FAKTA

Nr 3/2021

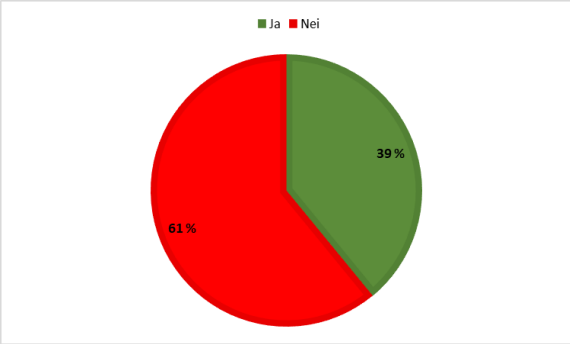
Sikring av driftskontrollsystemer

Digitalisering i kraftforsyningen medfører økt sårbarhet og flere angrepsflater mot driftskontrollsystemer. Dette kan kunne føre til at det blir mer krevende å beskytte seg mot målrettede og opportunistiske cyberangrep. Forebyggende sikringstiltak, evne til å oppdage hendelser og beredskap når hendelser inntreffer kan redusere risikoen for funksjonssvikt i driftskontrollsystemet.

NVE har gjennomført undersøkelse om informasjonssikkerhet for å danne et bilde av IKT-sikkerhetstilstanden i kraftforsyningen. Spørreundersøkelsen ble sendt til IKT-sikkerhetskoordinatorer. NVE mottok 117 svarskjema fra IKT-sikkerhetskoordinatorer i juni 2021. Besvarelsene fordeler seg på 45% nettselskap, 20% konsern, 20% kraftprodusenter, 9% fjernvarme og 6% annet. Det er flest små selskap i utvalget: 60% har 0-50 ansatte, 17% har 50-99 ansatte, 14% har 100-249 ansatte og 9% har 250 ansatte eller flere.

Driftsmodeller

Kraftberedskapsforskriften spesifiserer at «det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg», jf. kbf §7-1.
Undersøkelsen avdekker at 39% av virksomhetene kjøper driftskontrolltjenester av en annen KBO-enhet, illustrert i Figur 1. Resultatene er i liten grad påvirket av størrelsen på virksomhetene.



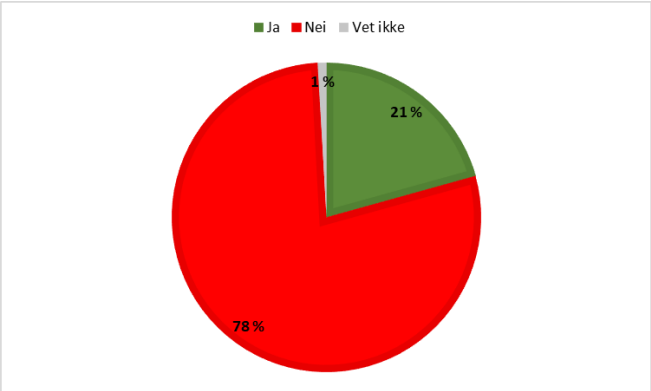
Figur 1: Kjøper virksomheten driftskontrolltjenester fra en annen KBO-enhet? N = 105

Videre kartlegger undersøkelsen i hvilken grad virksomhetene drifter driftskontrollsystem på vegne av andre KBO-enheter.

Figur 2 viser at virksomheter som drifter driftskontrollsystem på vegne av andre KBO-enheter utgjør 21% og er i hovedsak større selskap. 78% drifter ikke driftskontrollsystem på vegne av andre KBO-enheter.

NVE har ansvar for å forvalte landets vann- og energiressurser, utvikle samfunnets evne til å håndtere flom- og skredfare og varsle om naturfare. NVE har hovedkontor i Oslo og regionkontor i Narvik, Trondheim, Hamar, Førde og Tønsberg. I tillegg har vi senter for fjellskredovervåking i Stranda og Kåfjord.
Faktaarket er utarbeidet av Johannes Fagermyr, Gloria Treider, Fredrik Karlsen Tøien og Hanna Remvang

NVE hovedkontor
Middelthuns gt. 29
Postboks 5091, Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95
nve@nve.no



Figur 2: Drifter virksomheten driftskontrollsystem på vegne av andre KBO-enheter? N=116.

