



Nr. 19/2021

IKT-sikkerhetstilstanden i kraftforsyningen 2021

*Fredrik Karlsen Tøien, Johannes Fagermyr, Gloria Treider
og Hanna Remvang*

NVE Ekstern rapport nr. 19/2021

IKT-sikkerhetstilstanden i kraftforsyningen 2021

Utgitt av: Norges vassdrags- og energidirektorat
Redaktør: Janne Hagen
Forfatter: Fredrik Karlsen Tøien, Johannes Fagermyr, Gloria Treider og Hanna Remvang
Forsidefoto: Stig Storheil/NVE

ISBN: 978-82-410-2167-1
ISSN: 2535-8235
Saksnummer: 202104778

Sammenheng: Rapporten dokumenterer en spørreundersøkelse om IKT-sikkerhetstilstanden i kraftforsyningen for perioden 2020-2021. Rapporten viser at 8% av virksomhetene har hatt uønskede IKT-hendelser i administrative IKT-systemer med konsekvenser for virksomhetens drift. Rapporten dokumenterer sikkerhetspraksis målt mot bla. NSMs grunnprinsipper for IKT-sikkerhet.

Emneord: Cybersikkerhet, sikkerhetshendelser, informasjonssikkerhet, industrielle kontrollsystemer, SCADA-systemer

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

desember, 2021

Innholdsfortegnelse

Forord	4
1 Innledning	6
1.1 Bakgrunn.....	6
1.2 Problemstilling.....	7
1.3 Rapportens oppbygging.....	7
2 Om undersøkelsen	8
2.1 Metode.....	8
2.2 Prosjektorganisering.....	9
3 Trusler og uønskede hendelser	10
3.1 Sikkerhetsmyndighetenes trusselvurdering.....	10
3.2 KraftCERTs bilde av truslene mot kraftbransjen.....	11
3.3 Innrapporterte hendelser til NVE.....	12
3.4 Årsaker til IKT-sikkerhetshendelser.....	13
3.5 Varsel, rapportering og tiltak i etterkant av hendelser ..	14
3.6 Leverandørhendelse med stort skadepotensiale.....	14
3.7 Oppsummering.....	15
4 Strategisk sikkerhetsledelse og praktisk risikostyring	16
4.1 Sikkerhetsstrategi.....	16
4.2 Sikkerhetskultur.....	17
4.3 Styringssystem for informasjonssikkerhet.....	19
4.4 Sikker innovasjon og utvikling.....	20
4.5 Sikring av driftskontrollsystemer.....	21
4.5.1 Driftsmodeller.....	21
4.5.2 Overvåking og hendelsehåndtering i driftskontrollsystemer ...	22
4.6 Øvelser.....	23
4.7 Anskaffelser og tjenesteutsetting.....	23
4.8 Oppsummering.....	24
5 NSM Grunnprinsipper for IKT-sikkerhet	25
5.1 Kraftberedskapsforskriften og NSMs grunnprinsipper for IKT- sikkerhet.....	25
5.2 NSMs Grunnprinsipper prioritet 1-tiltak.....	26
5.3 NSMs Grunnprinsipper prioritet 2 tiltak.....	29
5.4 Oppsummering.....	33
6 Konklusjon	35
6.1 Hvordan er IKT-sikkerheten i den norske kraftforsyningen slik bransjen selv vurderer det?.....	35
6.2 I hvilken grad har cyberangrep hatt konsekvenser for funksjonaliteten til driftskontrollsystem, samt forsyningssikkerhet av elektrisitet og fjernvarme?.....	35
6.3 Videre arbeid.....	36
Vedlegg	38

Vedlegg 1 Datagrunnlaget	38
Vedlegg 2 Samlet tabellarisk oversikt over NSMs grunnprinsipper med svarfordeling	39
Bibliografi	42

Forord

NVE gjennomførte sommeren 2021 en spørreundersøkelse om IKT-sikkerhetstilstanden i kraftforsyningen. Undersøkelsen viser at 8% av virksomhetene har hatt uønskede sikkerhetshendelser i administrative IKT-systemer som har hatt konsekvenser for driften av virksomheten. 3% av virksomhetene har hatt uønskede hendelser i driftskontrollsystemet som har hatt konsekvenser for driftskontrollsystemets funksjon. Årsaken til de fleste hendelsene i administrative IKT-systemer er at virksomhetens leverandør har hatt uønskede IKT-hendelser. Undersøkelsen har ikke kartlagt antallet hendelser eller forsøk på datainnbrudd i kraftforsyningen. Ifølge NSM og KraftCERT foregår cyberangrep og forsøk på angrep i stort omfang, og denne undersøkelsen viser at 80% av beredskapslederne etterspør en uavhengig trussel-rapport rettet mot kraftbransjen.

Undersøkelsen viser videre at 80% av beredskapslederene mener virksomhetene har en IKT-sikkerhetsstrategi. Imidlertid viser undersøkelsen at 60% av IKT-sikkerhetskoordinatorerne mener at virksomheter mangler styringssystem for informasjonssikkerhet. Svarene tyder på avstand mellom beredskapsledelsens og IKT-sikkerhetskoordinatorernes oppfatning av IKT-sikkerhetsarbeidet i virksomheten.

I 2019 trådte kraftberedskapsforskriften i kraft. En viktig endring var nye krav til IKT-sikkerhet som bygget på NSMs grunnprinsipper for IKT-sikkerhet. Virksomhetene fikk tilbud om opplæring i de nye kravene i 2019 og i NSMs-grunnprinsipper for IKT-sikkerhet. På det grunnlaget kunne en forvente at virksomhetene i stor grad hadde iverksatt NSMs grunnprinsipper for IKT-sikkerhet på undersøkelsestidspunktet, midtveis i 2021. Funnene fra undersøkelsen viser at tiltak er innført i varierende grad og at IKT-sikkerheten ikke er på det nivået NVE forventer.

Arbeidet er gjennomført av studenter i et sommerprosjekt. Grunnlaget for analysen er spørreundersøkelser som er besvart av beredskapsledere og IKT-sikkerhetskoordinatorer, samt innspill fra referansegruppen for prosjektet. Referansegruppen har bestått av eksperter fra nettselskap, produksjonsselskap, leverandører, bransjeorganisasjoner, akademia og NSM. NVE vil takke samtlige i referansegruppen for gode diskusjoner og innspill til arbeidet.

NVE vil bruke resultatene fra prosjektet som grunnlag for områdeovervåking på IKT-sikkerhetstilstanden, og til å utvikle tiltak som løfter IKT-sikkerhetsnivået i kraftforsyningen. NVE anbefaler KBO-enhetene å iverksette de viktigste tiltakene i NSMs Grunnprinsipper for IKT-sikkerhet fordi disse understøtter kravene i kraftberedskapsforskriften. Det vil forbedre etterlevelsen av kravene i kbf § 6-9.

Anne Rogstad
Fungerende direktør

Eldri Naadland Holo
Seksjonssjef

Sammendrag

Rapporten bygger på data innhentet gjennom spørreundersøkelser i perioden 2020-2021.

Hvordan er IKT-sikkerheten i den norske kraftforsyningen slik bransjen selv vurderer det?

Vi har foreløpig ikke grunnlag for å gjøre en kvalitativ vurdering av sikkerhetsnivået. Resultatene fra spørreundersøkelsen som rettet seg mot beredskapsledere viser at 80% av virksomhetene har en IKT-sikkerhetsstrategi, noe som kan sies å være bra. Undersøkelsen avdekker imidlertid at kun 35% har styringssystem for informasjonssikkerhet.

NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper med tiltak for hvordan IKT-systemer bør sikres for å beskytte verdier og virksomhetenes leveranser. Kraftberedskapsforskriftens krav til sikring av digitale systemer (kbf § 6-9) bygger på disse grunnprinsippene. Grunnprinsippene er relevante for både egen drift og når driften er satt ut til leverandør. Grunnprinsippene beskriver hva en virksomhet bør gjøre for å forebygge og sikre et IKT-system, samt hvorfor det bør gjøres, men ikke hvordan. Undersøkelsen viser at selv om mange virksomheter har iverksatt flere av tiltakene knyttet til NSMs grunnprinsipper for IKT-sikkerhet, så er det fortsatt stor variasjon mellom virksomhetene når det gjelder sikkerhetspraksis, og det er nødvendig å fortsette å arbeide for å heve nivået på IKT-sikkerheten.

I hvilken grad har cyberangrep hatt konsekvenser for funksjonaliteten til driftskontrollsystem, samt forsyningssikkerheten av elektrisitet og fjernvarme?

Undersøkelsen refererer til statistikk fra KraftCERT og trusselrapportene fra norske sikkerhetsmyndigheter. NSM, PST og KraftCERT dokumenterer at den norske kraftforsyningen er utsatt for cyberangrep. I undersøkelsen til NVE rapporterte 8 % av virksomhetene at de har hatt alvorlige IKT-hendelser i administrative IKT-systemer med konsekvenser for virksomhetens drift. Undersøkelsen viser videre at 3% av virksomhetene har hatt hendelser i driftskontrollsystemet med kortvarig konsekvens for funksjonen til driftskontrollsystemet. Ingen av hendelsene i driftskontrollsystemene skyldes cyberangrep, og ingen av dem har hatt konsekvens for selve produksjonen eller fremføringen av elektrisitet eller fjernvarme til kundene.

Forsøk på innbrudd og angrep foregår hele tiden. Trusselrapportene fra ENISA, samt globale leverandører som for eksempel Microsoft og Dragos, gir et bilde av truslene mot kraftsektoren internasjonalt. De viser at det er viktig å fortsatt ha høy oppmerksomhet på IKT-sikkerhet. Mange virksomheter har mangelfull kartlegging av enheter og programvare. God oversikt er grunnlaget for godt sikkerhetsarbeid. Med mer digitalisering og, flere sensorer og enheter koplet til datanettverkene, blir denne oppgaven enda viktigere framover. NVE anbefaler virksomhetene å iverksette de 35 viktigste tiltakene i NSMs Grunnprinsipper for IKT-sikkerhet omtalt i denne rapporten. Det vil forbedre etterlevelsen av kravene i kraftberedskapsforskriftens § 6-9, som bygger på disse grunnprinsippene.

1 Innledning

1.1 Bakgrunn

Det siste året har det vært flere alvorlige cyberangrep globalt, og trenden er økende. Politiets sikkerhetstjeneste (PST) (PST, 2021) og Nasjonal sikkerhetsmyndighet (NSM) frykter sabotasje innenfor kraftforsyning, telekommunikasjon og annen kritisk infrastruktur. NSM peker i sin rapport RISIKO 2021 på et skjerpet digitalt risikobilde i leverandørkjeder (NSM, 2021). I mars 2021 offentliggjorde Riksrevisjonen sin rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Riksrevisjonen pekte også på kraftforsyningens digitale sårbarhet og de alvorlige konsekvensene som cyberangrep kunne medføre. Riksrevisjonsrapporten kritiserte videre blant annet at NVE ikke hadde god nok oversikt over IKT-sikkerhetstilstanden i kraftforsyningen og at NVE ikke i tilstrekkelig grad hadde påsett at det var god nok beredskap for å håndtere IKT-angrep i kraftforsyningen. I tillegg pekte Riksrevisjonen på mangelfull oppfølging av leverandører (Riksrevisjonen, 2021).

NVE ga i 2017 ut en rapport om informasjonssikkerhetstilstanden i energiforsyningen. Fra juni 2016 til juni 2017 hadde hele 70% av virksomhetene hatt uønskede IKT-sikkerhetshendelser. Dette inkluderte blant annet bedrageri over internett, som annenhver virksomhet hadde erfart, og datavirus, som 4 av 10 virksomheter hadde erfart. Undersøkelsen dokumenterte videre at om lag 80% av virksomhetene var avhengige av leverandørene for å håndtere hendelser i sine IKT- og driftskontrollsystemer og gjenopprette systemene dersom de feilet (NVE og NSM, 2017). Gitt trusselutviklingen som er observert internasjonalt (ENISA, 2021) (Microsoft, 2021) (Dragos, 2021) og også påpekt av norske sikkerhetsmyndigheter, er det grunnlag for å anta at angrepstrykket ikke er blitt mindre i løpet av perioden fram til i dag.

Revidert kraftberedskapsforskrift trådte i kraft i januar 2019 og har en egen paragraf § 6-9, som bygger på NSMs grunnprinsipper for IKT-sikkerhet. To år etter at kravene har trådt i kraft, og med økt oppmerksomhet i samfunnet på cyberangrep, kan man forvente at virksomhetene i kraftforsyningen har iverksatt mange av tiltakene innenfor NSMs grunnprinsipper. Denne rapporten gir et bilde på hva som er status per juni 2021, og resultatene viser at tiltakene i varierende grad er iverksatt.

I 2021 har NVE vesentlig bedre oversikt over trusselbildet takket være utviklingen av KraftCERT. KraftCERT overvåker utviklingen i sårbarheter i teknologi som virksomheter i kraftforsyningen bruker. KraftCERT overvåker og deler informasjon om IKT-trusler mot bransjen. Siden angrepstrykket mot kraftbransjens IKT-systemer er vurdert å være stort av både NSM og KraftCERT, retter årets undersøkelse oppmerksomheten kun mot hendelser i perioden juni 2020 til juni 2021 *som har hatt konsekvenser for virksomhetens drift, og funksjonaliteten til driftskontrollsystemene.*

Rapporten dokumenterer forskning som er gjennomført i NVEs FOU-prosjekt 80415 Sikkerhetstilstanden i norsk kraftforsyning.

1.2 Problemstilling

Rapporten svarer på to spørsmål:

- *Hvordan er IKT-sikkerheten i den norske kraftforsyningen slik bransjen selv vurderer IKT-sikkerheten?*
- *I hvilken grad har cyberangrep hatt konsekvenser for funksjonaliteten til driftskontrollsystem, samt forsyningssikkerheten av elektrisitet og fjernvarme?*

Rapporten bygger på statistikk innhentet gjennom tre spørreundersøkelser i perioden 28.mai til 4. juni 2021, samt kvalitative data innhentet gjennom diskusjon med referansegruppene i prosjektet i perioden 9. juni til 27.juli 2021. I tillegg bygger rapporten på statistikk fra KraftCERT og varslede og innrapporterte hendelser til NVE.

Rapporten har som målsetting å delvis svare ut kritikken fra Riksrevisjonen om NVEs manglende områdeovervåking av IKT-sikkerhetstilstanden. Når vi sier delvis, bygger det på at spørreundersøkelser bare gir et omtrentlig bilde. En annen målsetning med rapporten er å gi bransjen økt kunnskap og et sammenligningsgrunnlag som kan brukes for eget forbedringsarbeid på IKT-sikkerhet. Rapporten framhever derfor god praksis i tillegg til de viktigste forbedringsområdene.

1.3 Rapportens oppbygging

Rapporten består av følgende kapitler:

Kapittel 1 gir informasjon om bakgrunnen for studien.

Kapittel 2 beskriver gjennomføringen av undersøkelsen, metode og prosjektorganisering.

Kapittel 3 beskriver trusler og uønskede IKT-hendelser. Kapitlet bygger på rapporter fra sikkerhetsmyndighetene, KraftCERT og denne undersøkelsen.

Kapittel 4 presenterer hovedfunn fra tre spørreundersøkelser som er gjennomført av NVE. Dette kapitlet dekker temaene strategisk sikkerhetsledelse, risikostyring og sikkerhetskultur, og sikring av driftskontrollsystemer.

