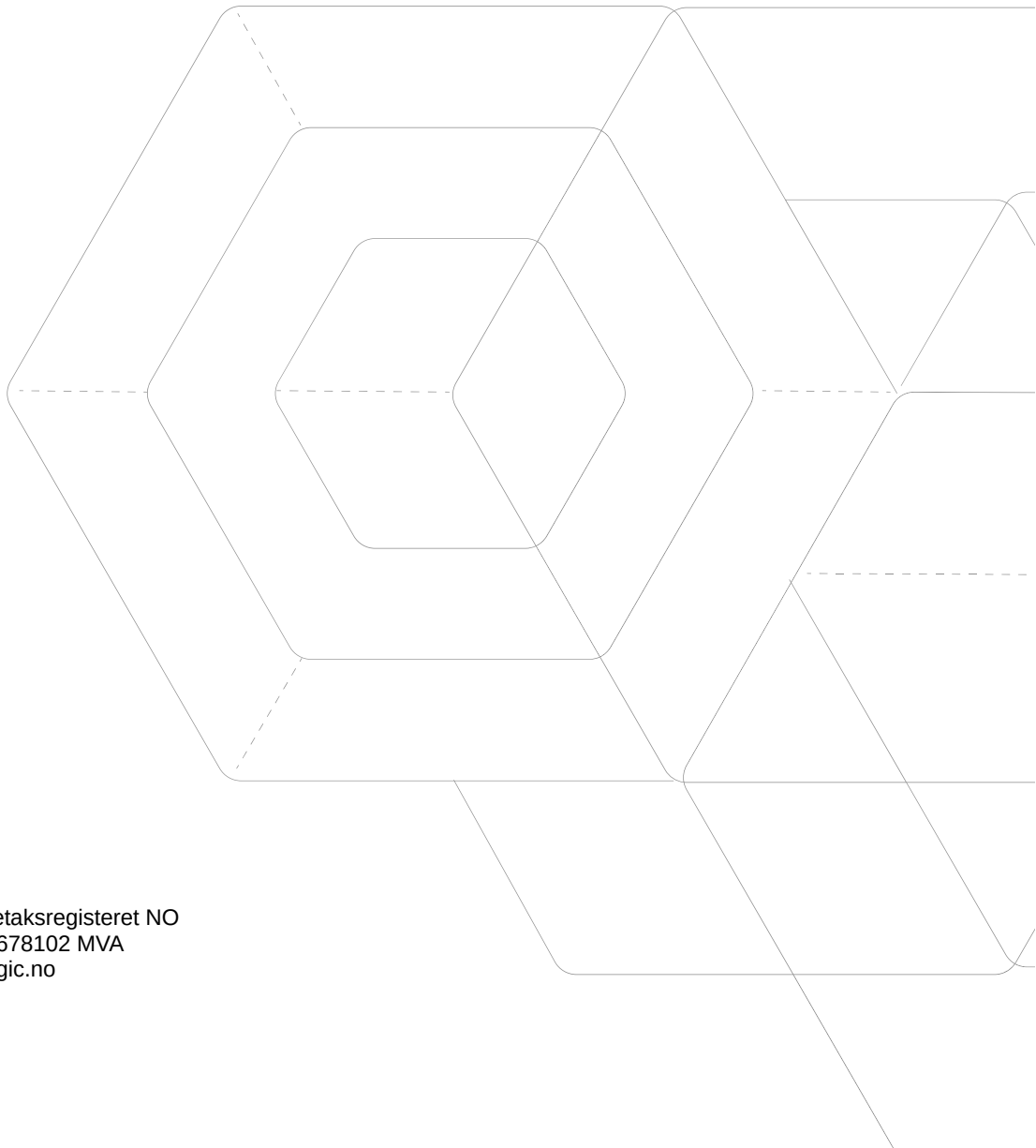
Powered by Knowledge.
Driven by Trust.

Oktober 2026

# Fem minutter og et standardpassord

OT-sikkerhet i matproduksjon: lagvis sikkerhet, regelverk og varsling



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-sikkerhet i matproduksjon: lagvis sikkerhet, regelverk og varsling

**Grunnlag:** Konstruert hendelse, bygget på mønsteret fra Bremanger 2025. Virksomheten, tidspunktene, adressene og loggene er fiktive.