Få uønskede IKT-hendelser i driftskontrollsystemer med konsekvenser for driftskontrollsystemets funksjonalitet

Driftskontrollsystemenes kritikalitet er synliggjort gjennom forskriftskrav som sier at disse systemene alltid skal virke etter sin hensikt (kbf § 7-1). Undersøkelsen viser at driftskontrollsystemer i mindre grad enn administrative IT-systemer har blitt utsatt for uønskede IKT-sikkerhetshendelser som har medført konsekvenser for drift. Undersøkelsen avdekker at 3% (4 nettselskap) blant 115 virksomheter oppgir å ha hatt sikkerhetshendelser med konsekvens for driftskontrollsystemets funksjon siste 12 måneder. Sikkerhetshendelsene har ført til kortere nedetid for driftskontrollsystemet. Hendelsene skyldes tekniske feil og naturhendelser og kan ikke knyttes direkte til cyberangrep. Hendelsene har heller ikke påvirket forsyning eller leveranse av elektrisitet.

KBO-enhetene skal varsle og rapportere alle ekstraordinære hendelser til NVE (kbf §§ 2.5-2.6). Alle uønskede hendelser i digitale systemer skal også varsles til KraftCERT (§ 6-9 bokstav c). Terskelen for å melde fra om hendelser skal være lav.

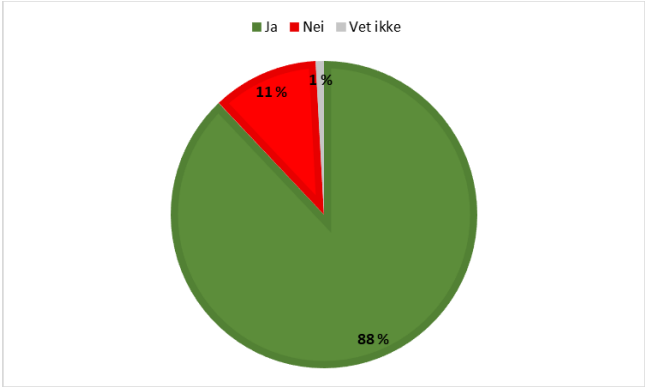
Trusler og angrep mot operasjonell teknologi i vekst

KraftCERT har observert få angrep rettet mot operasjonell teknologi (OT) i KraftCERTs medlemssektor og i Norden generelt. Internasjonalt har det vært målrettet phishing mot brukere på administrativt IT-system med påfølgende lateral bevegelse og angrep på OT-nett. Utpressingsskadevare på administrative IT-nettverk og prosessnett trekkes frem som viktige deler av trusselbildet. I undersøkelsen til NVE har 8% av virksomhetene rapportert om uønskede hendelser i administrativt IT-system som har hatt konsekvenser for virksomhetens drift.

Forebyggende sikring i driftskontrollsystemer gjennom tilgangskontroll og sårbarhetsadministrasjon

To viktige tiltak i forbyggende sikring er å rette sårbarheter i programvare og ha god tilgangskontroll. Risiko for alvorlige hendelser reduseres når sårbarhetsvarsler fra KraftCERT og leverandører blir rettet. Dersom sikkerhetsoppdatering ikke kan gjennomføres, må man vurdere andre sikringstiltak som reduserer risikoen.

I undersøkelsen svarer 88% av virksomhetene at de har rutiner for å håndtere sårbarhetsvarsel fra KraftCERT eller leverandører. 11% mangler rutiner, se Figur 3.



Figur 3 Har virksomheten rutiner for å håndtere sårbarhetsvarsel fra for eksempel KraftCERT eller leverandører? N=116

Rutiner alene er ikke nok. Det trengs også menneskelige ressurser. På spørsmål om virksomhetene har personell som håndterer sårbarhetsvarsel svarer 95% ja.

Undersøkelsen viser at 60% av virksomhetene har rollebasert tilgangskontroll til lokalkontrollanleggene, 30% har ikke slik tilgangskontroll og 10% vet ikke.

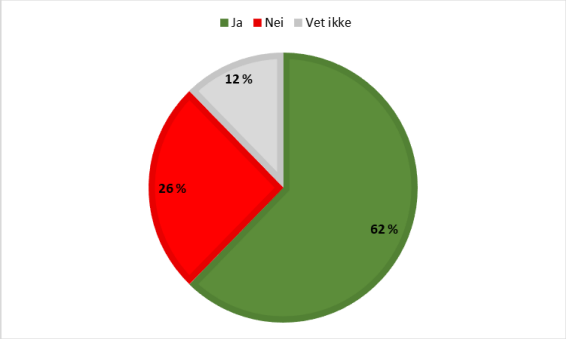
Monitorering/overvåkning

Med monitorering/overvåkning av nettverkstrafikken i driftskontrollsystemet er det mulig å oppdage om en trusselaktør forsøker å trenge seg inn i systemet.

Figur 4 viser at 62% av virksomhetene har monitorering/overvåkning av datanettverkstrafikken i driftskontrollsystemet, mens 26% har ikke slik overvåkning. 12% svarer vet ikke.

