NVE

Informasjonssikkerhetstilstanden i energiforsyningen

90
2017

RAPPORT

NSM

Rapport nr 90-2017
Informasjonssikkerhetstilstanden i energiforsyningen

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør:

Forfattere:

Trykk: NVEs hustrykkeri
Opplag:
Forsidefoto: Simon Oldani, NVE
ISBN 978-82-410-1645-5
ISSN 1501-2832

Sammendrag: Digitaliseringen av energiforsyningen fører til at kraftbransjen er mer utsatt for digitale angrep enn tidligere. Rapporten gir et bilde av sikkerhetstilstanden i energisektoren. Rapporten er basert på en undersøkelse som ble sendt ut til virksomheter i kraftbransjen i juni 2017 samt tre penetrasjonstester hos nettselskap. Rapporten understreker viktigheten av å heve nivået på grunnsikring av digitale systemer i bransjen, men også et sterkt behov for veiledning, kompetanseheving og revisjoner når det gjelder utsetting av IT-tjenester.

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

Desember 2017

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 cybertrusler og uønskede hendelser. Mye av dette har vi liten eller ingen erfaring med. Det er viktig for NVE å følge med på og også forstå denne utviklingen.

I 2016 fikk NVE rapportert inn 12 IKT-hendelser. Selskapene er pålagt å rapportere inn ekstraordinære hendelser, dvs. hendelser som har konsekvenser for forsyningen ev energi, men dette gir ikke et komplett bilde. NVE har derfor stilt spørsmålet: *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» som NVE har gjennomført i 2017.

Våren 2017 satte NVE ned en arbeidsgruppe. Gruppen har bestått av: Lars Erik Smevold, KraftCERT; Øystein Korum og Eirik Pettersen, Statnett; Øystein Hop, Statkraft; Jan-Ivar Andreassen, Hafslund Varme; Olav Vikøren, Validér; Solgun Furnes, EnergiNorge; Ståle Risem-Johansen, Forum for informasjonssikkerhet i kraftforsyningen; Maria Rodahl Johansen, Nettalliansen, Kåre Flatland, SiraKvina; Bente Hoff, Nasjonal Sikkerhetsmyndighet og Janne Hagen og Jon Martin Storm, NVE. Informatikkstudent ved UiO Namrah Azam har hatt et studentengasjement i prosjektet.

NVE fikk tillatelse av Næringslivets sikkerhetsråd (NSR) til å bruke spørsmålene fra Mørketallsundersøkelsen 2016. En tilpasning av spørreskjemaet ga mulighet for kartlegging av sikkerhetstilstanden, analyse og vurderinger i norsk energisektor, og drøfte funnene opp mot resultatene fra NSRs studie. NVE har også, som en del av FOU-prosjektet, gjennomført tre casestudier av tekniske sårbarheter. BDO og KraftCERT har bistått i dette arbeidet der tre nettselskaper fikk gjennomført penetrasjonstester. NVEs innrapporterte hendelser, resultater fra spørreundersøkelsen og penetrasjonstestene gir, sammen med NSMs hendelsesrapport for 2017, et bilde av sikkerhetstilstanden og -utfordringene i energisektoren.

Rapporten gir oversikt over hendelser og trusler, og kan brukes som grunnlag for bransjens egne ROS-analyser, for vurderinger av risiko og for valg av områder som bør følges opp med blant annet revisjon. I tillegg til å gi en beskrivelse av hendelser og sikkerhetstilstanden, gir rapporten noen råd om IKT-sikkerhet.

NVE takker alle som har bidratt i prosjektarbeidet.

Ingunn Åsgård Bendiksen

Avdelingsdirektør

Eldri N. Holo

Eldri Naadland Holo

Seksjonssjef

Sammendrag

Cyberangrep og IT-skandaler har preget nyhetsbildet i 2017. Mange virksomheter opplever uønskede hendelser. Angriperne er raske til å utnytte den stadig mer globaliserte og digitale verden. Det er viktig å følge med på trussel- og risikobildet. Det som skjer i energisektoren i andre land, kan skje i Norge. Både PST og E-tjenesten peker på at kritisk infrastruktur og energisektoren er utsatt for spionasje og etterretning.

NVE mottar påkrevde rapporter fra selskaper som har opplevd hendelser relatert til deres IKT-systemer, men det er ikke mange IKT-hendelser som blir rapportert. I 2016 ble 12 IKT-hendelser rapportert. Hendelsene omfattet tilfeldige feil, virus og skadevareinfeksjoner og informasjonslekkasje.

Cyberangrep er blitt en del av de daglige utfordringer for alle virksomheter. Energisektoren går heller ikke fri. Internasjonal energisektor har over flere år opplevd alvorlige cyberangrep. Angrepet mot ukrainsk energisektor illustrerer hvordan energisektoren kan bli rammet i en sikkerhetspolitisk spent situasjon og hvor alvorlige konsekvensene kan bli. Også krypteringsskadevaren WannaCrypt rammet tilfeldige virksomheter i energisektoren. Hendelsen hadde økonomiske konsekvenser for de som ble rammet. Denne rapporten viser et bilde av IKT-sikkerhetstilstanden slik den oppleves i norsk energiforsyning. Rapporten gir en oversikt over hendelser virksomheter i den norske kraftbransjen har opplevd de 12 siste månedene fra juni 2016 - juni 2017. Rapporten gir også et bilde på omfanget av hendelser. 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 er oppfattet som alvorlige. Hendelsene omfatter hovedsakelig dataskadeverk, bedrageri, virus/skadevareinfeksjon, forsøk på datainnbrudd og hacking. De fleste av virksomhetene har ikke rapportert alvorlige konsekvenser for driften og forsyningssikkerheten. Hos 21% av virksomhetene som svarte på spørsmål om den alvorligste hendelsen, har hendelsen likevel vært alvorlig nok til å involvere selskapets ledelse.

Mennesker vil alltid gjøre feil og mangel på sikkerhetsbevissthet hos de ansatte bidrar til at hendelser oppstår hos henholdsvis 24% og 35% av virksomhetene. 40% av virksomhetene som hadde alvorlige hendelser, oppgir at det ikke er blitt gjort noen endringer innad i organisasjonen i etterkant av hendelsen. 18% har oppgitt at de har investert i opplæringsprogram for de ansatte.

Rapporten viser videre at ca. 8 av 10 virksomheter er avhengige av leverandørene for å håndtere hendelser i sine IT- og driftskontrollsystemer og gjenopprette systemene dersom de feiler. Samtidig viser funnene fra penetrasjonstestene hos tre nettselskaper at mange sårbarheter kan koples til manglende leverandørkontroll, mangelfull sikkerhetsoppdatering av operativsystemer og programvare, samt virksomhetenes evne til å avvikle tjenester som ikke lenger er i bruk.

Med disse funnene understreker rapporten nødvendigheten av å heve nivået på grunnsikring av alle digitale systemer i bransjen, og særlig i administrative systemer. Bryterfunksjonen i smarte målere må sikres særskilt. Resultatene viser også et behov for kompetanseheving, veiledning og revisjoner når det gjelder utsetting av IT-tjenester. Funnen fra penetrasjonstestingen viser tydelig at virksomhetene må være klar over ansvaret de har når det gjelder IKT-sikkerhet, uansett om IT er satt ut eller driftet internt. Det er viktig å ha eget personell med tilstrekkelig kapasitet og kompetanse, uavhengig av hvilken IT-driftsmodell virksomheten har valgt.

Innholdsfortegnelse

Forord i
Sammendrag ii
Innholdsfortegnelse iii
1 Innledning 1
2 Om undersøkelsen 3
2.1 Metode 3
2.2 Arbeidsgruppen 3
2.3 Hvem har svart? 4
3 Hendelsesrapport fra NSM og KraftCERT 5
3.1 Digitale hendelser og trender i kraftsektoren 2017 5
3.1.1 Introduksjon 5
3.2 Internasjonale hendelser i perioden 09.16-08.17 6
3.3 Strategiske kompromitteringer våren 2017 6
3.3.1 Oppsummering 6
3.3.2 Tekniske detaljer 6
3.3.3 Nasjonale observasjoner 7
3.4 Destruktivt krypteringsvirus med spredning som orm juni 2017 7
3.4.1 Oppsummering 7
3.4.2 Tekniske detaljer 7
3.4.3 Nasjonale observasjoner 8
3.5 Skadevare rettet mot kontrollsystem i Ukraina desember 2016 8
3.5.1 Oppsummering 8
3.5.2 Tekniske detaljer 8
3.5.3 Nasjonale observasjoner 9
4 Dagens sikkerhetspraksis 10
4.1 Kontroll og administrasjonssystemer 10
4.2 Organisering av drift 11
4.2.1 Organisering av IT-driften 11
4.2.2 Tjenesteutsetting i utlandet 11
4.3 Leverandøravhengighet 12
4.4 Rammeverk for informasjonssikkerhet 13
5 Uønskede IKT-hendelser og cyberangrep 14
6 Den alvorligste hendelsen 18
6.1 Den mest alvorlige hendelsen 18
6.2 Hva førte hendelsen til? 18
6.3 Bakgrunnen for at hendelsen oppstod 19
6.4 Hvordan ble hendelsen oppdaget? 20
6.5 Hvem stod bak hendelsen? 21
6.6 Ble hendelsen rapportert til noen? 21
6.6.1 Innrapporterte ekstraordinære hendelser til NVE 22
7 Sårbarheter en ikke ser 23

7.1 Penetrasjonstester mot nettselskaper 23
7.2 Testresultater 23

8 Anbefalinger 25

8.1 Læring fra cyberangrep 25
8.2 Lærdom fra pentesting i norske selskap 26
8.3 Spesifikke anbefalinger basert på studien 27
8.3.1 Lær av dine feil 27
8.3.2 Innfør et styringssystem for informasjonssikkerhet 29
8.3.3 Bruk NSMs Grunnprinsipper for IKT-sikkerhet 30
8.3.4 Start sikkerhetsarbeidet allerede med rekrutteringsarbeidet 30
8.3.5 Bygg kunnskap og god sikkerhetskultur 30
8.3.6 Inkluder sikkerhet i IT-tjenestekjøp og tjenesteutsetting 31
8.3.7 Rapporter hendelser til KraftCERT 31

Referanser 32

1 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, maskinvare 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. Ifølge NSRs Mørketallsundersøkelse 2016 [1], har over en fjerdedel av norske virksomheter opplevd uønskede IT-sikkerhetshendelser.

