Powered by Knowledge.
Driven by Trust.

v3. 13.08. 2026

Norske bedrifter angripes hver eneste dag: slik ser det ut i fire ukesrapporter fra et norsk driftsmiljø

Fra 640 millioner observasjoner til 16 hendelser: hva overvåkingen faktisk fant på fire uker

nLogic AS

Foretaksregisteret NO
821678102 MVA
nLogic.no

Innhold

Figurer

Tabeller

Fant ingen figurlisteoppføringer.

Forfatter: Kim Hansen, Solution Architect Security, nLogic AS

Dato: 10. august 2026

Tema: Deteksjon, hendelseshåndtering og varslingsplikt

Grunnlag: Fire sammenhengende ukesrapporter fra en MDR-tjeneste med døgnkontinuerlig overvåking, 13. juli til 10. august 2026

Målgruppe: Del 1 for ledelse og beslutningstakere, del 2 for driftspersonell og sikkerhetsansvarlige

«Hver eneste dag er det cyberangrep mot Norge og andre Nato-nasjoner. Vi vet at Russland står bak noen av angrepene.»

Forsvarssjef Eirik Kristoffersen sa det til Dagbladet 11. august. Det stemmer. Spørsmålet en ledergruppe bør stille er ikke om det er sant, men hva det betyr for dem i deres eget miljø, denne uka.

Vi har gått gjennom fire sammenhengende ukesrapporter fra et norsk driftsmiljø med døgnkontinuerlig overvåking. Denne artikkelen viser hva «hver eneste dag» ser ut som når det måles, og hvilke fire spørsmål en ledergruppe kan stille seg.

Del 1 – For ledelsen

Hva forsvarssjefen sa, og hva som forsvant i gjengivelsene

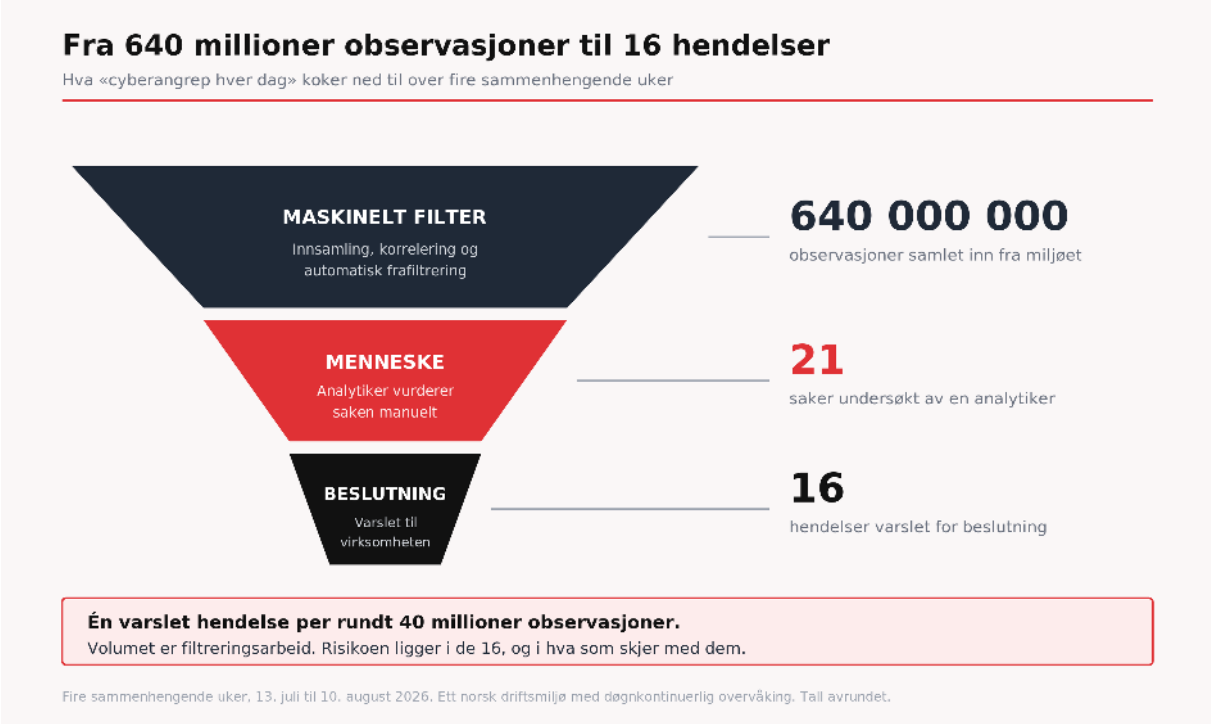
Han sa at det er cyberangrep hver dag, og at Russland står bak noen av dem, trolig for å teste samholdet i Nato. I det samme intervjuet sa han at Russland i dag ikke er i stand til å true Norge med et konvensjonelt militært angrep. Den andre halvdelen siteres sjeldnere.