**Målgruppe:** Ledelse og drifts-, automasjons- og sikkerhetsansvarlige i norsk havbruk og matproduksjon

***Fiktiv hendelse.*** *Eksempel Sjømat AS finnes ikke, og tidspunkter, adresser og logglinjer er laget for artikkelen. Adressene er fra blokkene som er reservert for dokumentasjon. Det som er ekte, er lenket til kilden.*

Klokka 19:58 en torsdag går en driftstekniker forbi kar 4 og ser at vannstanden er for lav. Skjermen i kontrollrommet viser normal drift. Han åpner inntaksventilen for hånd og starter reservepumpen. Først kl. 20:40 finner leverandøren en ukjent IP-adresse i loggen til fjernstyringspanelet.

Hendelsen er tenkt, men mønsteret er hentet fra virkeligheten. Den 7. april 2025 ble det oppdaget at noen hadde åpnet ventilen i demningen ved Risevatnet i Bremanger fra et fjernstyringspanel. Vannet forsyner et settefiskanlegg. Ventilen sto helt åpen i om lag fire timer, ifølge iLaks. En hackergruppe la ut skjermopptak av innbruddene på Telegram. PST knyttet angrepet til prorussiske aktører, men henla saken i oktober uten å finne gjerningspersonene (iLaks).

Den 27. oktober 2026 hevet NSM det nasjonale cyberrisikonivået til HØYT. NSM har sett en tredobling av vellykkede cyberoperasjoner mot norske virksomheter det siste halve året (NSM). For kritisk infrastruktur ber NSM blant annet om soner med autentisering og trafikkontroll, og om et minimumssystem som holder funksjonen i gang under en hendelse.

# Del 1: For ledergruppen

## Hva som skjedde

Eksempel Sjømat AS har et settefiskanlegg på Vestlandet. Leverandøren av vannbehandlingen har et nettbasert panel som styrer inntaksventilen og oksygeneringen. Da leverandøren byttet 4G-ruter for to måneder siden, fikk panelet en offentlig adresse. Standardpassordet var aldri byttet.

Ingen brøt seg gjennom IT-nettet. Angriperen fant panelet i et søk etter åpne styringspaneler og logget inn med passordet fra leverandørens manual. Etter fem minutter var alarmgrensene nullstilt, ventilen stengt og oksygenpumpen stoppet.

Fisken overlevde fordi en driftstekniker gikk runden sin akkurat da. Neste morgen lå et skjermopptak av innloggingen på Telegram, og en journalist ringte før ledelsen hadde rukket å samles.

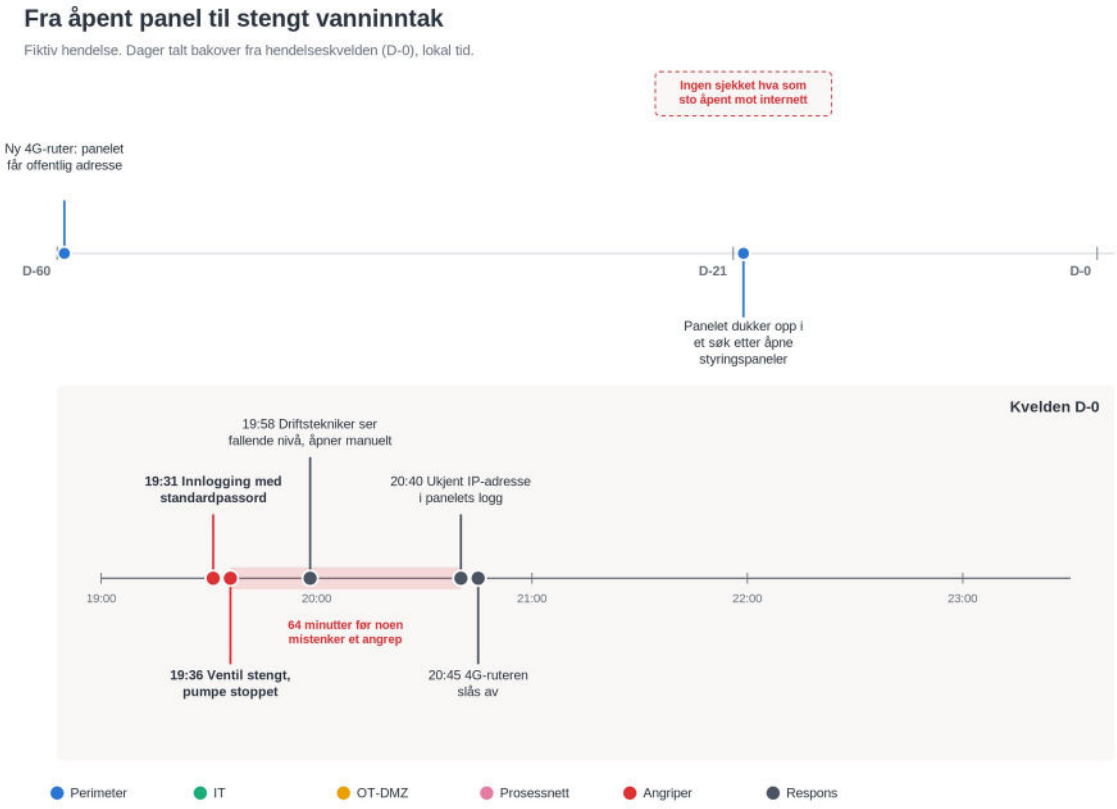
Dragos' årsrapport for 2025 beskriver dette mønsteret. 30 prosent av hendelsene Dragos håndterte, startet som et uforklart driftsproblem, og 82 prosent av virksomhetene manglet klare kriterier for når et driftsavvik skal utløse en cyberundersøkelse.