Trenden er at antall målrettede cyberangrep øker [2]. Angrepene innebærer risiko for at viktig informasjon blir stjålet eller lekket, store økonomiske tap, skade på utstyr og i verstefall at natur blir påvirket negativt og 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 Risiko 2017 at de gjennom flere år har sett en jevn økning av antall målrettede cyberangrep mot norske interesser, både offentlige og private. [2] 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 trusselbildet [2].

Denne rapporten er et internt forskningsprosjekt ved NVE, der NVE har som målsetting å beskrive sikkerhetstilstanden i energisektoren ved hjelp av blant annet statistikk. Prosjektet skal utvikle et verktøy (spørreskjema og analytisk fremgangsmåte) for å kunne analysere sikkerhetstilstanden og sammenligne bransjens sikkerhetstilstand opp 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 kan ramme dem.

Vi vet at menneskelig oppdagelsesevne er en viktig bidragsyter for å oppdage uønskede hendelser. Vi vet også fra tidligere Mørketallsundersøkelser gjennomført av NSR at mørketallene er store, og at mange hendelser ikke blir rapportert til myndigheter eller til politiet. Myndigheten og bransjen kan få et komplementert bilde til sektorCERTens (KraftCERTs) og NSM NorCERTs hendelsesstatistikk ved å gjennomføre spørreundersøkelser. Til sammen vil det 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. Industri 4.0 er som teknologiskifte imidlertid fundamentalt forskjellig fra de forrige industrielle revolusjoner. Den er preget av en rekke nye teknologier som fusjonerer de fysiske, digitale og biologiske verdener ved hjelp av Tingenes Internett (Internet of Things). 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 [35]. *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.*

Tesla berøringsskjerm: smart bil gjennom mobil IoT-kjøretøyteknikk

2 Om undersøkelsen

2.1 Metode

Spørreundersøkelsen om sikkerhetshendelser i kraftforsyningen 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 6. juni 2017 og lukket 27. juni 2017. Det ble sendt en påminnelse. 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. Dataene er analysert ved hjelp av statistikkverktøyet PSPP.

Penetrasjonstestene ble utført av BDO AS i løpet av september og oktober 2017. BDO er et rådgivnings- og revisjonsselskap med et eget operativt miljø innen IT-sikkerhet. KraftCERT bidro som del av teamet og var diskusjonspartner gjennom hele prosjektet.

Selskapene som ble testet var av ulik størrelse, og har driftskontrollsystem i henholdsvis klasse 1, 2 og 3. NVE stod for utvelgelsen av selskaper, og det ble inngått separate avtaler med hvert selskap.

Følgende tester ble utført:

- Utsidetest - Sårbarhetsskanning fra Internett.
- Innsidetest – Simulert målrettet trusselaktør med tilgang til administrasjonsnettverk.

Det ble ikke gjennomført tester for å vurdere hvor krevende eller lett det kan være for trusselaktører å oppnå tilgang til administrasjonsnettverk. Mørketallsundersøkelsen og hendelsesstatistikken forteller imidlertid at det generelt sett er mulig for trusselaktører å oppnå slik tilgang.

2.2 Arbeidsgruppen

NVE har satt ned en referansegruppe som har bidratt i arbeidet med å utforme spørsmål, gi innspill til arbeidet og drøfte resultatene. Gruppen har bestått av: Lars Erik Smedvold, KraftCERT; Øystein Korum, Statnett; Eirik Pettersen, Statnett; Øystein Hop, Statkraft; Jan-Ivar Andreassen, Hafslund Varme; Olav Vikøren, Validér; Solgun Furnes, EnergiNorge; Ståle Risem-Johansen, Forum for informasjonssikkerhet i kraftforsyningen; Maria Rodahl Johansen, Nettalliansen; Kåre Flatland, SiraKvina; Bente Hoff, NSM; Janne Hagen og Jon Martin Pettersen, NVE. Gruppen har hatt 6 møter i 2017, og har ellers samarbeidet på e-post. Informatikkstudent ved UiO, Namrah Azam, har bidratt med skriving og analyse.

2.3 Hvem har svart?

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

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

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*

3 Hendelsesrapport fra NSM og KraftCERT

3.1 Digitale hendelser og trender i kraftsektoren 2017

3.1.1 Introduksjon

Cyberangrep rettet mot kontrollsystemene for kraftsektoren er et relativt nytt fenomen på den digitale arenaen. Tidligere har kontrollsystemene som styrer prosessene vært fysisk isolert. Dette er i endring fordi større grad av fjernstyring av systemer gir mer effektiv drift, samt at nye utnyttelsesområder for data fra systemene åpner for nye tjenester. Som en konsekvens er kontrollsystemer nå mer utsatt for samme type trusler som tradisjonelle IKT-systemer.

NSM NorCERT er Norges nasjonale CERT* og cybersenter. NSM NorCERT håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon på tvers av ulike sektorer. NSM NorCERT drifter og organiserer et nasjonalt sensornettverk på internett; Varslingssystem for digital infrastruktur (VDI). KraftCERT er et responsmiljø dedikert til å koordinere hendelser i kraftsektoren. NSM NorCERT og KraftCERT jobber sammen for å sikre norsk kraftbransje og kontrollsystemer i norsk kritisk infrastruktur. I det som følger gir NSM og KraftCERT en oppsummering av de tre største internasjonale hendelsene, overordnet og teknisk, og ser på hvordan de har hatt skadepotensial for den norske kraftsektoren.

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]

3.2 Internasjonale hendelser i perioden 09.16-08.17

Det er særlig tre hendelser som helt eller delvis har truffet den internasjonale kraftbransjen det siste året. Den første er en sak hvor strategiske kompromitteringer[1] har blitt benyttet til å stjele ansattes innloggingsdata. Videre ser vi på skadeeffekten et krypteringsvirus kan påføre et internt nett når en angriper utnytter gyldige innloggingsdata. Vi går også gjennom skadevaren CRASHOVERRIDE, som kan ha blitt benyttet i angrep mot en transmisjonsstasjon i Ukraina desember 2016 [3] [4] [2].

3.3 Strategiske kompromitteringer våren 2017

3.3.1 Oppsummering

NSM NorCERT er kjent med at det våren 2017 har blitt utført målrettede angrep mot internasjonale organisasjoner i energisektoren. Angripere skal ha foretatt strategiske kompromitteringer av legitime nettsider hos energiselskap, partnere eller leverandører. De har deretter installert skadevare på dette stedet og så til slutt kjørt kampanjer for å lure ansatte i energiselskap til å gå inn på disse sidene [5] [6]. Dette er en kjent metode for å blant annet innhente folks innloggingsdata (man blir ledet til et «vannhull»). Måten dette ble gjort på var blant annet ved utsending av e-post med vedlegg som tilsynelatende var en CV for en kontrollsystemingeniør. Det er ikke uvanlig at dette blir sendt direkte videre til personalavdelingen i selskaper og har derfor vist seg å være en effektiv spredningsmekanisme.

3.3.2 Tekniske detaljer

I vannhullene har legitime JavaScript-filer blitt endret til å inkludere en referanse til en fil på angripers infrastruktur. Når dette JavaScriptet kjører i offerets nettleser, vil maskinen prøve å hente ned et dokument fra angripers infrastruktur. Dette vil initiere autentisering for fildelingen mellom maskinene over protokollen NTLMSSP[2] på Windows-baserte systemer [7]. Som en del av protokollen overføres innloggingsdetaljer beskyttet med en enveis-funksjon (såkalt hashing) til angripers infrastruktur. Svakheter i både protokollen og i måten enveis-funksjonen benyttes på i tidligere versjoner av NTLM kan utnyttes av en kapabel angriper, og er veldokumentert i åpne kilder [8]. Enkelte internasjonale kraftselskaper skal i tillegg skal ha mottatt målrettede e-poster med et avledningsdokument. Dokumentet skal ha vært godt utformet og relevant for mottaker. Disse avledningsdokumentene inneholdt en referanse til en fil på angripers infrastruktur for igjen å initiere fildeling med offeret, med et mål om å kunne stjele innloggingsdetaljer. Sårbarheten som ble utnyttet i dokumentene, har blitt beskrevet som 'template injection' [9], og er en metode for å legge inn ondsinnet kode i dokumenter eller på legitime nettsider. Fordi autentiseringen starter i bakgrunnen, trenger ikke angriper å lure offeret til å oppgi innloggingsdetaljer, noe som skiller dette fra for eksempel klassisk OWA-phishing (Outlook Web Application) [8]. Teknikken med å

---

[1] Strategiske kompromitteringer, også kalt vannhull, tar sikte på å kompromittere webtjenester en forventer at offeret vil besøke. For å unngå å kompromittere store mengder besøkende utenfor målgruppen kan angriper implementere en såkalt hvitlisting for at kun besøkende med et gitt IP eller versjon av programvare blir kompromittert.

