Regulering av IKT- sikkerhet

Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor

Janne Hagen, Ola Hermansen, Øyvind Toftegård, Jon-Martin Pettersen, Roger Steen, Synnøve Lill Paulen

26
2017

RAPPORT

Rapport nr 26-2017
Regulering av IKT- sikkerhet

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør:

Forfattere: Janne Hagen, Ola Hermansen, Øyvind Toftegård, Jon-Martin Pettersen, Roger Steen, Synnøve Lill Paulen

Trykk: NVEs hustrykkeri
Opplag: 200
Forsidefoto: NVE
ISBN 978-82-410-1578-6
ISSN 1501-2832

Sammendrag: Digitalisering og teknologiskifte i energiforsyningen krever et reguleringsregime som dekker de digitale utfordringene dette medfører. Rapporten gir en vurdering av dagens IKT-sikkerhetsregulering og en anbefaling til et helhetlig sikkerhetsregime for IKT-sikkerhet i energiforsyningen.

Emneord: IKT-sikkerhet, cybersikkerhet, informasjonssikkerhet, SCADA-sikkerhet, regulering

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

31. mars 2017

Innhold

Forord **8**

Sammendrag **9**

Del I Innledning og problembeskrivelse **11**

1 Innledning **12**

1.1 Bakgrunn 12
1.2 Mandat 13
1.3 Avgrensninger 14
1.4 Viktige begreper 15
1.4.1 Informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet 15
1.4.2 Forsvarlig sikkerhetsnivå 16
1.4.3 Prosesskontroll, driftskontrollsystem mv 16
1.5 Rapportens oppbygging 18

2 Digitale verdikjeder og systemer **18**

2.1 Verdikjeden 18
2.1.1 Det fysiske systemet for elektrisk energi 18
2.1.2 Kontrollsystemer og styringssystemer 19
2.2 Markedet 24
2.2.1 Handelen 24
2.2.2 Markedsplassen 24
2.2.3 Balanseavregning 26
2.2.4 Distribusjon av måledata 27
2.2.5 Andre verdikjeder i markedet 28

3 Energiforsyningens digitale sårbarhet **28**

3.1 Farer og trusler mot digitale systemer i energisektoren 28
3.1.1 Et mangfoldig fare- og trusselbilde 28
3.1.2 Målrettede trusler fra mennesker 29
3.2 Administrative systemer 31
3.2.1 Digitale sårbarheter i administrative systemer 31
3.2.2 Sikring av administrative systemer 35
3.3 Produksjonsanlegg, driftskontroll og nett 36
3.3.1 Digitale sårbarheter i lokalkontrollanlegg 36
3.3.2 Digitale sårbarheter i driftskontrollsystemer 37
3.3.3 Sikring av driftskontrollsystemer 38
3.4 Endret risikobilde med innføring av ny teknologi 41
3.5 Utilsiktet risiko i markedet 42
3.5.1 Konsentrasjonsrisiko 42
3.5.2 Komplekse interaksjoner og tette koblinger 44
3.5.3 Konsentrasjonsrisiko i energisektoren 44
3.6 Mangel på incentiver til å utvikle sikker programvare 46

Del II Internasjonale og nasjonale føringer **48**

4 Internasjonale føringer for energisektoren **49**

4.1 Initiativer og føringer fra EU 49

4.1.1 Europeisk program for beskyttelse av kritisk infrastruktur 49
4.1.2 EUs cyber security strategi 50
4.1.3 NIS-direktivet fra EU 51
4.1.4 EUs tredje energimarkedspakke 52
4.1.5 EUs initiativ for elektrisitets- og gassmarkeder i Europa 54
4.1.6 EUs tiltakspakke for ren energi 55
4.2 Beredskapssamarbeid i Norden 56
4.3 Nato og energiforsyningssikkerhet 56
4.4 The Federal Energy Regulatory Commission (USA) 57
4.5 Danmark 59