**Spørsmål til ledergruppen**

1. Hvem hos oss avgjør at et driftsavvik skal behandles som en mulig cyberhendelse, og hvilket kriterium gjelder?
2. Hvilke av leverandørene våre kan styre noe i anlegget fra utsiden, og hvem har sjekket det sist?
3. Hvem svarer pressen hvis et opptak fra anlegget vårt dukker opp på Telegram i morgen tidlig?

# Del 2: Hendelsen i detalj

## Tidslinje




*Figur 1: Tidslinje fra D-60 til kvelden D-0. Panelet får offentlig adresse D-60 og dukker opp i et søk D-21. På kvelden D-0 logger angriperen inn 19:31, stenger ventilen 19:36, og det går 64 minutter før noen mistenker et angrep kl. 20:40.*

| Tid | Hva som skjedde |
|---|---|
| D-60 | Leverandøren bytter 4G-ruter. Panelet får offentlig adresse. Standardpassordet står uendret |
| D-21 | Panelet registreres i en tjeneste som indekserer åpne styringspaneler (funnet i etterkant) |

| Tid | Hva som skjedde |
|---|---|
| D-0 19:31 | Innlogging som `service` fra 198.51.100.23 |
| D-0 19:33 | Alarmgrensene for lav vannstand og lavt oksygen settes til null |
| D-0 19:36 | Inntaksventil V-101 stenges, oksygenpumpe P-2 stoppes |
| D-0 19:58 | Driftstekniker ser lav vannstand i kar 4 og 5 på runde, åpner ventilen manuelt og starter reservepumpen |
| D-0 20:10 | Driftsleder ringer leverandøren |
| D-0 20:40 | Leverandøren finner innloggingen i panelets logg |
| D-0 20:45 | 4G-ruteren slås av. Ruterens logg er ikke kopiert |
| D+1 09:10 | Skjermopptak av innloggingen publiseres på Telegram |
| D+1 10:30 | Forholdet anmeldes til politiet |

Panelets egen logg viste innloggingen tydelig:

```
D-0 19:31:07  login ok   user=service  src=198.51.100.23
D-0 19:33:41  set        LL_LEVEL_K4=0  LL_O2_K4=0  LL_LEVEL_K5=0  LL_O2_K5=0
D-0 19:36:12  command    V-101 CLOSE
D-0 19:36:15  command    P-2 STOP
```

Ingen leste den. Loggen lå på panelet og ble bare sett når leverandøren logget inn for service.

## Hvilke lag som manglet




*Figur 2: Fem lag fra perimeter til siste barriere. Panelet sto mot internett med standardpassord og styrte PLS-en direkte, så IT-nettet og OT-DMZ var aldri i veien. Den siste barrieren var et menneske på runde.*

Lagvis sikkerhet forutsetter at angriperen må gjennom flere lag. Her gikk det an å hoppe over alle. Panelet hadde sin egen vei til internett gjennom leverandørens ruter, utenom brannmuren, utenom IT-avdelingen og utenom all overvåkning. Det er grunnen til at IT-sjefen ofte ikke vet at slike paneler finnes.