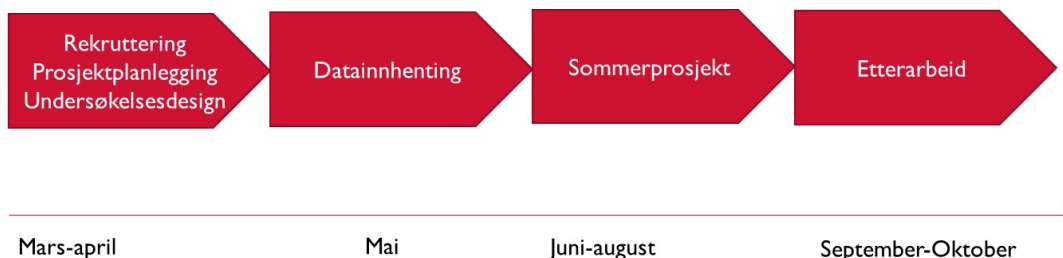
Kapittel 5 beskriver virksomhetenes sikkerhetspraksis vurdert opp mot NSMs grunnprinsipper for IKT-sikkerhet. Kapitlet setter søkelys på de 35 viktigste sikkerhetstiltakene (prioritet 1 og prioritet 2 tiltak) i grunnprinsippene for IKT-sikkerhet.

Kapittel 6 presenterer konklusjonen.

2 Om undersøkelsen

2.1 Metode

Prosjektet har vært gjennomført i fire faser som vist i Figur 2.1.



Figur 2.1 Prosjektarbeid i fire faser

Prosjektplanlegging og rekruttering av sommerstudenter som skulle arbeide på prosjektet, startet i mars. NVE etablerte også en referansegruppe bestående av virksomheter i bransjen, myndighetene, interesseorganisasjoner og leverandører til bransjen. Referansegruppen har bidratt med innspill til undersøkelsesdesignet og formulering av spørsmål til undersøkelsen, samt gitt kommentarer til resultatene.

IKT-sikkerhetskoordinatorer fikk også tilsendt et excel-skjema utviklet av NSM der de skulle besvare hvorvidt de hadde iverksatt de fleste, noen eller ingen sikkerhetstiltak tilknyttet NSMs grunnprinsipper. Totalt inngår 118 tiltak i NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0 (NSM, 2020). Tiltakene er gitt en prioritering hvor prioritet 1 er av grunnleggende art. Prioritet 1 tiltakene bør iverksettes før prioritet 2 og 3. De 35 viktigste tiltakene (prioritet 1 og 2) ble valgt ut for å bli med i undersøkelsen.

Undersøkelsen om sikkerhetstilstanden, med blant annet spørsmål om hendelser, er besvart av 117 virksomheter, og undersøkelsen om sikkerhetsledelse er besvart av 134. Se Vedlegg 1. På undersøkelsen om NSMs grunnprinsipper har 62 virksomheter gitt fullstendige svar som kunne brukes som datagrunnlag i undersøkelsen. Det er flere grunner til frafall, som f.eks. ikke tilstrekkelig utfylt skjema, for sent leverte svar og problemer med å åpne krypterte vedlegg. Noen konsern svarte for flere datterselskap. Vi har ikke analysert frafallene i svarene, men valgt å presentere statistikk fra dem som ga fullstendige svar på NSMs grunnprinsipper. Vi kommenterer enkeltvis der mange har svart «vet ikke» og «ikke relevant». Komplette oversikt finnes i vedlegg 2.

2.2 Prosjektorganisering

Prosjektet ble organisert med et studentteam som hadde arbeidssted NVE og ett studentteam med arbeidssted Universitetet i Stavanger (UiS)/hjemmekontor. Hvert studentteam hadde en utpekt teamleder. NVE har hatt prosjektledelsen for hele prosjektet med støtte fra professor Ove Njå, UiS.

Til sammen har syv studenter fra ulike utdanningsinstitusjoner og med ulik fagbakgrunn fra teknologi, økonomi, sikkerhet og samfunnsvitenskap, arbeidet i FOU-prosjektet sommeren 2021.

Prosjektet er finansiert av NVE, UiS og Norges Teknisk Naturvitenskaplige Universitet (NTNU). UiS og NTNU ansatte og finansiert tre studenter av de syv. De to studentteamene hos NVE og UiS/NTNU har hatt flere fellesmøter, men jobbet med ulike problemstillinger.

Følgende institusjoner og virksomheter har hatt representanter med i referansegruppen for prosjektet:

- Nasjonal sikkerhetsmyndighet (NSM)
- KraftCERT
- EnergiNorge
- Nettalliansen
- Elvia
- Arva
- Sira-Kvina
- Statnett
- Valider
- Siemens
- NC Spektrum
- NTNU
- UIS

Referansegruppen har bidratt i formuleringen av spørsmål til spørreundersøkelsen, samt gitt kommentarer og innspill til rapportutkastet. Totalt har prosjektet hatt tre referansegruppemøter og ettsluttseminar der foreløpige resultater ble presentert og drøftet. Referansegruppen fikk også utsendt et utkast til rapport som de kommenterte på.

3 Trusler og uønskede hendelser

3.1 Sikkerhetsmyndighetenes trusselvurdering

Norge står overfor et trusselbilde på tvers av flere sektorer, og dette øker behovet for et tett og godt samarbeid mellom NSM, Etterretningstjenesten og PST (Regjeringen, 2021).

NSM vurderer det digitale risikobildet i 2021 som skjerpet sammenlignet med 2020, og kriminelle aktører og staters kapasitet til å gjennomføre angrep med alvorlige konsekvenser for Norge er høy. Phishing e-poster er fremdeles en effektiv metode for å komme på innsiden av virksomheters informasjonssystemer. Teknikkene innenfor phishing forbedres stadig, og en kan forvente at phishing-nivået kommer til å holde seg høyt. Sosiale medier blir også tatt mer i bruk til phishing i tillegg til e-post, og noen trusselaktører har også tatt i bruk kunstig intelligens for å forbedre kvaliteten på phishing-operasjonen. Ifølge NSM er det tydeligere risiko knyttet til sammensatte trusler. Covid-19 pandemien har ført til raskere digitalisering og dermed også et forsterket risikobilde. Sårbarhetsbildet har også blitt tydeligere når det gjelder norske virksomheters leverandørkjeder og avhengigheter. Ifølge NSM vil trusselaktørene fortsette å utnytte at store samfunnsverdier legges over i det digitale domenet.

PST påpeker i nasjonal trusselvurdering for 2021 at etterretningsaktivitet vil utgjøre den største trusselen mot Norge. PST betegner russiske og kinesiske myndigheter som den største trusselen, og de vil i stor grad benytte seg av nettverksoperasjoner. Digital spionasje innebærer liten risiko for trusselaktøren og er dessuten kostnadseffektivt. PST vurderer at pandemien har gitt et økt mulighetsrom for etterretning. Etterretningstjenester vil utnytte reduserte digitale sikkerhetsmekanismer i hjemmekontorløsninger og det vil være økte muligheter for strategiske oppkjøp fra andre stater i Norge ved mulige konkurser (PST, 2021).

"I 2021 vil utenlandske etterretningstjenester bruke store ressurser på å bryte seg inn i norske datanettverk. De vil også forsøke å rekruttere kilder og agenter. Målet deres er å få tilgang til informasjon og å påvirke norske beslutningsprosesser" (PST 2021)

E-tjenesten påpeker at utenlandsk etterretning forblir en stor trussel mot norske interesser, og at variasjonen i både størrelse og type angrep har økt. I deres studie kommer det fram at bruk av desinformasjon har blitt trappet opp under pandemien. Nettverksoperasjoner brukes til etterretningsformål, men også til avskrekking og sabotasje (Forsvaret, 2021).

Næringslivets sikkerhetsråd kartlegger omfanget av datakriminalitet i norsk næringsliv og utgir annethvert år en studie, «Mørketallsundersøkelsen». Den siste Mørketallsundersøkelsen fra 2020 ble besvart av 1601 virksomheter i Norge med flere enn 5 ansatte. Undersøkelsen viste at 14% av de som svarte hadde opplevd forsøk på datainnbrudd, 13% opplevde phishing-e-poster og 11% hadde hatt virus eller skadevareinfeksjon (NSR, 2020).

De vanligste truslene mot digitale systemer

Phishing: Aktøren forsøker å hente ut sensitiv informasjon via nettsider eller e-post.

Hacking: Algoritmer eller personer utnytter svakheter i datasystemer for å utføre svindel, spre malware eller stjele opplysninger.

Malware (skadevare): Er en form for ondsinnet programvare som kan samle opplysninger, spionere eller ødelegge filene helt. Det kan for eksempel være virus, ormer eller trojanere.

Ransomware (løsepengevirus, utpressingsvirus): En type malware brukt for å stenge deg ute av dine egne systemer, eller kryptere alle filene dine.

DDoS-angrep (distribuert tjenestenektangrep): Hindre andre å få tilgang en database, nettside eller lignende ved bruk av et nettverk av datamaskiner (DigitalNorway, 2020).

3.2 KraftCERTs bilde av truslene mot kraftbransjen

KraftCERT er en viktig samarbeidspartner for NVE når det gjelder oversikt over de digitale truslene mot kraftforsyningen og håndtering av uønskede IKT-hendelser. NVE er kraftforsyningens sektorvise responsmiljø (SRM), men har delegert noen oppgaver til KraftCERT. Disse oppgavene er blant annet å formidle sårbarhetsinformasjon og informasjon om trusler til KBO-enhetene og å formidle trusselsituasjonen til NVE. KraftCERT ivaretar dermed viktig informasjonsinnhenting og -formidling om IKT-sikkerhet til kraftforsyningen. NVE har i veilederen til kraftberedskapsforskriften klargjort at virksomhetene iht. § 6-9 bokstav c må varsle alle uønskede hendelser mot sine digitale informasjonssystemer til KraftCERT. Alle ekstraordinære situasjoner skal i tillegg varsles til NVE (jf. kbf § 2-5) og ekstraordinære hendelser skal også rapporteres i etterkant til NVE (jf. kbf § 2-6).

KraftCERT registrerer et høyt angrepstrykk mot kraftforsyningen og vurderer at dette høye angrepstrykket vil vedvare, med kryptoskadevare (ransomware) som en av de største truslene mot kraftforsyningen i 2021. KraftCERT forventer at trusselaktørene vil fortsette å bruke godt kjente teknikker for svindel og kompromittering i tiden framover. Dette kan være phishing for å tilegne seg påloggingsinformasjon fra ansatte, tyveri av brukerdata fra leverandører og direktørsvindel via e-post. Trusselaktørene vil fortsette å bruke innbrudds-teknikker som passordknekking (brute-force-teknikker) for å utnytte programvaresårbarheter i sikrede oppkoblinger (VPN), e-post og fjernsupport (Remote Desktop) og benytte seg av eksisterende lokale IT-driftsverktøy for å bevege seg videre inne i datanettet hos virksomheter de har klart å komme på innsiden av.

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 ser en økning i antall hendelser spesielt mot systemer og teknologier som har stor utbredelse.

Selv om ny teknologi åpner for mer deteksjon og større grad av kontroll, åpner ny teknologi også opp for nye sårbarhetsflater (KraftCERT, 2021).

3.3 Innrapporterte hendelser til NVE

NVE setter krav til at KBO-enhetene skal varsle til NVEs beredskapsvakt om ekstraordinære situasjoner (kbf § 2-5) og sende en rapport etter uønskede hendelser innen tre uker (kbf § 2-6). Som et minimum skal KBO varsle og rapportere hvis det har oppstått følgende hendelser:

- a. Forsøk på inntrengning og/eller manipulasjon av hele eller deler av driftskontrollsystemet og avanserte måle- og styringssystem (AMS).*
- b. Innbrudd, hæververk, sabotasje eller andre kriminelle handlinger, eller forsøk på dette. (Dette inkluderer også datainnbrudd)*
- c. Ved begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter.*
- d. Situasjoner hvor kraftsensitiv informasjon er blitt kjent for andre enn rettmessige brukere, eller mistanke om dette.*
- h. Omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer.*

Driftskontrollsystemer omfatter driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner. Med anlegg forstås også tilhørende bygningstekniske konstruksjoner for driftskontrollfunksjoner. Driftskontrollfunksjoner er alle organisatoriske, administrative og tekniske tiltak for å overvåke, styre og beskytte anlegg i kraftforsyningen (kbf § 7.1). Kbf § 7-1 setter krav til at virksomheter med driftskontrollsystemer skal sørge for at disse til enhver tid virker etter sin hensikt og skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser.

En gjennomgang av NVEs saksbehandlingssystem viser at NVE i perioden januar 2020-juni 2021 har fått innrapportert 10 ekstraordinære IKT-hendelser fra til sammen 10 virksomheter.

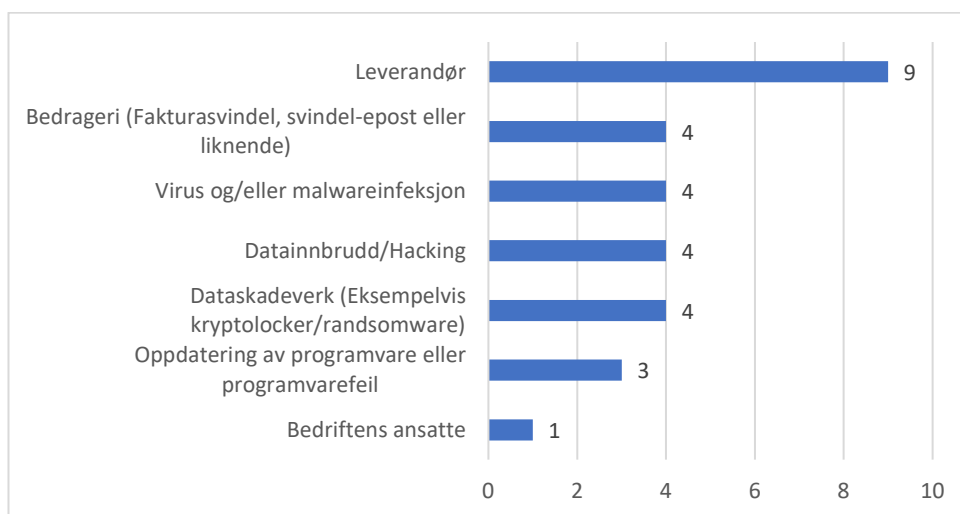
Av disse 10 IKT-hendelsene, skjedde fire hendelser i driftskontrollsystemet. Tre av hendelsene i driftskontrollsystemet kunne forklares med teknisk feil i driftskontrollsystemet. Den siste hendelsen i driftskontrollsystemet skyldtes lyn. Nedetiden som følge av hendelsene i driftskontrollsystemet var kortvarig for de tre virksomhetene med teknisk feil. Hos virksomheten som opplevde at lyn skadet driftskontrollsystemet, ble virksomhetens reservesystem benyttet. Ingen av hendelsene hadde konsekvens for forsyningssikkerheten og leveransen av elektrisitet til forbrukerne.

Spørreundersøkelsen i 2021 til IKT-sikkerhetskoordinatorerne viser at 3% (fire virksomheter) har hatt hendelser i driftskontrollsystemet som har hatt konsekvens for funksjonen til driftskontrollsystemet.