5 Digitaliseringspolitikk i Norge 60

5.1 Nasjonal IKT-politikk 60
5.2 Nasjonal modell for håndtering av IKT-hendelser 61
5.3 Nasjonal politikk for bruk av skytjenester 62
5.4 Nasjonalt grenseforsvar 64
5.5 Bruk av droner i Norge 65

Del III Regelverk og normer 67

6 Regelverk for IKT i energisektoren 68

6.1 Innledning 68
6.2 Sikkerhet- og beredskapsregler 68
6.2.1 Utviklingen 68
6.2.2 Energiloven 69
6.2.2.1 Kraftforsyningens beredskapsorganisasjon 69
6.2.2.2 § 9-2 Beredskapstiltak 70
6.2.2.3 § 9-3 Informasjonssikkerhet 71
6.2.3 Beredskapsforskriften 72
6.2.3.1 Forskriftens virkeområde og oppbygning 72
6.2.3.2 Kapittel 2 Generelle krav 73
6.2.3.3 Kapittel 5 Klassifiserings- og sikringstiltak 74
6.2.3.4 Kapittel 6 Informasjonssikkerhet 75
6.2.3.5 Kapittel 7 Sikring av driftskontrollsystemer 75
6.2.4 Energilovforskriften 76
6.2.4.1 Innledning 76
6.2.4.2 Krav til kompetanse 76
6.2.4.3 Kompetansekrav 76
6.2.5 Måle- og avregningsforskriften 76
6.2.5.1 Innledning 76
6.2.5.2 Styringsfunksjonalitet og sikkerhet 77
6.2.6 Damsikkerhetsforskriften 79
6.2.6.1 Innledning 79
6.2.6.2 § 7-8 Informasjonssikkerhet 79
6.2.7 Systemansvarsforskriften 80
6.2.7.1 Innledning 80
6.2.7.2 Myndighet og kontrollansvar knyttet til systemansvaret . 81
6.2.7.3 Konsekvenser av et mer digitalisert kraftmarked 81

7 Sektorovergripende regelverk for IKT-sikkerhet 82

7.1 Innledning 82
7.2 Sikkerhetsloven 82
7.2.1 Gjeldende lov 82
7.2.2 Forslaget til ny lov om forebyggende nasjonal sikkerhet 83
7.3 Personopplysningsloven 85
7.4 Forvaltningsloven.....86
7.5 Arkivloven 86
7.6 Bokføringsloven 87

8 Regler for IKT-sikkerhet i andre sektorer 88

8.1 El-tilsyn 88
8.2 Olje- og gass.....88
8.3 Elektronisk kommunikasjon.....89
8.4 Finans.....90

9 Standarder og veiledninger 91

9.1 Innledning 91
9.2 Internasjonale standarder og veiledere 91
9.2.1 Generell IKT-sikkerhet 91
9.2.2 Driftskontrollsystemer.....91
9.3 Nasjonale standarder og veiledere.....93
9.3.1 Generell IKT-sikkerhet 93
9.3.2 Sikkerhet i driftskontrollsystemer.....94

Del IV Vurderinger og anbefalinger til endringer i regelverk..... 95

10 Vurderinger til endringer i regelverket 96

10.1 Innledning 96
10.2 Vurdering av funksjonskrav eller spesifikke krav 97
10.2.1 Innledning.....97
10.2.2 Eksempel på bruk av funksjonsbasert regelverk.....97
10.2.3 Arbeidsgruppens vurderinger.....98
10.3 Vurdering av bruk av standarder eller forskriftskrav.....100
10.3.1 Innledning.....100
10.3.2 Arbeidsgruppens vurdering.....101
10.4 Vurdering av kompetansekrav, utdanning og veiledning.....102
10.4.1 Innledning.....102
10.4.2 Eksempler på internasjonale krav til kompetanse 102
10.4.3 Eksisterende nasjonale kompetansekrav for energiforsyningen 103
10.4.4 Eksisterende kompetansekrav i damsikkerhetsforskriften104
10.4.5 Arbeidsgruppens vurdering om kompetansekrav.....104
10.5 Vurdering av tjenesteutsetting, leverandørkjeder og fjernaksess106
10.5.1 Innledning.....106
10.5.2 Problemstillinger knyttet til tjenesteutsetting 106
10.5.3 Eksisterende regulering av tjenesteutsetting i energiforsyningen.....107
10.5.4 Arbeidsgruppens vurdering.....109
10.6 Vurdering av overvåkning, rapportering og hendelseshåndtering111