Sommerens mest synlige angrep peker samme vei. Tjenestenektangrepet mot ID-porten natt til 3. august tok innloggingen til rundt femtusen offentlige tjenester ut av drift i et døgn, og traff Digdirs driftspartner, uten at det var et innbrudd. Det samme skjedde i juni, og Digdir bekreftet den gangen at angrepet ikke førte til sikkerhetsbrudd. Konsekvensen var reell, men det var ingen kompromittering.

«Angrep» dekker altså alt fra bakgrunnsstøy til innbrudd. En ledergruppe som ikke skiller mellom dem, kan verken prioritere eller berolige.

Fra 640 millioner observasjoner til 16 hendelser

Hos en kunde samlet overvåkingen inn i størrelsesorden 640 millioner observasjoner i løpet av fire uker. 21 saker ble undersøkt av en analytiker. 16 hendelser ble varslet til virksomheten for beslutning.

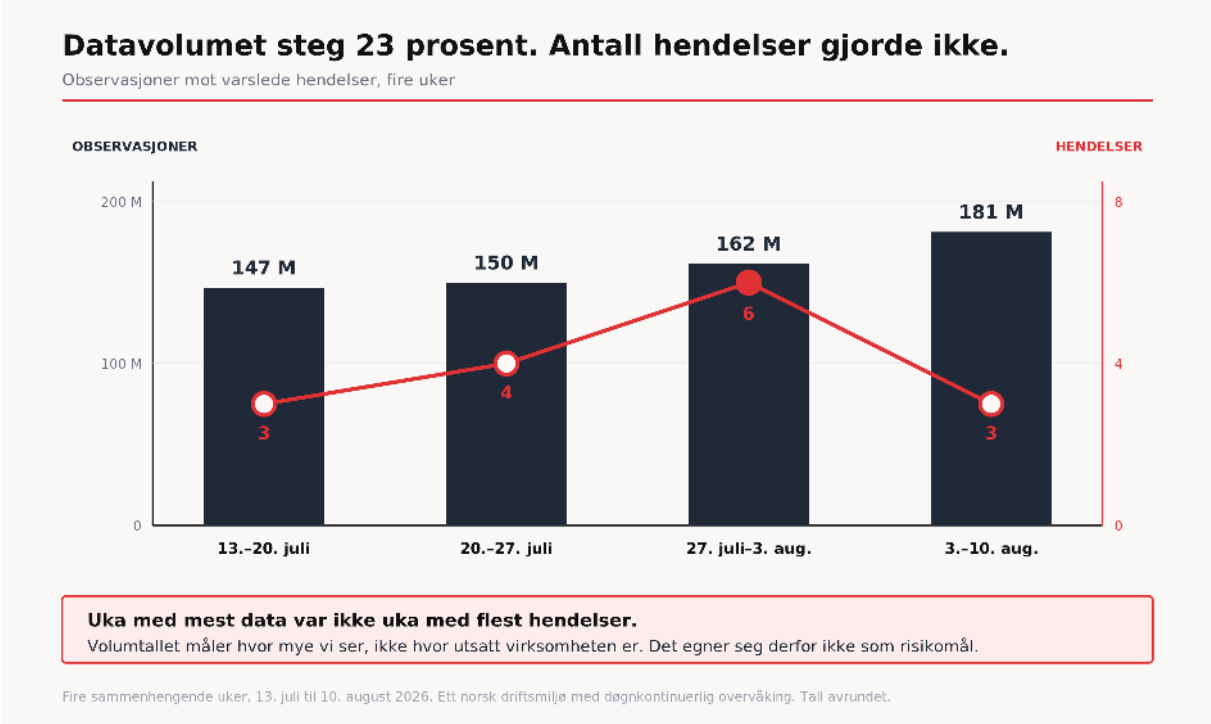


Figur 1 — Over fire uker gikk 640 millioner observasjoner ned til 21 saker undersøkt av et menneske, og videre ned til 16 hendelser varslet til virksomheten. Det er én varslet hendelse per rundt 40 millioner observasjoner.

Det er dette «hver eneste dag» betyr operativt: ikke daglig krise, men en jevn strøm som må filtreres, og en liten rest som må håndteres av noen med navn.

Volumtallet er det minst interessante i rapporten

Datavolumet steg 23 prosent gjennom de fire ukene, uten at antall hendelser gjorde det samme. Uka med mest data hadde færrest hendelser, og uka med flest hendelser lå midt på i volum.



Figur 2 — Observasjonene steg fra 147 til 181 millioner gjennom perioden, mens antall varslede hendelser gikk 3, 4, 6 og 3. Uka med mest data hadde færrest hendelser.

640 millioner er et tall som gjør inntrykk i en styrepresentasjon og som ikke betyr noe. Det måler hvor mye vi ser, ikke hvor utsatt virksomheten er. To virksomheter med samme risiko kan avvike med en faktor ti i volum, bare fordi den ene logger DNS-oppslag og den andre ikke gjør det.

