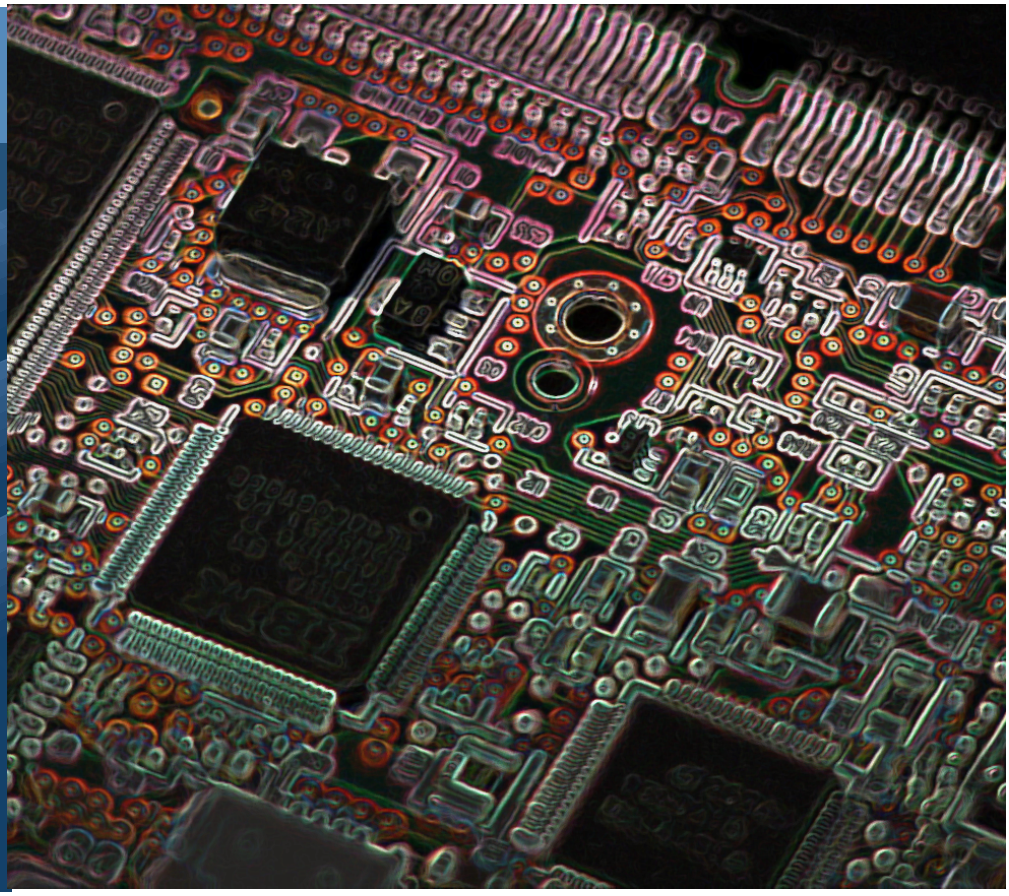
Informasjonssikkerhetstilstanden i energiforsyningen

Namrah Azam

74
2017



RAPPORT

Rapport nr 74-2017
Informasjonssikkerhetstilstanden i energiforsyningen

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør:

Forfattere: Namrah Azam

Trykk: NVEs hustrykkeri

Opplag:

Forsidefoto: Namrah Azam, NVE

ISBN 978-82-410-1627-1

ISSN 1501-2832

Sammendrag: Digitaliseringen av energiforsyningen fører til at kraftbransjen er mer utsatt for digitale angrep enn tidligere. Denne studentrapporten gir et bilde av sikkerhetshendelser som virksomhetene i kraftbransjen har opplevd de siste 12 månedene og en anbefaling til virksomhetene for hvordan de kan styrke informasjonssikkerheten. Rapporten er basert på en undersøkelse som ble sendt ut til virksomheter i kraftbransjen i juni 2017.

Emneord: Cybersikkerhet
Sikkerhetshendelser
Informasjonssikkerhet
Industrielle kontrollsystemer
IKT-sikkerhet
SCADA-systemer

Norges vassdrags- og energidirektorat
Middelthunsgate 29
Postboks 5091 Majorstua
0301 OSLO

Telefon: 22 95 95 95
Telefaks: 22 95 90 00
Internett: www.nve.no

September 2017

Innhold

Forord

Digitalisering treffer energiforsyningen gjennom digitale sensorer i infrastrukturen, skytjenester og utsetting av IT-drift og gjennom automatiske digitale strømmålere (AMS) mv. Digitaliseringen gir mulighet for å utvikle løsninger for smarte energiøkonomiske hus og for mer effektiv drift hos selskapene. Men, digitalisering og tilknytning av stadig flere komponenter til internett eksponerer også de samme komponentene for en rekke trusler og uønskede hendelser. Mange av disse har vi liten eller ingen erfaring med.

Hva er den digitale sikkerhetstilstanden i norsk energiforsyning (elkraft og varme) og hvordan vil denne utvikle seg over tid? Dette spørsmålet er grunnlaget for utformingen av FOU-prosjektet «Informasjonssikkerhetstilstanden i energiforsyningen».

NVE har fått tillatelse av Næringslivets sikkerhetsråd (NSR) til å bruke spørsmål fra Mørketallsundersøkelsen 2016. Med litt tilpasning gir dette spørreskjemaet en mulighet for kartlegging av sikkerhetstilstand, analyse og vurderinger i norsk energisektor. Bedre oversikt over uønskede hendelser og sikkerhetstilstanden vil kunne gi bidrag og innsikt til bransjens egne ROS analyser og til myndighetenes vurderinger av risiko og behov for revisjoner av regelverk. I tillegg til å gi en beskrivelse av sikkerhetstilstanden basert på statistikk, gir rapporten også noen råd om sikkerhet basert på funn i rapporten og offisielle sikkerhetsråd fra NSM og NSRs Mørketallsundersøkelse.

Rapporten er ført i pennen av student Namrah Azam sommeren 2017. Hun har hatt sommerjobb ved NVE og arbeidet i NVEs FOU-prosjekt «Informasjonssikkerhetstilstanden i energiforsyningen». Studentarbeidet er et av flere bidrag inn FOU-prosjektet. NVE vil utgi en sluttrapport for prosjektet om sikkerhetstilstanden innen årsskiftet.

.

Eldri Naadland Holo

Seksjonsjef

Sammendrag

Hastigheten og omfanget av den digitale transformasjonen påvirker flere bransjer, inkludert kraftbransjen. Den digitale agendaen drives av sammensmeltingen av flere ulike aspekter ved IT som cloud computing, maskinlæring og store data. Disse, sammen med mange andre teknologier, data og intelligens, står i sentrum av digitaliseringen. Endringen har stor innvirkning på alle segmenter i samfunnet, fra storindustri til forbruk i husholdningen. Informasjons- og kommunikasjonsteknologi gir virksomheter mulighet for mer effektiv drift, og bidrar til å spare penger, skape nye jobber, stimulere økonomisk vekst og beskytte miljøet. Bransjer og bedrifter befinner seg i en verden som er mer flyktig og mer kompleks. Dette krever større fleksibilitet, mer fart og mer digital kompetanse. Digitale teknologier spiller en stadig viktigere rolle i energiinfrastrukturen og brukes til å kontrollere energiproduksjon og distribusjon, overføre informasjon om forbruk og overvåke etterspørselen. Dette betyr imidlertid også at energisektoren er mer utsatt for cybertrusler: På grunn av stadig mer koblede infrastrukturer og industrielle kontrollsystemer, smart nett, digitale anlegg etc., øker risikoen for cyberangrep. Potensielle angrep kan skade datasystemene, som igjen kan resultere i fatale konsekvenser. Derfor er det svært viktig at energiinfrastrukturen er beskyttet mot mulige sikkerhetsbrudd og cyberangrep som kan resultere i informasjonstyveri, sikkerhetsproblemer, avbrudd og i verstefall få et utfall hvor naturen eller menneskeliv settes i fare.

Denne rapporten illustrerer et bilde over IKT-sikkerheten i den norske energiforsyningen og viser til hendelser virksomheter innenfor kraftbransjen har opplevd de 12 siste månedene. Dataene i rapporten baserer seg på en spørreundersøkelse som ble sendt ut til 350 ulike virksomheter i begynnelsen av juni 2017, hvorav 88 respondenter sendte inn sine svar. Undersøkelsen viser at bransjen er utsatt for uønskede IT-sikkerhetshendelser og cyberangrep. Nærmere 70 % av virksomhetene har hatt uønskede IT-sikkerhetshendelser. Blant alle virksomhetene som har svart på undersøkelsen, har 59% hatt hendelser som var alvorlige. Hendelsene omfatter hovedsakelig dataskadeverk, bedrageri, virus/malware infeksjon, forsøk på datainnbrudd og hacking. De fleste virksomhetene ikke rapportert alvorlige konsekvenser. Hos 21% av virksomhetene som svarte på spørsmål om den alvorligste hendelsen, har hendelsen vært alvorlig nok til å involvere selskapets ledelse. Menneskelig feil og mangel på sikkerhetsbevissthet hos de ansatte bidrar at hendelser oppstår, men 40% av virksomhetene som hadde alvorlige hendelser, oppgir at det ikke er blitt gjort noen endringer innad organisasjonen i etterkant av hendelsen. Anbefalingene i denne rapporten er gitt på grunnlag av hvordan sikkerheten bør styrkes i forhold til dataen som er blitt samlet inn:

- Styringssystem eller rammeverk for informasjonssikkerheten
- Styrke sikkerhetskultur gjennom opplæring og sikkerhetsrutiner
- Inkludere sikkerhet og beredskap i leverandørhåndtering

