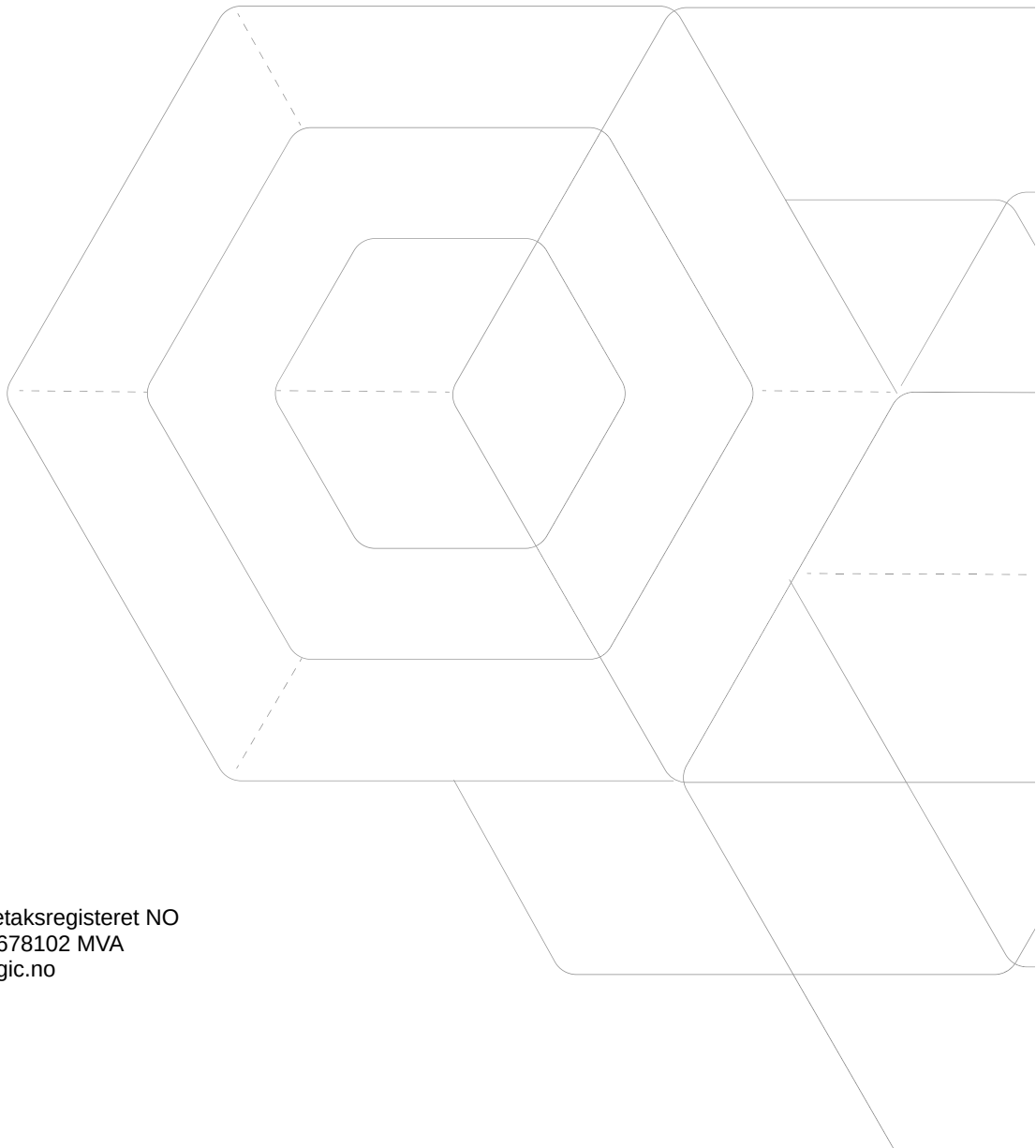
Powered by Knowledge.
Driven by Trust.

Oktober 2026

# Fyra minuter och ett delat konto

OT-säkerhet i fjärrvärme och kraftvärme: försvar i flera lager, cybersäkerhetslagen och incidentrapportering



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-säkerhet i fjärrvärme och kraftvärme: försvar i flera lager, cybersäkerhetslagen och incidentrapportering

**Grunnlag:** Konstruert hendelse. Angrepsveien bygger på dokumenterte mønstre fra 2024–2025. Virksomheten, tidspunktene, adressene og loggene er fiktive.