[2] For detaljer om NTLMSSP, se https://msdn.microsoft.com/en-us/library/windows/desktop/ms691272(v=vs.85).aspx

stjele hashede innloggingsdetaljer under autentisering med NTLM har eksistert i flere år, og antas å fortsatt være en virkningsfull metode det neste året. Det vil være få endringer som er nødvendige for å tilpasse denne angrepsmetoden til norske virksomheter da NTLM er benyttet i mange Windows-baserte kontornettverk i Norge. Med innloggingsdetaljer vil angriper kunne få tilgang til tjenester eksponert mot internett, og benytte disse til lateral bevegelse i nettverket. Dette kan gi angriper anledning til utstrakt rekognosering for videre bevegelser fra kontornettverket mot kontrollsystemet.

3.3.3 Nasjonale observasjoner

Både NSM NorCERT og KraftCERT har observert at norske virksomheter har blitt videresendt fra vannhullene til angripers infrastruktur. Det er også norske kraftselskap som har mottatt de målrettede e-postene som er beskrevet i åpne media, men det er ikke rapportert at norske virksomheter skal ha blitt frastjålet innloggingsdetaljer. Det siste året har både NSM NorCERT og KraftCERT håndtert hendelser med forsøk på å stjele innloggingsdetaljer fra norske virksomheter, blant annet gjennom OWA-phishing. I slike tilfeller videresendes ofte e-posten fra en kompromittert e-postkonto til hele kontaktlisten. Slike svindel-e-poster er gjerne koblet med leveranse av løsepengevirus, og er derfor gjerne økonomisk motiverte hendelser med mål om å treffe flest mulig. Valget av vannhull i denne hendelsen kan indikere at angrepet rettet seg mot spesifikke sektorer, noe som kan tilsi at angrepet ikke var opportunistisk, men en første fase i et målrettet angrep.

3.4 Destruktivt krypteringsvirus med spredning som orm juni 2017

3.4.1 Oppsummering

NotPetya var navnet på et krypteringsvirus med orm-lignende egenskaper[3] som spredde seg til et stort antall internasjonale virksomheter i juni 2017 [10] [11] [12].Blant de berørte virksomhetene skal det ha vært ukrainske kraftselskaper [13]. Spredningen skal ha startet ved at angriper kompromitterte et programvareselskap som leverte et mye brukt regnskapsprogram for selskaper med administrativt kontor i Ukraina [14]. NotPetya fikk store konsekvenser for selskapene som ble truffet.

3.4.2 Tekniske detaljer

På en av oppdateringsserverne til regnskapsselskapet M.E.Doc la angriper inn kode slik at forespørsler om programvareoppdatering ble besvart med å laste ned skadevare fra angripers infrastruktur i stedet. Dette førte til at M.E.Doc sine kunder lastet ned og kjørte den ondsinnede koden direkte. Skadevaren har en rekke teknikker for å bevege seg innover i nettet ved bruk av legitime innloggingsdetaljer, utnytting av sårbarheter og bruk av eksisterende funksjonalitet for å overføre ondsinnede filer mellom maskiner. For å kunne spre seg på det interne nettet besto skadevaren blant annet av funksjonalitet for scanning for å identifisere andre sårbare tjenester. Dette ble fulgt opp ved å utnytte blant

[3] En orm er en form for virus som har innebygd funksjonalitet for spredning og reproduksjon.

annet sårbarheten EternalBlue [15], som også ble benyttet i WannaCrypt-hendelsen, noe som førte til stor og rask spredning i de nettverkene som faktisk ble kompromittert. Mange maskiner og filer ble gjort utilgjengelige. Den destruktive konsekvensen kombinert med en lite robust og sårbar betalingsløsning forbundet med løsepengeviruset har ført til spekulasjoner om den var ment for sabotasje [16].

3.4.3 Nasjonale observasjoner

Saken illustrerer risikoen et angrep på leverandørkjeden innebærer. Mange virksomheter ble rammet av kun én underleverandør med et sikkerhetshull som kunne utnyttes. Angrepet førte til størst antall infeksjoner i Ukraina. Hendelsen traff norske virksomheter i liten grad, og kun virksomheter som har kontor i Ukraina og felles forretningsnett med disse ble rammet her. Et lignende angrep gjennomført mot en leverandør av programvare med stor andel norske kunder vil kunne gi svært store tilgjengelighetsutfordringer også her. Likevel anses skadevarens utnyttelse av sårbarheten EternalBlue å utgjøre mindre risiko i Norge enn en del andre land. Årsaken er at mange norske virksomheter har nyere systemer, med gode rutiner for oppdatering av programvare. Mulighetsvinduet for angriperen vil derfor lukkes raskere enn om en oppdaterer sent. Konsekvensen av dette så en under både WannaCrypt og NotPetya hvor spredningen blant annet ble begrenset i Norge grunnet oppdaterte systemer. Saken illustrerer også hvordan et fagsystem som kommuniserer i egne kanaler på tvers av selskaps- og landegrensene stilte de berørte bedriftene vidåpne for spredning av skadevaren.

3.5 Skadevare rettet mot kontrollsystem i Ukraina desember 2016

3.5.1 Oppsummering

17. desember 2016 ble det ukrainske kraftselskapet Ukrenergo utsatt for cyberangrep [17]. Selskapet mistet kontrollen over deler av sin infrastruktur og måtte derfor gå over på manuell drift. I motsetning til angrepet i 2015 [18], har det etter 2016-angrepet vært rapportert at angrepet kan ha innebefattet skadevare spesielt designet for kontrollsystemer [4]. Den analyserte skadevaren var fleksibel og kunne utnytte sårbarheter i utstyr fra flere leverandører. I angrepet ble blant annet iboende sikkerhetsmekanismer utnyttet slik at for eksempel en transformatorstasjon selv utløste å bli koblet fra nettet og måtte fysisk styres lokalt. Sikkerhetsselskapene ESET [3] og Dragos [4] publiserte 12. juni 2017 rapporter om denne skadevaren spesielt rettet mot kontrollsystemer for kraftsektoren.

3.5.2 Tekniske detaljer

Skadevaren ble henholdsvis gitt navnene Industroyer og CRASHOVERRIDE av selskapene ESET og Dragos. Skadevaren er konstruert som et modulært rammeverk, uavhengig av spesifikke teknologier og konfigurasjoner i nettet. Rammeverket muliggjør for eksempel at moduler for teknologispesifikke kommunikasjonsprotokoller kan lastes inn uten større endringer. På denne måten kan angriper benytte seg av legitim funksjonalitet i kontrollsystemene til å nå sine mål, blant annet ved å utløse iboende sikkerhetsmekanismer. Analysen fra Dragos konkluderer med at dette sannsynligvis var

skadevaren benyttet under angrepene mot strømnettet i Kiev Ukraina 17. desember 2016. Formålet med skadevaren ble i dette tilfellet vurdert til å være sabotasje [3], men gjennom den modulære strukturen kan skadevaren relativt enkelt modifiseres til informasjonsinnhenting og eksfiltrasjon [4]. ESET beskrev også et tjenestenektangrep mot beskyttelsesreléer av typen Siemens SIPROTEC gjennom utnyttelse av sårbarheten CVE-2015-5374 [3] [19]. Det skal ha vært mulig å inkludere dette som en modul i skadevaren [3] [4]. Ved å sende en spesielt utformet pakke til en sårbar enhet skal det være mulig å skru av beskyttelsesreléet, og dermed trigge en innebygd beskyttelsesmekanisme i nettet hvor den berørte delen blir isolert. Utførelsen av et storstilt tjenestenektangrep gjennom utnytting av denne sårbarheten vurderes av Dragos som ressurskrevende for en eventuell angriper [4]. Infeksjonsvektor for angrepet mot strømnettet i Ukraina desember 2016 er fortsatt ukjent.

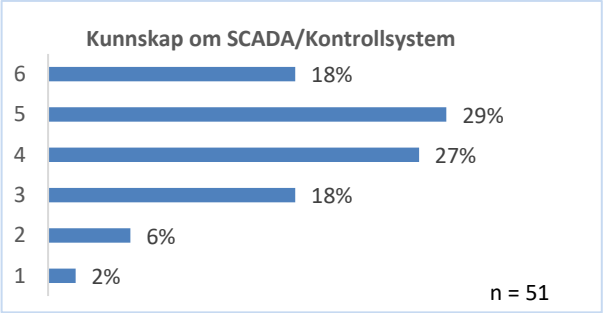
3.5.3 Nasjonale observasjoner

Den modulære strukturen til rammeverket CRASHOVERRIDE vil være et særlig effektivt virkemiddel mot industrielle kontrollsystemer, hvor teknologien ofte vil variere stort basert på type kontrollsystem. Selv om verken NSM NorCERT eller KraftCERT er kjent med at denne skadevaren har blitt benyttet mot norske virksomheter foreløpig, vil skadevarens modulære egenskaper øke sannsynligheten for at den kan bli benyttet i fremtidige angrep. Internasjonale angrepskampanjer mot kraftsektoren vil også kunne utgjøre en trussel mot norske virksomheter.