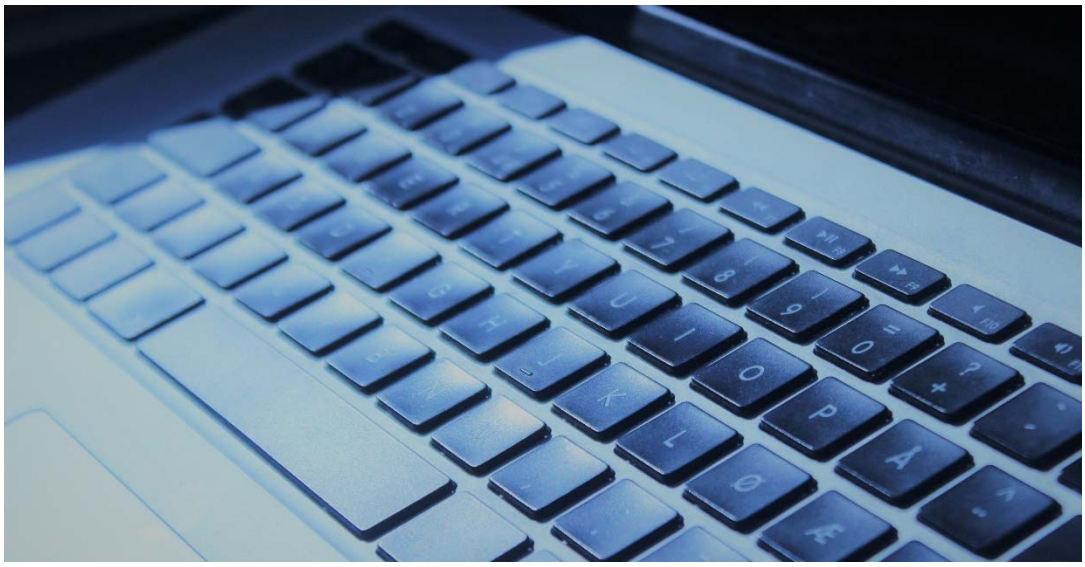
Innledning

Digitalisering av energisektoren endrer risikobildet. En digitalisert energisektor kan angripes gjennom internett av anonyme aktører via cyberangrep (datainnbrudd og sabotasje av digitale systemer). I tillegg kan feil i programvare, hardvare og konfigurasjon forplante seg i sammenkoplede digitale systemer og gi konsekvenser for virksomhetenes drift. Næringslivets sikkerhetsråd (NSR) har over flere år samlet inn primærdata om uønskede IKT-hendelser gjennom Mørketallsundersøkelser om datakriminalitet. I følge NSRs Mørketallsundersøkelse 2016 [1], har over en fjerdedel av norske virksomheter opplevd uønskede IT-sikkerhetshendelser. Trenden er at antall cyberangrep øker og blir mer sofistikerte. Angrepene innebærer risiko for at viktig informasjon blir stjålet eller lekket, store økonomiske tap, skade på utstyr og i verstefall at liv går tapt. Både Nasjonal sikkerhetsmyndighet (NSM) og Politiets sikkerhetstjeneste (PST) frykter sabotasje mot Norge; tele, kraftforsyning og annen kritisk infrastruktur er utsatt. NSM skriver i sin årlige trusselvurdering 2017 at de har sett en jevn økning av antall målrettede cyberangrep mot norske interesser, både offentlige og private. Disse angrepene utgjør en trussel mot norske verdier. NSM ser tegn på økt bevissthet om tekniske sårbarheter i mange virksomheter, men gjennomføring av sårbarhetsreduserende tiltak skjer ikke med samme takt som utviklingen i trussel bildet [2].

Denne rapporten er en delrapport i et internt forskningsprosjekt ved NVE der NVE har som målsetting å beskrive sikkerhetstilstanden i energisektoren ved hjelp av statistikk. Prosjektet skal utvikle et verktøy (spørreskjema og analytisk fremgangsmåte) for å kunne analysere sikkerhetstilstanden og sammenligne bransjens sikkerhetstilstand mot norsk næringsliv generelt slik det framstilles i Næringslivets sikkerhetsråds Mørketallsundersøkelser. Prosjektet vil gi NVE potensiale for å over tid å kunne følge med på utviklingen i sikkerhetstilstanden i energisektoren og gi bransjen en bedre forståelse for hvilke uønskede IKT-hendelser som rammer.

Vi vet at menneskelig oppdagelsesevne er en viktig bidragsyter for å oppdage uønskede hendelser. Vi vet også fra tidligere Mørketallsundersøkelser at mørketallene er store og at mange hendelser ikke blir rapportert til myndigheter eller til politiet. Gjennom innhenting av primærdata og påfølgende statistisk analyse kan myndigheten og bransjen få et komplementert bilde til sektorCERTens (KraftCERTs) hendelsesstatistikk. Det vil kunne gi grunnlag for bedre og mer relevante risikoanalyser.

I denne rapporten stiller vi følgende spørsmål: Hvordan er egentlig sikkerheten i den norske kraftforsyningen, hvor utsatt er kraftbransjen og hva ser bransjen selv?



INDUSTRI 4.0

De tidligere industrielle revolusjonene befridde menneskeheten fra dyremakt, gjorde masseproduksjon mulig og brakte digitale evner til milliarder mennesker. Industry 4.0 er som teknologiskifte imidlertid fundamentalt forskjellig. Det er preget av en rekke nye teknologier som fusjonerer de fysiske, digitale og biologiske verdener. Industry 4.0 påvirker alle disipliner; Økonomien, næringslivet og den utfordrer ideene om hva det betyr å være menneske. En digitalisert verden har potensiale til å koble milliarder mennesker til digitale nettverk, dramatisk forbedre effektiviteten til organisasjoner og til og med administrere eiendeler som kan bidra til å regenerere det naturlige miljøet, potensielt endre skadene fra tidligere industrielle revolusjoner. Det er imidlertid alvorlige aspekter ved dette teknologiskiftet [17]. Digitaliseringen av samfunnet skaper nye verdier og utviklingsmuligheter hele tiden, men utvider også sårbarheten [2]. Organisasjoner vil kanskje ikke kunne tilpasse seg, regjeringer kan mislykkes i å ansette og regulere ny teknologi for å gjøre nytte av fordelene, ulikhet kan vokse og samfunn bli fragmentert. Endringene kan skape nye sikkerhetsproblemer som utnyttes av ondsinnede aktører.

Om Undersøkelsen

1.1 Metode

Rapporten dokumenterer en spørreundersøkelse om sikkerhetshendelser i kraftforsyningen. Undersøkelsen omfatter store, mellomstore og små virksomheter i kraftbransjen som driver med produksjon av elektrisitet og varme, overføring av energi (nettselskap), formidling og salg. Spørreskjemaet ble sendt ut til 350 virksomheter den 6.juni og undersøkelsen ble lukket 27.juni. Spørsmålene omhandler situasjonen i virksomhetene de siste 12 månedene. Totalt svarte 88 virksomheter på undersøkelsen. Dette gir en svarprosent på 24. Spørreskjemaet og rapporten er bygget etter samme mal som NSRs Mørketallsundersøkelse 2016 [1], men er tilpasset kraftforsyningen av en egen arbeidsgruppe med representanter fra bransjen.

1.2 Hvem har svart?

Rundt 60% av respondentene har en stilling som IKT-sikkerhetskoordinator eller liknende, cirka 20% er daglig ledere, mens 23% har en annen faglig bakgrunn og stilling i virksomheten**.**

Figur 1: Hvilken stilling har du? (n er antall respondenter)

1.2.1 Virksomhetene

Undersøkelsen omfatter både store og små virksomheter, med et gjennomsnitt på 29 ansatte per virksomhet. Halvparten av svarene er fra mellomstore bedrifter med 20 til 99 ansatte. Av de større virksomhetene med flere enn 100 ansatte er det 18 som har svart på undersøkelsen.

De fleste respondentene jobber i følgende selskap i bransjen:

- Konsern (32%)
  - *Sammenslutning av flere selskaper*
- Nettselskap (25%)
  - *Ansvarlig for strømnettet, og for at strømmen blir levert fra kraftprodusent til forbrukere*
- Kraftprodusent (24%)
  - *Eier av kraftverk og ansvarlig for produksjon av energi*
- Fjernvarme (3%)
  - *Ansvarlig for produksjon og distribusjon av energi i form av varme (varmtvann)*
- Strømleverandør (3%)
  - *Salgsorganisasjon med ansvar for å formidle og levere strøm*

1.3 Organisering av drift

Spørsmålet om organisering av drift er todelt. Det er blitt spurt om organisering av administrativ IT-drift og driftskontrollfunksjoner innad virksomheten, om driften er satt ut eller organisert internt. Virksomhetene som har satt ut driften, har også fått spørsmål om de benytter seg av outsourcing av tjenester i utlandet.

1.3.1 Organisering av IT-driften

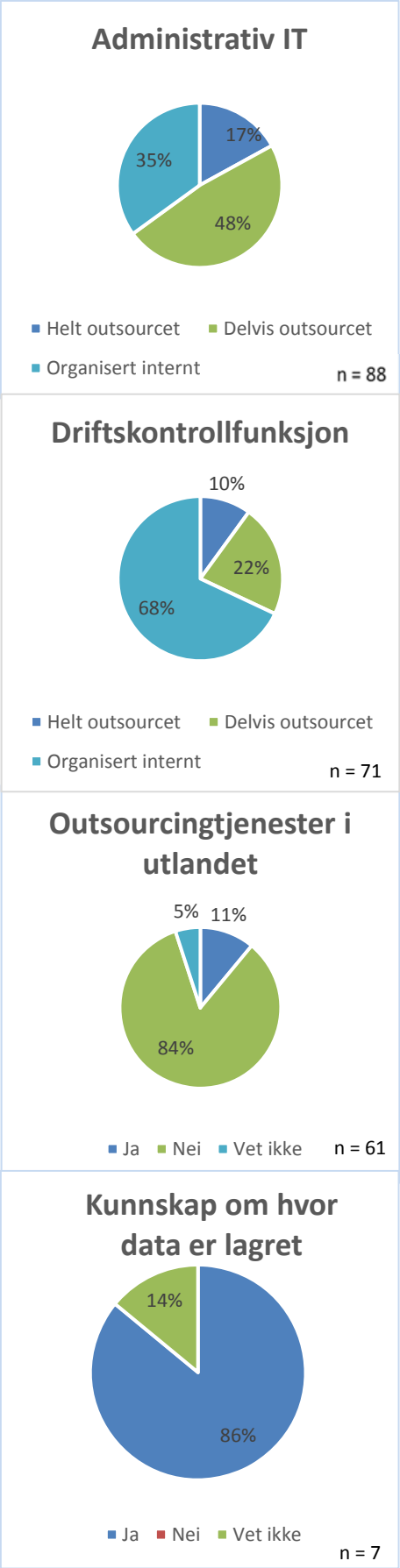
Halvparten av virksomhetene som har svart på undersøkelsen, har delvis outsourcet drift av administrativ IT, 35% har satt ut driften helt, mens 17% har valgt en intern løsning.

