb. Ingen havde aftalt med kommunen, hvem der beslutter en kogeanbefaling sent om aftenen, og pressen ringte, før borgerne havde fået besked.

## Lovkrav og indberetning




*Figur 4: Tidsakse på logaritmisk skala fra manipulationen kl. 19:40. Mistanken kommer 20:05 og bekræftelsen omkring 00:15. Fristerne på 24 timer for tidlig varsling og 72 timer for hændelsesunderretning er markeret, og den endelige rapport senest en måned efter underretningen.*

NIS 2-loven (lov nr. 434 af 6. maj 2025) trådte i kraft 1. juli 2025. Drikkevand står i lovens bilag 1 blandt sektorer af særlig kritisk betydning. Om en forsyning er omfattet, afhænger af dens størrelse, men en mindre enhed kan også blive udpeget. En væsentlig hændelse indberettes til CSIRT efter § 13:

| Trin | Frist | Bestemmelse |
|---|---|---|
| Tidlig varsling | Senest 24 timer efter kendskab | § 13, stk. 1, nr. 1 |
| Hændelsesunderretning | Senest 72 timer efter kendskab | § 13, stk. 1, nr. 2 |
| Foreløbig rapport | På anmodning | § 13, stk. 1, nr. 3 |
| Endelig rapport | Senest 1 måned efter hændelsesunderretningen | § 13, stk. 1, nr. 4 |

Indberetningen sker via virk.dk og sendes automatisk videre til sektormyndigheden og CSIRT (Digitaliseringsstyrelsen). Den tidlige varsling skal angive, om hændelsen mistænkes at skyldes ulovlige eller ondsindede handlinger. I vores eksempel var svaret ja fra kl. 20:05.

Vores anbefaling er at regne »kendskab« fra første begrundede mistanke og notere klokkeslættet. En tidlig varsling kan suppleres, når mere er kendt. Det er værre at varsle for sent.

### Spørgsmål om indberetning

- Er vi omfattet af NIS 2-loven på grund af vores størrelse, eller kan vi blive udpeget?
- Hvem sender den tidlige varsling til CSIRT kl. 21 en almindelig aften, og hvem træffer beslutningen?
- Hvem anmelder til politiet, og hvem sørger for, at logs sikres, før noget afbrydes?

### Tiltag, ejer og tidshorisont

| Hvornår | Tiltag | Ejer |
|---|---|---|
| Denne uge | Luk SSH og andre tjenester mod internettet, eller kræv MFA. Skift alle OT-adgangskoder, der har ligget i IT-systemer | IT |
| Denne måned | Få vurderet en trykaflastning eller et trykrelæ, der virker uden PLC'en | Drift og automation |
| Denne måned | Aftal med kommunen, hvem der beslutter kogeanbefaling og borgerinformation uden for normal arbejdstid | Ledelsen |
| Dette kvartal | Jumpserver med personlige konti og MFA. Regler mod procesnettet pr. protokol og funktionskode | IT og automation |
| Dette kvartal | Beredskabsplanen beskriver, hvornår en driftsforstyrrelse behandles som cyberhændelse, hvem der varsler CSIRT, og at logs sikres før afbrydelse | Ledelsen |
| Dette kvartal | Sikkerhedsalarmer til en navngiven vagt. Test, at de kommer frem | IT-sikkerhed |
| Næste budget | Udfas eller isolér systemer uden support. OT-overvågning, der skelner mellem læsning og skrivning | IT og automation |

## Kravene bag

### Lovkrav

| Regelsæt | Bestemmelse | Indhold |
|---|---|---|
| NIS 2-loven (lov nr. 434 af 6. maj 2025) | Bilag 1 | Drikkevand blandt sektorer af særlig kritisk betydning |
| NIS 2-loven | § 13 | Tidlig varsling inden for 24 timer, hændelsesunderretning inden for 72 timer, foreløbig rapport på anmodning, endelig rapport senest 1 måned efter |

