FAKTA

Nr 2/2021

Informasjonssikkerhetsledelse i kraftforsyningen

Informasjonssikkerhet inngår i styring og ledelse i enhver virksomhet. Kraftforsyningen er underlagt en rekke krav i kraftberedskapsforskriften som også dekker informasjonssikkerhet.

NVE har i 2021 gjennomført en spørreundersøkelse om ledelse av informasjonssikkerhet blant KBO-enheter. Svar fra 135 beredskapsledere ble mottatt i mai/juni 2021 og er fordelt på 42% nettselskap, 25% kraftprodusenter, 12% fjernvarmeselskap, 13% konsern, og 8% andre selskaper.

Digitalisering endrer risikobildet

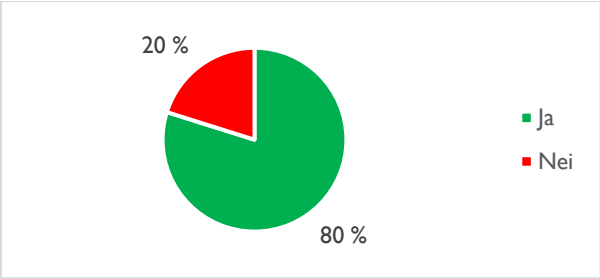
Mulighetene for feil og sårbarheter øker med økt systemkompeksitet og endret trusselbilde. Nasjonal sikkerhetsmyndighet (NSM) uttaler følgende : « Vi står overfor et taktskifte innenfor digital risiko i Norge. Antall alvorlige hendelser registrert hos Nasjonalt cybersikkerhetssenter (NCSC) i NSM i 2020 var tre ganger så mange som i 2019 (Nasjonal sikkerhetsmyndighet, 2021). Løsepengevirus rammer bredt og vilkårlig. I tillegg er sikkerhet i leverandørkjeder blitt en stor utfordring. KraftCERT ser at antall angrep gjennom leverandører, partnere og kunder øker. Det er stor variasjon i angrepsmål og angrepsteknikker, som igjen understreker trusselaktørenes evne til å tilpasse seg ulike forsvarsverk og angrepsmål (KraftCERT, 2021). I NVEs undersøkelse i 2021, kom det fram at 8% av virksomhetene hadde hatt uønskede IKT-hendelser i sine administrative IKT-systemer med konsekvenser for virksomhetens drift. Mange av hendelsene er knyttet til uønskede IKT-hendelser hos leverandører. 3% av virksomhetene hadde hatt uønskede hendelser i driftskontrollsystemet med betydning for driftskontrollsystemets funksjonalitet.

De fleste virksomhetene har en strategi for informasjonssikkerhet

Styret og toppledelsen har som ansvar å definere virksomhetens målsettinger, visjoner og verdigrunnlag, og de må balansere ulike hensyn. I undersøkelsen svarte 80% av beredskapslederne at de har en IKT-strategi eller digitaliseringsstrategi koplet til virksomhetens strategi og overordnet mål. Denne prosentandelen er like stor som prosentandelen som har svart at de har en IKT-sikkerhetsstrategi, se Figur 1.

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. Utarbeidet av Gloria Treider, Fredrik Tøien, Johannes Fagermyr og Hanna Remvang.

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

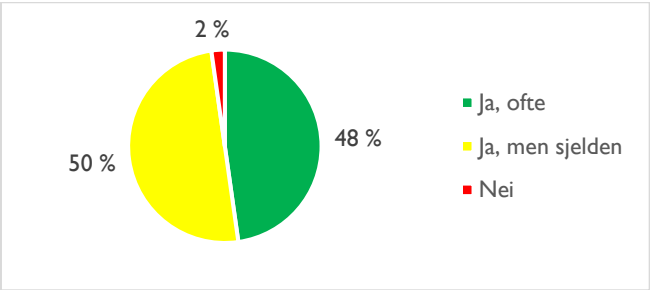


Figur 1 Har virksomheten en IKT-sikkerhetsstrategi? N= 134

Styring av informasjonssikkerhet består av å definere strategiske målsettinger for informasjonssikkerhet, sørge for at de blir nådd, styre sikkerhetsrisiko med effektiv bruk av organisatoriske ressurser, påse at ledelsessystemet for informasjonssikkerhet fungerer hensiktsmessig og at resultatet følger forventninger og målsettinger (ISACA, 2008).