**Målgruppe:** Ledning samt drift-, automations- och säkerhetsansvariga inom svensk energi och fjärrvärme

***Fiktiv incident.*** *Exempel Energi AB finns inte, och tidpunkter, adresser, kontonamn och loggrader är skapade för artikeln. Adresserna är hämtade ur de block som är reserverade för dokumentation. Det som är verkligt är länkat till källan.*

Klockan 19:44 en kall kväll stoppar säkerhetssystemet pannan på hög temperatur. Operatören ser larmet från skyddet, men HMI:n visar normala värden för framledning och flöde. Det dröjer till 20:28 innan någon frågar om det kan vara en cyberattack.

Incidenten är konstruerad. Att den inte är långsökt sade ministern för civilt försvar, Carl-Oskar Bohlin, i april. En prorysk grupp med kopplingar till rysk säkerhetstjänst angrep enligt ministern ett värmeverk i västra Sverige våren 2025. Det blev inga allvarliga följder, eftersom en inbyggd skyddsmekanism slog till (SVT). I samma inslag talade NCSC-chefen John Billow om att Sverige har en ”säkerhetsskuld” på cyberområdet.

Grannländerna har sedan dess skärpt sina bedömningar, på var sin skala. Danska Styrelsen for Samfundssikkerhed höjde den 24 september hotnivån för destruktiva cyberattacker till HØJ (Ritzau). Norska NSM höjde den 27 oktober den nationella cyberrisknivån till HØYT (NSM).

# Del 1: För ledningsgruppen

## Det här hände

Exempel Energi AB driver ett kraftvärmeverk med fjärrvärmenät i Mellansverige. PLC-leverantören har sedan driftsättningen ett VPN-konto för service. Kontot delas av leverantörens tekniker och kräver bara lösenord.

En månad före incidenten smittades en av teknikernas bärbara datorer av en infostealer, ett program som samlar in sparade lösenord och skickar dem vidare. Nio dagar före incidenten loggade någon in med kontot klockan 02:14. Ingen hos Exempel Energi eller leverantören reagerade, eftersom kontot användes ofta och vid alla tider.

Den kvällen det hände stängde angriparen först av tre larm och skrev över de värden HMI:n visar. Sedan höjdes börvärdet för framledningen och cirkulationspumpen stoppades. Säkerhetssystemet, som inte går via samma PLC, stoppade pannan efter fyra minuter. Pannan klarade sig. Fjärrvärmenätet har en tröghet som gav kunderna marginal, men utan pannan hade Exempel Energi en begränsad tid på sig innan vårdboenden och bostäder började märka det.