10.6.1 Innledning ... 111
10.6.2 Problemstillinger ... 111
10.6.3 Eksisterende regulering ... 111
10.6.4 Arbeidsgruppens vurdering ... 113

11 Anbefalinger til endringer i regelverket ... 115

11.1 Innledning ... 115
11.2 Anbefaling om overordnet sikkerhetsregime ... 116
11.2.1 Innledning ... 116
11.2.2 Arbeidsgruppens anbefaling ... 116
11.3 Anbefaling om sikringsplikt for informasjonssystemer ... 118
11.3.1 Innledning ... 118
11.3.2 Problemstilling ... 119
11.3.3 Eksisterende regulering ... 119
11.3.4 Arbeidsgruppens anbefaling ... 120
11.3.4.1 Behov for generelle krav til IKT-sikkerhet i energibransjen 120
11.3.4.2 Hvem skal kravene være rettet mot? ... 121
11.3.4.3 Grunnsikring IKT-sikkerhet ... 123
11.3.4.4 Logging og overvåking ... 124
11.3.4.5 Tjenesteutsetting ... 124
11.3.4.6 Dokumentasjon ... 124
11.3.4.7 Varsling og rapportering ... 125
11.3.4.8 Hendelseshåndtering og beredskap ... 125
11.3.4.9 Hvordan bør kravene implementeres? ... 125
11.3.4.10 Økonomiske og administrative konsekvenser av forslaget 126
11.4 Anbefaling om AMS- og målekjeden ... 126
11.4.1 Innledning ... 126
11.4.2 Problemstilling ... 127
11.4.3 Eksisterende regulering ... 127
11.4.4 Arbeidsgruppens anbefaling ... 128
11.4.4.1 Behov for ny regulering ... 128
11.4.4.2 Konkret forslag til regulering ... 129
11.4.4.3 Økonomiske og administrative konsekvenser av forslaget 130
11.5 Anbefaling om industrielle kontrollsystemer og driftskontrollsystemer 131
11.5.1 Innledning ... 131
11.5.2 Problemstilling ... 131
11.5.3 Eksisterende regulering ... 132
11.5.4 Arbeidsgruppens anbefaling ... 134
11.5.4.1 Behov for regulering ... 134
11.5.4.2 Konkret forslag til regulering ... 134
11.5.4.3 Økonomiske og administrative konsekvenser av forslaget 135

Del V Vedlegg ... 136

12 Vedlegg 137
12.1 Arbeidsmetode og informasjonsgrunnlag 137
12.2 Forkortelser og ordliste.....138
12.3 Standarder og veiledere 141
12.3.1 Kvalitetsledelse generelt.....141
12.3.2 IKT-ledelse/styringssystemer.....142
12.3.3 Informasjonssikkerhetsledelse.....142
12.3.4 Risikostyring 144
12.3.5 Kriseledelse.....147
12.3.6 Skytjenester.....147
12.3.7 Sikkerhet i SCADA og kritisk infrastruktur 148
12.3.8 Kommunikasjon generelt 150
12.3.9 Trådløs kommunikasjon.....152
12.3.10 Kryptering 153
12.3.11 Hashing 154
12.3.12 HAN port AMS (Referanser anbefales av NVE i dag) 154
12.3.13 Kartlegging av sårbarheter 155
12.3.14 Krav om internkontroll i det norske regelverket 155
13 Metode for vurdering av tiltak 156
13.1 Krav til utredninger av tiltak 156

Forord

NVE har i perioden april 2016 til mars 2017 gjort en gjennomgang av regelverket på IKT-sikkerhet i energisektoren. Denne rapporten ser nærmere på behovet for revisjon av forskriftene som regulerer IKT-sikkerhet i energiforsyningen. Rapporten er også en oppfølging av Lysne-utvalgets anbefaling til NVE om å gjennomgå sektorregelverket og se på funksjonsbasert regelverk og bruk av standarder.