Kraftberedskapsforskriften gir en utfyllende definisjon på driftskontrollsystemer. Andre IKT-systemer er bare nevnt som digitale informasjonssystemer. I denne undersøkelsen anser vi driftskontrollsystemer som definert i kraftberedskapsforskriften, og administrative IKT-systemer som digitale systemer som ikke er driftskontrollsystemer. IKT-sikkerhetskoordinatorerne ble spurt om deres virksomhet har hatt uønskede hendelser i administrative IKT-systemer som har hatt konsekvens for driften av virksomheten siste 12 måneder. Svarene viser at 8% av virksomheter har opplevd sikkerhetshendelser i administrative IKT-systemer som også har hatt konsekvens for driften av virksomheten. Svarene viser at det er viktig å beskytte administrative IKT-systemer. Funnet harmonerer også med KraftCERTs vurdering av sikkerhetsutfordringene der trusselaktørene i første omgang kommer på innsiden av administrative IKT-systemer, og deretter beveger seg videre inn mot driftskontrollsystemet.

3.4 Årsaker til IKT-sikkerhetshendelser

På spørsmålet om årsaken til informasjonssikkerhetshendelser de siste 12 månedene, svarte 13 av IKT-sikkerhetskoordinatorerne at forhold hos leverandøren er vanligste årsak sammen med andre årsaker som phishing, virus, datainnbrudd, dataskadeverk og programvarefeil knyttet til oppdatering. Ingen har oppgitt tjenestenektangrep (DDoS), tyveri av IT-utstyr, eller misbruk av IT-ressurser som årsak.



Figur 3.1 Hva var årsaken til hendelsen? (flere svar mulig) (N = 13)

3.5 Varsel, rapportering og tiltak i etterkant av hendelser

I undersøkelsen har 12 IKT-sikkerhetskoordinatorer svart på hvordan hendelsen ble oppdaget. Varsel fra leverandør, KraftCERT og rutinemessig sikkerhetsmonitorering er de vanligste årsakene til at hendelsene ble oppdaget, men også andre kontroller og negativ effekt på driften har bidratt til å avdekke hendelser. Undersøkelsen viser at bare en virksomhet har mottatt varsel fra NSM. NVE har ikke sendt ut varsel i denne perioden..

I undersøkelsen har bare syv IKT-sikkerhetskoordinatorer svart på spørsmålet om rapportering av hendelsene. Hendelsene rapporteres til NVE, KraftCERT, egen ledelse, leverandør og Datatilsynet. Ingen av hendelsene er rapportert til NSM eller politiet.

Hos de virksomhetene som har hatt en sikkerhetshendelse de siste 12 månedene, har fire satt inn andre tiltak som for eksempel etablert et sikkerhetsoperasjonssenter (SoC), eller iverksatt tiltak rettet mot leverandør, tre har endret rutiner, to har investert i opplæring, en har investert i nye tekniske sikkerhetstiltak og en har svart at de ikke har gjort noe endring.

3.6 Leverandørhendelse med stort skadepotensiale

Volue ble 5. mai 2021 rammet av et cyberangrep forårsaket av programvaren Ryuk. Volue tilbyr programvare og tjenester til energi-, strømnnett- og infrastrukturmarkedet. Selskapet har over 2000 kunder i 44 land (Volue, 2021). Angrepet har blitt klassifisert som ransomware. Ransomware er designet for å ødelegge tilgang til filer på maskiner og servere ved å kryptere dem og kreve betaling for å få tilgang til dekrypteringsnøkkelen. Ryuk sprer seg automatisk i datanettverket den infiserer. Programvaren krypterte både mapper og filer ved bruk av krypteringsalgoritmer.

I følge «Volue's post mortem rapport» om hendelsen, reagerte beredskapsteamet hos Volue raskt, og startet operasjonen *Stop & Recover*. I tillegg økte Volue innsatsen for å skalere operasjonen til relevante myndigheter og sikkerhetspartnere. I følge Volue bidro god beredskapsplan og -forberedelse til at virksomheten klarte å handle raskt mot angrepet. I etterkant av hendelsen har Volue utgitt en rapport som oppsummerer erfaringene med hendelseshåndteringen (Volue, 2021). Til tross for effektiv håndtering hos Volue, har angrepet likevel hatt store konsekvenser. Volue anslår et tap på 30-40 millioner kroner og skriver at angrepet påvirket interne forretningsutviklingsaktiviteter som påvirket vekst- og produksjonsinitiativer (Direkt, Infront TDN, 2021).

Volue hadde flere viktige læringspunkter etter hendelsen: kunne hendelsen vært unngått dersom følgende hadde vært på plass, her nevnes noen:

- Utvidet bruk av tofaktor-autentisering både hos kundesystemer og egne interne systemer kunne bidratt til å forhindre hendelsen.

- Døgkontinuerlig respons på overvåkning av sikkerhetsvarsler kunne bidratt til tidlig respons og reduksjon av konsekvenser
- Utelat muligheten for å betale ransom (løspenger) bidro til å sette søkelys på å forstå angrepet og hvordan reetablere normal drift raskere.
- Revisjon av all backup kan sikre at backup inkluderer alle kritiske systemer og data.
- Forbedret forståelse av kundedata, hvor de er lagret og konsekvenser ved tap av tilgang til data.

3.7 Oppsummering

Sikkerhetsmyndighetenes rapporter og KraftCERTs statistikk gir samlet sett et bilde av at kraftforsyningens virksomheter er utsatt for cybertrusler og kriminalitet, og at angrepstrykket er stort.

Svarene fra spørreundersøkelsen viser at 8% av virksomhetene har opplevd en sikkerhetshendelse i administrative IKT-systemer som også har hatt konsekvens for driften av virksomheten. Det er høyere enn for driftskontrollsystemer, der 3% av virksomhetene har hatt hendelser som har påvirket driftskontrollsystemets funksjon. Hendelsene som har rammet driftskontrollsystemet er imidlertid ikke forårsaket av cyberangrep. Svarene fra undersøkelsen harmonerer med bransjens innrapporterte ekstraordinære hendelser til NVE.

Resultatene viser at det er viktig å rette søkelyset mot å beskytte administrative IKT-systemer i tillegg til driftskontrollsystemet. For det første får cyberangrep og uønskede IKT-hendelser konsekvenser for virksomhetens drift. For det andre kan svakheter i administrative IKT-systemer gjøre at trusselaktører kan bevege seg videre inn til driftskontrollsystemene, som påpekt av KraftCERT.

NVEs innsamlede data i 2021 viser at hendelser hos leverandør eller tredjepart er den vanligste årsaken til IKT-sikkerhetshendelser hos virksomheter i kraftforsyningen, der hendelsen har konsekvenser for virksomhetens drift eller driftskontrollsystemets funksjon.

Manglende oversikt over verdikjeder og avhengigheter av leverandører på tvers av landegrenser er en kjent sårbarhet. Det observeres stadig flere tredjepartsangrep, og e-post-angrep gjennom leverandører, partnere og kunder øker. Det er grunn til å anta at risikoen for angrep vil øke ved bruk av IIoT (Industrial Internet Of Things) dersom underleverandørene har svak kontroll på egen verdikjede. IIoT øker også angrepsflaten ved at nye produkter og leverandører knyttes til virksomhetens datanett gjennom verdikjedene.

Volue-saken viser viktigheten av å ha på plass gode forebyggende sikkerhetstiltak, forberedte beredskapstiltak inklusive en kommunikasjonsplan, og å ha et avklart forhold til økonomisk utpressing dersom virksomheten skulle bli utsatt for utpressing.

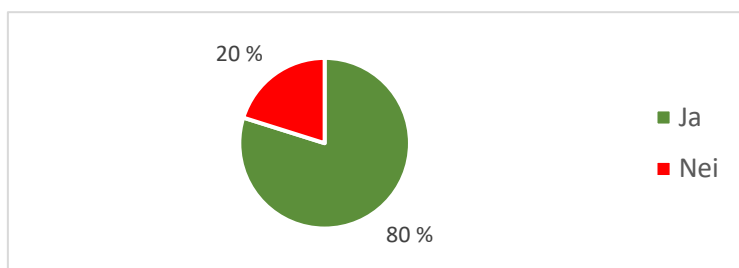
4 Strategisk sikkerhetsledelse og praktisk risikostyring

4.1 Sikkerhetsstrategi

KBO-enheter er underlagt kraftberedskapsforskriften, som stiller krav til IKT-sikkerhet og sikring av driftskontrollsystemer. Forskriften stiller krav til helhetlig sikring og beredskap og omfatter mer enn bare krav til digitale systemer. Forskriftens samlede krav skal bidra til at risiko for skade, havari og funksjonssvikt og andre uønskede hendelser *blir minst mulig* for klassifiserte anlegg (kbf. § 5-1). Forskriften stiller krav til risikostyring, redundante løsninger, krav til kompetanse, fysisk sikring og beredskap. Det er leder av virksomheten som har ansvar for at virksomheten etterlever forskriftskravene.

Sannsynligheten for at cyberangrep lykkes øker dersom virksomheten ikke har sikret IKT-systemene godt nok. Sikkerhetsbevissthet opparbeides blant annet gjennom å utvikle en god sikkerhetskultur i hele virksomheten. Sikkerhetskulturen vil være påvirket av den øvrige organisasjonskulturen. Organisasjonskultur skapes gjennom interaksjon mellom mennesker, og påvirkes gjennom ledelse. Bedrifter har ofte subkulturer med ulik sikkerhetskultur som igjen skyldes ulik påvirkning fra ledere og oppfatning fra ansatte. Organisasjonens prioriteringer kommuniseres gjennom lederne, og lederne har derfor en viktig rolle knyttet til sikkerheten på arbeidsplassen (NHO, u.d.). For å etablere god sikkerhet i virksomheten, er det ifølge NSM helt avgjørende at ledere er involvert og tar ansvar for det forebyggende sikkerhetsarbeidet. Det blir vanskeligere å investere i sikkerhetstiltak dersom ledelsen ikke er involvert (NSM, 2021).

Ledelse av informasjonssikkerhet innebærer å utvikle strategi, styringssystem og sørge for en god sikkerhetskultur. En strategi er en plan for å nå et mål, og sier mer om *hva som skal gjøres enn hvordan det skal gjøres* (Wikipedia, 2021). Det bør være samsvar mellom IKT-strategien og virksomhetens overordnede forretningsstrategi.



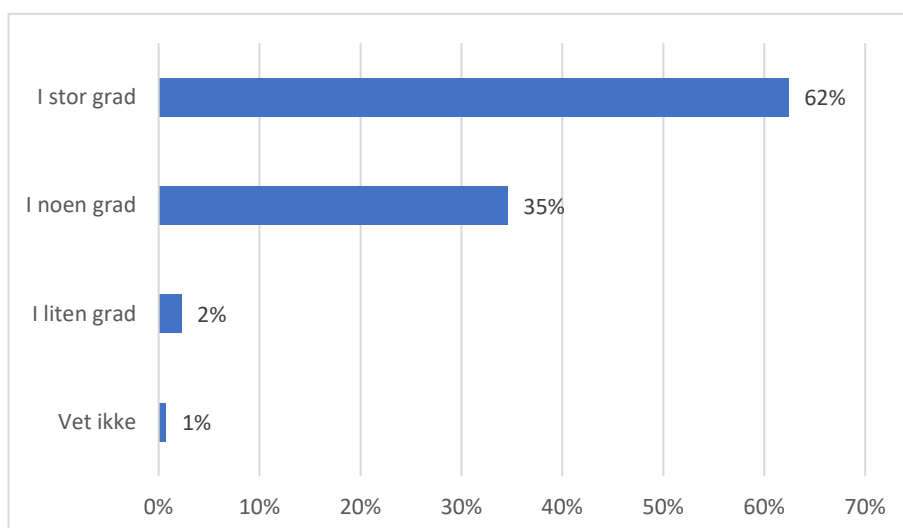
Figur 4.1 Har virksomheten en IKT-sikkerhetsstrategi? (N = 134)

NVE stilte spørsmål til beredskapslederne om de har en IKT-sikkerhetsstrategi. Svarene viser at 80 % av beredskapslederne mener virksomheten har en IKT-sikkerhetsstrategi, mens 20 % mener de ikke har en IKT-sikkerhetsstrategi.

4.2 Sikkerhetskultur

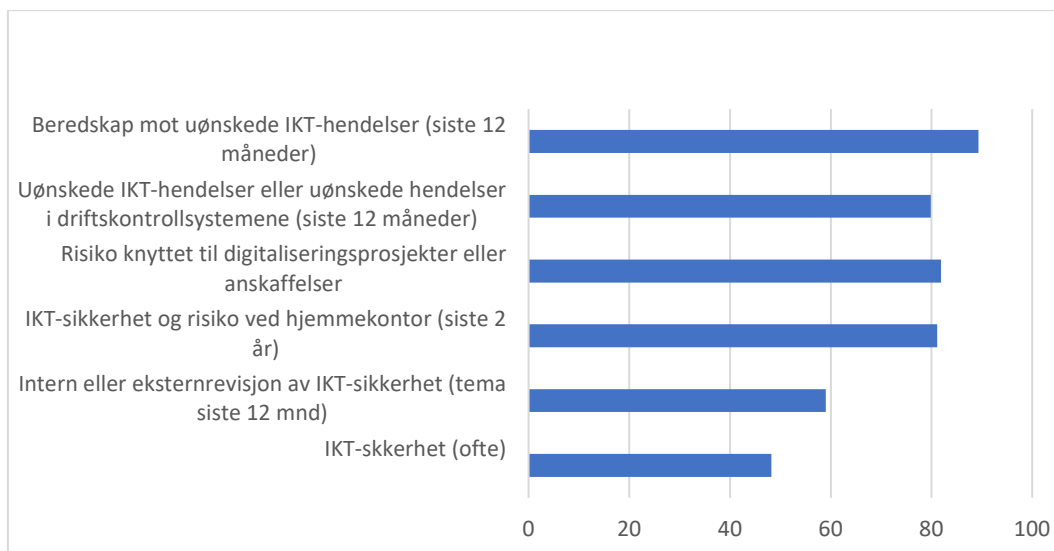
En god sikkerhetskultur bidrar til at ansatte utfører arbeidet i tråd med arbeidsgivers sikkerhetsinstruks og politikk. Dersom ansatte vet hva som er forventet av dem, tar ansvar for egne handlinger og har en forståelse for hvorfor sikkerhetstiltak eksisterer, vil de også melde fra om sikkerhetsmessige forhold som virksomheten bør vite om. Virksomhetene må styre mange former for risiko: helse, miljø og sikkerhet (HMS), IKT-sikkerhet og en praksis i samsvar med samfunnets normer og regelverk. Kompetanseheving gjennom læring fra daglig arbeid og hendelsehåndtering, kurs, og øvelser er med på å øke kunnskapsnivået og styrke sikkerhetskulturen i en virksomhet.

I undersøkelsen ble beredskapsledere spurt om i hvilken grad de anser at IKT-sikkerhet, HMS, næringslivsetikk og økonomisk kriminalitet inngår i sikkerhetskulturen. Svarene gitt ved undersøkelsen viser at de fleste av virksomheter anser at IKT-sikkerhet, HMS, næringslivsetikk og økonomisk kriminalitet inngår i sikkerhetskulturen. Det kan imidlertid innvendes at spørsmålsformuleringen fra NVE kan tolkes både som hva som er et normativt ideal, eller hvordan det rent deskriptivt er i deres virksomhet. Dette gir noe usikkerhet knyttet til resultatet.