Den siste barrieren var et menneske. Det holdt denne kvelden, men ingen hadde valgt det som barriere. En lokal nivåbryter som starter reservevann uten å gå gjennom PLS-en, ville gjort jobben uansett hvem som hadde logget inn.

**Spørsmål å ta med til neste driftsmøte**

- Finnes det rutere, modemer eller paneler i anlegget som leverandører har satt opp, og som ikke står i IT-avdelingens oversikt?
- Er standardpassordene byttet på alt som kan styres utenfra, og hvordan vet vi det?
- Hvilken barriere stopper skaden hvis PLS-en gjør akkurat det den får beskjed om?

## Hva som gikk bra, og hva som ikke gjorde det

Driftsteknikeren gjorde det riktige for fisken. Leverandøren fant innloggingen etter en halvtime. Begge deler skyldtes at folk kjente anlegget.

Problemene kom etterpå. Ruteren ble slått av før noen kopierte loggen, så politiet fikk mindre å jobbe med. Ingen hadde bestemt hvem som snakker med pressen, og opptaket på Telegram kom før ledelsen hadde et felles bilde. Ingen kunne heller svare på om andre anlegg med samme leverandør hadde samme panel.

## Regelverk og varsling




*Figur 3: Tidsakse på logaritmisk skala fra ventilen ble stengt kl. 19:36. Mistanken kommer kl. 20:40 og bekreftelsen fra leverandøren rundt 22:00. Digitalsikkerhetsloven omfatter ikke mat og havbruk, men politi, Mattilsynet, forsikringsselskap og kunder kan trenge å vite.*

Digitalsikkerhetsloven gjelder virksomheter som leverer samfunnsviktige tjenester innen energi, transport, helse, vannforsyningssystemer, bank, finansmarkedsinfrastruktur og digital infrastruktur (NSM). De skal varsle hendelser som virker betydelig inn på tjenesteleveransen, til tilsynsmyndigheten, med kopi til NSM som nasjonalt kontaktpunkt, senest 24 timer etter at de fikk kjennskap til hendelsen (digitalsikkerhetsforskriften § 17). For vannverk er Mattilsynet tilsynsmyndighet (Mattilsynet). Mat og havbruk står ikke på lista. NIS2 er ikke tatt inn i norsk rett, og det er ikke avklart hvilke sektorer en norsk gjennomføring vil omfatte.

At loven ikke gjelder, betyr ikke at ingen skal vite. Mattilsynet har et eget skjema for varsling av hendelser som gir dårlig velferd for oppdrettsfisk. Politiet trenger en anmeldelse for å etterforske, og forsikringsselskapet vil ha beskjed tidlig.

Vår anbefaling er å regne «kjennskap» fra første begrunnede mistanke, her kl. 20:40, og skrive ned klokkeslettet. Et varsel kan oppdateres når mer er kjent. Det er verre å varsle for sent.

### Spørsmål om varsling

- Hvilke av tjenestene våre er omfattet av digitalsikkerhetsloven, for eksempel hvis vi også leverer drikkevann til naboer?
- Hvilken plikt har vi til å varsle Mattilsynet når fiskevelferden er truet, og hvem sender varselet?
- Hvem bestemmer om vi anmelder, og hvem sørger for at logger sikres før noe slås av?

## Tiltak, eier og tidshorisont

| Når | Tiltak | Eier |
|---|---|---|
| Denne uka | Søk etter egne offentlige adresser i en tjeneste som indekserer åpne enheter. Steng alt som er et styringspanel | IT, med leverandøren |
| Denne uka | Bytt alle standardpassord på utstyr som kan styres utenfra | Leverandøren, kontrollert av driftsleder |

| Når | Tiltak | Eier |
|---|---|---|
| Denne måneden | Lag en oversikt over all fjerntilgang leverandører har, med kontaktperson og formål | Driftsleder og innkjøp |
| Dette kvartalet | Fjerntilgang bare gjennom én løsning med personlige kontoer, MFA og logg. Skriv det inn i leverandøravtalene | IT og innkjøp |
| Dette kvartalet | Beredskapsplanen beskriver når et driftsavvik behandles som cyberhendelse, hvem som varsler hvem, og at logger sikres før frakobling | Ledelsen |
| Neste budsjett | Lokal nivåbryter og oksygenalarm som virker uten PLS-en | Automasjon og leverandør |