På dette spørsmålet er det forskjeller knyttet til virksomhetsstørrelse. Blant små virksomheter er det en

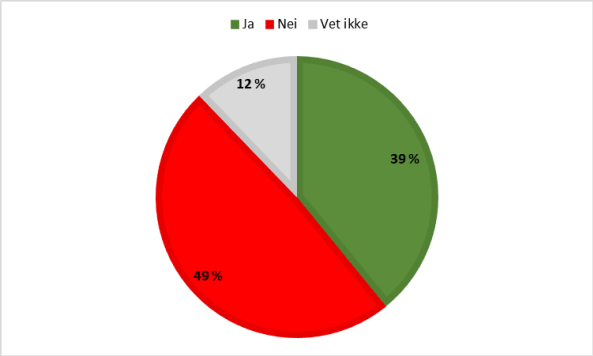
større andel, 36% (24 virksomheter), som ikke har monitorering sammenlignet med større virksomheter.



Figur 4 Har driftskontrollsystemet monitorering/overvåkning av datanettverkstrafikk?, N=116

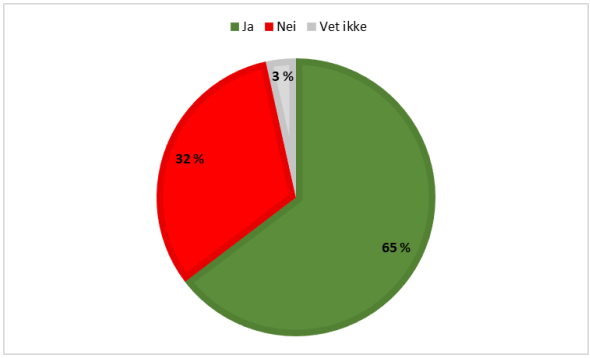
Håndtering av hendelser -verktøy, prosedyrer og bistand fra tredjepart

I undersøkelsen opplyser 39% av virksomhetene at de benytter sikkerhetsstyringsverktøy (Security Incident and Event Management) eller lignende, 49% benytter ikke slike verktøy og 12% vet ikke (Figur 5).



Figur 5 Benytter virksomheten seg av SIEM verktøy eller lignende, for eksempel logging, analyse og hendelsesoversikt? N= 115

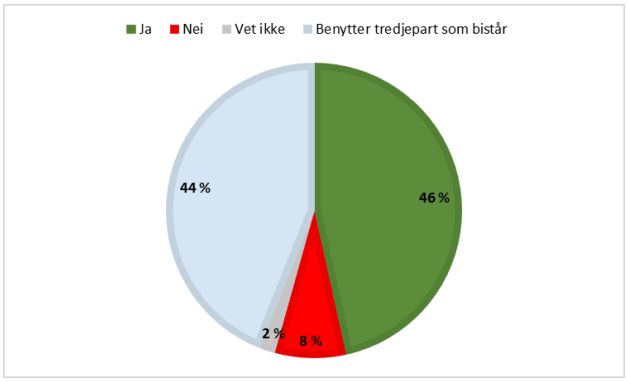
25% drifter SIEM-systemet selv, 40% har delvis satt ut tjenesten til leverandør, og 35% har satt ut tjenesten helt til leverandør.



Figur 6 Har virksomheten prosedyrer for å undersøke hendelser i driftskontrollsystemet? N=116

Selv om halvparten av virksomhetene ikke har et SIEM-system eller tilsvarende på plass, er det en større andel som opplyser at de har prosedyrer for å undersøke hendelser i driftskontrollsystemet. Figur 6 viser at 65% har prosedyrer for å undersøke hendelser i driftskontrollsystemet, 32% har ikke prosedyrer og 3% vet ikke.

Av 44 virksomheter som har internt organisert driftskontrollfunksjon, er det 8 som har opplyst at de ikke har prosedyrer for å undersøke hendelser i driftskontrollsystemet. Samtlige av disse virksomhetene er små selskaper med færre enn 50 ansatte.



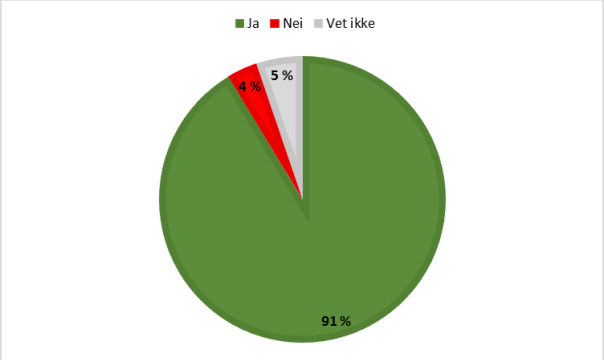
Figur 7 Overvåker og håndterer virksomheten selv hendelser i driftskontrollsystemet? N=116

På spørsmål om virksomheten selv overvåker og håndterer hendelser i driftskontrollsystemet svarer 46% at de gjør det selv, 44% benytter tredjepart (leverandør) som bistår, og 8% svarer nei (Figur 7).