Tallene som betyr noe ligger i den andre enden av trakten.

Fire spørsmål å stille seg

1. **Hvor mange av forrige måneds varslede hendelser er lukket, og hvem hos oss bekreftet det?** Ikke hvor mange som står som løst i leverandørens portal.
2. **Hvilke datakilder skal overvåkes, og hvordan får vi vite at én slutter å sende?** En stille kilde ser identisk ut med en kilde uten hendelser.
3. **Hvilke plattformer dekker deteksjonen vår faktisk?** Dekning er en egenskap ved kombinasjonen plattform og sensor, ikke ved verktøyet vi kjøpte.
4. **Hvem har myndighet til å varsle etter digitalsikkerhetsloven, og innen hvilken frist?** Svaret bør være et navn og et tall, ikke en avdeling.

Regelverket som faktisk gjelder i Norge nå

Her er det verdt å rydde, fordi det skrives feil mange steder.

NIS2 er ikke innlemmet i norsk rett per august 2026. Direktivet er ikke innlemmet i EØS-avtalen, det finnes verken norsk proposisjon eller høring om gjennomføring, og ingen ikrafttredelsesdato er fastsatt ennå. NSM skriver det selv i introduksjonsheftet til digitalsikkerhetsloven: NIS2 «skal også innføres i norsk rett, sammen med CER-direktivet, men arbeidet med det pågår fortsatt».

Det som gjelder er digitalsikkerhetsloven, i kraft 1. oktober 2025, med tilhørende digitalsikkerhetsforskrift. Den gjennomfører NIS1. Tilbydere av samfunnsviktige tjenester skal melde inn tjenestene sine, og varsle om hendelser som virker betydelig inn på leveransen.

Fristen er 24 timer. Overtredelsesgebyr kan ilegges med inntil 25 G eller fire prosent av årsomsetningen, med et tak på 50 millioner kroner. NSMs veiledere til loven og forskriften er utgangspunktet for den som skal finne ut om virksomheten er omfattet.

Denne fristen forutsetter at noen oppdager hendelsen, klassifiserer den og har myndighet til å varsle. Det er nøyaktig dette som er kritisk. Det er ikke nok å oppdage hendelsen — den må analyseres og varsles, og det er kravet i regelverket.