Konsern, nettselskaper og kraftprodusenter har fått spørsmål om hvordan de organiserer driftskontrollfunksjon (SCADA, lokalkontollsystem) i virksomheten. Nærmere 70% har svart at de velger å organisere driftskontrollfunksjoner internt. Av de større virksomhetene (med flere enn 100 ansatte) er det ingen som har satt ut driften. De drifter alt internt. For virksomhetene med mindre enn 99 ansatte derimot, viser svarene at de enten setter ut driften delvis eller helt – dette gjelder både administrativ IT-drift og driftskontrollfunksjon.

1.3.2 Tjenesteutsetting i utlandet

Kun 5% av de som har valgt å sette ut driften, sier at de benytter seg av outsourcingtjenester i utlandet. Av de spurte, svarer 11% at de har satt ut driften, mens 5% svarer at de ikke vet om driften er outsourcet til utlandet eller ikke.

Virksomhetene som har satt ut IT-driften til utlandet, har fått spørsmål om de vet hvor data er lagret og hvor de blir behandlet. Her svarer 86% at de har kunnskap om dette, mens 14% svarer at de ikke vet. Ettersom kun 7 har svart på dette spørsmålet, har man lite grunnlag å gå på for å trekke noen konklusjoner for hvorfor noen ikke vet hvor data er lagret. For IKT-sikkerhetskoordinatorer er det helt essensielt å vite hvor data er lagret. Det at noen her har svart at de ikke vet hvor dataen er lagret, er negativt da dette kan bli et problem for virksomheten hvis de utsettes for et angrep.

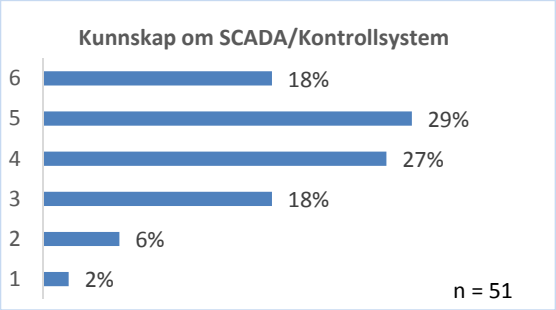


Figur 2: Outsourcing

2 Kunnskap om egne systemer og leverandørhåndtering

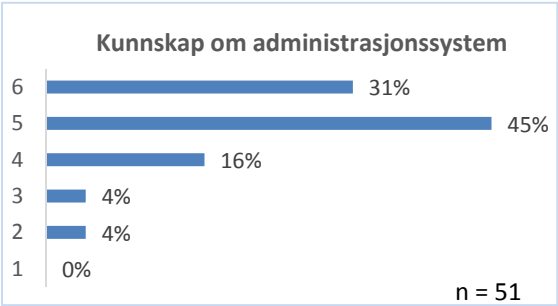
2.1 Kontroll og administrasjonssystemer

IKT-sikkerhetskoordinatorer har blitt bedt om å redegjøre for deres kunnskapsnivå innen administrasjonssystemer og kontrollsystemer. For 74% viser svarene at deres kunnskapsnivå om SCADA -kontrollsystem (*Figur 3*) ligger over 4. Gjennomsnittet er på 4.3.



Figur 3: Hvor stor er din kunnskap om systemene som benyttes i din virksomhet? (1 er dårlig og 6 er meget god)

Hele 92% av IKT-sikkerhetskoordinatorene svarer at deres kunnskap om administrasjonssystemene (*Figur 4*) ligger over nivå 4. Gjennomsnittet i dette tilfellet ligger på 5.



Figur 4: Hvor stor er din kunnskap om systemene som benyttes i din virksomhet? (1 er dårlig og 6 er meget god)

I undersøkelsen har størrelse på bedrift ikke hatt noe å si for respondentens kunnskapsnivå når det gjelder administrasjonssystemene og/eller kontrollsystemene.

KUNNSKAP OM SIKKERHETSTILSTANDEN

påvirkes av hvilken innsats vi legger i å sikre verdiene våre. Kunnskap om egne verdier og sårbarheter, og forståelse for ulike trussel aktører, er avgjørende for egen risikoerkjennelse. Slik kunnskap er også viktig for å fatte gode beslutninger og hvilke sikringstiltak som må implementeres eller hvilken risiko en virksomhet er villig til å akseptere [2]

INDUSTRIELLE KONTROLLSYSTEMER

(Industrial Control System (ICS)): flere typer kontrollsystemer og tilhørende instrumentering som brukes i industriell produksjonsteknologi, inkluderer enheter, systemer, nettverk og kontroller som brukes til å drive og automatisere industrielle prosesser. Dette kan være SCADA-systemer (*Supervisor Control And Data Acquisition*), distribuerte kontroll systemer (*Distributed Control Systems(DCS)*), overvåkningssystemer og programmerbare logikkontroller *(Programmable Logic Controls(PLC)).* Industrielle kontrollsystemer finnes i industrisektorer og brukes til kontroll av kritisk infrastruktur, i bransjer som trafikksignaler og transport, strømforsyninger og vannverk. [14]

ADMINISTRASJONSSYSTEM

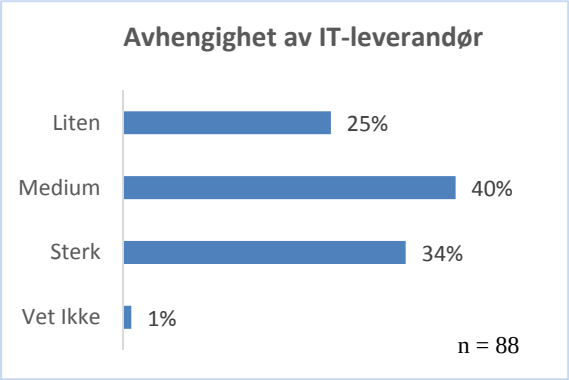
Begrepet administrasjonssystem (administrativsystem), gjelder systemer som håndterer økonomi, IT-drift, logistikk, vedlikehold, kunde og personal-støtte ol.

2.2 Leverandøravhengighet

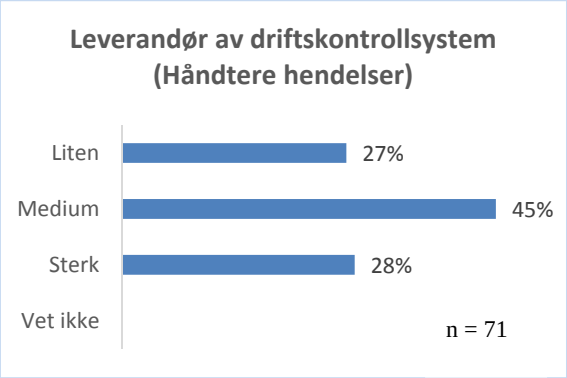
Tjenesteutsetting av IT og bruk av skytjenester treffer mange virksomheter i energisektoren. Trusselbildet og leverandørmarkedet er i stadig endring. I undersøkelsen har virksomhetene blitt spurt om hvor avhengige de er av sin IT-leverandør for å håndtere hendelser.

Av 88 virksomheter, svarer 40% at de er middels avhengige av IT-leverandøren for å håndtere en hendelse som oppstår i deres systemer (både SCADA og administrasjonssystemer), 34% sier de er sterkt avhengige av at leverandøren skal håndtere dette, mens 25% oppgir at de i liten grad er avhengige av leverandøren (*Figur 5*).

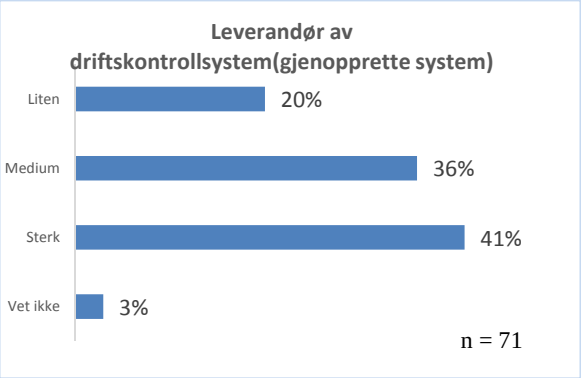
Konsern, nettselskapene og kraftprodusentene har i tillegg til det ovennevnte spørsmålet, fått to spørsmål som omhandler avhengighet av leverandør når det gjelder hendelser i driftskontrollsystemene. Når det kommer til håndtering av hendelser i driftskontrollsystemene, svarer 27% av virksomhetene at de er lite avhengige av at IT-leverandøren skal håndtere dette, 40% er medium avhengige og 34% oppgir at de er sterkt avhengige (*Figur 6*). På spørsmål om å gjenopprette driftskontrollsystemet som følge av en hendelse, svarer 41% av virksomhetene at de er sterkt avhengige av sin IT leverandør, for å gjenopprette systemet (*Figur 7*).



Figur 5: Hvor avhengig er du av din IT-leverandør for å håndtere hendelser?



Figur 6: Hvor avhengig er du av din leverandør av driftskontrollsystem for å håndtere hendelser?



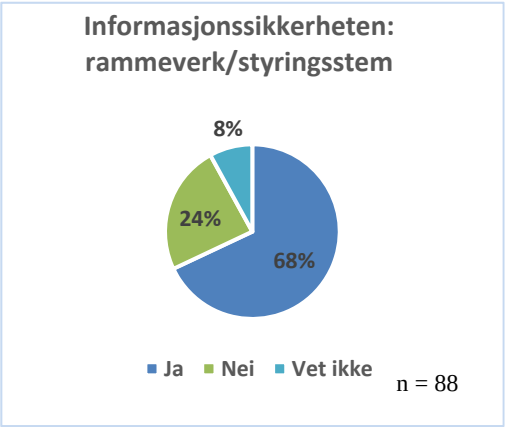
Figur 7: Hvor avhengig er du av din leverandør av driftskontrollsystem for å restore/gjenopprette system?