4 Dagens sikkerhetspraksis

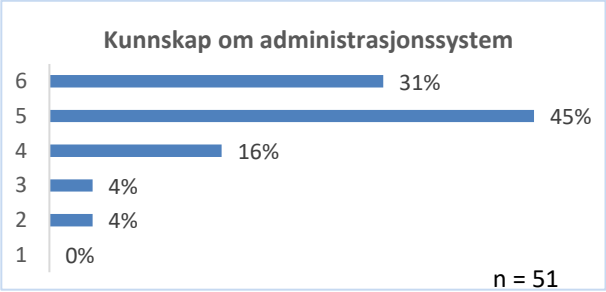
4.1 Kontroll og administrasjonssystemer

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 2*) ligger over 4. Gjennomsnittet er på 4.3.



Figur 2: Hvor stor er din kunnskap om systemene som benyttes i din virksomhet? (1 er dårlig og 6 er meget god)

Av IKT-sikkerhetskoordinatorene svarer 92% at deres kunnskap om administrasjonssystemene (*Figur 3)* ligger over nivå 4. Gjennomsnittet i dette tilfellet ligger på 5.



Figur 3: 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.

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 [20].

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. [32]

ADMINISTRASJONSSYSTEM

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

4.2 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 tjenesteutsetting i utlandet.

4.2.1 Organisering av IT-driften

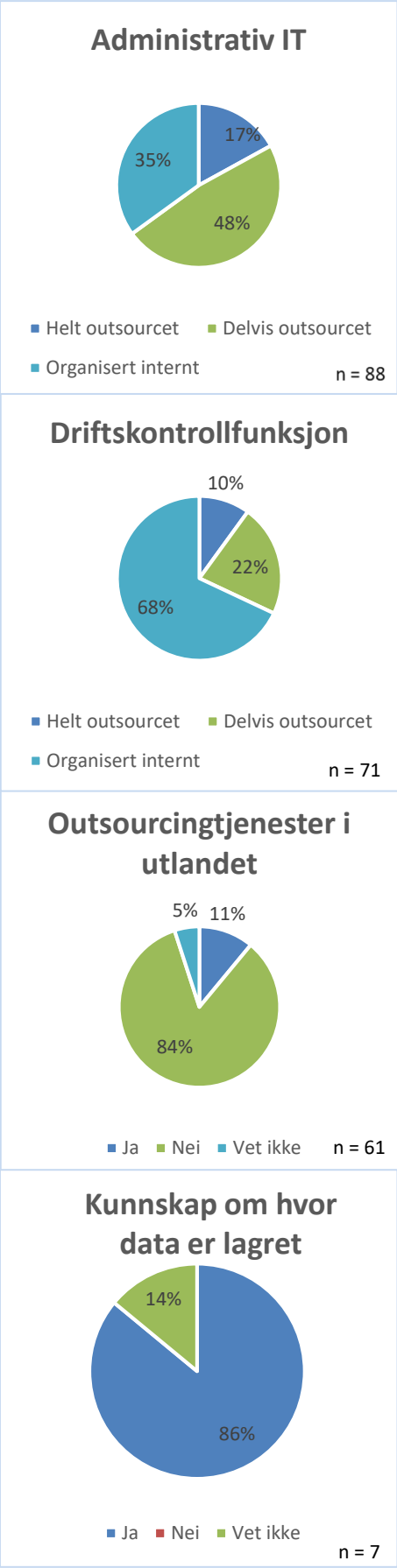
Halvparten av virksomhetene som har svart på undersøkelsen, har delvis satt ut drift av administrativ IT, 35% har satt ut driften helt, mens 17% har valgt en intern løsning.

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.

4.2.2 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 satt 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.



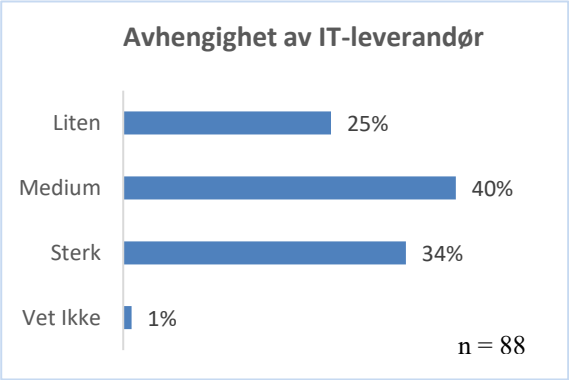
Figur 4: Outsourcing

4.3 Leverandøravhengighet

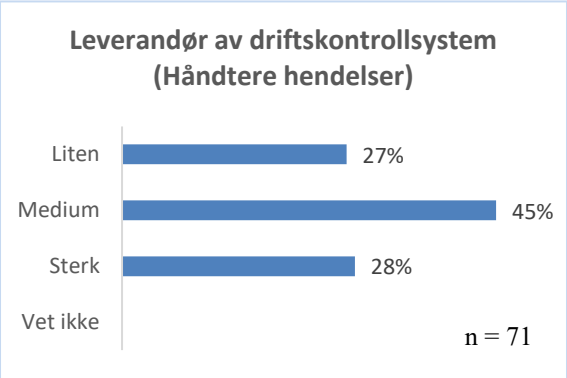
Tjenesteutsetting av IT og bruk av skytjenester treffer mange virksomheter i energisektoren. Trusselbildet og leverandørmarkedet er i stadig endring. I undersøkelsen har virksomhetene blitt spurt om hvor avhengige de er av sin IT-leverandør for å håndtere hendelser.

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*).

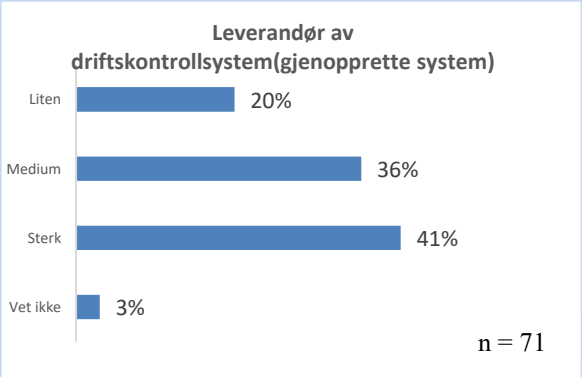
Konsern, nettselskapene og kraftprodusentene har i tillegg til det ovennevnte spørsmålet, fått to spørsmål som omhandler avhengighet av leverandør når det gjelder hendelser i driftskontrollsystemene. Når det kommer til håndtering av hendelser i driftskontrollsystemene, svarer 27% av virksomhetene at 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?



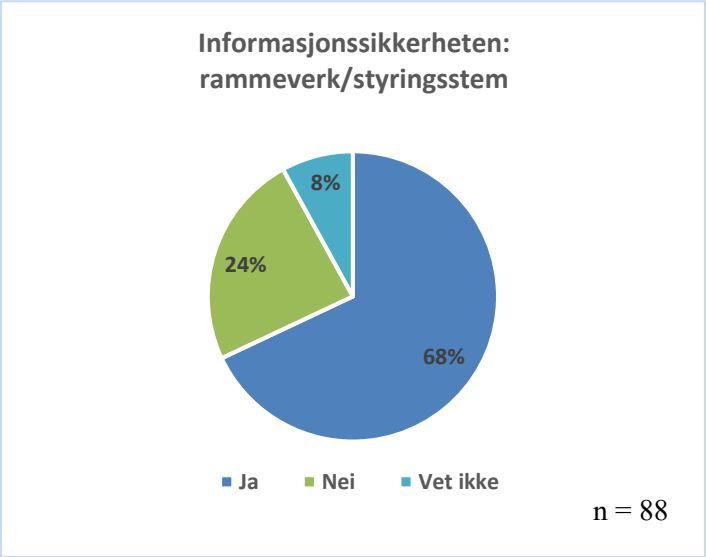
Figur 7: Hvor avhengig er du av din leverandør av driftskontrollsystem for å håndtere hendelsen/gjenopprette system?

4.4 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 de 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 for informasjonssikkerhet. 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 informasjonssikkerhet 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. Svarene man har fått fra begge undersøkelsene viser et behov 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.



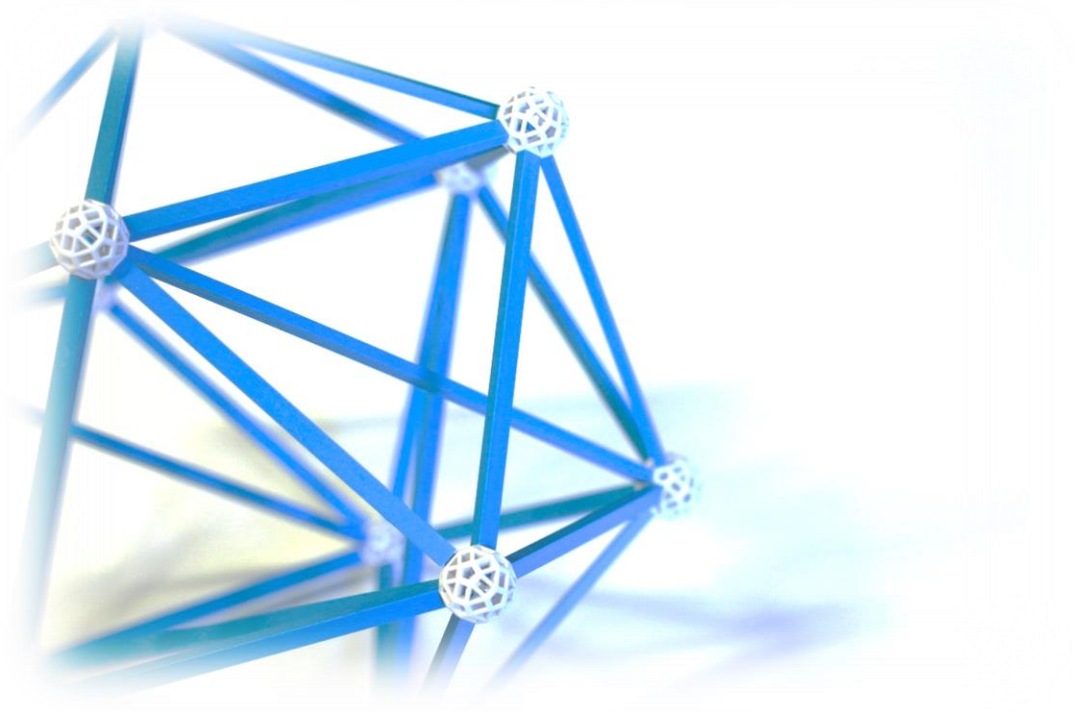
Figur 8: Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerheten?