### Anbefalede rammer

| Ramme | Punkt | Ordret titel | Hvad det gælder her |
|---|---|---|---|
| CIS Controls v8.1 | 6.4 (IG1) | Require MFA for Remote Network Access | SSH mod internettet uden MFA |

| Ramme | Punkt | Ordret titel | Hvad det gælder her |
|---|---|---|---|
| CIS Controls v8.1 | 6.5 (IG1) | Require MFA for Administrative Access | Jumpserveren |
| CIS Controls v8.1 | 2.2 (IG1) | Ensure Authorized Software is Currently Supported | Windows Server 2008 R2 uden support |
| CIS Controls v8.1 | 7.3 (IG1) | Perform Automated Operating System Patch Management | Opdateringen fra marts 2017, der manglede |
| CIS Controls v8.1 | 3.11 (IG2) | Encrypt Sensitive Data at Rest | OT-adgangskoder i klartekst i databasen |
| CIS Controls v8.1 | 12.2 (IG2) | Establish and Maintain a Secure Network Architecture | Adskillelse mellem IT, OT-DMZ og procesnet |
| CIS Controls v8.1 | 13.4 (IG2) | Perform Traffic Filtering Between Network Segments | Regler pr. protokol og funktionskode mod PLC'en |
| CIS Controls v8.1 | 13.3 (IG2) | Deploy a Network Intrusion Detection Solution | Overvågning, der skelner mellem læsning og skrivning |
| CIS Controls v8.1 | 13.6 (IG2) | Collect Network Traffic Flow Logs | Flowlogs, der viser vejen gennem netværket |
| CIS Controls v8.1 | 17.1 (IG1) | Designate Personnel to Manage Incident Handling | Hvem der beslutter den tidlige varsling |
| CIS Controls v8.1 | 17.7 (IG2) | Conduct Routine Incident Response Exercises | Øvelse med kommune og vagt |
| CIS Controls v8.1 ICS Guide | Hele guiden | CIS Critical Security Controls v8.1 Industrial Control Systems (ICS) Guide | CIS' fortolkning af kontrollerne for industrielle styresystemer |

# Kilder

Links kontrolleret 28.–29.10.2026. Bilag 1 på Retsinformation blev kontrolleret 14.08.2026.


- Forsvarets Efterretningstjeneste, »Rusland er ansvarlig for destruktive og forstyrrende cyberangreb mod Danmark« (18.12.2025):

<https://www.fe-ddis.dk/da/nyheder/2025/rusland-er-ansvarlig-for-destruktive-og-forstyrrende-cyberangreb-mod-danmark/>
- Kristeligt Dagblad, »FE tilskriver cyberangreb pro-russere med forbindelse til staten« (18.12.2025): <https://www.kristeligt-dagblad.dk/danmark/fe-tilskriver-cyberangreb-pro-russere-med-forbindelse-til-staten>
- Styrelsen for Samfundssikkerhed via Ritzau, »Truslen fra destruktive cyberangreb hæves til høj« (24.09.2026). Styrelsen henviser til vejledningerne »Beskyt dig mod destruktive cyberangreb« og »Beskyttelse af OT«: <https://via.ritzau.dk/pressemeddelelse/15180895/truslen-fra-destruktive-cyberangreb-haeves-til-hoj?lang=da>
- Digitaliseringsstyrelsen, »Incident notifications«: <https://en.digst.dk/digital-governance/nis-2/incident-notifications/>
- NIS 2-loven (Retsinformation): <https://www.retsinformation.dk/eli/lta/2025/434>
- NIS 2-loven § 13 (Lovguiden): <https://www.lovguiden.dk/loven/nis-2-loven/13>
- Dragos, »Dragos 2026 OT Cybersecurity Year in Review Now Available« (17.02.2026): <https://www.dragos.com/blog/dragos-2026-ot-cybersecurity-year-in-review>
- Microsoft, MS17-010 (14.03.2017): <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>
- Node-RED, »Securing Node-RED«: <https://nodered.org/docs/user-guide/runtime/securing-node-red>
- MITRE ATT&CK for ICS, T0878 og T1692.001: <https://attack.mitre.org/techniques/T0878/>, <https://attack.mitre.org/techniques/T1692/001/>



**Kim Hansen**

Solution Architect Security
+47 40448800
kim.hansen@nlogic.no

**Kontakt oss**

nLogic AS
Karenslyst Allé 20, 0278 Oslo
Org.nr.: 821 678 102
info@nlogic.no

Powered by Knowledge.
Driven by Trust.