3 Rammeverk for informasjonssikkerhet

Digitaliseringen fører til at gamle løsninger endres, og nye arbeidsmetoder og rutiner innføres. I dag kommuniserer vi og omgås på helt andre måter enn det vi gjorde noen tiår tilbake. I en slik omskiftende verden, hvor det meste er teknologidrevet, er det viktig å ha kontroll over risikoene som finnes og iverksette hensiktsmessige tiltak for å fjerne dem eller redusere disse til et akseptabelt nivå. Statistikken fra både denne undersøkelsen og NSRs Mørketallsundersøkelse 2016 [1] viser at mange norske virksomheter ikke har noen form for rammeverk og/eller et styringssystem. Dette kan resultere i at virksomhetene mangler oversikt og kontroll, og ikke vet hvor sårbar deres virksomhet egentlig er.

Ifølge denne undersøkelsen svarer 24% av virksomhetene at de ikke har et rammeverk eller styringssystem for informasjonssikkerheten i deres virksomhet, 68% svarer at de har, mens 8% svarer at de ikke vet. Tallene fra Mørketallsundersøkelsen 2016, viser til sammenligning at 443 virksomheter av 1500, dvs. 30% av norske virksomheter, ikke har et rammeverk eller styringssystem.

Både NSRs Mørketallsundersøkelse fra 2016 [1], og denne undersøkelsen, viser at antallet virksomheter som svarer at de ikke har et rammeverk for styring av informasjonssikkerhet, er betydelig høyere for mindre bedrifter med færre ansatte. Ut i fra svarene man har fått gjennom begge undersøkelsene, ser man behovet for økt oppfølging av at norske virksomheter etablerer rammeverk for informasjonssikkerhet. Det er viktig at virksomhetene forstår nytten av å ha et rammeverk for informasjonssikkerhet.



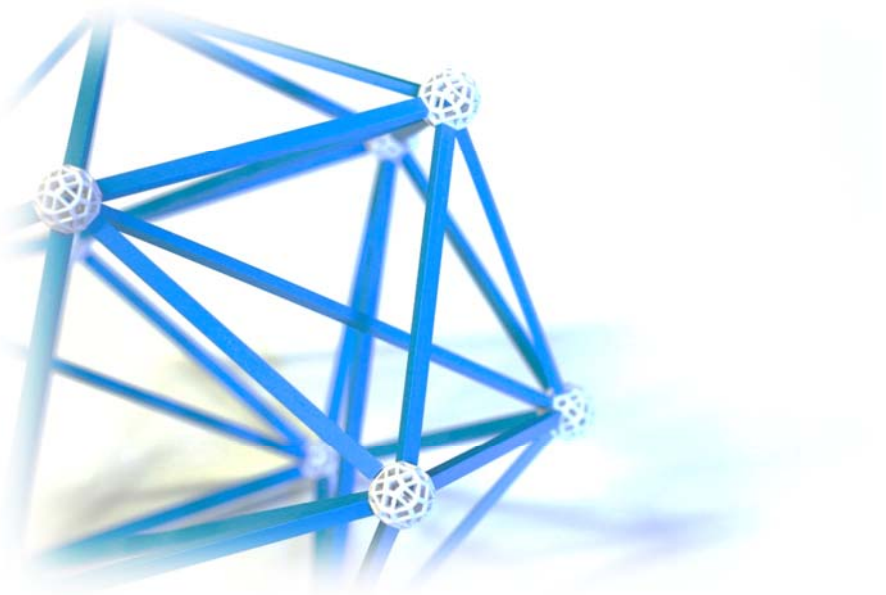
Figur 6: Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerheten?

4 Cyberangrep og sikkerhetshendelser

Cyberangrep mot Norge øker sterkt, i fjor avslørte norske myndigheter mer enn 22 000 tilfeller av dataangrep mot norske bedrifter og offentlige stater [3]. Undersøkelser viser at det ligger store mørketall bak dette. Mange av hendelsene som virksomhetene blir utsatt for, blir dessverre ikke rapportert. Risikoen for at kritiske samfunnsfunksjoner i landet blir rammet av spionasje, sabotasje, terror og andre alvorlige handlinger øker jo mer samfunnet digitaliseres.

I følge PSTs åpne trusselvurdering 2017, vil Norge og norske interesser i 2017 utsettes for fremmed etterretningsvirksomhet som kan ha et stort skadepotensial. Det er hovedsakelig innen tre hovedområder PST mener det vil gjennomføres etterretningsoperasjoner: forsvars- og beredskapssektoren, politiske beslutningsprosesser og kritisk infrastruktur. PST anser at det i tillegg til dette er høyst sannsynlig med nye etterretningsoperasjoner mot norske teknologivirksomheter. Datanettverksoperasjoner vil være en integrert del av de ulike etteretningsoperasjonene mot mål i Norge [4].

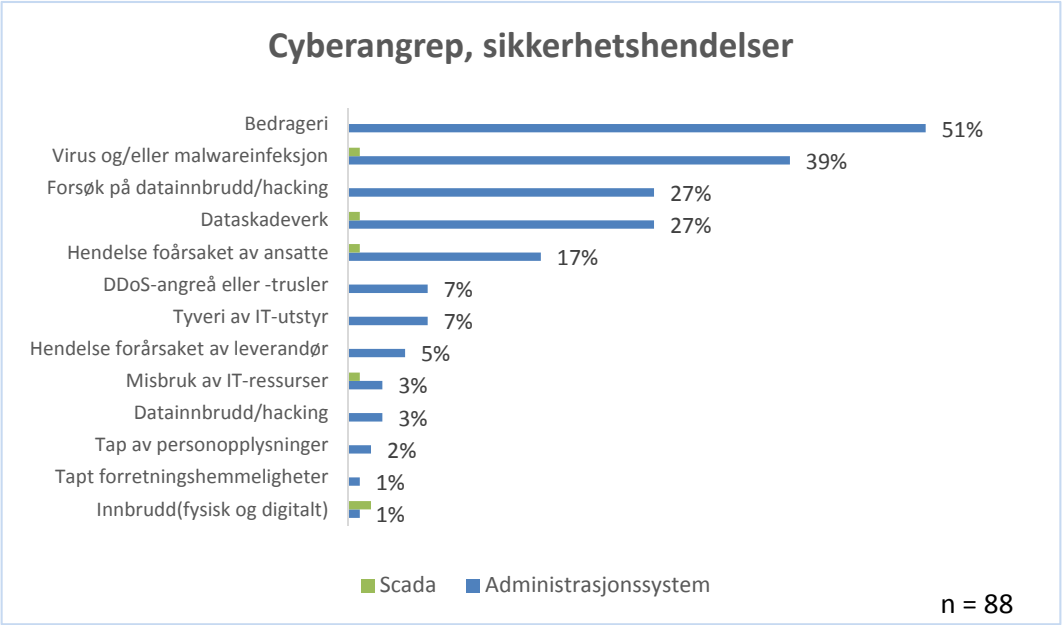
Fremmede makter kan gjennom nettverksbaserte etterretningsoperasjoner i fredstid erverve inngående kjennskap til kritisk infrastruktur. Denne kunnskapen kan i krisetid benyttes til å gjennomføre sabotasjeaksjoner. Flere stater utvikler skadevare som vil kunne brukes til å sabotere eller forstyrre kritiske samfunnsfunksjoner. Denne delen av rapporten omhandler sikkerhetshendelser virksomhetene i kraftbransjen har vært utsatt for. Hvilke hendelser har så virksomhetene i kraftbransjen selv oppdaget og opplevd?



I undersøkelsen kommer det fram at 51% av virksomhetene har opplevd bedrageri rettet mot sine administrasjonssystemer de 12 siste månedene. De fleste skriver at dette hovedsakelig dreier seg om svindelforsøk via e-post og brev, men at forsøkene er blitt oppdaget og stoppet. Ifølge NSRs Mørketallsundersøkelse 2016 [1], rammet virus og skadeverk minst en av fem virksomheter i 2015, dette var også den hendelsen de fleste var utsatt for. Denne undersøkelsen, viser at bedrageri er den type hendelse som virksomhetene er mest utsatt for. Av de 88 virksomhetene som har svart på denne undersøkelsen, har 39% opplevd å få virus og malware infisert i systemene sine. Bedriftene har blitt forsøkt hacket (27%), og opplevd skadeverk (27%) i form av kryptolocker eller ransomware o.l. (uautorisert endring/sletting av data, målrettede aksjoner som har til hensikt å redusere tilgjengeligheten).

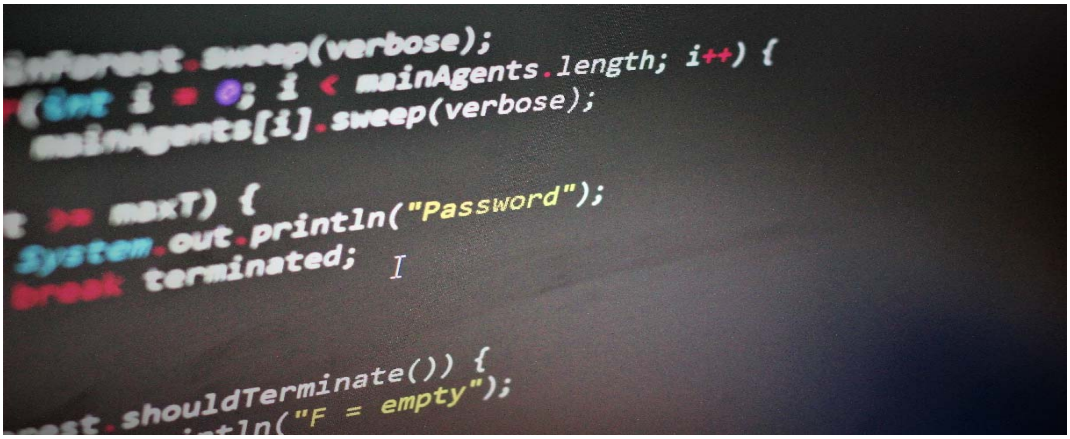
Dersom en ser på trusselen fra innsiden av virksomhetene, viser NSR sin Mørketallsundersøkelse fra 2016 [1] at sikkerhetshendelser forårsaket av bedriftens ansatte, ligger på topp tre. Dette er en type hendelse som også kommer fram i denne undersøkelsen: 17% av virksomhetene oppgir at dette er noe de har opplevd i løpet av de siste 12 månedene. Av de 88 virksomhetene svarer videre 7% at de har vært utsatt for tjenestenektangrep (DDOS-angrep), men angrepet har ikke fått noen alvorlige følger, da dette ikke kommer fram i spørsmålet om alvorlige hendelser. Tjenestenektangrep er som oftest små, og korte, men veldig effektive. Det skal som regel ikke så mye til for at et slikt angrep kan få alvorlige konsekvenser. Denne type angrep kan brukes for å tilrettelegge for et annet større angrep senere. Hos 5% av virksomhetene har sikkerhetshendelsen vært forårsaket av leverandøren. En statistisk test i statistikkprogramvaren PSPP viser at sikkerhetshendelser rammer tilfeldig, uavhengig av om en drifter selv eller setter ut tjenesten.