Del 2 – For drift og sikkerhetsansvarlige

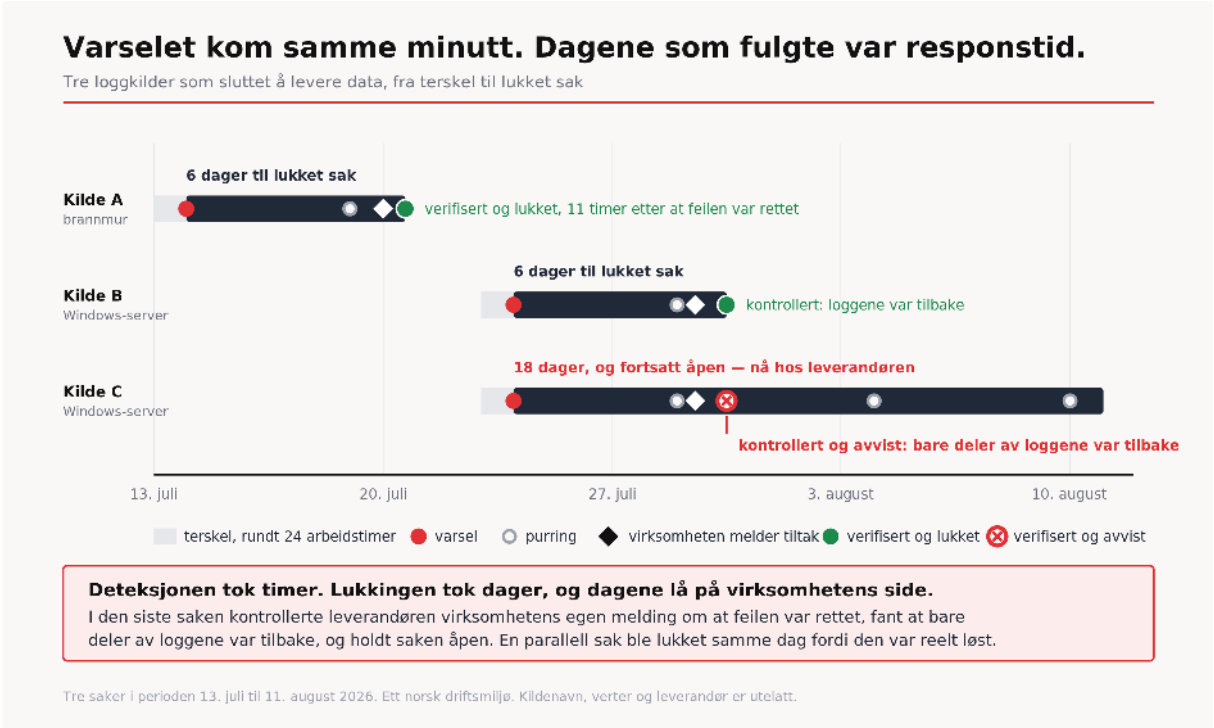
Fire mønstre gikk igjen gjennom de fire ukene. Ingen av dem er et angrep i seg selv, men alle fire avgjør om et angrep faktisk ville blitt sett.

Kilden som ble stille, og hvor fort noen sa fra

Tre loggkilder sluttet å levere data i løpet av perioden: én brannmur og to Windows-servere.

I alle tre tilfellene gikk varselet til virksomheten **i samme minutt som terskelen ble brutt**. Terskelen er rundt 24 arbeidstimer uten data fra en kilde som har levert stabilt. To av kildene ble oppdaget i samme sekund. Deretter fulgte automatiske purringer til den navngitte saksbehandleren hos virksomheten, og analytikere som kontrollerte om dataene faktisk kom tilbake.

Det er verdt å være presis her, fordi liggetid er lett å lese som blindhet: **deteksjonen tok timer, mens dagene som gikk med til å finne og rette årsaken, lå på virksomhetens side.**



Figur 3 — Tre loggkilder som ble stille. Varselet gikk i samme minutt som terskelen ble brutt i alle tre tilfellene. Den siste saken ble kontrollert av leverandøren og avvist, fordi bare deler av loggene var tilbake.

Brannmuren viste seg å ha en konfigurasjonsfeil etter en endring. Den ble rettet, og leverandøren bekreftet og lukket saken elleve timer etter at virksomheten meldte fra.