Ledermøter følger opp informasjonssikkerheten

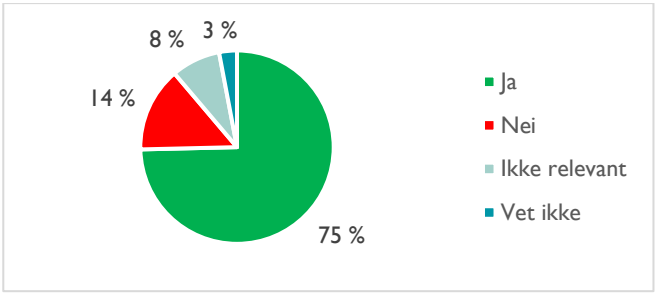
Ledermøtene er viktige for å følge opp strategiske målsettinger. I undersøkelsen har NVE stilt spørsmål om tema på ledermøtene. IKT-sikkerhet er ofte tema på ledermøter hos 48% av virksomhetene. 50% av virksomhetene svarer at IKT-sikkerhet er sjelden tema på ledermøtene, se Figur 2.



Figur 2 Er IKT-sikkerhet et tema på møter? N= 134

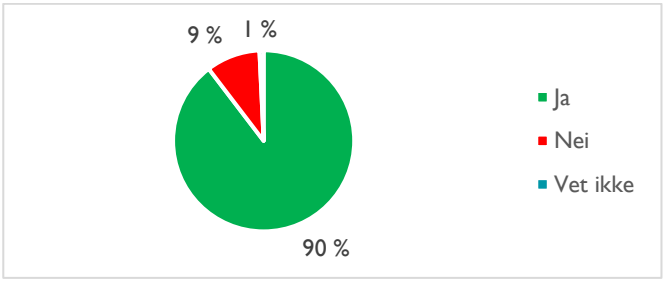
I risikofaget kan risiko defineres som et potensial eller mulighet for uønskede hendelser og tap. Uønskede hendelser er avvik fra virksomhetens mål. Tilstrekkelig sikkerhet oppnås ved å etablere og følge opp en helhetlig systematikk i det samlede risikoarbeidet. Når man har kontroll på risikoene, vil man også nå virksomhetens mål (Aven, 2021).

På spørsmål om ledelsen har diskutert risiko knyttet til digitalisering eller anskaffelser svarer 75% ja. 14% svarer nei.



Figur 3 Har ledelsen diskutert risiko knyttet til digitaliseringsprosjekter eller anskaffelser? N=134

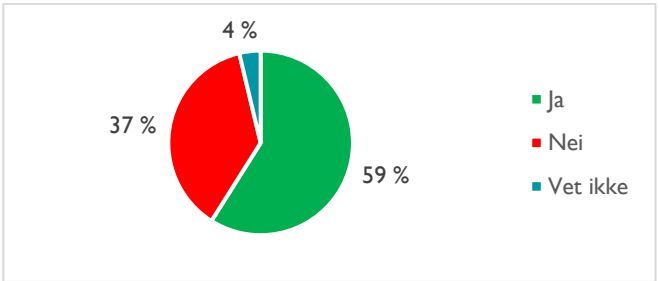
I undersøkelsen har NVE også stilt spørsmål om beredskap mot uønskede IKT-hendelser har vært tema på ledermøter siste 12 månedene ? 90% svarer ja, 9% nei.



Figur 4 Har beredskap mot uønskede IKT-hendelser vært tema på ledermøter siste 12 måneder? N= 134

Arbeidet med styring og kontroll i virksomheten bør jevnlig evalueres – enten helheten, eller ulike deler. Slike evalueringer bør inkludere både styringsaktivitetene og sikkerhetstiltak som er iverksatt.