Energiloven gir alle selskap med vesentlig betydning for produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi eller fjernvarme plikt til å sørge for effektiv sikring og beredskap mot ekstraordinære hendelser. Denne plikten inkluderer IKT-sikkerhet. Beredskapsforskriften er en presisering av sikrings- og beredskapsplikten i energiloven. I tillegg til beredskapsforskriften har damsikkerhetsforskriften og måle- og avregningsforskriften krav om beskyttelse av informasjon.

Et godt regelverk er et viktig verktøy for tilsynsmyndigheten. Det er kun gjennom veiledning og tilsyn i henhold til klare krav at NVE kan bidra til at det skapes en norm for et forsvarlig nivå på IKT-sikkerhet i energisektoren. En god forskrift, som inngår i et helhetlig sikkerhetsregime, kan bidra til at risikoen blir redusert. Det vil likevel finnes en restrisiko som det må dekkes opp for i beredskapsplaner og beredskapstiltak. Også dette forholdet dekkes av regelverket.

Prosjektet har vært gjennomført over en periode på ett år der bransjen, leverandører, interesseorganisasjoner og andre myndigheter har gitt innspill. Jeg vil med dette takke alle som har bidratt til arbeidet. Rapporten vil bli sendt ut for kommentarer og NVEs ledelse skal deretter skal ta stilling til hvordan forslagene følges opp.

Oslo, 28. mars 2017.

Per Sanderud
Vassdrags- og energidirektør

Sammendrag

Norge har i dag en god forsyningssikkerhet av energi. Både drift og marked for strøm og fjernvarme er avhengig av fungerende driftskontrollsystemer og administrative IT-systemer, som igjen henger på digitale verdikjeder som krysser landegrenser. Utrullingen av digitale målere hos norske strømkunder og bruk av droner gir muligheter for å effektivisere driften av distribusjonsnettet, for distribuert energiproduksjon, for utvikling av tjenester til forbrukere og trygg inspeksjon av linjer. I fremtiden kan energiforsyningen bli enda mer automatisert. Denne utviklingen gir betydelige bidrag til verdiskapningen og bidrar til økt forsyningssikkerhet.

Den digitale utviklingen både i energisektoren og samfunnet for øvrig medfører også en endring i energisystemets risiko- og sårbarhetsbilde. Energisektoren kan som andre sektorer angripes gjennom internett av anonyme aktører. Feil i programvare er en annen faktor som kan få konsekvenser for virksomhetenes drift. Utrykket «liten tue kan velte stort lass» er svært relevant i en digitalisert verden der system og komponenter er koplet sammen i nettverk. Tillit til de digitale systemene er vesentlig for et velfungerende energimarked. Denne tilliten bygges gjennom blant annet sikkerhetsmekanismer, som reduserer risikoen for svikt og feil i IT-systemene. Skal tilliten bevares også i framtiden, er det nødvendig med et helhetsfokus på sikring av alle digitale systemer i energisektoren.

I rapporten gir en arbeidsgruppe i NVE anbefalinger om å styrke arbeidet med å håndtere risikoen som følger med digitalisingen av energiforsyningen. Energibransjen består av selskap med enerett (nettselskap) og markedsaktører (produsenter av energi, kjøpere og selgere av energi, og andre tredjeparter). Selv om reguleringen for øvrig er forskjellig mellom monopol og marked, er det på området IKT- sikkerhet felles utfordringer som tilsier at det bør være et minste fellesnivå av IKT-sikkerhet. Mandatet peker ut noen tema særskilt; logging, skytjenester, fjerntilgang til systemer og brytefunksjonen i digitale målere. Arbeidsgruppen har ikke drøftet problemstillingen om formell utnevnelse av et sektorvis responsmiljø. Dette ivaretas i en egen prosess. I dag ivaretar KraftCERT en responsfunksjon for energisektoren der medlemskap er frivillig. KraftCERT er KBO-enhet.