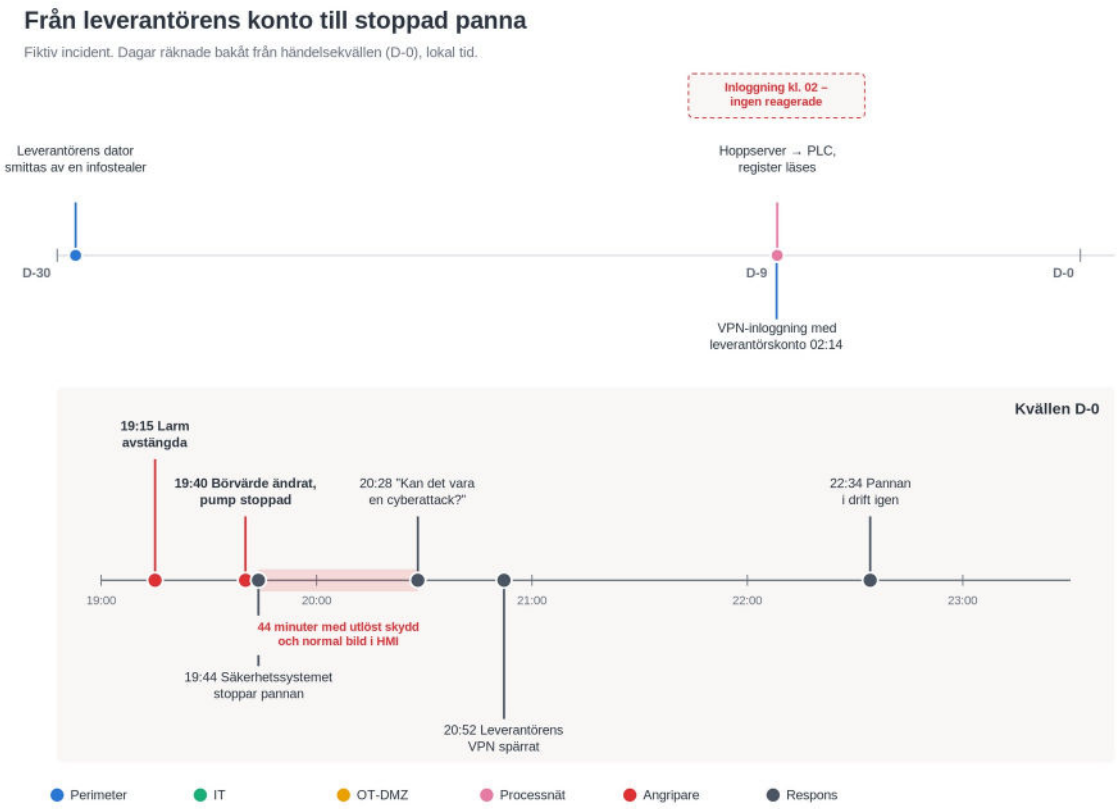
Mönstret är vanligt. I 73 procent av de incidenter Dragos hanterade under 2025 ingick kompromitterade inloggningsuppgifter till VPN eller hoppservrar (Dragos).

**Frågor till ledningsgruppen**

1. Vilka leverantörer kan i dag logga in i vår anläggning, och vem godkänner varje inloggning?
2. Vilka av våra skyddsfunktioner är oberoende av styrsystemet, och när provades de senast?
3. Vem avgör att en driftstörning ska hanteras som en möjlig cyberincident, och vad är kriteriet?

# Del 2: Incidenten i detalj

## Tidslinje




*Figur 1: Tidslinje från D-30 till kvällen D-0. Leverantörens dator smittas D-30 och kontot används kl. 02:14 D-9. Kvällen D-0 stängs larmen av 19:15, börvärdet ändras 19:40 och skyddet löser ut 19:44. Det går 44 minuter med utlöst skydd och normal bild i HMI innan någon misstänker en attack.*

| Tid | Händelse | Källa |
|---|---|---|
| D-30 | En av leverantörens tekniker får en infostealer på sin bärbara dator | Leverantörens utredning, i efterhand |
| D-9 02:14 | VPN-inloggning med kontot `lev-service` från 192.0.2.77, utan MFA | VPN-gatewayens logg |
| D-9 02:19 | Fjärrskrivbord till hoppservern `hopp01` i IT-nätet | Brandväggslogg |

| Tid | Händelse | Källa |
|---|---|---|
| D-9 02:40 | Programmeringsverktyget på hopp01 läser register i plc-fv | PLC:ns händelselogg |
| D-0 19:12 | Ny VPN-inloggning med lev-service från samma adress | VPN-gatewayens logg |
| D-0 19:15 | Tre larm stängs av: hög framledningstemperatur, lågt flöde och pumpstopp | Pcap, PLC:ns händelselogg |
| D-0 19:40 | Börvärdet för framledning höjs över tillåten gräns. Cirkulationspump P1 stoppas | PLC:ns händelselogg |
| D-0 19:44 | Säkerhetssystemet stoppar pannan på hög temperatur | Säkerhetssystemets logg |
| D-0 20:28 | Driftansvarig ringer IT-jouren och frågar om det kan vara en attack | Driftjournal |
| D-0 20:41 | VPN-loggen exporteras. Sessionen för lev-service är fortfarande aktiv | Incidentlogg |
| D-0 20:52 | Kontot lev-service spärras. Leverantören informeras | Incidentlogg |
| D-0 22:34 | Pannan är i drift igen | Driftjournal |
| D+1 09:00 | Polisanmälan. Leverantören börjar gå igenom andra kunder med samma konto | Incidentlogg |