5 Uønskede IKT-hendelser og cyberangrep

Cyberangrep mot Norge øker i omfang. I fjor registrerte NSM NorCERT mer enn 22 000 tilfeller av dataangrep mot norske bedrifter og offentlige etater [21]. 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.

Ifølge PSTs åpne trusselvurdering 2017, vil Norge og norske interesser i 2017 bli utsatt for fremmed etterretningsvirksomhet som kan ha et stort skadepotensiale. Datanettverksoperasjoner vil være en integrert del av de ulike etteretningsoperasjonene mot mål i Norge [22].

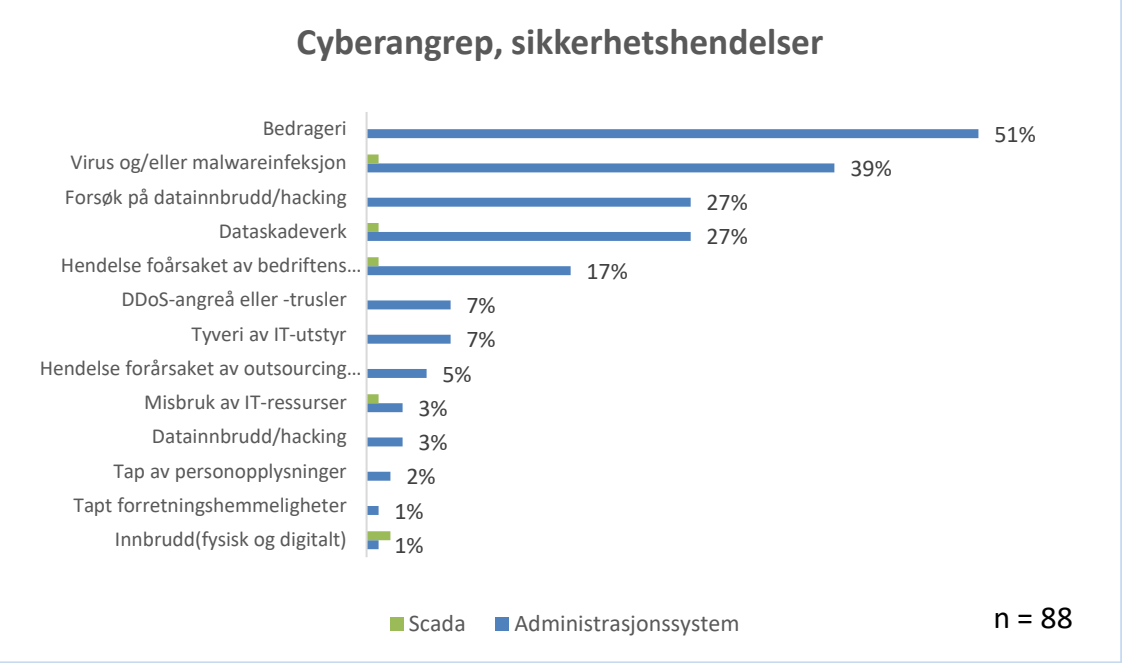
Fremmede makter kan gjennom nettverksbaserte etterretningsoperasjoner i fredstid erverve inngående kjennskap til kritisk infrastruktur. Denne kunnskapen kan i krisetid benyttes til å gjennomføre sabotasjeaksjoner. Flere stater utvikler skadevare som vil kunne brukes til å sabotere eller forstyrre kritiske 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 skadevare som har infisert systemene deres. 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 skadevare, og det har vært innbrudd i organisasjonens systemer. I de større virksomhetene, altså gruppen med 20 til 99 ansatte og gruppen med flere enn 100 ansatte, har færre vært utsatt for hendelser forårsaket av bedriftens ansatte. Færre har 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 [23]. Slike cyberangrep kan mørklegge byer, og truer i verste fall helse, miljø og sikkerhet. Derfor må styringssystemene sikres godt.



Figur 9: Hvilke informasjonssikkerhetshendelser har virksomheten vært utsatt for de siste 12 månedene?
**** Flere svar mulig***

Tabell 1: Angrepsstatistikk norsk næringsliv (2015) og norsk energisektor(2016-2017)

Type angrep	**NSR 2015**	**NVE 2016**
Bedrageri	2%	51%
Virus/malwareinfeksjon	20%	39%
Forsøk på datainnbrudd/hacking	8%	27%
Dataskadeverk	4%	27%
Hendelse forårsaket av ansatte	10%	17%
Hendelse forårsaket av outsourcingsleverandør	2%	5%
DDoS-angrep eller trusler	4%	7%
Tyveri av IT-utstyr	5%	7%
Misbruk av IT-ressurser	3%	3%
Datainnbrudd/hacking	-	3%
Tap av personopplysninger	1%	2%
Tapt forretningshemmeligheter	0%	1%
Innbrudd(digitalt/fysisk)	2%	1%

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 de 13% virksomhetene. Disse virksomhetene har videre fått spørsmål om hvor mange av hendelsene som gjaldt driftskontrollsystemene. For 3 av virksomhetene har dette dreid seg om 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 [36].

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.* [34]

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 [23].

Spydfiske: *En type spoofing-angrep hvor angriperen sender en forfalsket e-post med ondsinnede lenker eller vedlegg til en bestemt organisasjon eller enkeltperson. Ved hjelp av e-posten 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.*

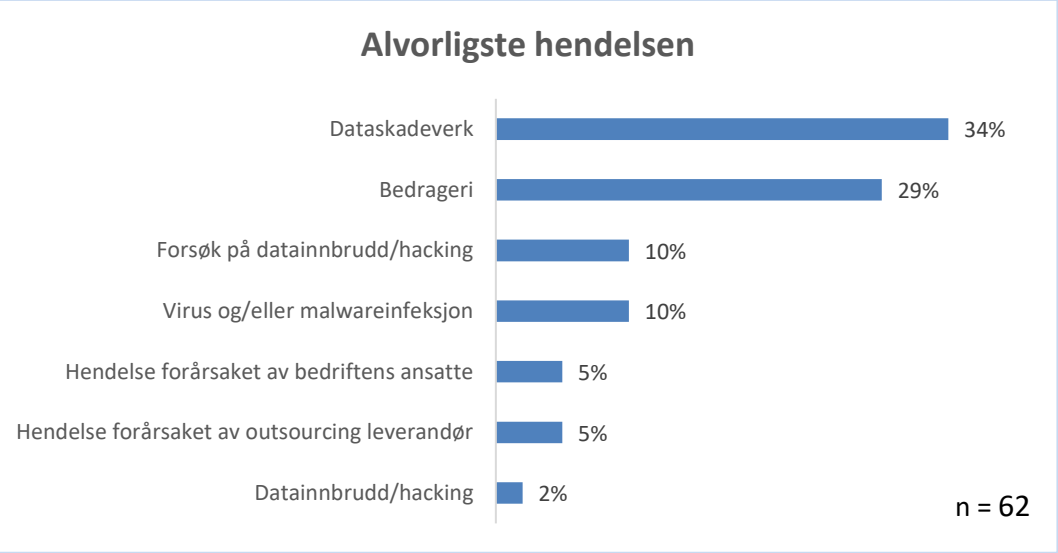
BlackEnergy3(BE3): *En trojansk hest (ondsinnet dataprogram som brukes til å hacke seg inn i en datamaskin) utviklet for å få i gang et tjenestenektangrep (DDoS), laste ned egendefinert spam og bankinformasjon-tyveri plugins.* ***BE*** *var kjent for å ha blitt brukt til å levere KillDisk, en funksjon 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.* [33]

6 Den alvorligste hendelsen

6.1 Den mest alvorlige hendelsen

Rapporten er 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.

Dataskadeverk (kryptolocker/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 10*). For 29% av virksomhetene var bedrageri den mest alvorlige hendelsen, dette i form av fakturasvindel, svindel-e-post 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 10: Hva var den mest alvorlige informasjonssikkerhetshendelsen de 12 siste månedene?
****Flere svar mulig***

6.2 Hva førte hendelsen til?

Ifølge 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*** [30]

Kvalitetsjusterte inntektsrammer ved ikke levert energi (KILE): ***Omfatter kortvarige (< 3min) og langvarige (>3min) avbrudd, som skyldes planlagte utkoplinger og driftsforstyrrelser i elektriske anlegg*** [31]

Figur 11: Førte hendelsen til noe av det følgende?
**** Flere svar mulig***

6.3 Bakgrunnen for at hendelsen oppstod

De fleste virksomhetene vet ikke hva som førte til at hendelsen oppstod, 42% av virksomhetene svarer at de ikke vet grunnen (*Figur 12*). 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 12: Var noen av følgende faktorer medvirkende til at hendelsen oppstod?
****Flere svar mulig***

6.4 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 *(Intrusion detection and prevention systems, IDPS).* 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.