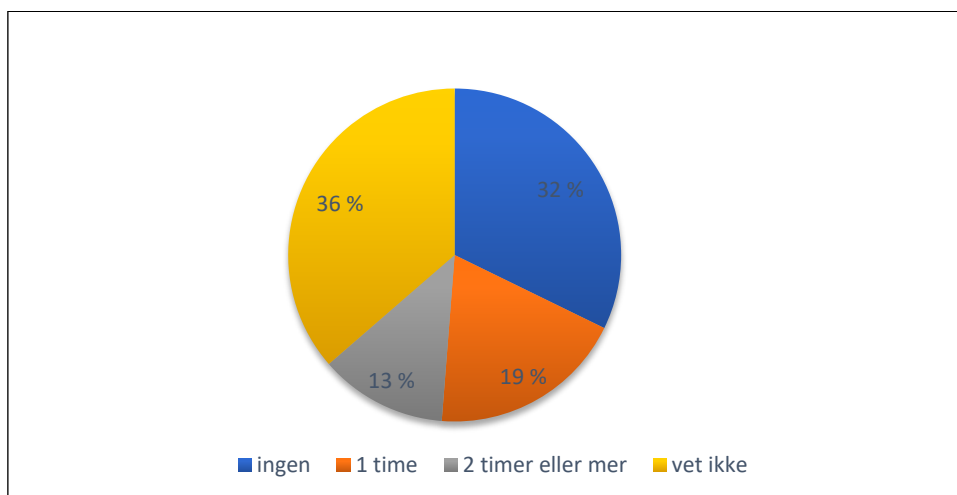
Figur 4.2 : I hvilken grad anser ledelsen at IKT-sikkerhet, HMS, næringslivsetikk og økonomisk kriminalitet inngår i sikkerhetskulturen? Antall svar fordelt på «i stor grad, i noen grad, i liten grad og vet ikke. (n= 133)

NVE har stilt spørsmål om hvilke temaer som er på dagsorden på ledermøtene. Figur 4.3 gir en oversikt og viser at beredskap, risiko og uønskede IKT-hendelser er tema som tas opp på ledermøter hos om lag 90% av KBO-enhetene. IKT-sikkerhetsrevisjon har vært tema hos omtrent halvparten av virksomhetene siste 12 månedene. Om lag 60 % av virksomhetene har hatt intern eller ekstern revisjon av IKT-sikkerhet som tema på ledermøtene. Halvparten har hatt IKT-sikkerhet på dagsorden ofte.



Figur 4.3 Prosentandel virksomheter som har hatt ulike tema på ledermøter.

NVE har også stilt spørsmål om hvor mange timer i uka som er satt av for ansatte til kompetanseheving. Figur 4.4. gir en oversikt.



Figur 4.4 Hvor mange timer i uka i snitt er satt av til kompetanseheving for fast ansatt personell? (N=121)

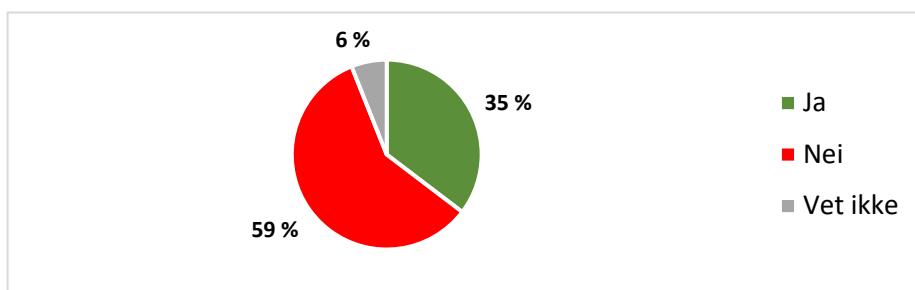
32% har ikke satt av timer per uke til kompetanseheving, og 36% vet ikke omfanget av dette. Det kan innvendes at kompetanseheving er behovsstyrt, og at man derfor ikke har satt av et bestemt antall timer til dette.

I undersøkelsen stilte NVE også spørsmål til beredskapslederne om de hadde behov for kompetanseheving. 36% av beredskapslederne hadde stort behov for opplæring i informasjonssikkerhetsledelse og 40% av dem hadde stort behov for opplæring i kraftberedskapsforskriftens krav til IKT-sikkerhet. Dette kan tolkes som at mange beredskapsledere gir uttrykk for å mangle kompetanse på informasjonssikkerhetsledelse, og manglende oversikt over kraftberedskapsforskriftens krav til IKT-sikkerhet. Samtidig er det også positivt at mange ser et behov for opplæring innen IKT-sikkerhet, og med det viser en vilje til å tilegne seg kompetanse på IKT-sikkerhet. Kontinuerlig forbedring er en

forutsetning for å etablere og vedlike holde et godt sikkerhetsnivå, og det er derfor viktig at alle har et mål om kontinuerlig kompetanseheving.

4.3 Styringssystem for informasjonssikkerhet

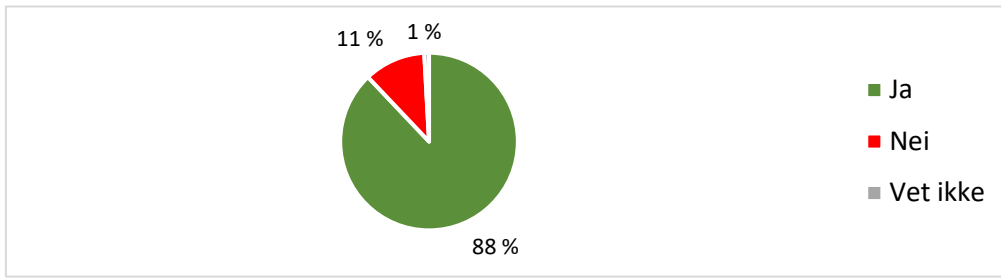
Når det gjelder den praktiske risikostyringen, har NVE stilt spørsmålene til IKT-sikkerhetskoordinatorene. 59% av IKT-sikkerhetskoordinatorene har svart at de ikke har et styringssystem for informasjonssikkerhet, 35% har svart at de har mens 6% har svart at de ikke vet, se Figur 4.5. NSM har påpekt at det er viktig å ha et styringssystem for informasjonssikkerhet på plass og har utviklet egne grunnprinsipper for sikkerhetsstyring (NSM, 2021). Et styringssystem for informasjonssikkerhet er retningslinjer og prosedyrer for systematisk styring av informasjonssikkerhet og er bygget på tre pilarer - mennesker, prosesser og teknologi. Styringssystemet sikrer forretningskontinuitet og minimerer risiko ved å aktivt å redusere sannsynlighet for sikkerhetsbrudd og ved å begrense virkningen av dem (ISMS, u.d.).



Figur 4.5 : Har virksomheten et styringssystem for informasjonssikkerheten (ISMS)? (N = 116)

I praktisk sikkerhetsarbeid er det viktig med kontinuerlig forbedring, risikovurdering og håndtering av nye typer risiko. NVEs veileder til Kraftberedskapsforskriften gir råd om hvordan virksomheter kan oppfylle kravene i forskriften. NVE anbefaler å følge med på sårbarhetsvarsler og sikkerhetsråd utsendt fra KraftCERT og fra virksomhetens leverandører. På denne måten kan en redusere egen sårbarhet og med det sannsynligheten for at cyberangrep lykkes.

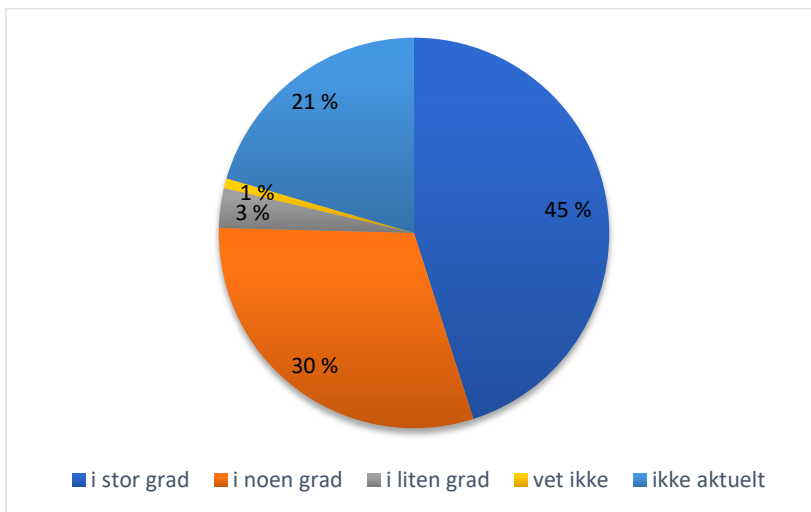
Ved å holde oversikt og administrere sårbarheter får man muligheten til å finne og rette mulige svakheter i systemet. Målet er å håndtere kjente sårbarheter før en angriper utnytter disse i et cyberangrep. Ved å ha rutiner og personell for å håndtere sårbarheter bidrar man i praksis til å identifisere, analysere og løse feil og forhindre mulige cyberangrep. I undersøkelsen oppgir 88% av IKT-sikkerhetskoordinatorene at de har rutiner for å håndtere sårbarhetsvarsler fra KraftCERT eller leverandør. 11% oppgir at de mangler rutiner.



Figur 4.6 Har virksomheten rutiner for å håndtere sårbarhetsvarsel fra for eksempel KraftCERT eller leverandører? (N = 116)

4.4 Sikker innovasjon og utvikling

For å håndtere utfordringene knyttet til IKT-sikkerhet, er det viktig at virksomheter iverksetter sikkerhetstiltak i alle deler av driften. Dette gjelder også ved nyskaping/ innovasjon. Kraftbransjen er opptatt av digitalisering, og det er mange innovasjonsprosjekter i gang som involverer økt bruk av sensorer og dataanalyse (Røyksund & Valdal, 2020). I pilotprosjekter utvikles nye løsninger, og disse kan etter pilotperioden ende opp som endelige systemer i bruk. Dersom risiko ikke er vurdert og sikkerhet tatt hensyn til under utvikling og pilotering, vil innføring av nye systemer bety større sikkerhetsrisiko.



Figur 4.7 I hvilken grad er sikkerhet tema i pilotprosjekter? (N= 122)

Blant IKT-sikkerhetskoordinatorene som besvarte spørsmål om sikkerhet i pilotprosjekter, svarer 45% at de i stor grad har sikkerhet som tema i disse prosjektene, mens 30% sier at sikkerhet i noen grad er et tema. 21% svarer at det ikke er aktuelt, som kan forstås som at de ikke driver med denne type utviklingsarbeid.

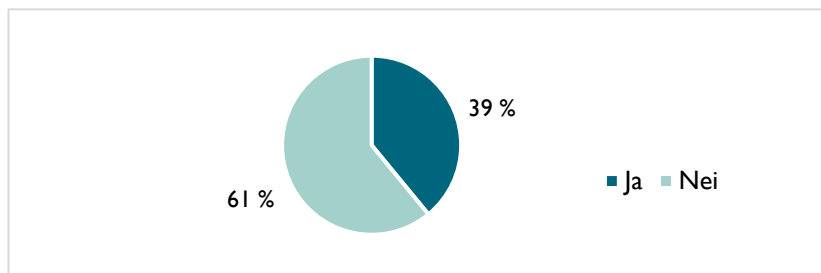
4.5 Sikring av driftskontrollsystemer

Driftskontrollsystemer har i mindre grad enn administrative IKT-systemer blitt utsatt for uønskede IKT-sikkerhetshendelser. Undersøkelsen besvart av IKT-sikkerhetskoordinatorer avdekker at 3% av virksomhetene har hatt uønskede hendelser med konsekvens for driftskontrollsystemets funksjon. Sikkerhetshendelsene har i flere tilfeller ført til nedetid, men hendelsen kan imidlertid ikke knyttes direkte til cyberangrep.

KraftCERT bemerker at det er observert svært få angrep rettet mot operasjonell teknologi (driftskontrollsystemer) i KraftCERTs medlemssektor og i Norden generelt. Samtidig kan en målrettet angriper bruke svært lang tid (måneder og år) på etterretning og på å komme seg inn i et system. Internasjonalt er situasjonen annerledes enn i Norge, og nylig observerte angrepsmetoder inkluderer blant annet målrettet phishing mot ressurser på administrative IKT-systemer med påfølgende lateral bevegelse og angrep på operasjonell teknologi. Også utpressingsvirus på administrative IKT-systemer og operasjonell teknologi trekkes frem som viktige deler av trusselbildet mot KraftCERTs medlemssektor (KraftCERT, 2021).

4.5.1 Driftsmodeller

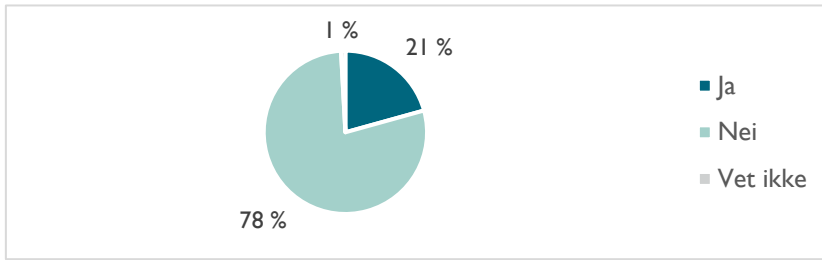
Kraftberedskapsforskriften setter krav til sikring og funksjonaliteten til driftskontrollsystemet. Forskriften spesifiserer at «det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg», jf. kbf. § 7-1.



Figur 4.8 Kjøper virksomheten driftskontrolltjenester fra en annen KBO-enhet? (N= 105)

Undersøkelsen avdekker at 39% kjøper driftskontrolltjenester fra en annen KBO-enhet, dette er illustrert i Figur 4.8. Andelen virksomheter som kjøper driftskontrolltjenester er i liten grad korrelert med størrelse, med kun få prosentpoeng forskjell mellom små, mellomstore og store virksomheter.

21% av virksomhetene drifter driftskontrollsystem på vegne av andre KBO-enheter. Virksomheter som drifter driftskontrollsystem på vegne av andre er i hovedsak virksomheter i større selskap målt i antall ansatte.

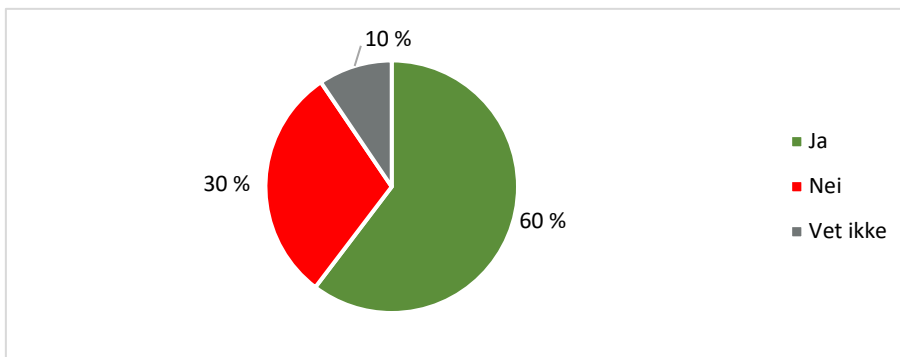


Figur 4.9 Drifter virksomheten driftskontrollsystem på vegne av andre KBO-enheter? (N = 116)

NVE har laget retningslinjer for nettselskapenes samarbeid om driftssentral (Bendiksen, 2018). To hovedkrav må være tilfredsstillt:

1. Hvert nettselskap som inngår i samarbeidet, må ha minst én ansatt som inngår i driftssentralens bemanning og utfører deler av driftsfunksjonen ved sentralen.
2. Nettselskapene som inngår i et slikt samarbeid, må kunne dokumentere at de har rutiner og tekniske løsninger for god intern kontakt mellom driftssentralen og øvrig driftspersonell hos nettselskapet.