VPN-gatewayen loggade allt som behövdes:

```
D-9 02:14:51  vpn-gw  auth ok   user=lev-service  src=192.0.2.77  mfa=none
D-9 02:16:03  vpn-gw  session   user=lev-service  assigned=10.10.8.21
D-9 02:19:40  fw      allow     10.10.8.21 -> 10.10.0.30:3389
D-0 19:12:08  vpn-gw  auth ok   user=lev-service  src=192.0.2.77  mfa=none
```

Loggen skickades till ett loggsystem som sparade den i 90 dagar. Ingen regel tittade på när kontot användes eller varifrån.

## Lager för lager




*Figur 2: Angreppsvägen genom fem lager. Leverantörens VPN-konto saknade MFA, hoppservern stod i IT-nätet och det fanns ingen OT-DMZ, så vägen till PLC:n var fri. Säkerhetssystemet var det enda lager som höll.*

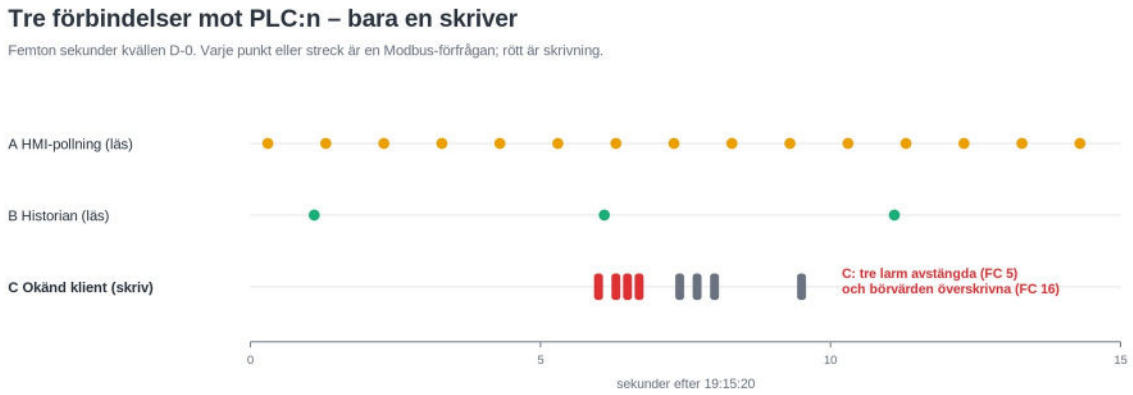
Försvar i flera lager betyder att ett enda genombrott inte ska räcka. Här räckte ett lösenord hela vägen till PLC:n, eftersom leverantörsåtkomsten gick in i IT-nätet och hoppservern där nådde processnätet direkt. Det fanns ingen OT-DMZ som angriparen behövde ta sig igenom.

Det som höll var säkerhetssystemet. Det mäter temperaturen själv och stoppar pannan oavsett vad PLC:n gör. MITRE beskriver de två teknikerna som Alarm Suppression (T0878) och Command Message (T1692.001). Det första gör operatören blind, det andra gör skadan.

### Frågor till nästa driftmöte

- Har varje tekniker hos våra leverantörer ett eget konto, eller delar de ett?
- Kan en leverantör logga in utan att någon hos oss öppnar åtkomsten först?
- När provade vi senast att säkerhetssystemet löser ut, och var finns protokollet?

## Trafiken som stack ut




*Figur 3: Femton sekunder Modbus-trafik mot PLC:n. HMI-pollningen läser varje sekund och historian var femte. Den okända klienten skickar skrivningar som stänger av tre larm och skriver över börvärden.*

HMI:n och historian frågar PLC:n hela tiden, och ingen av dem skriver. Förbindelse C kom från hoppservern, som också hade tillåtelse att prata med PLC:n. En brandvägg som bara ser adresser släppte igenom den. En övervakning som skiljer läsning från skrivning hade sett den på sekunden.

## Det som gick bra och det som inte gick bra

Säkerhetssystemet gjorde sitt jobb, och driftpersonalen körde anläggningen manuellt tills pannan var i drift igen. IT-jouren exporterade VPN-loggen innan kontot spärrades, så polisen och leverantören fick ett underlag att arbeta med.