Svarene fra undersøkelsen viser videre at de fleste angrepene er rettet mot administrasjonssystemene, men SCADA/kontrollsystemene har i noen virksomheter også vært utsatt for angrep. Gruppen med 1 til 19 ansatte har hatt flere sikkerhetshendelser mot SCADA-systemene sammenlignet med de større virksomhetene. SCADA-systemene til denne gruppen har vært utsatt for dataskadeverk, IT ressursene har vært misbrukt, systemene har blitt infisert med virus og malware og det har vært innbrudd i organisasjonens systemer. I de større virksomhetene, altså gruppen med 20 til 99 ansatte og gruppen med flere 100 ansatte, har færre vært utsatt for hendelser forårsaket av bedriftens ansatte og hatt innbrudd i bedriftens SCADA-systemer. Driftskontrollsystemer har omfattende krav til sikring. Hvis driftskontrollsystemet utsettes for et cyberangrep, for eksempel DDoS eller krypteringsskadevare, så kan det få fatale konsekvenser. Dette skjedde i Ukraina i desember 2015, hvor angrepet startet med at hackerne gjorde et innbrudd i SCADA-systemene. Datamaskiner og servere ble deretter infisert av virus, som gjorde selskapenes styringssystemer ute av stand til å styre strømnettet [5]. Slike cyberangrep kan mørklegge byer, og truer i verste fall helse, miljø og sikkerhet. Derfor må styringssystemene sikres godt.



Figur 7: Hvilke informasjonssikkerhetshendelser har virksomheten vært utsatt for de siste 12 månedene?
**** Flere svar mulig***

Virksomhetene har fått spørsmål om hvor mange av informasjonssikkerhetshendelsene som påvirket organisasjonen negativt (tapt produksjon, økonomiske tap, omdømmetap, svekket markedsposisjon) de 12 siste månedene. Totalt har 13% av de 88 respondentene svart at de har hatt hendelser som har fått negative konsekvenser som tapt produksjon, økonomiske tap, omdømmetap eller svekket markedsposisjon. Det er rapportert 77 hendelser med de ovennevnte konsekvensene fordelt på 13% virksomheter. Disse virksomhetene har videre fått spørsmål om hvor mange av hendelsene som gjaldt driftskontrollsystemene. For 3 av virksomhetene har dette dreid seg driftskontrollsystemene.



STUXNET - ET ANGREP PÅ KONTROLLSYSTEMER

De siste årene har industrielle systemer tatt i bruk mer standard teknologi. Som følge av anvendelsen av teknologien, blir kritiske systemer mer utsatt for fysiske og digitale angrep. Den kjente skadelige datamaskinormen Stuxnet, som direkte var rettet mot kontrollsystemer, beviste at det var mulig å angripe kontrollsystemer og påføre fysisk ødeleggelse. Stuxnet er kjent som det første cyberfysiske våpenet, der programvaren bevisst ble brukt for å skade fysiske komponenter. Dette har bidratt til økt oppmerksomhet rundt dette temaet. Skadevaren var hovedsakelig utviklet for å sabotere atomanrikningsanlegg i byen Natanz i Iran. I 2007 ble Stuxnet infisert i et prosesskontrollsystem i atomanlegget for å sabotere deres anlegg for anrikning av uran og dermed stoppe det iranske atomprogrammet. Det var hovedsakelig to angrep atomanlegget ble utsatt for: Målet med det første angrepet var å øke overtrykket i sentrifugene, dette var en skjult operasjon, hvor angriperne holdt lav profil. Det andre angrepet hadde som mål å øke hastigheten på sentrifugemotorene for å ødelegge dem. Skadevaren ble infisert i anlegget, og la seg som et *«man –in-the-middle»* - angrep. Dermed overstyrte viruset operatørene. Stuxnet ødela omtrent 1000 av 6000 sentrifuger på atomanlegget i Natanz [11].

Man in the middle (MITM): *Et angrep hvor kommunikasjon mellom to parter passerer gjennom en uønsket tredjepart og vedkommende er i stand til å overvåke, etterligne, endre eller holde tilbake innholdet på kommunikasjonen.* [16]

UKRAINA 2015

Den 23.desember 2015, rapporterer et elektrisitetsdistribusjonsfirma (Kyivoblenergo) serviceavbrudd til kundene. Det blir kjent at avbruddene skyldes en tredjepart og ulovlig innbrudd i selskapets datamaskiner og kontrollsystemer (SCADA). Senere erklæringer indikerte at cyberangrepet påvirket ytterligere deler av distribusjonsnettet og tvang operatørene til å bytte til manuell drift. Cyberangrepene utført mot selskapene var godt planlagt og koordinert. Angrepene bestod av flere elementer, som innebar aktivering og støttet angrepssegmenter. Trusselaktørene var fjerntilkoblet og samhandlet. I forkant av angrepet sendte angriperne en målrettet e-post til bestemte personer i organisasjonen. E-posten syntes tilsynelatende å være fra en klarert kilde, men inneholdt ondsinnet vedlegg (*spydfiske, eng: spearphishing*). En analyse av angrepet viser at det skal være brukt BlackEnergy3 for å etablere fotfeste og bruke tastetrykkloggere for å utføre en legitimasjonstest. Ved å gjøre de ovennevnte stegene i forkant av angrepet, oppnådde angriperne den nødvendige bevegelsesfriheten og kunne dermed tukle med IT-infrastrukturen. Etter dette begynte de å utnytte den nødvendige informasjonen og oppdage vertsenhetene. Slik kunne de utarbeide et angrepskonsept for å kapre SCADA systemet, og deretter manipulere brytere for å forårsake strømbrudd [5].

Spydfiske: *En type spoofing-angrep hvor angriperen sender en forfalsket epost med ondsinnede lenker eller vedlegg til en bestemt organisasjon eller enkeltperson. Ved hjelp av eposten søker gjerningsmannen uautorisert tilgang til sensitiv informasjon. Ettersom angrepet er målrettet med en spesifikk hensikt, blir spydfiske ikke initiert av tilfeldige hackere, men heller utført av en person for økonomisk gevinst, handelshemmeligheter eller militær informasjon.*

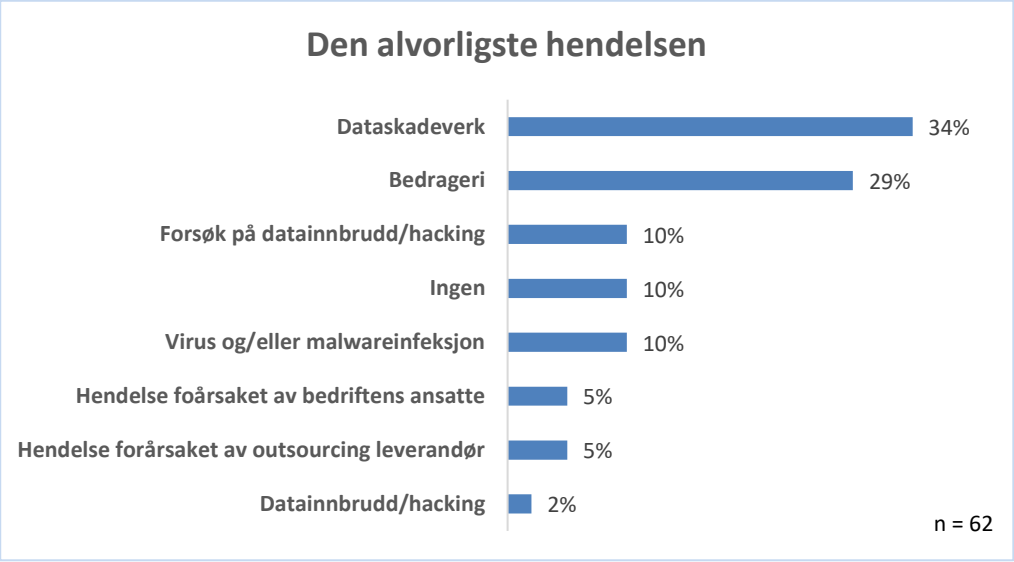
BlackEnergy3(BE3): *En trojansk hest (ondsinnet dataprogram som brukes til å hacke seg inn i en datamaskin) utviklet for å få i gang et tjenestenektangrep (DDoS), laste ned egendefinert spam og bankinformasjon-tyveri plugins. BE var kjent for å ha blitt brukt til å levere KillDisk, en funksjon som kunne gjøre systemer ubrukelige og som kunne utrydde kritiske komponenter på et infisert system. Det ble rapportert å ha bemerkelsesverdige funksjoner som kunne sette industrielle kontrollsystemer i fare.* [15]

5 Den alvorligste hendelsen

Rapporten er videre basert på svar fra 62 virksomheter som har hatt uønskede IT-hendelser, og omhandler den alvorligste hendelsen virksomheten har opplevd. Respondentene er blitt bedt om å svare på hva konsekvensene ble som følge av den alvorligste hendelsen og hva som er gjort av endringer innad virksomheten i etterkant.

5.1 Den mest alvorlige hendelsen

Dataskadeverk (kryprolocker/ransomware, i betydning uautorisert sletting/endring av data, målrettede aksjoner som har til hensikt å redusere tilgjengeligheten) oppgis som den mest alvorligste hendelsen for 34% av de 62 virksomhetene (*Figur 8*). For 29% av virksomhetene var bedrageri den mest alvorlige hendelsen, dette i form av fakturasvindel, svindel-epost eller andre former for manipulering. Forsøk på datainnbrudd/hacking har for 10% av bedriftene vært den alvorligste hendelsen. Av virksomhetene oppgir 1 av 10 at de ikke har hatt noen alvorlige sikkerhetshendelser de 12 siste månedene. Av hendelsene som er rapportert i undersøkelsen, har 52 virksomheter hatt hendelser som er alvorlige.