4.5.2 Overvåking og hendelsehåndtering i driftskontrollsystemer



Figur 4.10 Har driftskontrollsystemet monitorering/overvåking av datanettverkstrafikk? (N = 114)

Gjennom overvåking av nettverkstrafikken i driftskontrollsystemet er det mulig å oppdage unormal trafikk og om en trusselaktør forsøker å trenge seg inn i systemet. Undersøkelsen viser at 60% har monitorering/overvåking av datanettverkstrafikken, mens 30% ikke har det, og 10% vet ikke.

Uavhengig av virksomhetens organisering av driftskontrollfunksjon oppgir hver tredje virksomhet at de ikke har prosedyrer for å undersøke hendelser i driftskontrollsystemet.

Virksomheters manglende eller begrensede mulighet for å undersøke hendelser i driftskontrollsystemene avdekker svakheter ved de aktuelle virksomhetenes sikkerhet.

Undersøkelsen viser at de fleste virksomhetene med driftskontrollsystemer er i stand til å isolere systemene for å håndtere alvorlige situasjoner med minimale konsekvenser. Det er kun fire virksomheter som har oppgitt at de ikke kan isolere driftskontrollsystemene i en beredskapssituasjon. Disse er små nettselskaper som i stor grad benytter tredjepart for monitorering og hendelsesdeteksjon.

4.6 Øvelser

I undersøkelsen oppgir om lag 6 av 10 av beredskapslederene at de har vært involvert i øvelser som involverer svikt i IKT-systemer eller driftskontrollsystemer siste tre år.

Kraftberedskapsforskriften § 2-7 stiller krav til øvelser knyttet til ekstraordinære situasjoner. KBO-enheter må øve på et bredt utvalg av aktuelle ekstraordinære hendelser som naturfenomener, teknisk svikt og IKT-hendelser. Undersøkelsen har bare kartlagt om det har blitt øvd på IKT-hendelser siste tre år. Enkelte KBO-enheter har en lengre tidshorison på sine øvelsesplaner. Øvelser knyttet til alvorlige situasjoner, herunder målrettede cyberangrep med konsekvens for driftskontrollfunksjonen eller virksomhetens drift, må inkludere ledelsen. God beredskap forutsetter at det foreligger gode rutiner for hendeshåndtering som er trent på i forkant av hendelsen. I ekstraordinære situasjoner som involverer cyberangrep, vil KraftCERT kunne støtte virksomheten gjennom hele prosessen. Øvelser som involverer KraftCERT og/eller leverandør er derfor anbefalt i tillegg til egne, interne øvelser.

4.7 Anskaffelser og tjenesteutsetting

Grunnlaget for god digital beredskap starter allerede i anskaffelsesfasen. Leverandørene er viktige brikker i en virksomhets beredskap. For å ha en god beredskap mot uønskede digitale hendelser og krisesituasjoner er det viktig med et godt samarbeid med leverandørene. Det er viktig at IKT-sikkerhet tas hensyn til allerede i en tidlig fase av en anskaffelse eller tjenesteutsetting. Samtidig må IKT-sikkerhet være et tema gjennom hele levetiden til produktet eller tjenesten. Dette inkluderer også fasen med avhending eller skifte av leverandør. NVE har derfor gitt ut en sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting. Sjekklisten bygger på krav fra Energiloven og kraftberedskapsforskriften, i tillegg til veiledere fra NVE og NSM. Sjekklisten er bygget rundt ulike faser i en anskaffelses- og tjenesteutsettingsprosess (NVE, 2020).

NVE har stilt spørsmål om beredskapslederene kjenner til NVEs retningslinjer for IKT-sikkerhet i anskaffelser. 76% av beredskapslederene bekrefter at de kjenner til retningslinjene. 45% sier at retningslinjene blir etterlevd i stor grad, mens 34 % sier de etterlever disse i noen grad.

På spørsmål om virksomhetene kjøper kun basispakken fra leverandører eller også avanserte sikkerhetstjenester, svarer 59% av beredskapslederne at de også kjøper avanserte sikkerhetstjenester, 31% kjøper kun basispakken, mens 10% vet ikke.

4.8 Oppsummering

Denne delen av undersøkelsen har vært rettet mot informasjonssikkerhetsledelse. De fleste spørsmålene er besvart av beredskapsledere, mens noen er besvart av IKT-sikkerhetskoordinatorer.

Oppsummert viser resultatene at beredskapsledelsen er oppmerksom på IKT-sikkerhet:

- 80% av virksomhetene har IKT-sikkerhetsstrategi
- 80% av virksomhetene har diskutert IKT-sikkerhet, IKT-beredskap og risiko i ledermøter
- I 60% av virksomhetene har ledelsen i løpet av siste treårsperiode vært involvert i øvelser med tema IKT-sikkerhet eller sikkerhet i driftskontroll

Praktisk risikostyring og sikkerhetsarbeid:

- 35% av virksomhetene oppgir å ha styringssystem for informasjonssikkerhet
- 85% av virksomhetene har rutiner for å håndtere sårbarhetsvarsler fra KraftCERT
- 79% av virksomhetene etterlever enten i noen grad eller i høy grad NVEs retningslinjer for IKT-anskaffelser

Kompetansebehov:

- 36% av beredskapslederne har stort behov for opplæring i informasjonssikkerhetsledelse
- 40% av beredskapslederne har stort behov for opplæring i kraftberedskapsforskriftens krav til IKT-sikkerhet.

Resultatene må forstås innenfor rammen av virksomhets-størrelse i kraftforsyningen. Omtrent halvparten av virksomhetene er små med inntil 50 ansatte. Sikkerhet er et stort fagfelt, og små virksomheter har begrenset med personellressurser.

5 NSM Grunnprinsipper for IKT-sikkerhet

5.1 Kraftberedskapsforskriften og NSMs grunnprinsipper for IKT-sikkerhet

Kbf. § 6-9 stiller krav til grunnsikring i digitale informasjonssystemer. Denne grunnsikringen bygger på NSMs grunnprinsipper for IKT-sikkerhet, og NVE har henvist til NSMs grunnprinsipper for IKT-sikkerhet i veiledningen til forskriften.

Denne rapporten dokumenterer i hvilken grad 62 virksomheter i kraftbransjen mener de selv oppfyller NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0. I undersøkelsen er virksomhetene bedt om å ta utgangspunkt i *administrative IKT-systemer* når de svarer. I Vedlegg 2 til rapporten ligger en liste over alle tiltak fra både prioritet 1 og prioritet 2. Listen har i tillegg oversikt over antall virksomheter som har svart «høy grad», «moderat grad», «lav grad», «ikke relevant» og «ikke vurdert». Se Figur 5.1. De to siste svaralternativene er ikke tatt hensyn til i sammenstillingen i dette kapittelet, men kommenteres separat når det er mange som har svart ikke relevant og ikke vurdert.

Benytt valgene som ligger i drop down menyen i kolonne F i spørreskjema. Her velges vurdering ihht kriterier gitt nedenfor.	
Høy grad	Det finnes flere og gode overlappende sikringstiltak som beskytter verdiene
Moderat grad	Det eksisterer sikringstiltak som beskytter verdien, men de er mangelfulle
Liten grad	Det eksisterer få eller ingen sikringstiltak som beskytter verdien og/ eller sikringstiltakene er mangelfulle
Ikke relevant	Prinsipp ikke relevant for systemet som vurderes.
Ikke vurdert	Standardverdi når prinsipp ikke er vurdert. Prinsippet blir ikke med i videre totalvurdering

Figur 5.1: Svaralternativene i undersøkelsen

NSMs grunnprinsipper er inndelt i fire hovedkategorier:

- *Identifisere og kartlegge.* Dette innebærer å opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere.
- *Beskytte og opprettholde.* Dette innebærer å ivareta en forsvarlig sikring av IKT-miljøet og opprettholde den sikre tilstanden over tid og ved endringer.
- *Oppdage.* Dette innebærer å ha løsninger for å oppdage sikkerhetstruende hendelser.
- *Håndtere og gjenopprette.* Dette innebærer å håndtere sikkerhetstruende hendelser effektivt.

Spørreskjemaet tok utgangspunkt i prioritet 1 og 2 tiltak. De fire kategoriene ovenfor er representert i begge kategoriene. Tiltakene bygger på hverandre hvor det er viktigst å ha på plass grunnleggende sikkerhetstiltak i prioritet 1 for så å bygge videre på ytterligere

sikkerhetstiltak i prioritet 2 og prioritet 3. Siden tiltakene bygger på hverandre, er enkelte tiltak en forutsetning for at andre skal kunne iverksettes og virke effektivt.

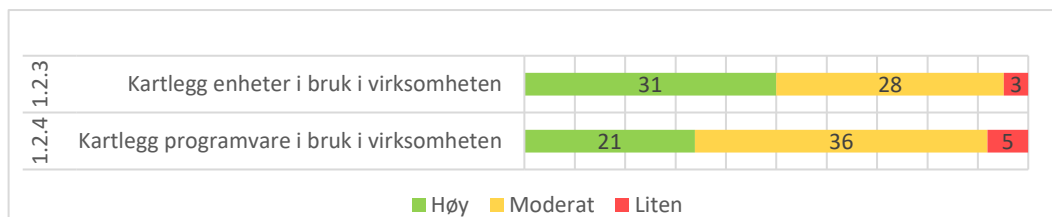
For å oppnå god risikoreduksjon bør sikkerhetstiltak iverksettes i henhold til både verdien på informasjonen de skal beskytte og resultatet av risikovurderinger. Det er nødvendig å sikre systemene og virksomheten ved å ha flere barrierer og tiltak for å hindre tilsiktede og utilsiktede IKT-hendelser.

5.2 NSMs Grunnprinsipper prioritet 1-tiltak

Identifisere og kartlegge er den første kategorien i NSMs grunnprinsipper. Kartlegging av enheter og programvare er viktig for å få oversikt over IKT-infrastrukturen i virksomheten. Kartlegging av enheter bør dekke virksomhetsstyrte enheter, legitime enheter med begrensede rettigheter og «ukjente enheter». Enheter er utstyr som for eksempel datamaskiner, servere, nettverksutstyr som rutere og svitsjer og skrivere. Listen er ikke uttømmende.

Noen virksomheter har liten eller ingen kontroll på sikkerhetstilstanden til disse enhetene, og de har små muligheter til sikkerhetsovervåkning. Enheter kan bli kompromittert, eller kan allerede være kompromittert, og kompromitterte enheter kan benyttes til å angripe interne ressurser.

I praksis kan det være utfordrende for virksomheter å ha full kontroll på hele IKT-infrastrukturen. I en del tilfeller vil ikke virksomheten ha kontroll på en gitt type utstyr. For eksempel kan dette gjelde når eksterne leverandører drifter system eller når virksomheten tillater bruk av ikke-forvaltede enheter. Virksomheten må være bevisst rundt sikkerhetsutfordringene dette medfører og vurdere kompenserende tiltak som for eksempel forsterket deteksjonsevne, segregering av nettverk og lavere eksponering av verdifull informasjon og IKT-systemer.



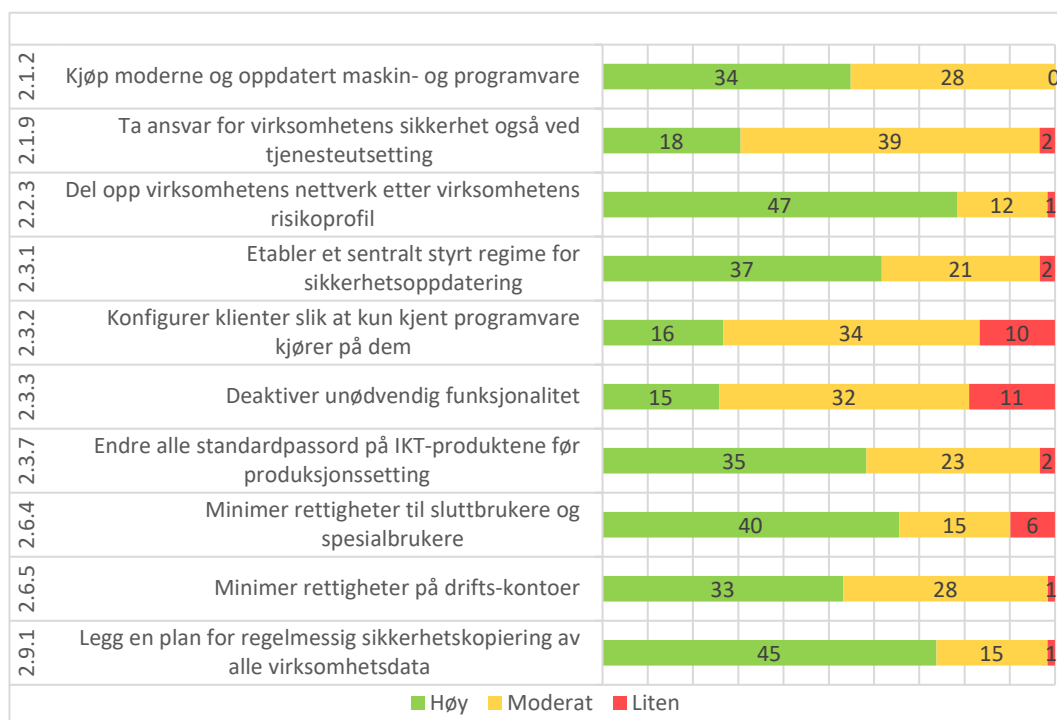
Figur 5.2: Virksomhetenes svar på om de identifiserer og kartlegger enheter og programvare (N=62), prioritet 1 tiltak. Figuren viser for hvert nummerert tiltak antall svar fordelt på kategorien høy, moderat og liten.

En angriper vil gå minste motstands vei for å komme inn og få kontroll over et informasjonssystem. Dersom man har dårlig planskisse før «bygging», lite kontroll på «byggeprosessen» og manglende vedlikehold etterpå, vil det være mange hull og inngangsdører som en angriper kan utnytte. Resultatene viser at det er mindre oversikt over programvare enn over fysiske enheter, og det er et forbedringspotensial generelt sett.

Uten å ha kartlagt installert programvare er det utfordrende å ha oppdaterte IKT-systemer. Man kjenner ikke til sårbarhetene som ligger i programvaren og mangler oversikt over installerte programvareversjoner. Slik mangel kan føre til dårlig oppfølging av sårbarhetsvarsler fra leverandør og at man ikke klarer å fange opp kritiske programoppdateringer.