«Nødknapp» når uhellet er ute

Undersøkelsen viser at 91% av virksomhetene kan lett isolere driftskontrollsystemet i en beredskapssituasjon. 4%

har svart at de ikke kan isolere systemet mens 5% har svart at de ikke vet, se Figur 8.



Figur 8 Kan driftskontrollsystemene lett isoleres i en beredskapssituasjon? N= 116

Hendelseshåndtering er en organisert reaksjon på en sikkerhetshendelse. Målet er å begrense skade og minimere gjenopprettingstap. De tekniske aspektene ved hendelseshåndtering omfatter flere trinn (Ljøsang, 2021):

1. Triage – sortering av hendelser
2. Analyse av hendelsen
3. Skadebegrensning
4. Utryddelse av trusselen
5. Gjenoppretting
6. Lukke saken

I kraftforsyningen er det i tillegg krav til varsling og rapportering av hendelser (Kbf §§ 2.5-2.6 og 6-9 bokstav c).

Forskriftskrav til sikring av driftskontrollsystemer

Kbf § 6-9 stiller krav til sikring av alle digitale systemer (NVE, 2019). Forskriftskravene bygger på NSMs Grunnprinsipper for IKT-sikkerhe,t og kravene gjelder også for driftskontrollsystemer. Sintef har gjort en evaluering av NSMs Gunnprinsipper for IKT-sikkerhet og funnet at med noen tilpasninger kan disse også brukes i prosesskontrollsystemer (Jaatun, Karin, & Stine, 2021).

Kbf kapittel 7 omhandler sikring av driftskontrollsystemet. Kbf regulerer imidlertid et helhetlig sikringsregime, og dekker både teknologi, organisasjon og personell. Det er viktig å lese hele forskriften dersom man skal sikre driftskontrollsystemene.

NVE har utarbeidet veileder til forskriften som forklarer hvordan virksomheter som er underlagt kraftberedskapsforskriften, kan tilfredsstille de regulatoriske kravene. Veilederen henviser til nasjonale veiledere og aktuelle internasjonale standarder (NVE, 2020).

Sikkerhetsråd

- Sørg for å ha god oversikt over driftskontrollsystemets oppbygging, grensenitt mot andre systemer og arkitektur, programvarelisenser og tjenesteleveranser, rutiner for deteksjon, logging og håndtering av hendelser. God oversikt er grunnlaget for alt sikkerhetsarbeid.
- Sørg for å ha personell, rutiner og systemer som hjelper til med å overvåke driftskontrollsystemene, til å oppdage og håndtere uønskede IKT-hendelser i driftskontrollsystemene.

Sørg for IKT-sikkerhet i tjenesteutsatte deler av virksomheten. Se for eksempel NVEs retningslinjer for IKT-sikkerhet i anskaffelser (Maal, Krogedal, & Gjengstø, 2018)

Etabler og vedlikehold gode rutiner for mottak og håndtering av sårbarhetsvarsler fra KraftCERT eller leverandører. Uten at man følger med, er det svært vanskelig å opprettholde sikkerhetsnivået i driftskontrollsystemet. Dersom sårbarheter ikke kan lukkes fordi det kommer i konflikt med systemtilgjengelighet eller andre hensyn, må KBO-enheten vurdere andre sikringstiltak som reduserer risikoen.

Kontakt

For spørsmål til faktaarket ta kontakt med beredskapsseksjonen ved NVE.

Referanser

Jaatun, M. G., Karin, B., & Stine, K. S. (2021). *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer. IKT-sikkerhet – Robusthet i petroleumssektoren 2020.* Trondheim: Sintef digital.

Ljøsang, A. (2021). *Informasjonssikkerhet. Teori og praksis.* Oslo: Universitetsforlaget.

Maal, M., Krogedal, K., & Gjengstø, A. (2018). *IKT-sikkerhet i anskaffelser og tjenesteutsetting, NVE Rapport nr 1/2020.* Oslo: NVE.

NVE. (2019, 01 01). *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften). Récupéré sur lovdata.no: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157?q=kraftberedskapsforskriften*

NVE. (2020, 12 20). *Veiledning til kraftberedskapsforskriften.* Récupéré sur nve.no: https://www.nve.no/energi/tilsyn/kraftforsyningsber edskap/veiledning-til-kraftberedskapsforskriften/