# Kravene dette henger på

### Lovkrav

| Regelverk | Punkt | Innhold |
|---|---|---|
| Digitalsikkerhetsloven | Virkeområde | Samfunnsviktige tjenester i sju sektorer. Mat og havbruk er ikke blant dem |
| Digitalsikkerhetsforskriften | § 17 | Varsel senest 24 timer etter kjennskap, for virksomheter som er omfattet |

### Anbefalte rammeverk

| Rammeverk | Punkt | Ordrett tittel | Hva det gjelder her |
|---|---|---|---|
| NSMs grunnprinsipper 2.5 | 2.5.1 | Styr dataflyt mellom nettverks-soner. | Panelet skal ikke ha egen vei til internett |
| NSMs grunnprinsipper 2.5 | 2.5.7 | Ha kontroll på trafikk mellom virksomheten og samarbeidspartnere/ tjenesteleverandører. | Leverandørens ruter og fjerntilgang |
| NSMs grunnprinsipper 2.6 | 2.6.7 | Bruk multi-faktor autentisering, som smartkort, sertifikater eller engangspassord, for å autentisere brukere. | Innlogging på alt som kan styres utenfra |

| Rammeverk | Punkt | Ordrett tittel | Hva det gjelder her |
|---|---|---|---|
| NSMs grunnprinsipper 4.1 | 4.1.1 | Etabler et planverk for hendelseshåndtering som ivaretar behovet for virksomhetskontinuitet ved beredskap og krise. | Kriterium for cyberhendelse, varsling, logger før frakobling |
| NSMs grunnprinsipper 4.1 | 4.1.4 | Utarbeid avtaler med relevante tredjeparter slik at disse er klare til å yte støtte dersom det kreves ved en hendelse. | Leverandøren som bistår når noe skjer |
| CIS Controls v8.1 | 1.1 (IG1) | Establish and Maintain Detailed Enterprise Asset Inventory | Oversikt over rutere og paneler leverandører har satt opp |
| CIS Controls v8.1 | 4.7 (IG1) | Manage Default Accounts on Enterprise Assets and Software | Standardpassordet fra manualen |
| CIS Controls v8.1 | 6.4 (IG1) | Require MFA for Remote Network Access | MFA på fjerntilgang |
| CIS Controls v8.1 | 12.7 (IG2) | Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure | Fjerntilgang gjennom virksomhetens egen løsning |
| CIS Controls v8.1 ICS Guide | Hele guiden | CIS Critical Security Controls v8.1 Industrial Control Systems (ICS) Guide | CIS' tolkning av kontrollene for industrielle kontrollsystemer |

# Kilder

Kontrollert 28.–29.10.2026.


- NSM, «NSM hever det nasjonale cyberrisikonivået til HØYT» (27.10.2026): <https://nsm.no/aktuelt/nsm-hever-det-nasjonale-cyberrisikonivaet-til-hoyt>
- NSM, «Ny digitalsikkerhetslov i Norge» (01.10.2025): <https://nsm.no/aktuelt/ny-digitalsikkerhetslov-i-norge>
- iLaks, «Steinvik Fiskefarm var målet til russiske hackere» (12.09.2025): <https://ilaks.no/steinvik-fiskefarm-var-malet-til-russiske-hackere/>
- iLaks, om at PST henla saken (03.10.2025): <https://ilaks.no/pro-russiske-hackere-apnet-vannkilden-til-postsmoltanlegg-na-har-pst-henlagt-saken/>
- 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>
- Mattilsynet, skjema for varsling av hendelser som gir dårlig velferd for oppdrettsfisk: <https://mattilsynet.no/skjemaer/varsling-hendelser-som-gir-darlig-velferd-for-oppdrettsfisk>
- Lovdata, forskrift om digital sikkerhet (digitalsikkerhetsforskriften): <https://lovdata.no/dokument/SF/forskrift/2025-06-20-1131>

- Mattilsynet, «Krav til vannverk i digitalsikkerhetsloven»: <https://mattilsynet.no/drikkevannsforsyning/krav-til-vannverk-i-digitalsikkerhetsloven>



**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.