Beskytte og opprettholde er den andre kategorien i NSMs grunnprinsipper. Beskytte og opprettholde innebærer at virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstillir virksomhetens behov for sikkerhet. Det innebærer at virksomheten har etablert rutiner for sporing, rapportering og korrigerende av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

De tiltakene som har høyest «rød svar-andel», tiltaksnummer 2.3.2 og 2.3.3 fra Figur 5.3 nedenfor (resultat oppgitt i antall i figur), forteller at 10 og 11 virksomheter i liten grad har det man ofte kaller hvite- og svartelisting av programmer og funksjonalitet på plass. Det å minimere programvare som er tillatt å kjøre er tidkrevende og er en kontinuerlig prosess. Sikkerheten økes betraktelig dersom virksomheten har god kontroll på tillatt programvare. Seks virksomheter har ikke minimert rettigheter til sluttbrukere og spesialbrukere (tiltak 2.6.4). Dette er ett av de fire viktigste sikkerhetstiltakene som har vært framhevet av NSM i en årrekke.



Figur 5.3 Virksomhetenes svar på om de beskytter og opprettholder sikkerheten, N= 62, prioritert 1 tiltak. Figuren viser for hvert nummerert tiltak, antall svar fordelt på kategorien høy, moderat og liten.

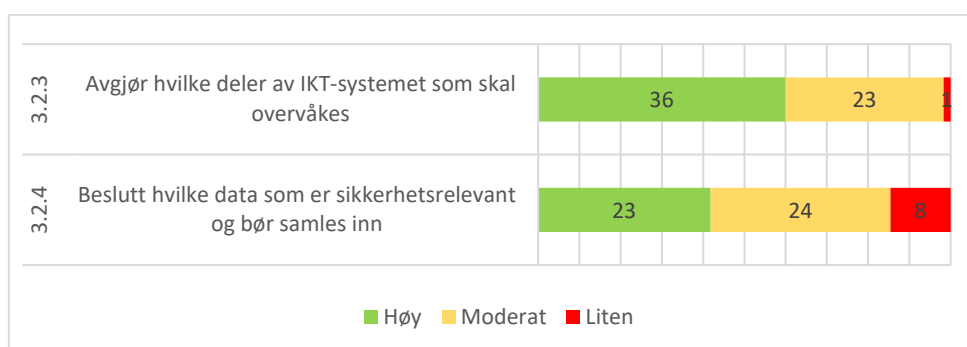
Nesten alle virksomheter har delt opp datanettverket etter risikoprofil og har plan for regelmessig sikkerhetskopiering (tiltak 2.2.3). Bare en virksomhet sier at de i liten grad har gjort dette, mens 47 virksomheter har i høy grad dette tiltaket på plass. 12

virksomheter svarer «moderat grad». Dette er tiltak som i mange år har vært en del av kraftberedskapsforskriften og som resultatene her viser, er kjent i bransjen.

Oppdage er den tredje kategorien i NSMs grunnprinsipper. Analyse og innsamling av sikkerhetsrelevant data kan bidra til å forstå hendelsesforløpet og oppdage sikkerhetshendelser tidlig. Det kan også være avgjørende for at virksomheten skal gjenopprette normaltilstand så raskt som mulig og for å hindre gjentakende hendelser. Sikkerhetsbrudd og uautoriserte handlinger bør oppdages så tidlig som mulig slik at skaden kan minimeres og aller helst forhindres.

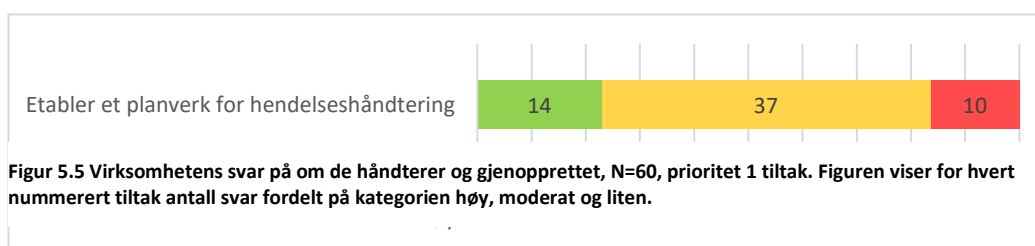
For at hendelser skal oppdages er det nødvendig å identifisere kritiske systemer og data, og beslutte hvilke data som skal er sikkerhetsrelevante og skal samles inn (tiltak 3.2.4). 8 virksomheter har i liten grad dette tiltaket på plass. I tillegg er det syv virksomheter, som vist i Vedlegg 2 til rapporten, som ikke vet eller har vurdert tiltaket. Dette forsterker usikkerheten knyttet til gjennomføring av dette tiltaket.

Angripere kan skjule handlinger og aktiviteter i virksomhetens informasjonssystemer dersom virksomheten har mangelfull sikkerhetsovervåkning i informasjonssystemer og mangelfull analyse av sikkerhetsrelevant data. Dersom virksomheten ikke har etablert tilstrekkelig sikkerhetsovervåkning, vil de ofte være blinde for detaljer når enheter eller systemer blir infiltrert.



Figur 5.4 Virksomhetens svar på om de oppdager hendelser, N=60, prioritert 1 tiltak. Figuren viser for hvert nummerert tiltak antall svar fordelt på kategorien høy, moderat og liten.

Håndtere og gjenopprette er den fjerde kategorien i NSMs grunnprinsipper for IKT-sikkerhet. Forsøk på innbrudd i IKT-systemer skjer hele tiden, og det er viktig at virksomheter har en plan og en prosess for hendeshåndtering for å begrense skaden og gjenopprette normaltilstanden. Det er for sent å utarbeide gode planer når en hendelse allerede har inntruffet.



Figur 5.5 Virksomhetens svar på om de håndterer og gjenoppretter, N=60, prioritert 1 tiltak. Figuren viser for hvert nummerert tiltak antall svar fordelt på kategorien høy, moderat og liten.

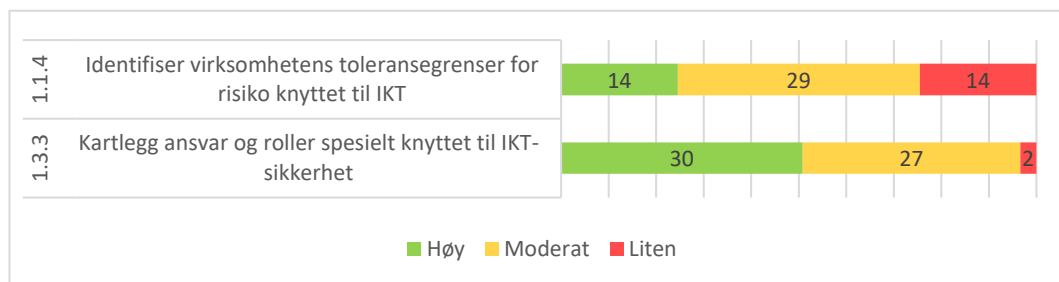
Et planverk bør støttes av et hendelsehåndteringssystem (f.eks. SIEM), samt ansvarsoversikt og prosedyrer som skal brukes ved digitale hendelser. Det er viktig å inkludere ledelsen og krisestaben i planverket. En innsatsplan for IKT-hendelser koplet til virksomhetens beredskapsplan vil være en nyttig start. Denne innsatsplanen bør også involvere leverandør og KraftCERT, og inneholde varsling til NVE og KraftCERT. Mange virksomheter i kraftforsyningen bruker samme leverandører, og dersom en virksomhet er infisert kan det fort gjelde flere. NVE med støtte av KraftCERT bidrar med å dele informasjon i sektoren slik at andre virksomheter kan varsles og iverksette tiltak. På den måten kan det mulige skadeomfanget i sektoren blir redusert. 14 virksomheter svarer at de i høy grad har på plass planverk for hendelsehåndtering, mens 60 % svarer at planverket er på plass i moderat grad. 10 virksomheter svarer at de i liten grad har etablert dette.

5.3 NSMs Grunnprinsipper prioritet 2 tiltak

Prioritet 2 tiltak bygger på prioritet 1 tiltak.

Identifisere og kartlegge. Manglende styringsstrukturer og prosesser for risikovurdering kan føre til at ledelsen ikke får tilstrekkelig informasjon til å prioritere og styre virksomhetens sikkerhetsarbeid.

På tiltak 1.1.4 vises det at 14 av virksomhetene i liten grad har identifisert toleransegrenser for risiko knyttet til IKT. I Vedlegg 2 framgår det i tillegg at fem virksomheter ikke vet eller har vurdert dette tiltaket. Dette gir et bilde av at det er krevende å iverksette dette tiltaket. Ledelsen må fastsette hvilke grenser for risiko virksomheten aksepterer, hva som er uakseptabel risiko og etablere kriterier for hvordan man evaluerer risiko sett opp mot virksomhetenes sikkerhetsmål. Dette må kommuniseres på tvers i organisasjonen. Tiltak 1.3.3. handler om å ha oversikt over ansvar og roller knyttet til IKT-sikkerhet. Utydelige roller og ansvar kan føre til at noen oppgaver ikke blir utført.



Figur 5.6: Virksomhetenes svar på om de identifiserer og kartlegger risiko, ansvar og roller (N=62), prioritet 2 tiltak. Figuren viser for hvert nummerert tiltak, antall svar fordelt på kategorien høy, moderat og liten.

Beskytte og opprettholde. Her har NSM listet en rekke tiltak som til sammen skal bidra til å beskytte data og systemer og opprettholde et sikkerhetsnivå. Tiltak 2.1.1 handler om å integrere IKT-sikkerhet i anskaffelsesprosesser. Det første tiltaket vist i diagrammet, se

Figur 5.7, viser i hvilken grad IKT-sikkerhet er innlemmet i anskaffelsesprosesser. Gitt leverandørens viktige rolle i kraftforsyningen, så er dette et viktig tiltak. Tiltaket innebærer at virksomheter skal inkludere sikkerhet i hele livsløpet fra anskaffelse til avhending. 6 av virksomhetene har i liten grad gjort dette. NVE har utgitt retningslinjer for IKT-sikkerhet i anskaffelser og tjenesteutsetting som gir mer detaljerte råd (NVE, 2020).

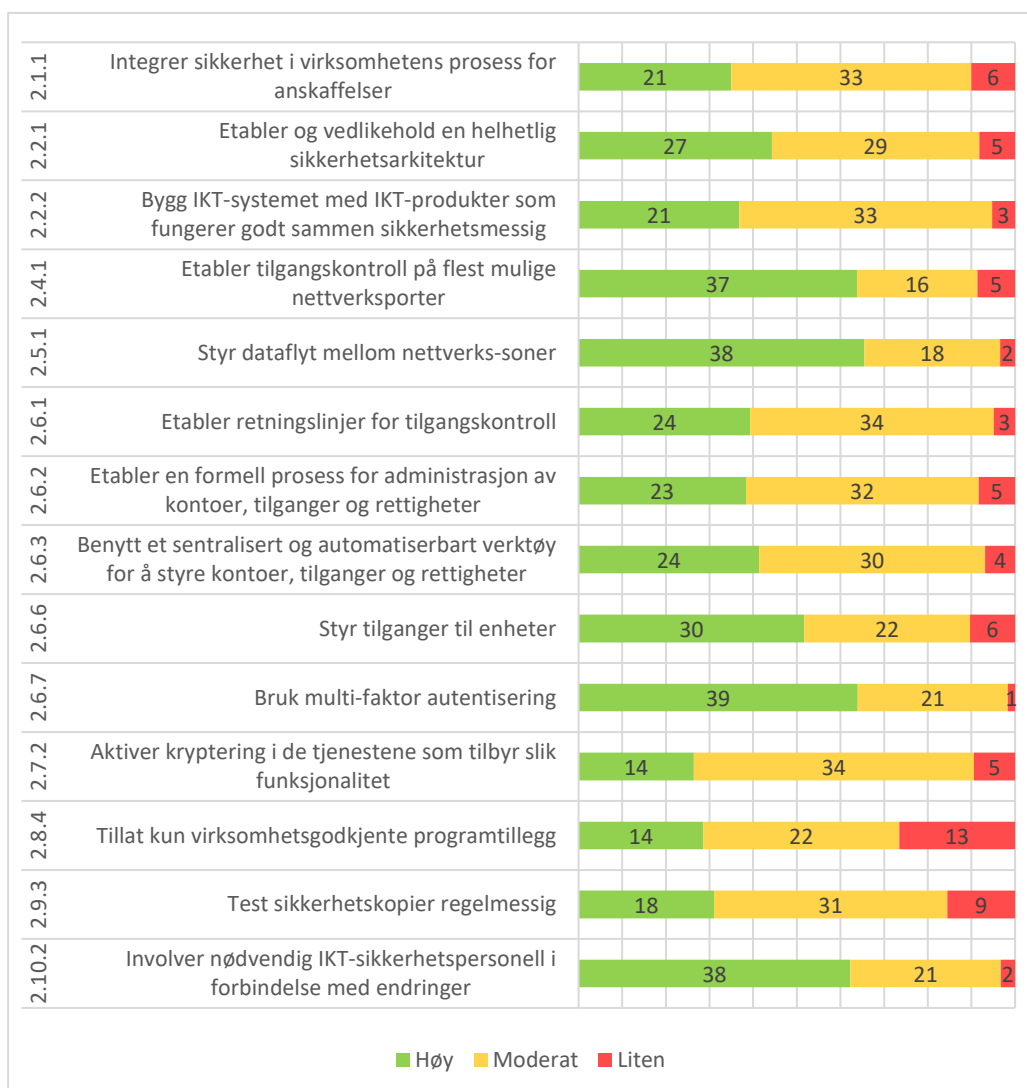
Mange av tiltakene i denne prioriteringsgruppen og kategorien handler om å bygge en god sikkerhetsarkitektur med god styring på tilgangsrettigheter fra ulike brukere og dataflyt. Tiltak 2.1.1, etabler og vedlikehold en god sikkerhetsarkitektur, krever at man har god oversikt over hele systemet, det som en drifter selv, og det som er satt ut til leverandør.

Hensikten med tiltak 2.8.4, om å bare tillate virksomhetsgodkjente programtillegg, er at virksomheten minimerer angriperes mulighet til å manipulere menneskelig oppførsel i forbindelse med bruk av e-postklienter og nettlesere. For mange virksomheter er nødvendige programtillegg (plugins), kun de som integreres i e-postleser og nettleser mot for eksempel sak- og arkivsystemer. Tillegg som ikke er nødvendige for virksomheten kan utgjøre en sårbarhet, og bør derfor ikke installeres. Mengden valg og funksjoner som tillegg kan tilby, kan innebære komplekse konfigureringsmuligheter og dermed åpne for sikkerhetsproblemer. 13 av virksomhetene har i liten grad dette tiltaket på plass. Problemet forsterkes ved at 11 virksomheter ikke vet eller har vurdert tiltaket, se Vedlegg 2.

Det er ikke uvanlig at brukere har tilgang til systemer og tjenester de ikke har behov for og har mer rettigheter enn de trenger for å gjøre jobben sin. Tilgangen til de ulike delene av et informasjonssystem bør derfor styres ut ifra behovet gitt av arbeidsoppgaver for å redusere skaden fra en mulig kompromittering av en ansattkonto eller en utro ansatt. En virksomhet må ha kontroll på de ulike brukerne, kontoene de disponerer og hvilke rettigheter en gitt konto har. Dette betyr å ha kartlagt ansvarsroller internt i virksomheten, bl.a. sikkerhetssjef, IT-sjef, applikasjonsansvarlig, men også roller og oppgaver som gjøres av eksterne leverandører og partnere. Deretter må tilgang til ulike tjenester og systemer styres. Dette gjøres gjennom prosesser for tilgangsstyring og ved bruk av et sentralisert system for styring av kontoer og tilgangsrettigheter (tiltak 2.6.1 og 2.6.3). Multifaktor-autentisering (tiltak 2.6.7) er et viktig tiltak for å redusere muligheten for at en angriper kan ta over brukerkontoer. Virksomhetene benytter ulike systemer og applikasjoner, og resultatene viser at selv om dette tiltaket i høy grad er på plass hos mange virksomheter, er det fortsatt en del virksomheter som i varierende grad har iverksatt flerfaktor-autentisering. En mulig forklaring er at ikke alle systemer og tjenester har tilbud om flerfaktor-autentisering.