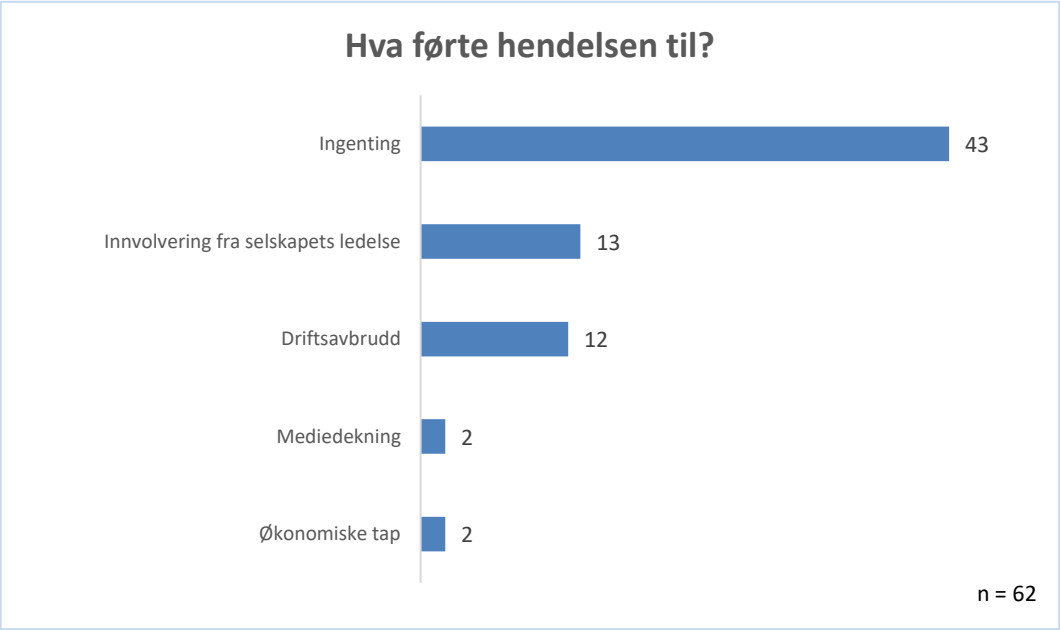
Figur 8: Hva var den mest alvorlige informasjonssikkerhetshendelsen de 12 siste månedene?
****Flere svar mulig***

5.1.1 Hva førte hendelsen til?

I følge undersøkelsen fikk ikke hendelsen noen konsekvenser for 69% av virksomhetene som svarte på dette spørsmålet (n=62), men for 21% av virksomhetene ble selskapets ledelse involvert og 19% opplevde driftsavbrudd. Til tross for at virksomheten har vært utsatt for hendelser, har ingen av virksomhetene svart at hendelsen har hatt konsekvenser hvor kunden har blitt påvirket i form av kortvarige og langvarige avbrudd (KILE) eller at virksomheten ikke fikk levert energi til kunden (ILE). Kun 2% opplevede økonomiske tap. For 2% av virksomhetene førte hendelsen til mediedekning.

Ikke levert energi (ILE) *Beregnet mengde energi som ville ha blitt levert til sluttbruker dersom svikt i leveringen ikke hadde inntruffet* [12]

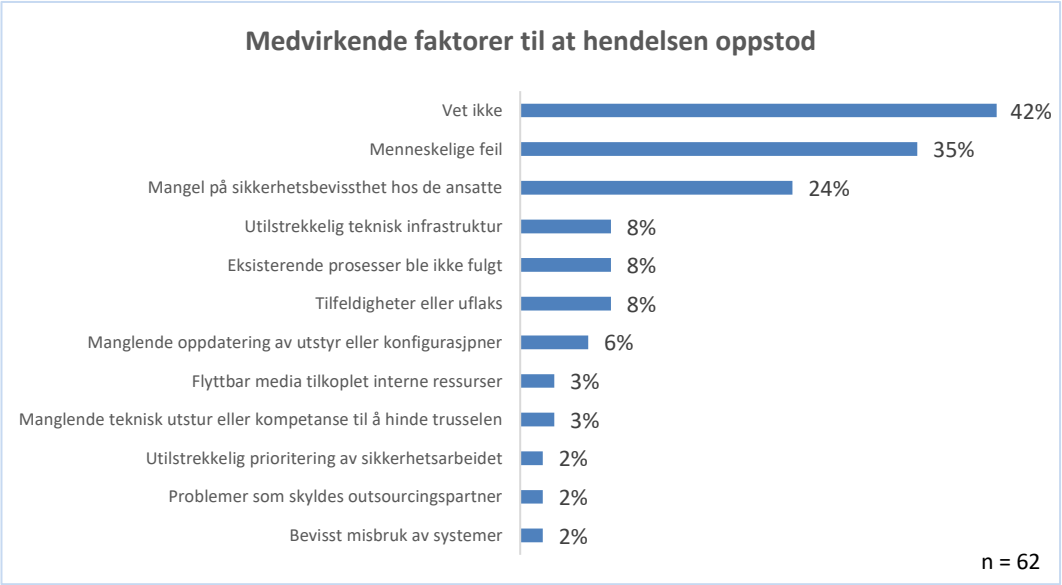
Kvalitetsjusterte inntektsrammer ved ikke levert energi (KILE): *Omfatter kortvarige (< 3min) og langvarige (>3min) avbrudd, som skyldes planlagte utkoplinger og driftsforstyrrelser i elektriske anlegg* [13]



Figur 9: Førte hendelsen til noe av det følgende?
**** Flere svar mulig***

5.1.2 Bakgrunnen for at hendelsen oppstod

De fleste virksomhetene visste ikke hva som førte til at hendelsen oppstod, 42 % virksomheter svarer at de ikke vet grunnen (*Figur 10*). Av totalt 17 virksomheter i gruppen 1-19 ansatte har 75% svart at de ikke vet hvorfor hendelsen oppstod, i gruppen virksomheter med 20-99 ansatte svarte 37% vet ikke, mens i gruppen med flere enn 100 ansatte er det kun 8% som har svart at de ikke vet. I denne undersøkelsen kommer det fram at den minste gruppen virksomheter med 1-19 ansatte ser ut til å ha flere vet-ikke-svar sammenlignet med virksomheter med flere ansatte. Undersøkelsen viser videre at medarbeidere i 35% av tilfellene gjorde en feil som bidro til at sikkerhetshendelsene oppstod, og 24% av virksomhetene svarer at det var mangel på sikkerhetsbevissthet hos de ansatte som var skyld i at hendelsen oppstod. Undersøkelsen viser videre, at også manglende investering og prioritering av sikkerhetsarbeid ligger bak en andel av hendelsene: utilstrekkelig teknisk infrastruktur (8%), eksisterende prosesser ble ikke fulgt (8%), manglende oppdatering av utstyr eller konfigurasjoner (6%). Dette forekommer også i Mørketallsundersøkelsen 2016 [1].



Figur 10: Var noen av følgende faktorer medvirkende til at hendelsen oppstod?
** Flere svar mulig*

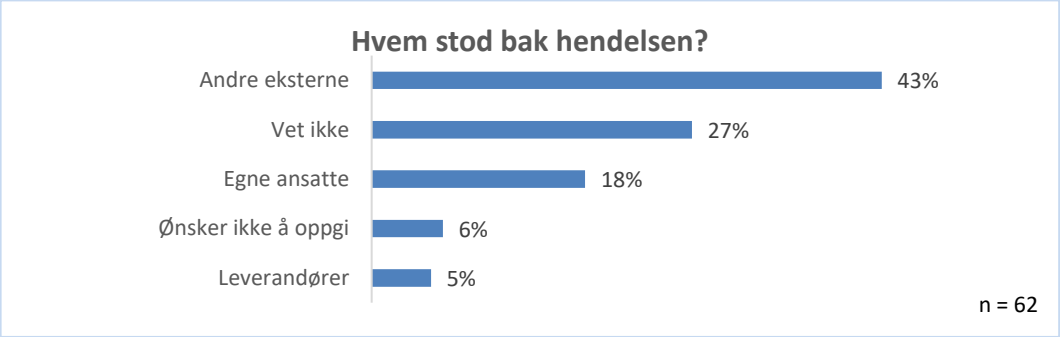
5.1.3 Hvordan ble hendelsen oppdaget?

Hendelsen ble ifølge undersøkelsen for 40% av virksomhetene oppdaget ved rutinemessig sikkerhetsmonitorering. Mørketallsundersøkelsen 2016, gjennomført av NSR, viser at 46% av de uønskede IT-hendelsene ble oppdaget ved en tilfeldighet og 34% av dem som følge av negativ effekt på virksomhetens drift. Det har over tid blitt stilt strenge krav til sikkerheten i systemene som blir brukt i kraftbransjen sammenlignet med virksomheter i enkelte andre bransjer. Dette kan være en grunn til at feil og hendelser i kraftsektoren ser ut til å bli oppdaget i en større grad gjennom rutinemessig sikkerhetsmonitorering sammenlignet med norsk næringsliv generelt. I tillegg til dette kan det skyldes gode overvåkningssystemer for å oppdage hendelser (IDS). For 18% av virksomhetene var det negativ effekt på drift som gjorde at hendelsen ble oppdaget, mens 16% svarer at de ikke vet hvordan hendelsen ble oppdaget.

Figur 10: Var noen av følgende faktorer medvirkende til at hendelsen oppsto?
**** Flere svar mulig***

5.1.4 Hvem stod bak hendelsen?

Ut i fra statistikken fra undersøkelsen ser man at de fleste hendelsene er forårsaket av eksterne aktører, 43% virksomheter svarer at det er noen utenfor deres virksomhet som stod bak sikkerhetshendelsen. Hele 27% svarer at de ikke vet hvem som stod bak hendelsen, mens hos 18% av virksomhetene oppgis det at egne ansatte stod bak hendelsen. Undersøkelsen gir ikke svar på om dette er en handling utført med hensikt eller om den skyldes tilfeldig feil, men noen svar i undersøkelsen indikerer at prosesser og styringssystem er mangelfulle hos noen virksomheter (*figur 10, figur 6*).