Den mest lærerike av de tre er den siste. Virksomheten restartet loggagenten på to servere samme ettermiddag og meldte begge som løst. Leverandøren kontrollerte begge. Den ene var reelt løst og ble lukket dagen etter. **Den andre ble ikke lukket.** Hendelseslogger fra verten kom fram igjen, men webserverloggene gjorde det fortsatt ikke. Saken ble holdt åpen, purret på nytt, og til slutt eskalert til en forespørsel om agentens konfigurasjonsfil og loggfil.

Dette er prinsippet «verifisert, ikke antatt» satt ut i praksis av noen andre enn oss selv, mot vår egen melding om at noe var fikset. En leverandør som lukker på kundens ord, ville ha avsluttet saken 30. juli, og da hadde en delvis blindsone stått åpen uten at noen visste om den.

Nyansen som er lett å miste: verten var aldri helt stille: Windows-hendelsesloggene kom hele veien, og det var bare én kildetype fra samme vert som falt bort. En overvåking som teller verter framfor kilder, ville rapportert grønt.

Ærlighetspunkt om rammeverkene: NSMs grunnprinsipper har ikke noe tiltak som dekker at en kilde slutter å levere. 3.2.5 krever at innsamlingen verifiseres, og 3.2.6 handler om manipulering av innsamlede data. Nærmest kommer 3.2.5, men kravet om per-kilde-overvåking med terskel og varsling må hentes fra CIS Control 8, særlig Safeguard 8.11 om jevnlig gjennomgang av logger.

Dekningsgapet

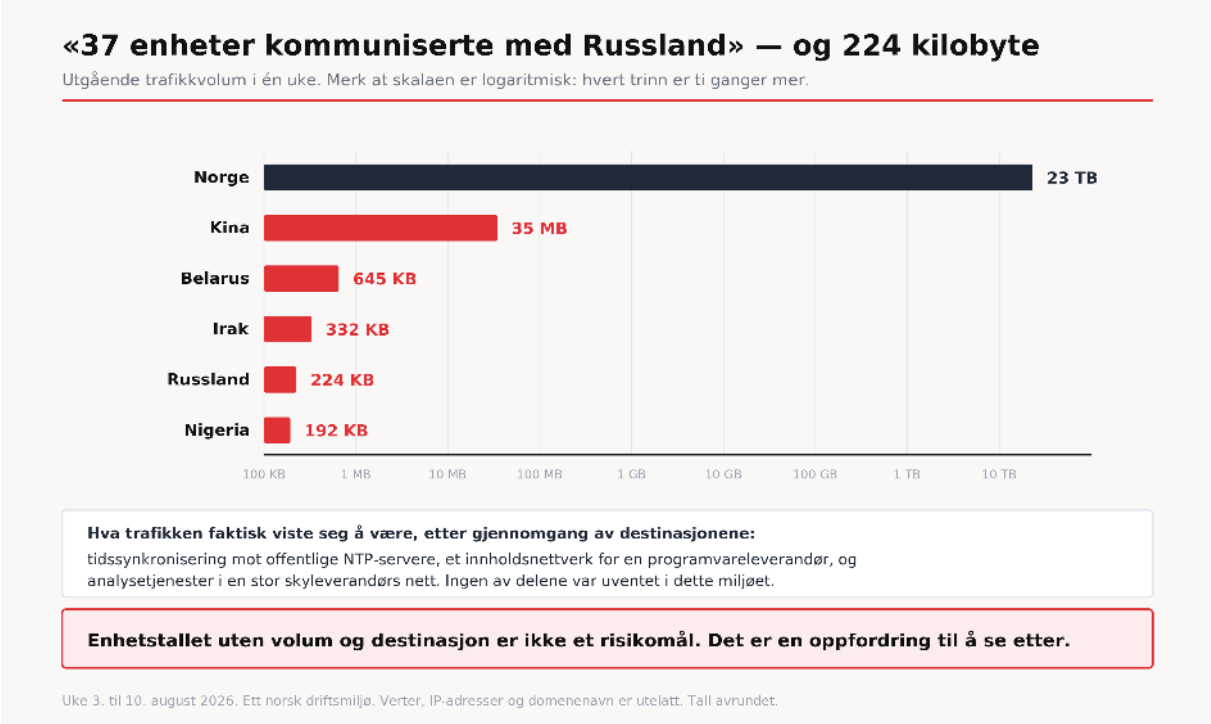
En kjent sårbarhet ble ikke rapportert på en nyere serverplattform i miljøet, ikke fordi den var lukket, men fordi kombinasjonen av sårbarhet og plattform ikke var dekket av innsamlingen. Også dette kom som en sak fra leverandøren selv, meldt som et dekningsgap framfor å bli oppdaget av kunden.