Det tog 44 minuter från att skyddet löste ut till att någon misstänkte en attack. Under den tiden visade HMI:n normala värden, och ett utlöst skydd med normal bild borde i sig ha varit ett kriterium. Ingen hade heller bestämt vem som informerar kommunen och de största kunderna, och leverantören visste inte hur många andra kunder som delade samma konto.

## Lagkrav och rapportering




*Figur 4: Tidsaxel på logaritmisk skala från manipulationen kl. 19:40. Skyddet löser ut 19:44 och misstanken kommer 20:28. Fristerna 24 timmar för upplysning och 72 timmar för incidentanmälan är markerade, och slutrapporten senast en månad efter incidentanmälan.*

Cybersäkerhetslagen (2025:1506) gäller sedan den 15 januari 2026 och genomför NIS2-direktivet, där energisektorn även omfattar fjärrvärme och fjärrkyla (NIS2, bilaga I). Den som

omfattas ska vidta riskhanteringsåtgärder enligt 2 kap. 3 §, och ledningen ska gå utbildning i cybersäkerhet enligt 2 kap. 4 §. En betydande incident rapporteras i steg:

| Steg | Frist | Lagrum |
|---|---|---|
| Upplysning | Senast 24 timmar efter kännedom | 2 kap. 5 § |
| Incidentanmälan | Senast 72 timmar efter kännedom | 2 kap. 6 § |
| Delrapport | På begäran | 2 kap. 7 § |
| Slutrapport | Senast en månad efter incidentanmälan | 2 kap. 8 § |

Rapporterna går till CSIRT-enheten vid Försvarets radioanstalt, och Statens energimyndighet har tillsyn över energisektorn (cybersäkerhetsförordningen (2025:1507) 6, 7 och 31 §§). Myndigheten för civilt försvars föreskrifter MCFFS 2026:8 gäller sedan den 1 juli 2026 och anger vad varje rapport ska innehålla. Föreskrifterna räknar 24-timmarsfristen från att incidenten identifierats som betydande, medan lagen talar om kännedom.

Vår rekommendation är att räkna från första välgrundade misstanke, här 20:28, och skriva ned klockslaget. En upplysning kan kompletteras när mer är känt. Det är värre att rapportera för sent.

**Frågor om rapportering**

- Har vi anmält verksamheten enligt cybersäkerhetslagen, och vet ledningen att den har utbildningskravet i 2 kap. 4 §?
- Vem skickar upplysningen till FRA klockan 21 en vanlig kväll, och vem fattar beslutet?
- Vem gör polisanmälan, och vem ser till att loggar säkras innan något spärras eller stängs av?

## Åtgärder, ägare och tidshorisont

| När | Åtgärd | Ägare |
|---|---|---|
| Den här veckan | Spärra delade leverantörskonton. Öppna åtkomst bara på begäran och för en begränsad tid | IT, med leverantören |
| Den här veckan | MFA på all VPN-åtkomst, också för leverantörer | IT |
| Den här månaden | Larm på leverantörsinloggning utanför avtalad tid och från nya adresser, till en namngiven jour | IT-säkerhet |
| Det här kvartalet | Hoppserver i en egen OT-DMZ med personliga konton. Regler mot processnätet per protokoll och funktionskod | IT och automation |
| Det här kvartalet | Krav på MFA, personliga konton och incidentanmälan i alla leverantörsavtal | Inköp och ledning |

| När | Åtgärd | Ägare |
|---|---|---|
| Det här kvartalet | Beredskapsplanen anger när en driftstörning hanteras som cyberincident, vem som rapporterar till FRA och att loggar säkras först. Utlöst skydd med normal bild i HMI är ett kriterium | Ledningen |
| Nästa budget | OT-övervakning som skiljer läsning från skrivning. Provning av säkerhetsfunktionerna enligt plan | Automation och IT-säkerhet |