Figur 11: Hvem stod bak hendelsen?
****Flere svar mulig***

5.1.5 Ble hendelsen rapportert til noen?

I følge undersøkelsen rapporterte 42% av virksomhetene ikke hendelsen til noen, 24% av virksomhetene rapporterte til administrator av det aktuelle tekniske systemet, og 18% av virksomhetene meldte ifra til KraftCert eller tilsvarende. Ingen oppga at de rapporterte til NorCERT eller forsikringsselskap. Dette virker naturlig da det er KraftCert som hovedsakelig rapporterer videre. Det er svært få norske virksomheter som per dags dato har cyberforsikring. Størrelse på virksomhet eller bedriftstype har ikke hatt noe å si i denne undersøkelsen for hvordan virksomhetene har svart på dette spørsmålet. I henhold til beredskapsforskriften, er selskapene forpliktet til å rapportere ekstraordinære situasjoner til NVE, statistikken viser at kun 6% gjorde dette. Dette kan skyldes at rapporteringsplikten gjelder kun nettselskaper (KBO-enheter) og at det er ekstraordinære hendelser som skal rapporteres.

Figur 12: Ble hendelsen rapportert til noen av de følgende?
****Flere svar mulig***

6 Oppsummering og anbefalinger

Cyberangrep og IT-skandaler preger overskrifter og nyhetsbildet i 2017, og antallet hendelser øker. Angriperne er raske til å utnytte den stadig mer globaliserte og digitale verden. Et nøkkelpunkt er at det er veldig viktig å kontinuerlig følge med på trussel- og risikobildet, og innrette seg etter det som skjer i andre land og det som kan skje i Norge.

Denne undersøkelsen gir et bilde av norsk energiforsynings sikkerhetstilstand slik det ser ut fra 88 virksomheter som svarte på undersøkelsen, og 62 som svarte på spørsmål om den verste hendelsen. I undersøkelsen er funnene kommentert opp mot NSRs Mørketallsundersøkelse 2016. Selv om denne undersøkelsen viser at større andel virksomheter innenfor energisektoren oppdager sikkerhetsbrudd sammenlignet med norske virksomheter generelt (jf. NSRs Mørketallsundersøkelse), betyr dessverre ikke det at sikkerheten er god nok. De færreste alvorlige dataangrep blir noen gang oppklart, årsaken er det er så lett å skjule sine spor for hva man har gjort og hvem man er. Alt som gjøres digitalt har reelle konsekvenser. Selv om norske virksomheter ikke har rapportert hendelser som har resultert i KILE-kostnader, betyr det ikke at konsekvensene kan være store. Det er flere eksempler på aktører og virksomheter i Norge som ikke har hatt gode nok sikkerhetsrutiner, hvor dette blant annet har resultert i store økonomisk tap, sensitiv informasjon og personopplysninger har kommet på avveie. Norske virksomheter påfører seg selv en risiko, dersom de ikke har en god nok forståelse for sikkerheten. IT-skandaler i våre naboland viser hvor alvorlige konsekvenser manglende forståelse for sikkerhetsrutiner kan få når beslutningstagere ikke har tilstrekkelig sikkerhetskompetanse, og velger å ikke følge regelverket [6]. Sikkerhetshendelser i andre land understreker hvor viktig det er at sensitiv informasjon og systemer beskyttes mot adgang av uautoriserte personer, enheter og prosesser. Tydelige regler og sikkerhetsrutiner er helt avgjørende for å ivareta sikkerheten.

NSMS ÅRLIGE RISIKOVURDERING (2017):

Økt digitalisering kan bidra til å gjøre samfunnsfunksjoner sårbare. Som en følge av digitaliseringen er ofte mange virksomheter knyttet sammen i produksjon av varer og tjenester, noe som skaper lange og uoversiktlige verdikjeder. Disse verdikjedene inkluderer ofte tjenester i andre land. For virksomheter som er avhengig av digitale tjenester, er det derfor vanskelig å ha tilstrekkelig innsikt i, og kontroll over, egne sårbarheter. Samfunnet blir stadig mer avhengig av disse tjenestene, samtidig som det har vært en jevn økning i kompleksitet de senere årene. NSM mener dette må forventes å øke ytterligere i tiden fremover. Digitaliseringstakten er rask, og mange av virksomhetene har god evne til å utvikle seg og ta i bruk nye løsninger. NSMs vurdering er at virksomhetene ikke har tilsvarende evne til å ivareta sikkerheten, slik at utviklingen kan gjøres på en kontrollert og sikker måte. [2]

Av de 88 virksomhetene i undersøkelsen har 70% hatt sikkerhetshendelser, hvorav 52 av virksomhetene har hatt hendelser som havner i kategorien «den alvorligste hendelsen». For 21% av virksomhetene som svarte på spørsmålet om den alvorligste hendelsen, var situasjonen så alvorlig, at selskapets ledelse ble involvert.

Av virksomhetene som har svart på spørsmålet om den alvorligste sikkerhetshendelsen, hadde nærmere halvparten ikke kjennskap til medvirkende faktorer som gjorde at hendelsen forekom. Hadde man visst hva som var med på å forårsake hendelsen, ville denne kunnskapen vært til hjelp for å forhindre at noe lignende skulle skje i framtiden. Menneskelig feil og mangel på sikkerhetsbevissthet hos de ansatte er faktorer som har vært med på å forårsake hendelsen. Årsaken til at sikkerhetshendelser forekommer er i mange tilfeller grunnet ledelse eller ansatte som ikke har tilstrekkelig sikkerhetskompetanse og forståelse for konsekvensene av teknologibruken.

Undersøkelsen viser videre at 40% av virksomhetene som hadde hendelser som kan kategoriseres som alvorligste hendelse, faktisk ikke gjorde noen endringer i organisasjonen som følge av hendelsen. Alt for få virksomheter har gjort endringer i sin policy eller rutiner (*21%*), enda færre har investert i opplæringsprogram for de ansatte *(18%)*. Det indikerer at det er store mangler i sikkerhetsarbeidet som det virksomhetene må jobbe videre med. Dette er en stor forskjell fra NSRs Mørketallsundersøkelse 2016 [7], hvor 44% av virksomhetene gjorde endringer i organisasjonens policy og sikkerhetsrutiner, og 20% investerte i utvikling av sikkerhetsprosesser og etablerte et sikkerhetsmiljø.

Figur 13: Som et resultat av hendelsen, ble noen av de følgende endringene gjort i organisasjonen?
****Flere svar mulig***

6.1 Anbefalinger og sikringstiltak

6.1.1 Styringssystem for informasjonssikkerhet

Nærmere 25% virksomheter mangler ifølge denne undersøkelsen et styringssystem for informasjonssikkerhet. Her ser man at det er rom for forbedring. En virksomhet bør ha et rammeverk eller et styringssystem for informasjonssikkerheten. Styringssystemet bør inneholde:

- Retningslinjer for sikker drift av IT-infrastruktur (backup, patching, herding endringskontroll, mm.)
- Planer for håndtering av de viktigste informasjonssikkerhetshendelsene
- Krav til gjennomføring av de systematiske øvelser knyttet til IT-beredskap
- Oversikt over alle personopplysninger som behandles i virksomheten
- Oversikt og kontroll på brukeridentiteter med til gang til virksomhetens system (tilgangsstyring)
- Rutiner for håndtering av kraftsensitiv informasjon og personopplysninger (internkontroll)
- Retningslinjer for håndtering av avvik (kraftsensitiv og personopplysning)
- Sikkerhetsinstruks for brukere, ledere og sikkerhetsansvarlige
- Krav til at det utpekes en informasjonssikkerhetsansvarlig

Punktene bygger på fra NSRs Mørketallsundersøkelse 2014 og denne undersøkelsen [7]

En god måte å arbeide med informasjonssikkerhet er å følge en standard som inkluderer punktene ovenfor. Ikke bare gjør disse standardene at sikkerhetsrisikoen innad en organisasjon håndteres og styres, men overholdelse av standardene overfører en viktig melding til kunder og samarbeidspartnere. Mange rammeverk spiller en viktig rolle i overvåking, gjennomgang, vedlikehold og forbedring av styringssystemet for informasjonssikkerhet, og gir trolig andre organisasjoner og kunder større tillit til måter de samhandler med virksomheten. Rammeverket gjør at sikkerhetsrisikoen blir kostnadseffektiv. Eksempler på standarder er:

- COBIT
- ISO 27000 Seriene
- NIST SP 800 Seriene

Disse standardene gir retningslinjer som inkluderer og tydeliggjør punktene nevnt ovenfor.

6.1.2 Leverandørhåndtering

Undersøkelsen indikerer en avhengighet av leverandører *(figur 5*-7). Under en tredjedel av dem som svarte er i liten grad avhengig av leverandører når det gjelder å håndtere hendelser og gjenopprette systemer. Dette gjelder for både driftskontrollsystemer og administrative systemer. Denne avhengigheten er viktig å ta inn over seg både når det gjelder forebyggende uønskede hendelser og når det gjelder beredskap. Det vil for eksempel være en god ide å inkludere leverandører og rutiner opp mot leverandører i beredskapsplaner og å øve eller gjennom gå dette sammen med leverandøren.

6.1.3 Etablere god sikkerhetskultur

Man kan aldri få et fasit svar på hvordan en ansatt kommer til å handle i ulike situasjoner, men gjennom bevisstgjøring, god trening og motivasjon, er man i stand til å redusere usikkerheten i virksomheten. Man trenger god sikkerhetskultur for å være godt rustet til å forebygge og håndtere hendelser.

HVA ER SIKKERHETSKULTUR?

NSM definerer sikkerhetskultur som følgende: *Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd*

Det er viktig å ta i bruk elementer som bevisstgjøring, informasjon, kunnskap og motivasjon for å skape en positiv endring i sikkerhetskulturen. Undersøkelsen viser at det er svært få virksomheter som har investert i opplæringsprogram for de ansatte. Opplæring er viktig for både å hindre hendelser, men også for å oppdage hendelser. Virksomhetene bør jevnlig sette fokus på farene ved virus, phishing og sosial manipulering [7], og gi nyansatte en skikkelig sikkerhetsgjennomgang. Ved å holde oversikt over rapporterte sikkerhetsbrudd, sikkerhetstruende hendelser som dataangrep eller virusinfeksjoner og nettverksaktivitet, kan man øke bevisstheten rundt dette temaet til både ledere og ansatte, og dermed forbedre sikkerhetsatferden i virksomheten.