Det er viktig å identifisere eksisterende sikkerhetstiltak og vurdere effektiviteten av disse opp imot verdiene de skal beskytte. Et viktig tiltak som spesielt kan nevnes her, er regelmessig testing av sikkerhetskopier (tiltak 2.9.3). Regelmessig testing må gjøres for å sjekke om sikkerhetskopier fungerer etter sin hensikt. Ved skadevareangrep (ransomware) vil sikkerhetskopier være en viktig redningsplanke. Det er også viktig at

sikkerhetskopiene er beskyttet godt, slik at virksomheten kan benytte en ikke-infisert sikkerhetskopi. Ni av virksomhetene har i liten grad slik testing på plass.

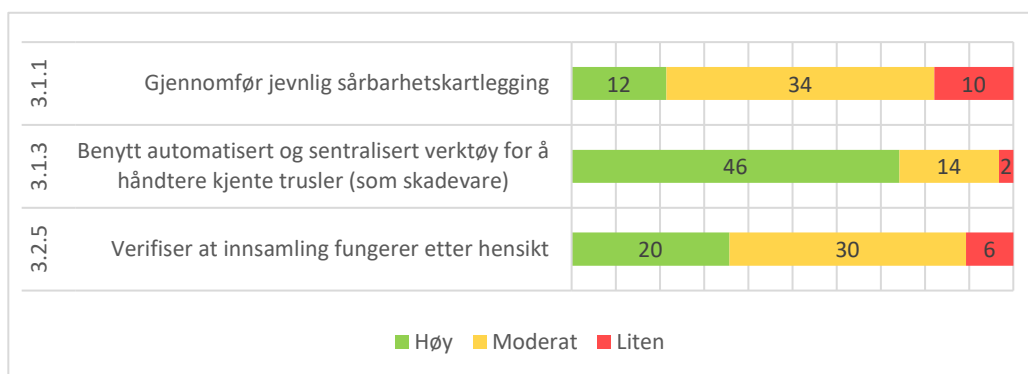


Figur 5.7: Virksomhetenes svar på om de beskytter og opprettholder sikkerheten, N= 62, prioritert 2 tiltak. Figuren viser for hvert nummerert tiltak, antall svar fordelt på kategorien høy, moderat og liten, målt mot en prosentvis skala.

Oppdage. Analyse og innsamling av sikkerhetsrelevante data kan bidra til å forstå hendelsesforløpet og oppdage sikkerhetshendelser tidlig. Dette kan også være avgjørende for at virksomheten skal gjenopprette normaltilstand så raskt som mulig, og for å hindre gjentakende hendelser. Sikkerhetsbrudd og uautoriserte handlinger bør oppdages så tidlig som mulig slik at skaden kan minimeres og aller helst forhindres. For at hendelser skal oppdages raskt, er det nødvendig å kartlegge sårbarheter.

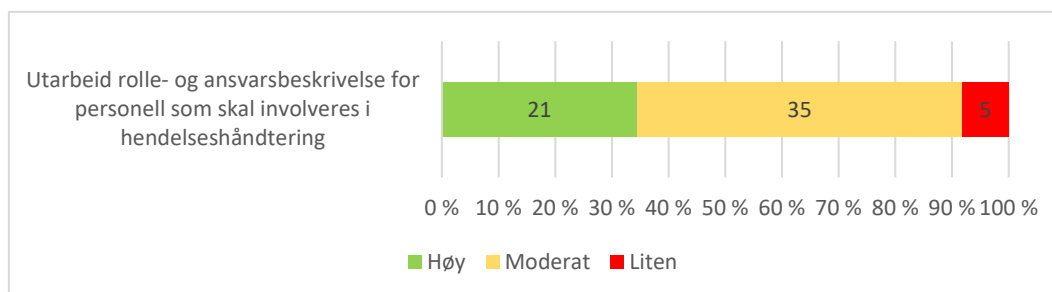
Angriperne kan skjule handlinger og aktiviteter i virksomhetens informasjonssystemer dersom virksomheten har mangelfull sikkerhetsovervåking av informasjonssystemene og datanettverket, og mangelfull analyse av sikkerhetsrelevante data. Dersom virksomheten ikke har etablert tilstrekkelig sikkerhetsovervåking, vil virksomheten ofte

være blindet for detaljer når maskiner eller systemer blir infiltrert. 10 av virksomhetene gjennomfører i liten grad sårbarhetskartlegging (tiltak 3.1.1) og bare 12 har dette på plass i høy grad. Det er også få virksomheter som i høy grad verifiserer at innsamling av sikkerhetsdata fungerer etter sin hensikt (tiltak 3.2.5). De aller fleste av virksomhetene benytter automatisert og sentraliserte verktøy for å håndtere kjente trusler som skadevare (ransomware).



Figur 5.8: Virksomhetens svar på om de oppdager hendelser, N=62, prioritert 2 tiltak. Figuren viser for hvert nummerert tiltak, antall svar fordelt på kategorien høy, moderat og liten, målt mot en prosentvis skala.

Håndtere og gjenopprette. Virksomheten bør ha tydelig rolle- og ansvarsbeskrivelser for personale som skal bidra i hendelseshåndteringen. Hendelseshåndtering inkluderer arbeidsoppgaver innen deteksjon, skadevurdering (triage), tiltak for skademinimering, sikring av bevis ved angrep og gjenoppretting av integriteten til systemer og IT-nettverk.



Figur 5.9: Virksomhetenes svar på om de håndterer og gjenoppretter system etter hendelser, (N=62), prioritert 2 tiltak. Figuren viser for hvert nummerert tiltak, antall svar fordelt på kategorien høy, moderat og liten, målt mot en prosentvis skala.

NSM anbefaler at virksomheter har personell med spesifikke oppgaver, for eksempel en plattformansvarlig eller en IT-sjef. NSM anbefaler også å ha ledere med beslutningsansvar på ulike nivåer og beredskapsvakter som er tilgjengelig utenfor normal arbeidstid. I tillegg anbefaler NSM å sørge for øving og opplæring av personell i henhold til beskrivelse i planverket. Det er en fordel å ha forhåndsgodkjente handlingsmønstre for å unngå forsinkelser når man blir truffet av for eksempel en alvorlig skadevare. Et oppdatert og testet planverk, god planlegging og døgkontinuerlig vaktordning kan bety mye for en virksomhet når dataangrep treffer virksomheten. Figur 5.9 viser at de fleste virksomheter har på plass rolle- og ansvarsbeskrivelser for personell som skal involveres i hendelseshåndteringen, men bare en tredel svarer at dette i høy grad er på plass.

5.4 Oppsummering

Rapporten har kartlagt i hvilken grad virksomhetene har innført sikkerhetstiltak som anbefalt i NSMs grunnprinsipper for IKT-sikkerhet. Totalt 62 virksomheter inngår i datagrunnlaget. NSM har gruppert tiltakene i fire kategorier:

- Identifisere og kartlegge – dette er grunnleggende for all sikkerhetsstyring, risikostyring og forvaltning av IT.
- Beskytte og opprettholde – omhandler å sikre systemene og data gjennom hele levetiden.
- Oppdage – det er ikke mulig å sikre seg fullstendig mot uønskede hendelser som feil og dataangrep, derfor er det viktig å oppdage angrep og feiltilstander.
- Håndtere og gjenopprette – sterk avhengighet av digitalisert informasjon og data gjør at det er viktig å kunne håndtere uønskede hendelser, rette feil og gjenopprette funksjonaliteten til systemene.

NSMs grunnprinsipper for IKT-sikkerhet inkluderer totalt 118 tiltak. NSM har prioritert og gruppert enkelttiltak. Tiltakene er gitt prioritet 1,2 3, hvor prioritet 1 tiltakene er grunnleggende, mens prioritet 2 og 3 tiltak vil tilføre ytterligere sikkerhet for virksomhet og systemer. Denne undersøkelsen dekker kun de 35 viktigste tiltakene i prioritet 1 og 2 og representerer samtlige kategorier i grunnprinsippene.

Sammenstillingen av svarene viser at de fleste virksomhetene i noen grad har sikkerhetstiltak på plass. Avhengig av type tiltak, er det variasjon mellom hvor stor andel av virksomhetene som har de fleste tiltakene på plass (som har svart i høy grad), og de som har tiltak, men oppgir at tiltakene er mangelfulle (som har svart i moderat grad). Det totale bildet viser at det er gjort mye godt sikkerhetsarbeid i mange virksomheter, men også at det er et rom for forbedring hos mange virksomheter. Virksomhetene bør i første omgang prioritere prioritet 1 tiltakene. Prioritet 1 tiltak er forutsetning for at andre tiltak skal ha effekt, for eksempel prioritet 2 tiltakene. IKT-sikkerheten kan styrkes ved å arbeide systematisk med NSMs grunnprinsipper for IKT-sikkerhet. Samtidig vil virksomheten bidra til å styrke etterlevelsen av kravene i kbf § 6-9.

Svarene viser at minst 7 av 10 av virksomhetene i stor eller moderat grad har innført følgende tiltak:

- Inndelt IT-nettverket etter risikoprofil
- Tatt i bruk automatisk og sentralisert programvare for å håndtere kjente trusler
- Innført multifaktorautentisering
- Etablert plan for sikkerhetskopiering

Svarene viser også at virksomhetene har størst rom for forbedring på følgende tiltak:

- Konfigurere klienter og programvare samt deaktivere unødvendig programvare
- Identifisere tålegrense for IKT-risiko -dette er en oppgave for ledelsen
- Styre tilgangen til enheter
- Teste sikkerhetskopier regelmessig

- Tillate kun virksomhetsgodkjent programvare
- Gjennomføre jevnlig sårbarhetsskanning

Selv om halvparten av virksomhetene i kraftforsyningen er små med færre enn 50 ansatte, er alle tiltakene relevante både små og store virksomheter. Dersom virksomheten ikke har intern kompetanse og kapasitet så finnes det en leverandørindustri som kan bistå.

6 Konklusjon

Rapporten bygger på datagrunnlag innhentet gjennom spørreundersøkelser rettet mot beredskapsledere og IKT-sikkerhetskoordinatorer i perioden mai-juni 2021.

6.1 Hvordan er IKT-sikkerheten i den norske kraftforsyningen slik bransjen selv vurderer det?

Vi har foreløpig ikke tilstrekkelig grunnlag for å gjøre en kvalitativ vurdering av om nivået på sikkerhet avdekket i denne undersøkelsen. Undersøkelsen viser at 80% av virksomhetene har en IKT-strategi og at IKT-sikkerhet, risiko og beredskap er på agendaen i ledermøter hos svært mange virksomheter. Dette kan sies å være bra, men vi ser likevel et forbedringspotensial i å innføre styringssystem for informasjonssikkerhet og involvere ledelsen i øvelser. Flere beredskapsledere har ønsket seg en uavhengig trusselrapport for kraftforsyningen og opplæring i kraftberedskapsforskriftens krav til IKT-sikkerhet og informasjonssikkerhetsledelse.

Leverandører er viktige for virksomhetene i kraftforsyningen. Halvparten av beredskapslederne har svart at retningslinjene for IKT-sikkerhet i anskaffelser utgitt av NVE i stor grad blir fulgt og samme andel svarer at de i noen grad blir fulgt.

Resultatene fra denne studien viser at det gjøres mye godt sikkerhetsarbeid i kraftforsyningen. Likevel er det svakheter i sikkerhetsarbeidet hos mange virksomheter. Mange virksomheter har mangelfull kartlegging av enheter og programvare. God oversikt er grunnlaget for godt sikkerhetsarbeid. Med mer digitalisering og, flere sensorer og enheter koplet til datanettverkene, blir denne oppgaven enda viktigere framover. Virksomhetene som ikke allerede har gjort det, må iverksette tiltak i henhold til NSMs grunnprinsipper for IKT-sikkerhet for prioritet 1 og 2 tiltak, slik at de oppnår større grad av beskyttelse mot digitale trusler. Med en slik praksis oppnås også bedre etterlevelse av kraftberedskapsforskriftens krav til sikring av digitale systemer (Kbf § 6-9).

6.2 I hvilken grad har cyberangrep hatt konsekvenser for funksjonaliteten til driftskontrollsystem, samt forsyningssikkerhet av elektrisitet og fjernvarme?

Forsøk på innbrudd og angrep foregår hele tiden. Denne undersøkelsen viser at i kraftforsyningen har 8% av virksomhetene opplevd uønskede IKT-hendelser i administrative IKT-systemer som har gitt konsekvenser for driften, og 3% har opplevd uønskede hendelser som har hatt konsekvenser for driftskontrollsystemets funksjon. Hendelsene i driftskontrollsystemet skyldes ikke cyberangrep. Ingen av hendelsene i driftskontrollsystemet har hatt konsekvens for forsyningssikkerheten av elektrisitet eller fjernvarme. Mange av hendelsene i administrative IKT-systemer kan forklares ved at virksomheten blir rammet via leverandører som er rammet. Uten sammenligningsgrunnlag over tid eller med andre sektorer, er det vanskelig for oss å

bedømme situasjonen som alvorlig eller mindre alvorlig. Rapporten gir et startpunkt for senere trendanalyser.

Bildet av uønskede IKT-hendelser samsvarer med KraftCERTs trusselbilde for den norske kraftforsyningen. Omfanget av innbruddsforsøk og svindelforsøk er høyt og må tas på alvor. IKT-sikkerhetsarbeidet må fortsatt prioriteres. Dersom virksomheter i kraftforsyningen tar høyere risiko i forbindelse med digitaliseringsinitiativer, må virksomhetene samtidig styre denne risikoen ved å investere i IKT-sikkerhetstiltak, prosedyrer og beredskap.

6.3 Videre arbeid

NVE vurderer at som følge av den økende digitaliseringen, vil den digitale infrastrukturen ekspandere. Dermed øker kompleksiteten og angrepsflaten. En større angrepsflate er vanskeligere å beskytte. Det er viktig å være oppmerksom på framtidrisikoen: Risikoen øker når leverandørene ikke lenger tilbyr støtte for enhetene og programvaren som er i bruk, og eiere ikke har vedlikeholdsbudsjett til å erstatte gammel teknologi med ny. Kriminelle vil uavhengig av virksomhetenes ressurser til IKT-sikkerhetsarbeid utnytte sårbarheter for egen vinning. Dersom virksomhetene ikke har høy bevissthet på IKT-sikkerhet og god styring på risiko, kan virksomhetene framover komme til å oppleve flere angrep og kompromitteringer med konsekvenser for driften.