Intern- eller eksternrevisjon bidrar til å kontrollere at virksomheten har iverksatt tiltak i overenstemmelse med lov- og forskriftskrav, og at tiltakene bidrar til virksomhetens måloppnåelse. I undersøkelsen har 59% hatt intern eller ekstern revisjon av IKT-sikkerhet på ledermøter siste 12 måneder. 37% har ikke hatt dette som tema på ledermøte, se Figur 5.

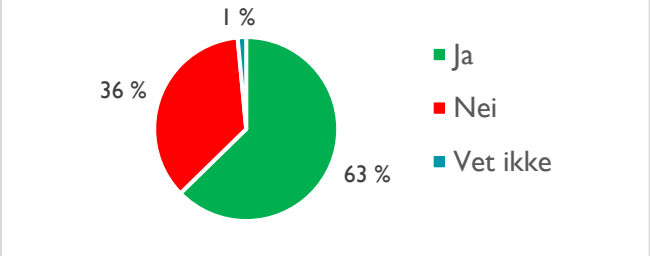


Figur 5 Har intern eller ekstern revisjon av IKT-sikkerhet vært tema på ledermøter siste 12 måneder? N=134

6 av 10 beredskapsledere har øvd på svikt i IKT-systemer

Beredskapslederne ble også spurt om de har vært involvert i øvelser som omhandler svikt i IKT-systemer eller drift kontrollsystemer i løpet av de siste tre årene. Øvelser er viktig for å være forberedt dersom virksomheten for eksempel utsettes for løsepengevirus. Da er det viktig å ha en plan som er øvd på i forkant om hvordan man skal håndtere hendelsen, slik at skaden blir redusert og nedetiden så kort som mulig.

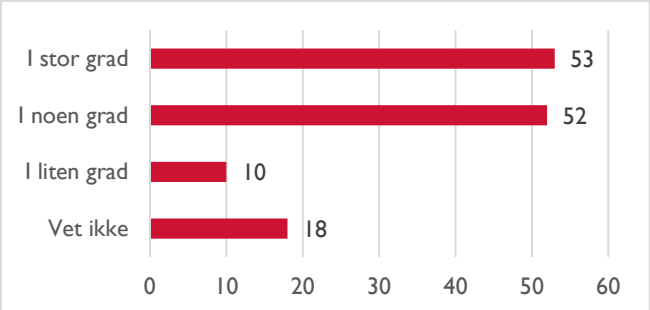
Figur 6 viser at 63% av beredskapslederne har vært med på øvelser siste tre år, 36% har ikke.



Figur 6 Har ledelsen vært involvert i øvelser som omhandler svikt i IKT-systemer eller driftskontrollsystemer siste tre år? N=134.

Beredskapsledelsen etterspør kompetanse

Berdskapslederne har svart på i hvilken grad ledelsen har nytte av kurs rettet mot ledere i kraftberedskapsforskriftens krav til IKT-sikkerhet. Figur 7 viser fordelingen av svar fra beredskapsledere. 53 beredskapsledere vil i stor grad ha nytte av kurs i beredskapsforskriftens krav til IKT-sikkerhet, 52 beredskapsledere i noen grad.

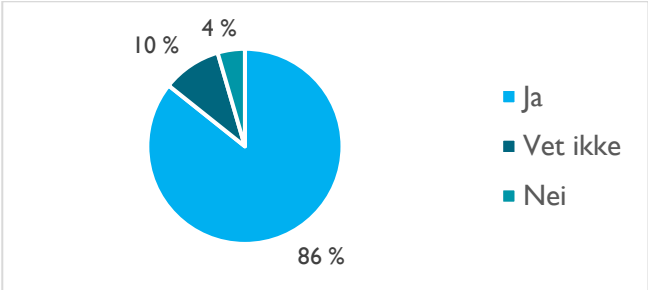


Figur 7 Har virksomhetens ledelse nytte av kurs rettet mot ledere i kraftberedskapsforskriftens krav til IKT-sikkerhet? N= 133