# Kraven det hänger på

### Lagkrav

| Regelverk | Lagrum | Innehåll |
|---|---|---|
| Cybersäkerhetslagen (2025:1506) | 2 kap. 3–4 §§ | Riskhanteringsåtgärder; ledningens utbildning |
| Cybersäkerhetslagen (2025:1506) | 2 kap. 5–8 §§ | Upplysning inom 24 timmar, incidentanmälan inom 72 timmar, delrapport på begäran, slutrapport inom en månad |
| Cybersäkerhetsförordningen (2025:1507) | 6, 7 och 31 §§ | Rapporter till CSIRT-enheten vid FRA; Energimyndighetens tillsyn |
| MCFFS 2026:8 | 2 kap. 3–5 §§ | Innehåll och frister för upplysning, incidentanmälan och slutrapport |

### Rekommenderade ramverk

| Ramverk | Punkt | Ordagrann titel | Vad det gäller här |
|---|---|---|---|
| CIS Controls v8.1 | 6.4 (IG1) | Require MFA for Remote Network Access | MFA på all VPN-åtkomst, också leverantörers |
| CIS Controls v8.1 | 6.5 (IG1) | Require MFA for Administrative Access | MFA på hoppservern |
| CIS Controls v8.1 | 5.3 (IG1) | Disable Dormant Accounts | Leverantörskonton som står öppna mellan uppdragen |

| Ramverk | Punkt | Ordagrann titel | Vad det gäller här |
|---|---|---|---|
| CIS Controls v8.1 | 15.1 (IG1) | Establish and Maintain an Inventory of Service Providers | Vilka leverantörer som har åtkomst |
| CIS Controls v8.1 | 15.4 (IG2) | Ensure Service Provider Contracts Include Security Requirements | Krav på MFA, personliga konton och incidentanmälan i avtalen |
| CIS Controls v8.1 | 12.2 (IG2) | Establish and Maintain a Secure Network Architecture | Hoppserver i egen OT-DMZ |
| CIS Controls v8.1 | 13.4 (IG2) | Perform Traffic Filtering Between Network Segments | Regler mot processnätet per protokoll och funktionskod |
| CIS Controls v8.1 | 8.2 (IG1) | Collect Audit Logs | VPN-loggen som fanns, men som ingen tittade på |
| CIS Controls v8.1 | 13.3 (IG2) | Deploy a Network Intrusion Detection Solution | Övervakning som skiljer läsning från skrivning |
| CIS Controls v8.1 | 17.1 (IG1) | Designate Personnel to Manage Incident Handling | Vem som beslutar och rapporterar till FRA |
| CIS Controls v8.1 | 17.7 (IG2) | Conduct Routine Incident Response Exercises | Övning på upplysning och incidentanmälan |
| CIS Controls v8.1 ICS Guide | Hela guiden | CIS Critical Security Controls v8.1 Industrial Control Systems (ICS) Guide | CIS tolkning av kontrollerna för industriella styrsystem |

# Källor

Länkarna kontrollerade 28.–29.10.2026.


- SVT, ”Prorysk hackerattack mot Sverige” (15.04.2026): <https://www.svt.se/nyheter/inrikes/regeringen-om-cyberhotet-mot-sverige>
- Cybersäkerhetslag (2025:1506): <https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/cybersakerhetslag-20251506_sfs-2025-1506/>
- Cybersäkerhetsförordning (2025:1507): <https://data.riksdagen.se/dokument/sfs-2025-1507.html>
- MCFFS 2026:8, föreskrifter om incidentrapportering (beslutade 13.05.2026): <https://www.mcf.se/contentassets/bf5f875837754fecaf5627012e1762ce/mcffs-2026-8.pdf>
- Europaparlamentets och rådets direktiv (EU) 2022/2555 (NIS2): <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

- 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>
- Styrelsen for Samfundssikkerhed via Ritzau, ”Truslen fra destruktive cyberangreb hæves til høj” (24.09.2026): <https://via.ritzau.dk/pressemeddelelse/15180895/truslen-fra-destruktive-cyberangreb-haeves-til-hoj?lang=da>
- NSM, ”NSM hever det nasjonale cyberrisikonivået til HØYT” (27.10.2026): <https://nsm.no/aktuelt/nsm-hever-det-nasjonale-cyberrisikonivaet-til-hoyt>
- MITRE ATT&CK for ICS, T0878 och 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.