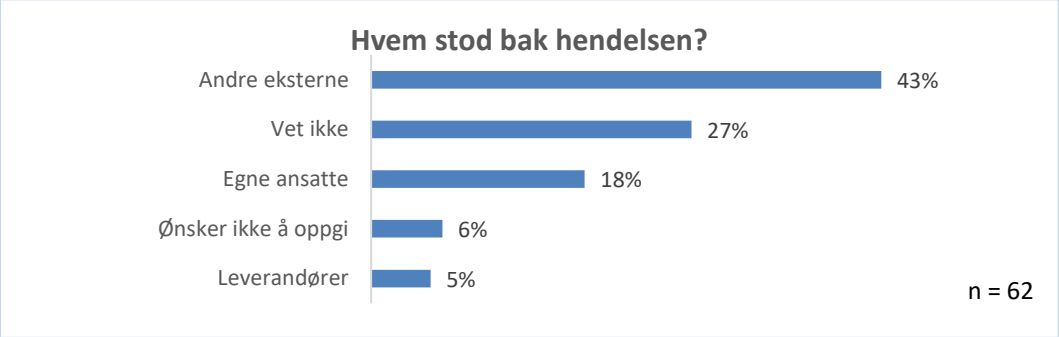
Figur 13: Hvordan ble hendelsen oppdaget?
****Flere svar mulig***

Tabell 2: Hendelsesoppdagelse norsk næringsliv (2015) og norsk energisektor (2016-2017)

Hvordan ble hendelsen oppdaget?	NSR 2015	NVE 2016
Rutinemessig på sikkerhetsmonitorering	32%	39%
Negativ effekt på virksomhetens drift	34%	18%
Vet ikke	-	16%
Annet	14%	23%
Andre kontroller og revisjoner	21%	10%
Ved en tilfeldighet	46%	8%
Varsel fra offentlige myndigheter og politi	1%	5%

6.5 Hvem stod bak hendelsen?

Ut ifra statistikken fra undersøkelsen ser man at de fleste hendelsene er forårsaket av eksterne aktører, 43% av virksomhetene 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 13, Figur 14*).

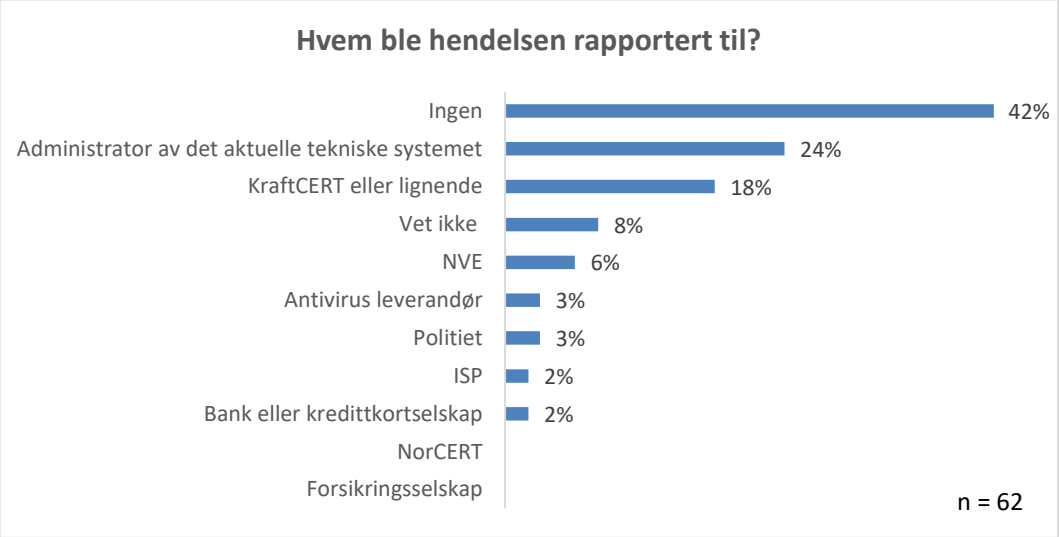


Figur 14: Hvem stod bak hendelsen?
****Flere svar mulig***

6.6 Ble hendelsen rapportert til noen?

Ifølge 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 hendelser til NVE, statistikken viser at kun 6% gjorde dette. Slike hendelser kjennetegnes av at de har negative konsekvenser for leveransen av energi til kundene, og at de rammer mange

kunder. Den manglende rapporteringen kan skyldes at rapporteringsplikten kun gjelder KBO-enheter og at det er ekstraordinære hendelser som skal rapporteres.



Figur 15: Ble hendelsen rapportert til noen av de følgende?
****Flere svar mulig***

6.6.1 Innrapporterte ekstraordinære hendelser til NVE

NVE og KraftCERT utgjør til sammen energisektorens responsmiljø. NVE og KraftCERT skal sammen ha en god oversikt over hva som skjer av uønskede IKT-sikkerhetshendelser i sektoren.

NSM er det nasjonale fagmiljøet for IKT-sikkerhet. NSM NorCERT har en egen rolle mot kraftsektoren bla gjennom VDI-samarbeidet. KraftCERT samarbeider også med NSM NorCERT for å sikre norsk kraftbransje. De varsler hverandre og sektoren om relevante sårbarheter og observerte angrep.

Dersom vi ser tilbake på kalenderåret 2016, så fikk ikke NVE innrapportert spesielt mange alvorlige IKT-hendelser. I kalenderåret 2016 ble det til sammen rapportert 12 IKT-hendelser. Ingen av hendelsene hadde konsekvenser for leveransen av strøm til kundene. Blant hendelsene finner vi skadevare/virus, utilsiktede hendelser som følge av legitim oppgradering av programvare, og hendelser der kraftsensitiv informasjon ble utilsiktet lekket og gjort tilgjengelig på internett.

De fleste IKT-hendelsene NVE får rapportert inn dreier seg om tilfeldige feil og ikke direkte målrettede angrep. Hendelsene har ikke fått noen alvorlige konsekvenser for forsyningen av elektrisitet, i form av ILE eller KILE, men har likevel resultert i at systemet til bedriftene måtte gjenopprettes.

Ansatte er ikke påpasselig når det gjelder sikkerhetsrutiner rundt e-poster, vedlegg og lenker. Den dominerende angrepsmetoden for målrettede angrep er infiserte vedlegg i e-poster sendt til utvalgte personer, såkalt spearphishing. Trusselaktørens intensjon er å få mottakeren til å klikke på vedlegget, som er infisert med skadevare for å ta kontroll over den aktuelle klienten [2].

7 Sårbarheter en ikke ser

7.1 Penetrasjonstester mot nettselskaper

Som en del av dette FOU prosjektet, har BDO sammen med KraftCERT, gjennomført penetrasjonstester hos tre nettselskaper i energisektoren. Disse selskapene var valgt ut av NVE. Basert på det generelle digitale trusselbildet nasjonalt og internasjonalt, samt behovet for å sikre energisektoren på best mulig måte, ble det utført utsidetester og innsidetester. Utsidetestene var en sårbarhetsskanning fra internett. Innsidetestene ble utført på en mer omfattende måte, og gikk ut på å simulere en målrettet trusselaktør med tilgang til administrasjonsnettverket, hvor målet var å oppnå uautorisert tilgang til virksomhetens driftskontrollsystemer. Slike sikkerhetstester synliggjør sårbarheter en ikke ser med det blotte øyet og med bruk av ordinære driftsverktøy.

Testingen ble utført som en blackbox-test hvor testerne ikke hadde tilgang til kildekode

Black-box testing (funksjonell testing): Under denne type testing behandles programvare under test som en svart boks, uten å kjenne innholdet.

eller annen dokumentasjon.

Hensikten med penetrasjonstestingen har vært å

1. Identifisere digitale sårbarheter i virksomhetenes IKT-systemer
2. Gi konkrete råd for å lukke sårbarhetene i systemene
3. Gi innsikt i hvor krevende eller lett det er for uvedkommende å komme seg inn i systemene, med hovedfokus på driftskontrollsystemer

7.2 Testresultater

Samlet sett scorer de tre nettselskapene godt på beskyttelse av driftskontrollsystemer. Det ble imidlertid funnet sikkerhetshull i administrasjonsnettverket hos alle selskapene. Hos et av selskapene ble det også funnet en kritisk sårbarhet som kan utnyttes fra Internett. Det er imidlertid viktig å understreke at funnene som ble gjort ikke er spesielle for kraftforsyningen. Sårbarhetene som ble funnet er vanlige i alle sektorer der BDO har gjennomført penetrasjonstesting. Flere av funnene fra både utside- og innsidetestene viser at sårbarheter kan unngås dersom virksomhetene hadde hatt bedre

- Leverandørkontroll
- Sikkerhetsoppdatering av operativsystemer og programvare
- Evne til å avvikle tjenester som ikke lenger er i bruk

Hos alle tre selskapene ble det i løpet av 1 til 3 timer funnet sikkerhetshull som gjorde det mulig å oppnå rettigheter som domeneadministrator i administrasjonsnettverket. En

målrettet trusselaktør kan utnytte slike rettigheter til å etablere et permanent fotfeste i administrasjonsnettverket, og dermed over tid lære mer om aktuelle angrepsvektorer mot driftskontrollsystemer.