Denne undersøkelsen bygger på NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0 og prinsippene er anvendt i andre samfunnssektorer. Vi vurderer at resultatene i denne undersøkelsen er nyttige for å få en oversikt over tilstanden, men likevel for grovmasket til at det er mulig å identifisere tydelige og spesifikke mangler i bransjen. Måling av sikkerhetstilstanden bør gjennomføres på nytt om ett til to år, med en skala med noe høyere oppløsning. Siden mange virksomheter ikke har alle tiltakene i prioritet 1 og 2 på plass, bør virksomhetene prioritere å få på plass disse 35 tiltakene i første omgang. På lengre sikt vil NVE undersøke status på resterende tiltak i prioritet 3.

NVE setter søkelyset på etterlevelse av kraftberedskapsforskriftens krav til sikring av digitale systemer når NVE gjennomfører tilsyn med IKT-sikkerheten. Disse kravene bygger på NSMs Grunnprinsipper for IKT-sikkerhet, noe som er dokumentert i NVEs veileder til kraftberedskapsforskriften (NVE, 2020). Å måle status i bransjen kan bidra til å vurdere om sikkerhetsnivået forbedres over tid.

Sintef Digital har gjort en studie for Petroleumsstilsynet der de har undersøkt relevansen av NSMs grunnprinsipper for industrielle kontrollsystemer. Gjennomgangen viser at de fleste tiltakene i NSMs grunnprinsipper er relevante også for industrielle kontrollsystemer (Jaatun, Wille, Bernsmed, & Kilsgard, 2021). For kraftforsyningen gjelder kravene til sikring av digitale systemer i kbf også for driftskontrollsystemer.

Denne undersøkelsen har fokusert på administrative IKT-system. En tilsvarende kartlegging kan gjøres for industrielle kontrollsystemer for å få et bedre bilde av tilstanden her. I dette kartleggingsarbeidet er det fornuftig å velge ut tiltak som Sintef har pekt på har høy grad av relevans for industrielle kontrollsystemer.

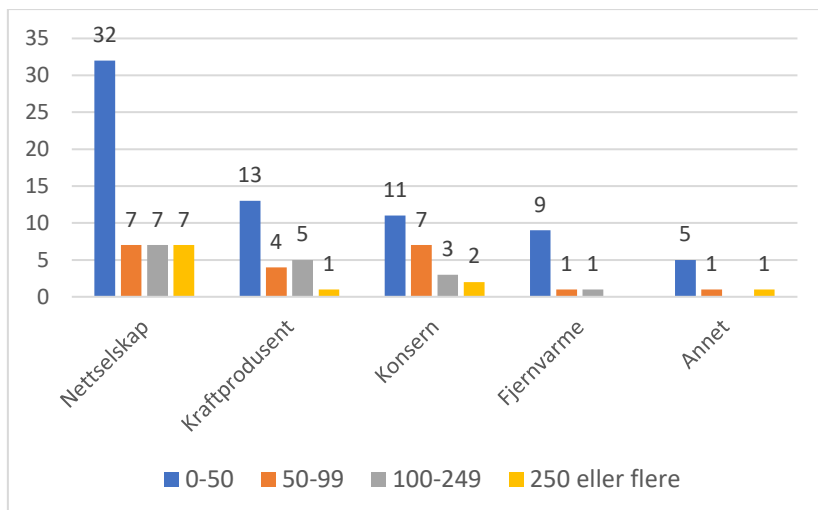
Undersøkelsen peker på uønskede IKT-hendelser hos leverandørene som årsak til de fleste hendelsene som hadde konsekvenser for virksomhetens drift. Undersøkelsen viser viktigheten av at NVE iverksetter arbeid for å vurdere hvordan NVE og aktørene i kraftforsyningen kan bidra i å redusere utfordringene knyttet til sårbarhet i leverandørkjedene.

NVE vil arbeide videre for å heve kompetansen og styrke beredskapsarbeidet i kraftforsyningen. Denne studien gir et utgangspunkt for å øke bevisstheten i kraftforsyningen og utforme relevante tiltak som hever sikkerhetsnivået.

Vedlegg

Vedlegg 1 Datagrunnlaget

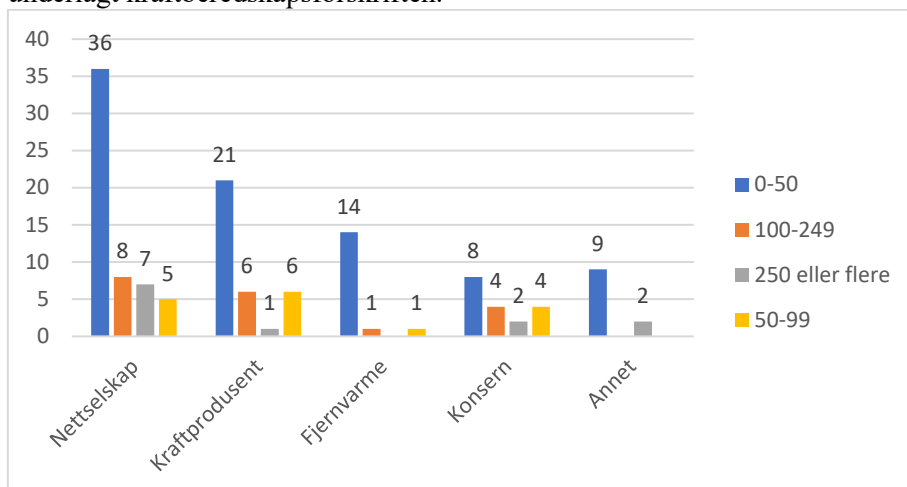
Undersøkelsen om sikkerhetstilstanden i kraftforsyningen er besvart av 117 IKT-sikkerhetsansvarlige i virksomheter som er underlagt kraftberedskapsforskriften.



Figur V.1 Bransjeinndelt og størrelsesinndelt fordeling av respondentene i undersøkelsen om sikkerhetstilstanden i kraftforsyningen (n = 117)

IKT-sikkerhetskoordinatorer har også besvart spørsmål om virksomheten har iverksatt tiltak som anbefalt av NSM i NSMs grunnprinsipper for IKT-sikkerhet. Ikke alle leverte skjema innenfor tidsfristen. Noen sendte ett skjema og svarte for flere virksomheter i konsernet. I den grad vi fanget opp dette, er det korrigert. Meningen var at ett skjema skulle fylles ut for hvert organisasjonsnummer. Etter en gjennomgang av e-poster og vedlegg satt vi igjen med 62 besvarelser som var komplette og som ble brukt i den videre analysen av kraftforsyningens IKT-sikkerhetstiltak basert på NSMs grunnprinsipper.

Undersøkelsen om sikkerhetsledelse er besvart av beredskapsleder for virksomheter underlagt kraftberedskapsforskriften.



Figur V.2 Bransjeinndelt og størrelsesinndelt oversikt over undersøkelsens respondenter (n = 134)

Vedlegg 2 Samlet tabellarisk oversikt over NSMs grunnprinsipper med svarfordeling

Tabell med NSMs grunnprinsipper tiltak oversikt som inngår i hvert grunnprinsipp

Tiltak	Pri	Tiltaksoversikt	Høy	Moderat	Liten	Ikke relevant	Ikke vurdert
1.2.3	1	Kartlegg enheter i bruk i virksomheten	31	28	3	0	0
1.2.4	1	Kartlegg programvare i bruk i virksomheten	21	36	5	0	0
2.1.2	1	Kjøp moderne og oppdatert maskin- og programvare	34	28	0	0	0
2.1.9	1	Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting	18	39	2	3	0
2.2.3	1	Del opp virksomhetens nettverk etter virksomhetens risikoprofil	47	12	1	0	2
2.3.1	1	Etabler et sentralt styrt regime for sikkerhetsoppdatering	37	21	2	2	0
2.3.2	1	Konfigurer klienter slik at kun kjent programvare kjører på dem	16	34	10	1	1
2.3.3	1	Deaktiver unødvendig funksjonalitet	15	32	11	1	3
2.3.7	1	Endre alle standardpassord på IKT-produktene før produksjonssetting	35	23	2	2	0
2.6.4	1	Minimer rettigheter til sluttbrukere og spesialbrukere	40	15	6	1	0
2.6.5	1	Minimer rettigheter på drifts-kontoer	33	28	1	0	0
2.9.1	1	Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata	45	15	1	0	1

3.2.3	1	Avgjør hvilke deler av IKT-systemet som skal overvåkes	36	23	1	1	1
3.2.4	1	Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn	23	24	8	0	7
4.1.1	1	Etabler et planverk for hendelsehåndtering	14	37	10	0	1
1.1.4	2	Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT	14	29	14	0	5
1.3.3	2	Kartlegg ansvar og roller spesielt knyttet til IKT-sikkerhet	30	27	2	0	3
2.1.1	2	Integrer sikkerhet i virksomhetens prosess for anskaffelser	21	33	6	2	0
2.2.1	2	Etabler og vedlikehold en helhetlig sikkerhetsarkitektur	27	29	5	1	0
2.2.2	2	Bygg IKT-systemet med IKT-produkter som fungerer godt sammen sikkerhetsmessig	21	33	3	3	2
2.4.1	2	Etabler tilgangskontroll på flest mulige nettverksporter	37	16	5	0	4
2.5.1	2	Styr dataflyt mellom nettverks-soner	38	18	2	1	3
2.6.1	2	Etabler retningslinjer for tilgangskontroll	24	34	3	1	0
2.6.2	2	Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter	23	32	5	1	1
2.6.3	2	Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter	24	30	4	3	1
2.6.6	2	Styr tilganger til enheter	30	22	6	1	3
2.6.7	2	Bruk multi-faktor autentisering	39	21	1	1	0
2.7.2	2	Aktiver kryptering i de tjenestene som tilbyr slik funksjonalitet	14	34	5	2	7

2.8.4	2	Tillat kun virksomhetsgodkjente programtillegg	14	22	13	9	4
2.9.3	2	Test sikkerhetskopier regelmessig	18	31	9	0	4
2.10.2	2	Involver nødvendig IKT-sikkerhetspersonell i forbindelse med endringer	38	21	2	1	0
3.1.1	2	Gjennomfør jevnlig sårbarhetskartlegging	12	34	10	0	6
3.1.3	2	Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare)	46	14	2	0	0
3.2.5	2	Verifiser at innsamling fungerer etter hensikt	20	30	6	2	4
4.1.3	2	Utarbeid rolle- og ansvarsbeskrivelse for personell som skal involveres i hendelseshåndtering	21	35	5	1	0

Bibliografi

- Aven, T. (2020, 09 10). *Risikostyring*. Hentet fra SNL.no: <https://snl.no/risikostyring>
- Bendiksen, I. (2018, 01 22). *Felles driftssentral for flere nettselskaper – energilovens krav til ordningen*. Hentet fra nve.no: <https://webfileservice.nve.no/API/PublishedFiles/Download/201800914/2289575>
- DigitalNorway. (2020, 02 3). *DigitalNorway*. Hentet 07 01, 2021 fra De fleste dataangrep rammer småbedrifter – der konsekvensene kan være størst: <https://digitalnorway.com/de-fleste-dataangrep-rammer-smabedrifter/>
- Direkt, Infront TDN. (2021, 07 12). *Volue venter tap på inntil 40 millioner etter dataangrep*. Hentet 07 14, 2021 fra e24.no: <https://e24.no/boers-og-finans/i/M1ozaK/volue-venter-tap-paa-inntil-40-millioner-etter-dataangrep>
- Dragos. (2021, 9). *Global Electric Cyber Threat Perspective*. Hentet fra www.dragos.com: <https://www.dragos.com/resource/electric-utility-cyber-threat-perspective/>
- ENISA. (2021). *ENISA Threat landscape 2021*. Aten: ENISA.
- Forsvaret. (2021, 01 26). *Fokus 2021. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Oslo: Forsvaret. Hentet 12 07, 2021 fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf
- ISMS. (u.d.). *ISMS*. Hentet fra [isms.online](https://www.isms.online): <https://www.isms.online/information-security-management-system-isms/>
- Jaatun, M. G., Wille, E., Bernsmed, K., & Kilsgard, S. S. (2021). *Grunnprinsipper for industrielle IKT-systemer. IKT-sikkerhet - robusthet i petroleumssektoren 2020*. Trondheim: Sintef Digital.
- Kirkebø, E., & Ljøsne, M. (2018). *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen*. Oslo: NVE.
- KraftCERT. (2021). *Trusselvurdering 2021 (U.OFF)*.
- Microsoft. (2021). *Microsoft Digital Defense Report 2021*. Hentet fra [www.microsoft.com](https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report): <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>
- Maal, M., Krogedal, K., & Gjengstø, A. (2020). *IKT-sikkerhet i tjenesteutsetting og anskaffelser - sjekklister, NVE-rapport nr 1/2020*. Oslo: NVE.
- NHO. (u.d.). *Sikkerhetskultur*. (NHO) Hentet 06 23, 2021 fra [nho.no](https://arbinn.nho.no/hms/sikkerhet-og-beredskap/sikkerhet/sikkerhet/sikkerhetskultur/): <https://arbinn.nho.no/hms/sikkerhet-og-beredskap/sikkerhet/sikkerhet/sikkerhetskultur/>
- NSM. (2020). *NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0*. Oslo: NSM.
- NSM. (2021). *Grunnprinsipper for personellsikkerhet*. Hentet fra [nsm.no](https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/): <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/>

- NSM. (2021). *Grunnprinsipper for sikkerhetstyring*. Hentet fra www.nsm.no:
<https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/>
- NSM. (2021). *Risiko 2021 Helhetlig sikring mot sammensatte trusler*. Oslo: Nasjonal sikkerhetsmyndighet.
- NSR. (2020). *Mørketallsundersøkelsen 2020*. Oslo: Næringslivets sikkerhetsråd.
- NVE. (2020, 12 7). *Veiledning til kraftberedskapsforskriften*. Hentet fra NVE:
<https://webfileservice.nve.no/API/PublishedFiles/Download/5a464d8a-be24-4239-8ccd-ea3a705b7593/202017038/3390048>
- NVE og NSM. (2017). *Informasjonssikkerhetstilstanden i energiforsyningen, NVE Rapport 90:2017*. Oslo: NVE.
- PST. (2021). *Nasjonal trusselvurdering 2021*. Hentet 07 12, 2021 fra PST.no:
<https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/>
- PST. (2021). *Nasjonal trusselvurdering 2021*. Hentet 6 30, 2021 fra pst.no:
<https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/>
- Regjeringen. (2021, 02 08). *Dette mener E-tjenesten, PST og NSM er truslene mot norsk sikkerhet*. Hentet 07 08, 2021 fra Regjeringen.no:
<https://www.regjeringen.no/no/aktuelt/dette-mener-e-tjenesten-pst-og-nsm-er-truslene-mot-norsk-sikkerhet/id2832393/>
- Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Dokument 3:7 (2020-2021)*. Oslo: Riksrevisjonen.
- Røyksund, M., & Valdal, A.-K. (2020). *Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning*. Oslo: NVE.
- Volue. (2021). *Post mortem. A review of the cyberattack on Volue*. Oslo-Trondheim: Volue.
- Volue. (2021). *Volue - who we are*. Hentet 07 22, 2021 fra volue.no:
<https://www.volue.com/>
- Wikipedia. (2021, 04 29). *Strategi*. Hentet 06 23, 2021 fra
<https://no.wikipedia.org/wiki/Strategi>



NVE

Norges vassdrags- og energidirektorat

MIDDELTHUNS GATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (47) 22 95 95 95

www.nve.no