Varierende kjennskap til trusselrapporter

Undersøkelsen har også kartlagt i hvilken grad beredskapslederne er kjent med de åpne trusselrapportene som for eksempel PST (Politiets sikkerhetstjeneste, 2021), Etterretningstjenesten (Etterretningstjenesten, 2021) og NSMs Helhetlige risikobilde (Nasjonal sikkerhetsmyndighet, 2021). 69% av beredskapslederne kjenner til rapportene i noen grad eller høy grad. 27% kjenner i liten grad til disse rapportene.

Beredskapslederne har også fått spørsmål om virksomhetens ledelse har nytte av en uavhengig årlig trusselrapport for kraftbransjen? Her svarer hele 85% ja på spørsmålet, 10% vet ikke og 4% svarer nei.



Figur 8 Har virksomhetens ledelse nytte av en uavhengig årlig trusselrapport for kraftbransjen? N=133

Å kartlegge hvilke farer og trusler virksomheten er utsatt for, er et viktig skritt som må fullføres før en prøver å prioritere eller iverksette tiltak for å beskytte organisasjonen. Krigsherren Sun Tzu uttalte i « The art of War » : Så det sies at hvis du kjenner fiendene dine og kjenner deg selv, kan du vinne 100 slag uten et eneste tap. Hvis du bare kjenner deg selv, men ikke motstanderen din, kan du vinne eller tape. Hvis du hverken kjenner deg selv eller motstanderen din, vil du alltid sette deg i fare ».

Råd :

1. Fra et styringsperspektiv er ikke informasjonssikkerhet et mål i seg selv, men informasjonssikkerhet skal bidra til å oppnå virksomhetens mål.
2. Risikostyring er viktig for alle sikkerhetsaktivitene i en organisasjon og er et verktøy for å prioritere tiltak innenfor de ressurser som er tilgjengelige.
3. Kompetanse og ledelsesystemer med gode, standardiserte prosedyrer, som er kommunisert

og kjent i organisasjonen, gjør det mulig å redusere administrasjonskostnader

4. Informasjonssikkerhet bidrar til verdiskapning ved å redusere tap, styrke omdømmet og tilliten i markedet. Informasjonssikkerhet har også en lenke mot HMS ved at feil informasjon kan få konsekvenser for liv og helse, for eksempel ved arbeid på strømførende linjer.
5. Grad av informasjonssikkerhet må måles indirekte gjennom vurdering av kvalitet i prosesser og kan til sist uttrykkes som modenhet i styring av informasjonssikkerhet. Intern- eller eksternrevisjon, og sikkerhetsstester, kan bidra til å måle sikkerhetsnivået og skape forbedring.

Kontakt

For spørsmål kontakt beredskapsseksjonen ved NVE.

Referanser

Aven, T. (2021). *Risiko.* Récupéré sur www.snl.no: www.snl.no/risiko

Direktoratet for forvaltnig og IKT. (2021). *Risiko.* Récupéré sur www.snl.no: https://snl.no/risiko

Etterretningstjenesten. (2021). *Fokus 2021. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Oslo: Etterretningstjenesten.

ISACA. (2008). *Information Security Governance: guidance for Information security Managers.* ISACA.

KraftCERT. (2021). *Trusselvurdering 2021 (U.Off).* Oslo: KraftCERT.

Nasjonal sikkerhetsmyndighet. (2021). *Nasjonalt digitalt risikobilde 2021.* Oslo: Nasjonal Sikkerhetsmyndighet (NSM).

Nasjonal sikkerhetsmyndighet. (2021). *Risiko 2021. Helhetlig sikring mot sammensatte trusler. Oslo: Nasjonal sikkerhetsmyndighet (NSM).*

Politiets sikkerhetstjeneste. (2021). Nasjonal trusselvurdering 2021. Oslo: Politiets sikkerhetstjeneste (PST).