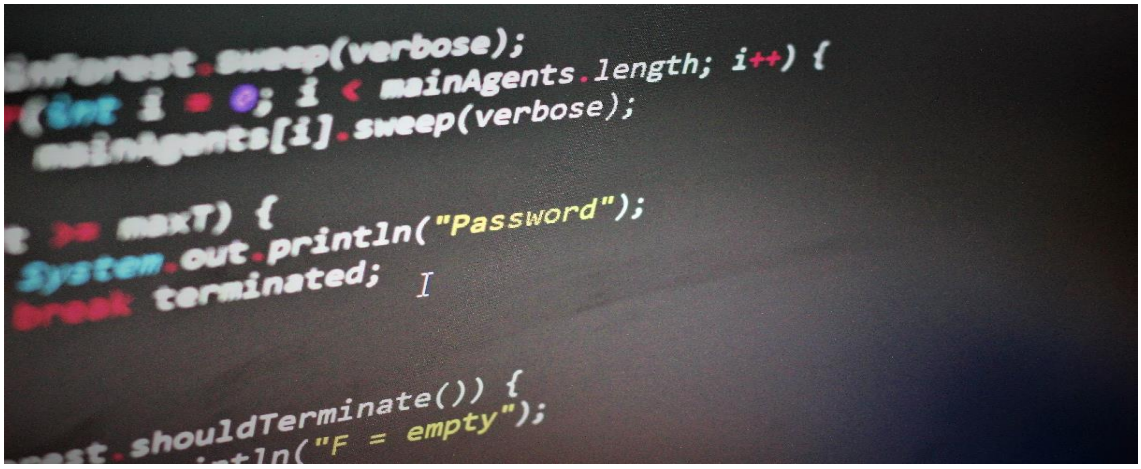
Med fulle rettigheter i administrasjonsnettverket er det også mulig å påføre vedvarende utilgjengelighet på administrative systemer som selskapene er avhengige av. Hos de tre selskapene lyktes det i løpet av to arbeidsdager å oppnå tilgang til og å administrere virtuell infrastruktur. Det lyktes også hos et av selskapene å få tilgang til en pålogget sesjon i Nord Pool Intraday trading. Det kunne dermed være mulig å få innsyn i og påvirke energimarkedet. Det avhenger imidlertid av trusselaktørens evne til å operere over tid uten å bli oppdaget, og hvilke verktøy aktøren allerede har i sin «verktøykasse».

Testresultatene viste at driftskontrollsystemene generelt var bedre beskyttet mot innsidetrusler enn AMS-løsningene, og at det er større risiko for at en trusselaktør som har fått fotfeste i det administrative nettverket, kan få tilgang til bryterfunksjonaliteten i AMS-løsningen.

Det er også verdt å merke seg at flere AMS-løsninger, også bryterfunksjonaliteten, driftes av leverandører. Trusselaktører kan dermed oppnå tilgang til bryterfunksjonaliteten ved

Gamle tjenester som er eksponert på internett, men som ikke er i bruk, bør avvikles. Det bør være en sårbarhetsskanning av webapplikasjoner. Oppdatering til supportert operativsystem (OS) på databaseserver er nødvendig for å minimere sårbarhetene. OS WinOS, Ubuntu, ugyldige sertifikater må oppdateres. Ugyldige sertifikater gjør det mulig for en angriper å implementere eget sertifikat uten å bli oppdaget. Det kan igjen føre til at sensitiv informasjon kommer på avveier.

først å gjennomføre datainnbrudd hos leverandøren. Datainnbrudd hos en AMS-leverandør kan potensielt utnyttes til å skru av strømmen til individuelle forbrukere hos mange selskaper samtidig. [24]



8 Anbefalinger

8.1 Læring fra cyberangrep

Trussel-beskrivelsen viser hvor viktig det er å sikre kommunikasjon og leveranser, fra leverandører eller mellom selskap. Ifølge NSM og KraftCERT, må virksomhetene både iverksette tekniske tiltak og opplæring av ansatte. Bedre sikkerhet er viktig hos produsenter, nettselskap, omsettere og leverandører til bransjen. Det er videre viktig å overvåke datatrafikk inn og ut av selskapet, ikke bare inngående. Cyberangrep som har skjedd lærer oss/har lært oss følgende:

Det blir stadig viktigere å etablere god grunnsikring av IKT-løsninger for å sikre motstandsdyktige IKT-løsninger. God grunnsikring er beskrevet i NSMs Grunnprinsipper for IKT-sikkerhet [25].

NSM erfarer at trusselaktører gjerne benytter kjente sårbarheter. Tiden fra en sårbarhet gjøres kjent til trusselaktører har skadevare på plass blir kortere og kortere. Virksomheter må automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Kontinuerlig revisjon av eksponerte tjenester mot internett er like viktig som før. I forbindelse med innføring av nye digitale tjenester vil dette også medføre en kartlegging av omfanget av den nye eksponeringsoverflaten.

Det er fortsatt svært populært hos angripere å benytte ansattes innloggingsdata som startpunkt for angrep. Det er derfor viktig å sikre tilgangsstyringen med 2-faktor-autentisering [3] [26], og i tillegg ha et godt autorisasjonsregime og tilstrekkelig sikkerhetsovervåking.

Internasjonale media har det siste året beskrevet flere hendelser som har truffet kraftsektoren. Hendelsene omfattet både informasjonsinnhenting og sabotasje, og i tillegg blir denne type angrep også ansett som en potensiell del av politiske konflikter. Det er derfor viktig at man ikke undervurderer angriperes interesse for norsk infrastruktur. Angriperes motiv og bakgrunn varierer sterkt og de fleste store internasjonale angrepskampanjer mot kraftsektoren vil også kunne utgjør en trussel mot norske virksomheter

8.2 Lærdom fra pentesting i norske selskap

Forebygging mot målrettede angrep handler om å designe en forsvarbar infrastruktur, primært ved å
1) bygge sikkerhetsbarrierer
2) overvåke aktiviteten i nettverk og systemer for å oppdage ondsinnet aktivitet
3) utføre sikkerhetstesting for å verifisere at barrierer og overvåking fungerer.

Erfaringer fra penetrasjonstestene gir også innsikt i hvordan man kan beskytte systemene. BDO anbefaler følgende elleve konkrete tiltak [24]:

1. Prioriter sikkerhetsoppdatering av operativsystem og applikasjoner på servere.

2. Bruk segmentering mellom klienter og servere ved hjelp av brannmurregler som kun åpner for nødvendige tjenester/porter.

3. Bruk streng passordpolicy for administratorkontoer og servicekontoer.

4. Endre standardpassord. Ikke godta at eksterne leverandører velger svake passord.

5. Beskytt privilegerte brukerkontoer ved å konfigurere «Protected Accounts»

6. Isoler driftsgrensesnitt i egne nettverk, slik at disse ikke er tilgjengelig for vanlige klientmaskiner.

7. Gjør regelmessig sårbarhetsskanning i interne nettverk.

8. Ha sikkerhetsovervåking ved hjelp av IDS og logganalyse.

9. Lag gode rutiner for å stille krav til og følge opp leverandører innen både IKT, AMS og SCADA.

10. Sørg for å avvikle systemer og tjenester som ikke lenger er i bruk.

11. Vurder fortløpende risikoreduserende tiltak som herding og segmentering for eldre systemer som ikke umiddelbart kan oppgraderes.

8.3 Spesifikke anbefalinger basert på studien

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. Mennesket vil alltid gjøre 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.

8.3.1 Lær av dine feil

Undersøkelsen viser 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. Virksomhetene må jobbe videre med dette. Dette er en tydelig forskjell fra NSRs Mørketallsundersøkelse 2016 [26], hvor 44% av virksomhetene gjorde endringer i organisasjonens policy og sikkerhetsrutiner, og 20% investerte i utvikling av sikkerhetsprosesser og etablerte et sikkerhetsmiljø.

Figur 16: Som et resultat av hendelsen, ble noen av de følgende endringene gjort i organisasjonen?
****Flere svar mulig***

Det er svært viktig å ta lærdom fra hendelser og gjennomføre nødvendige endringer i både systemet og innad i organisasjonen i etterkant. I forkant av en hendelse bør man foreta en risikoanalyse for å få avdekket sikkerhetshull, samt få på plass en god måte å håndtere hendelser på. Hendelseshåndtering må inngå i prosessen allerede før en hendelse inntreffer, dette for å minimere skade og for å få kontroll over situasjonen så raskt som mulig.

Tabell 3: Endring i organisasjon i etterkant av IKT-hendelse i norsk næringsliv (2015) [1] og norsk energisektor (2016)

Endringer i organisasjon etter hendelsen	**NSR, 2015**	**NVE, 2016**
Ingen	-	40%
Endring i policy	44%	21%
Investert i opplæringsprogram	15%	18%
Investert i sikkerhetsutstyr	25%	16%
Økt interne ressurser til sikkerhetsarbeid	-	14%
Sterkere kontroll av eksterne leverandører	19%	6%
Investert i utvikling av sikkerhetsprosesser	20%	3%
Vet ikke	-	3%
Disiplinære tiltak	-	2%
Leid inn tjenesteleverandører	20%	2%
Ansatt flere kompetente mennesker	3%	2%
Byttet leverandør	-	0%
Outsourcing av sikkerhetsfunksjonene	13%	0%

8.3.2 Innfør et styringssystem for informasjonssikkerhet

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

- Retningslinjer for sikker drift av IT-infrastruktur (patching, backup, herding endringskontroll, mm.)
- Planer for håndtering av de viktigste informasjonssikkerhetshendelsene
- Krav til gjennomføring av 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 NSRs Mørketallsundersøkelse 2014 og denne undersøkelsen [26]

En god måte å arbeide med informasjonssikkerhet på er å følge en standard som inkluderer punktene ovenfor. Ikke bare gjør disse standardene at sikkerhetsrisikoen innad i en organisasjon håndteres og styres, men overholdelse av standardene sender et viktig signal 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 på. Rammeverket gjør at sikkerhetsrisikoen blir kostnadseffektiv. Eksempler på standarder er:

- COBIT
- ISO 27000 Seriene
- NIST SP 800 Seriene
- IEC 62443

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

8.3.3 Bruk NSMs Grunnprinsipper for IKT-sikkerhet

NSMs grunnprinsipper for IKT-sikkerhet [25] definerer et sett med prinsipper for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser. Grunnprinsippene gjelder for både egen drift og når driften er satt bort til leverandører. De beskriver hva en virksomhet bør gjøre for å sikre et IKT-system, hvorfor det bør gjøres, men ikke hvordan. Grunnprinsippene kompletterer, men erstatter ikke en virksomhets sikkerhetsstyringsarbeid.