Samme periode viser bevegelsen den andre veien: fjorten nye loggkilder ble oppdaget automatisk 27. juli. Dekningsflaten endrer seg hele tiden, i begge retninger.

Dekning er ikke en egenskap ved verktøyet, men ved hver enkelt kombinasjon av plattform, agent og datakilde, og den endrer seg hver gang det rulles ut en ny OS-versjon. En virksomhet som tar i bruk en ny serverplattform arver ikke dekningen fra den gamle. Ny plattform i produksjon er derfor en dekningshendelse, ikke bare en driftshendelse, og kartlegging og sårbarhetsskanning må oppdateres i samme endring.

Støyen som ser farlig ut

Rapportene har en egen seksjon for utgående trafikk til land som regnes som interessante. Titalls enheter kommuniserte utgående mot Kina og Russland hver eneste uke i perioden. Det er tallet som havner i en ledelsesoppsummering.



Figur 4 — Utgående trafikkvolum i én uke på logaritmisk skala. 23 terabyte innenlands, mot 35 megabyte til Kina og 224 kilobyte til Russland.

Går man inn i destinasjonene, viser det seg å være tidssynkronisering mot offentlige NTP-servere, et innholdsnettverk for en programvareleverandør, og analysetjenester i en stor skyleverandørs nett. Volumet mot Russland var noen hundre kilobyte for hele uka. Samme uke gikk det over tjue terabyte innenlands.

Det betyr ikke at trafikken er uinteressant, men at enhetstallet ikke kan leses som en trussel før destinasjonene er sett på. En ledergruppe som får «trettisju enheter snakket med Russland» uten den analysen, tar enten feil beslutning eller ingen.

Det som faktisk gjentok seg

I tre av fire uker kom det varsler om autentisering eller enhetsregistrering fra hostingleverandører med lav utbredelse, ikke fra samme kilde og ikke som en samlet kampanje, men som en jevn bakgrunnsstøy av forsøk fra infrastruktur som er leid for anledningen.

Det er dette «hver eneste dag» ser ut som fra innsiden: ikke et angrep med navn, men kontinuerlig testing av identitetslaget fra billig og kortlevd infrastruktur. Deteksjonen fanget forsøkene fordi hostingleverandørens utbredelse i seg selv er et signal. Det forutsetter at noen kjenner normaltilstanden i miljøet, slik NSM 3.3.2 krever.

Hva dette faktisk sier om leverandørvalget

Fire uker er for kort til å bedømme en leveranse. Men tre ting i materialet er verdt å ta med i en vurdering av hvilken tjeneste en virksomhet skal ha.

Overvåking av loggkildenes helse må være en del av tjenesten, ikke noe kunden må be om. Varsler må gå til en navngitt person hos kunden og purres automatisk når de blir liggende. Og en sak skal lukkes på verifisert observasjon framfor på kundens melding om at noe er gjort. Det siste er det som skiller en tjeneste som produserer varsler fra en tjeneste som produserer kontroll.

Vår erfaring er at dette er kjøpsvilkår som er verdt å be om skriftlig, framfor å anta at de følger med.

Modenhetsnivået dette forutsetter

Mesteparten av det vi beskriver over ligger på CIS Implementation Group 2, ikke IG1. **Control 13 har ingen IG1-safeguards i det hele tatt.** Sentralisert varsling (13.1) og sentralisert logglagring (8.9) er begge IG2.

Det betyr ikke at en IG1-virksomhet er sjanseløs, men at rekkefølgen ligger fast: få IG1 på plass først, og ikke kjøp en overvåkingstjeneste i troen på at den erstatter kontrollene under.