6.1.4 Rapportere og anmelde

En siste anbefaling vil være å slutte å være hemmelighetsfulle når det gjelder hendelser. Virksomhetene bør offentliggjøre mer, rapportere til KraftCERT, anmelde datakriminalitet til politiet og kontakte media. På denne måten vil man lære mer av hverandre og tilegne seg kunnskap om trusselen og risikoen som følger med digitaliseringen.

7 Appendix

7.1 Spørsmål fra undersøkelsen

1. Hvor mange ansatte er det i din virksomhet?
2. Hva slags selskap jobber du i?
3. Hvilken stilling har du?
4. Hvor stor er din kunnskap om systemene som benyttes i din virksomhet?

   IKT-sikkerhetskoordinatorer har fått dette spørsmålet

   4.1. Om SCADA/kontrollsystem

   4.2. Om administrasjonssystem
5. Hvordan er virksomhetens administrativ IT organisert?
6. Hvordan er virksomhetens driftskontrollfunksjon (SCADA, lokalkontrollsystem og tilsvarende) organisert?

   Kraftprodusenter, konsern og nettselskaper har fått dette spørsmålet
7. Hvor avhengig er du av din IT-leverandør for å håndtere hendelser?
8. Hvor avhengig er du av din leverandør av driftskontrollsystem for å håndtere hendelser?

   Kraftprodusenter, konsern og nettselskaper har fått dette spørsmålet
9. Hvor avhengig er du av din leverandør av driftskontrollsystem for å restore/gjenopprette system?

   Kraftprodusenter, konsern og nettselskaper har fått dette spørsmålet
10. Benyttes outsourcingtjenester i utlandet?

    Spørsmål til de som har svart at de har en outsourcet drift(helt/delvis)
11. Vet du hvor data fysisk er lagret og blir behandlet?

    Spørsmål til de som har svart at de har satt driften til utlandet
12. Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerheten?
13. Hvilke informasjonssikkerhetshendelser har virksomheten vært utsatt for siste 12 måneder? (Flere svar mulig)

    13.1. Datainnbrudd/Hacking

    13.2. Forsøk på datainnbrudd/hacking

    13.3. Dataskadeverk (Eksempelvis kryptolocker/randsomware, i betydning uautorisert endring/sletting av data, målrettede aksjoner som har til hensikt å redusere tilgjengeligheten)

13.4. Bedrageri (Fakturasvindel, svindel-epost eller andre former for manipulering)

13.5. Misbruk av IT-ressurser (Med IT-ressurser menes her PC/nett/server)

13.6. Tapt forretningshemmeligheter gjennom informasjonstyveri/digitalspionasje

13.7. Tyveri av IT-utstyr (PC, server, nettbrett, smarttelefoner etc.)

13.8. Virus og/eller malwareinfeksjon

13.9. Hendelse forårsaket av bedriftens ansatte

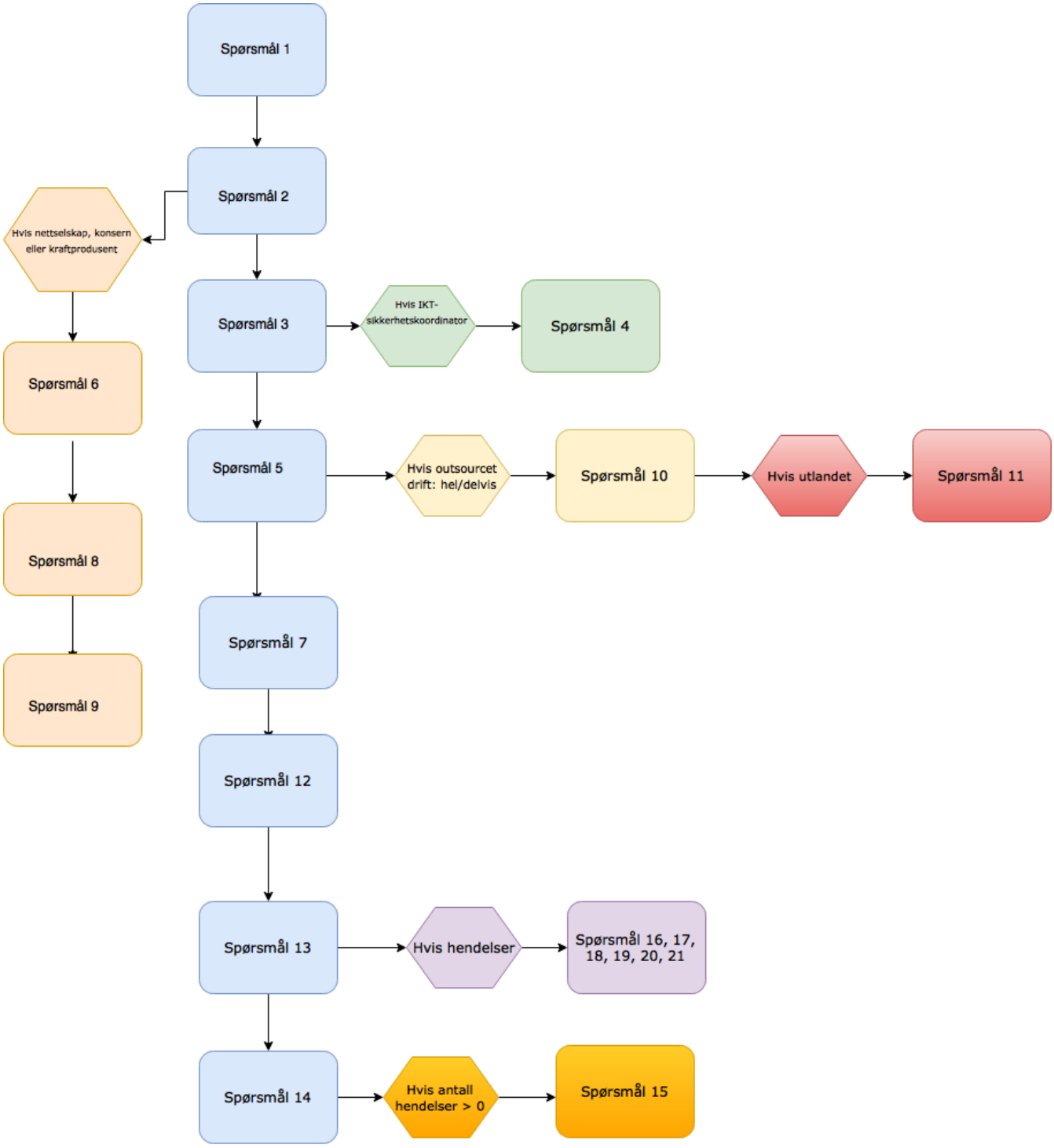
13.10. Hendelse forårsaket av outsourcingsleverandør

13.11. Innbrudd i organisasjonens sikkerhetssystemer (både fysisk og digitalt)

14. Tjenestenektangrep (DDoS) eller trusler omHvor mange informasjonssikkerhetshendelser som påvirket organisasjonen negativt hadde dere siste 12 måneder? (Med konsekvenser som tapt produksjon, økonomisk tap, omdømmetap eller svekket markedsposisjon)
15. Hvor mange av disse gjaldt driftskontrollsystem?
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene
16. Hva var den mest alvorlige informasjonssikkerhetshendelsen siste 12 måneder?
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene
17. Førte hendelsen til noe av det følgende? (Flere svar mulig)
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene
18. Var noen av følgende faktorer medvirkende til at hendelsen oppsto? (flere svar mulig)
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene
19. Var noe av følgende årsak til at hendelsen ble oppdaget? (Flere svar mulig)
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene
20. Ble hendelsen rapportert til noen av de følgende? (Flere svar mulig)
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene
21. Hvem sto bak hendelsen?
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene
22. Som et resultat av hendelsen, ble noen av de følgende endringene gjort i organisasjonen? (Flere svar mulig)
    Hvis man har hatt minst en sikkerhetshendelse de 12 siste månedene

7.2 Flytdiagram for undersøkelsen om sikkerhetstilstanden

7.2.1 Diagram



Referanser

[1] Næringslivets Sikkerhetsråd, «Mørketallsundersøkelsen,» NSR, Oslo, 2016.

[2] Nasjonal Sikkerhetsmyndighet, «Risiko og sårbarheter i en ny tid,» NSM, 2017.

[3] S. K. Hotvedt, «Cyberangrep mot Norge øker sterkt,» NRK, 2017.

[4] Politiets Sikkerhetstjeneste, «Trusselvurdering 2017,» Politiets Sikkerhetstjeneste (PST), Oslo, 2017.

[5] R. Lee, M. Assante og T. Conway, «Analysis Of The Cyber Attack On The Ukranian Power Grid,» E-ISAC, 2016.

[6] H. H. Røset og T. Bakke, «ITskandalen i Sverige: -Sannsynlig at noe lignende vil skje i Norge,» NRK, 2017.

[7] Næringslivets Sikkerhetsråd, «Mørketallsundersøkelsen 2014,» Næringslivets Sikkerhetsråd, 2014.

[8] Bistandsaktuelt, «Globalisert kriminell økonomi truer verdensordenen,» Bistandsaktuelt, 2017.

[9] Trend Micro, «Why Do Attackers Target Industrial Control Systems,» Trend Micro, 2017.

[10] Krypsys, «What is ISO27001 and why is it so important for organisations?».

[11] J. Hagen, O. Hermansen, J.-M. Pettersen og S. L. Paulen, «Regulering Av IKT-Sikkerhet,» NVE, Oslo, 2017.

[12] Lovdata, «Forskrift om endring i forskrift om økonomisk og teknisk rapportering, inntektsramme for nettvirksomheten og overføringstariffer,» Oslo, 2002.

[13] SINTEF, «KILE - Kvalitetsjusterte inntektsrammer ved ikke levert energi».

[14] Norges Offentlige Utredninger - NOU, «Digital Sårbarhet - Sikkert Samfunn,» NOU, 2015.

[15] Trend Micro, «Black Energy,» 2016.

[16] Høgskolen i Sør-Trøndelag, «Man-In-The-Middle Attack,» 2009.

[17] K. Schwab, The Fourth Industrial Revolution, London: Penguin Books Ltd, 2016.

Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no