NSM peker på at viktige suksessfaktorer for å lykkes med implementering av grunnprinsippene er at ledelsen involverer seg, at man har sikkerhetskompetanse i virksomheten og etablerte styrings- og risikosløyfer. Utvelgelse av sikringstiltak bør videre baseres på det ordinære risikoarbeidet. Her vil grunnprinsippene hjelpe virksomhetene med å velge ut riktige sikringstiltak.

Grunnprinsippene til NSM er organisert i fire kategorier:

- Identifisere og kartlegge, dette innebærer å opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere. Utvikling av gode sikringstiltak er en kontinuerlig prosess.

- Beskytte, dette innebærer å ivareta en forsvarlig sikring av IKT-miljøet.

- Opprettholde og oppdage, dette innebærer å opprettholde den sikre tilstanden over tid og ved endringer, og oppdage sikkerhetstruende hendelser.

- Håndtere og gjenopprette, dette innebærer å håndtere sikkerhetstruende hendelser effektivt.

8.3.4 Start sikkerhetsarbeidet allerede med rekrutteringsarbeidet

Et første steg er sikkerhet i rekrutteringsfasen. Dette inkluderer bakgrunnssjekk med kontroll og sjekk av identitet, kontroll av attester, vitnemål og CV. Sikkerhetsarbeidet hos virksomhetens ansatte stopper ikke her, men er en del av det daglige arbeidet. Det er derfor viktig å sørge for tilstrekkelig opplæring, bevisstgjøring, god trening og motivasjon. Da kan ansatte forstå den digitale risikoen og kunne reagere riktig i henhold til rutiner og beredskapsplaner dersom uønskede IKT-hendelser oppstår i virksomheten. Man trenger god sikkerhetskultur i form av kunnskap og årvåkenhet for å være godt rustet til å forebygge og håndtere hendelser. Sikkerhetskultur er nødvendig hos alle profesjoner i virksomheten.

8.3.5 Bygg kunnskap og god sikkerhetskultur

Kunnskap og sikkerhetskultur må heves til et annet nivå, inn i andre fagområder og opp til ledernivå. Kunnskap og sikkerhetskultur er nødvendig i beslutningsprosesser og i administrative prosesser. Tidligere har en skyldt på de ansattes feilvurderinger og – handlinger. Det som er viktig er å fatte riktige beslutninger slik at en har kjøpt inn korrekt utstyr, valgt riktig teknologi, fått riktige krav inn i anbudsprosesser og kontrakter, m.m.

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 både for å forhindre hendelser og for å oppdage hendelser. Virksomhetene bør jevnlig sette fokus på farene ved virus, spydfisking og sosial manipulering [26], og gi nyansatte en skikkelig gjennomgang av sikkerhetsregelverk og rutiner. Virksomheten kan øke bevisstheten rundt dette temaet, både blant ledere og ansatte, ved å ha oversikt over rapporterte sikkerhetsbrudd, sikkerhetstruende hendelser som dataangrep eller virusinfeksjoner og nettverksaktivitet.

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*

WannaCrypt viste at leverandører av kontrollsystemer har ulike grader av «sense of urgency» og forberedelser til sikkerhetspatching av systemene som i mange år har vært ansett som sikre og avskjermet. Det er viktig å håndtere leverandører profesjonelt og stille krav til patching, at patcher sluppet fra Microsoft og andre skal være testet sentralt på systemenes ulike versjoner, eventuelt testet mot prosjektspesifikke tilpasninger av programvare.

8.3.6 Inkluder sikkerhet i IT-tjenestekjøp og tjenesteutsetting

Undersøkelsen indikerer en tydelig avhengighet av leverandører *(Figur 5-7*). Under en tredjedel av de 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. Avhengigheten av leverandører er viktig å ta inn over seg og både når det gjelder forebyggende sikkerhet og når det gjelder beredskap.

Resultatet av penetrasjonstestingen viser at sikkerheten ikke er tilstrekkelig ivaretatt i forbindelse med kjøp og utsetting av IT-tjenester til leverandører. Med tjenesteutsetting følger også digitale sårbarheter. Virksomhetene kan ikke sette bort sikkerhetsansvaret til en leverandør. Det vil derfor være en god ide å gjøre risikovurdering og sikkerhetsteste systemene før en setter ut tjenester, og videre sjekke sikkerhetstilstanden regelmessig også etter at tjenester er satt ut. Videre er det fornuftig å involvere leverandører i utvikling og øvelse av beredskapsplaner. Statistikken viser at relasjonen mellom leverandør og virksomhet er viktig.

8.3.7 Rapporter hendelser til KraftCERT

En siste anbefaling vil være å rapportere hendelser til KraftCERT [25], anmelde datakriminalitet til politiet og kontakte media. På denne måten vil vi kunne spre informasjon om pågående kampanjer og advare andre, lære mer fra hverandre og tilegne oss kunnskap om risikoen som følger med digitaliseringen.

Referanser

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

[2] NSM, «Risiko 2017. Risiko og sårbarheter i en ny tid. En vurdering av sårbarheter og risiko i Norge.,» Nasjonal sikkerhetsmyndighet (NSM), 2017.

[3] A. Cherepanvo, «www.welivesecurity.com,» 12 Juni 2016. [Internett]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf. [Funnet 28 Juli 2017].

[4] Dragos INC, «Dragos,» 13 Juni 2017. [Internett]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf. [Funnet 28 Juli 2017].

[5] E. Kovacs, «Securityweek,» 10 Juli 2017. [Internett]. Available: http://www.securityweek.com/template-injection-used-attacks-us-critical-infrastructure. [Funnet 2 August 2017].

[6] CIPProject, «Ci-project,» 11 Juli 2017. [Internett]. Available: https://www.ci-project.org/blog/2017/7/10/document-indicates-campaign-may-have-targeted-european-energy-and-critical-infrastructure-in-march-2017. [Funnet 02 August 2017].

[7] Microsoft, «Microsoft,» Microsoft, [Internett]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/ms691272(v=vs.85).aspx. [Funnet 3 August 2017].

[8] INFOSEC Institute, [Internett].

[9] S. Baird, E. Carter, E. Galinkin, C. Marczewski og J. Marshall, «Talos,» 7 Juli 2017. [Internett]. Available: http://blog.talosintelligence.com/2017/07/template-injection.html. [Funnet 2 August 2017].

[10] Kaspersky Lab, «Kaspersky,» 27 Juni 2017. [Internett]. Available:] https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/. [Funnet 2 August 17].

[11] Microsoft, «Microsoft TechNet,» Microsoft, 27 Juni 2017. [Internett]. Available: https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/. [Funnet 2 August 2017].

[12] Nasjonal Sikkerhetsmyndighet(NSM), «NSM Stat,» NSM, 27 Juni 2017. [Internett]. Available: https://nsm.stat.no/aktuelt/ny-ransomware-kampanje-observert/. [Funnet 2 August 2017].

[13] T. Fox-Brewster, «Forbes,» Forbes Staff, 03 Juli 2017. [Internett]. Available: https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#2cc2aaed6b89. [Funnet 02 August 2017].

[14] D. Maynor, A. Nikolic, M. Olney og Y. Younan, «Talos,» Talos, 05 Juli 2017. [Internett]. Available: http://blog.talosintelligence.com/2017/07/the-medoc-connection.html?m=1. [Funnet 03 August 2017].

[15] A. Islam, N. Oppenheim og W. Thomas, «FireEye,» 26 Mai 2017. [Internett]. Available: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html. [Funnet 08 August 2017].

[16] «Securelist,» GReAT, 28 Juni 2017. [Internett]. Available: https://securelist.com/schroedingers-petya/78870/. [Funnet 09 August 2017].

[17] P. Polityuk, O. Vukmanovic og S. Jewkes, «Reuters,» Reuters, 18 Januar 2017. [Internett]. Available: http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA. [Funnet 09 August 2017].

[18] ICS-CERT Industrial Control Systems Cyber Emergency Response Team, «ICS-CERT,» 25 Februar 2016. [Internett]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. [Funnet 10 August 2017].

[19] SIEMENS, «Siemens,» Siemens, 12 Juli 2015. [Internett]. Available: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-732541.pdf. [Funnet 28 Juli 2017].

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

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

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

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

[24] BDO AS, «FOU-Prosjekt 90160: Erfaringer fra penetrasjonstesting innen energiforsyningen(U.off),» BDO, 2017.

[25] NSM, NSMs grunnprinsipper for IKT-sikkerhet. Versjon 1.0., Oslo: Nasjonal sikkerhetsmyndighet (NSM), 2016.

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

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

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

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

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

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

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

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

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

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

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

Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no