Kravene dette henger på

Rammeverk	Punkt	Hva det krever
NSMs grunnprinsipper 3.2	3.2 – Etabler sikkerhetsovervåkning	Avgjør hvilke deler av IKT-systemet som skal overvåkes
NSMs grunnprinsipper 3.2	3.2.5	Verifiser at innsamling fungerer etter hensikt. **Nærmeste analogi for stille kilder, ikke et direkte treff**
NSMs grunnprinsipper 3.3	3.3.2 og 3.3.6	Kjenn normaltilstanden i informasjonssystemene, og etabler rutine for eskalering av alarmer
NSMs grunnprinsipper 1.2	1.2 – Kartlegg enheter og programvare	Grunnlaget for å vite hva deteksjonen skal dekke
CIS Controls v8.1	Safeguard 8.2 (IG1), 8.9 og 8.11 (IG2)	Samle logger, sentralisere dem, og gjennomgå dem jevnlig
CIS Controls v8.1	13.1 og 13.6 (IG2), 13.11 (IG3)	Sentralisert varsling, flow-logging, og justering av terskler
CIS Controls v8.1	17.1 og 17.3 (IG1)	Utpek hvem som håndterer hendelser, og etabler prosess for rapportering
Digitalsikkerhetsloven	I kraft 01.10.2025	Varslingsplikt ved hendelser som virker betydelig inn på tjenesteleveransen. 24 timer
NIS2-direktivet (EU) 2022/2555	21(2)(b) og 21(2)(f)	Hendelseshåndtering, og prosedyrer for å vurdere om tiltakene faktisk virker. **Ikke gjennomført i norsk rett**

Har dere en MDR-tjeneste i dag, er de fire spørsmålene over et rimelig sted å begynne. Vi har satt dem sammen til en kort sjekkliste med hva et godt svar ser ut som, hvilken kontroll det svarer på, og hva som er det vanligste dårlige svaret. Den kan bes om fra nLogic: kim.hansen@nlogic.no

Om grunnlaget

Tallene er hentet fra fire sammenhengende ukesrapporter, 13. juli til 10. august 2026, fra ett norsk driftsmiljø med døgnkontinuerlig overvåking. Virksomheten er ikke navngitt, og rapportene

er gjennomgått med tanke på at ingen enhetsnavn, IP-adresser, domenenavn, kontonavn eller saksnumre skal kunne leses ut av teksten eller figurene. Volumtall er avrundet.

Ett miljø over fire uker er nok til å vise et mønster, men for lite til å generalisere til norsk næringsliv, og det er heller ikke poenget her. Poenget er at tallene finnes, at de kan leses, og at spørsmålene de reiser er de samme uansett hvilken leverandør som produserer rapporten.

Kilder

Alle lenker verifisert 11.08.2026.

Nyhetssaken

- Dagbladet 11.08.2026 – «Det er cyberangrep hver dag» – primærkilden for sitatet fra forsvarssjefen
- Aftenposten 11.08.2026 – Forsvarssjefen: Daglige cyberangrep mot Norge
- Aftenposten 03.–04.08.2026 – Normal drift hos alle offentlige tjenester etter dataangrep – tjenestenektangrepet mot ID-porten

Regelverk

- NSM – Veiledere til digitalsikkerhetsloven og digitalsikkerhetsforskriften – inngangen for virksomheter som skal avklare om de er omfattet
- Digitalsikkerhetsloven (LOV-2023-12-20-108) – i kraft 01.10.2025
- Digitalsikkerhetsforskriften (FOR-2025-06-20-1131) – § 24 om overtredelsesgebyr
- NIS2-direktivet (EU) 2022/2555 – artikkel 20, 21 og 23
- Justis- og beredskapsdepartementets EØS-notat om NIS2 – status på gjennomføring. Sist oppdatert 23.08.2023

Rammeverk

- NSMs grunnprinsipper for IKT-sikkerhet v2.1 – kapittel 1 Identifisere og kartlegge, kapittel 3 Oppdage, kapittel 4 Håndtere og gjenopprette
- CIS Critical Security Controls v8.1 – Control 8, 13 og 17 med Implementation Group-merking

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.