Rapporten viser at selv om dagens regelverk i stor grad samsvarer med internasjonale standarder og praksis, er det behov for en ytterligere presisering av regelverket slik at virksomheter og systemer i energisektoren skal være beskyttet mot bredden av digitale trusler. Rapportens del IV gir en nærmere redegjørelse for vurderinger og anbefalinger.

<u>Anbefalinger:</u>

På bakgrunn av de vurderingene arbeidsgruppen har gjort har arbeidsgruppen kommet med følgende hovedanbefalinger.

- *Arbeidsgruppen anbefaler at NVE utarbeider krav til informasjonssikkerhet i henhold til et overordnet sikkerhetsregime, som plasserer informasjonssikkerhet som en del av det helhetlige arbeidet med forebyggende sikkerhet og beredskap i energiforsyningen.* Forsyningssikkerhet er komplisert og krevende å forvalte. Det underliggende temaet sikkerhet og beredskap skal sørge for en helhetlig forebygging, håndtering og begrensning av virkningene av ekstraordinære

situasjoner i energiforsyningen. Krav til sikring av informasjonssystemer må derfor kunne passe inn i et sett av krav som omfatter blant annet helhetlig sikkerhetsstyring, sikring av informasjon og fysisk sikring av anlegg.

- *Arbeidsgruppen anbefaler en tydeliggjøring av den generelle sikringsplikten mot uønskede hendelser og handlinger i dagens krav. Arbeidsgruppen anbefaler at det stilles krav til grunnsikring for alle digitale informasjonssystemer hos aktører som har anlegg eller system av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme i energiforsyningen*. Arbeidsgruppen anbefaler at dette gjøres ved å etablere funksjonskrav for informasjonssystemer som sørger for et minstenivå på informasjonssystemsikkerhet. De digitale støttesystemene til virksomhetene i energiforsyningen får økende betydning for driften. Kravet bør gjelde alle nettselskaper, omsettere, produsenter og andre aktører som til sammen kontrollerer produksjon på over 25 MW. Arbeidsgruppen anbefaler at de generelle kravene omfatter krav til logging og logganalyse og krav til sikkerhet ved tjenesteutsetting.

- *Arbeidsgruppen anbefaler at systemer der avbrudd har større konsekvens for forsyningssikkerheten har noe strengere sikringskrav enn den anbefalte generelle grunnsikringen. Bryterfunksjonen i digitale strømmålere bør sikres særskilt med tiltak som begrenser uautorisert tilgang og manipuleringsmuligheter.* Arbeidsgruppen anbefaler at det bør fjernes fra regelverket at annen informasjon enn måledata skal kunne gjøres tilgjengelig via HAN port, da dette ikke er nødvendig og kun bidrar til en mindre sikker løsning. Prisinformasjon kan på en enkel måte i stedet sendes over vanlig internett til enheter som mobiltelefoner, PCer og annet internett-tilkoblet utstyr. For å utføre et effektivt tilsyn med sikkerhet i AMS er det behov for konkrete krav om sikkerhetstiltak som nettselskapene må følge opp. Dette kan løses gjennom å klargjøre i veilederen hva NVE anser som minimumskrav til sikkerhet i AMS.

- *Arbeidsgruppen anbefaler at driftskontrollsystemer har strengere sikringskrav enn grunnsikring, og at det tas hensyn til driftskontrollsystemenes særegenhet med krav til særlig integritet og tilgjengelighet. Dette innebærer at systemer som overvåker og styrer energiforsyningen, for eksempel dagens driftskontrollsystemer, beholder dagens sikkerhetsnivå for driftskontrollsystemer.* Arbeidsgruppen anbefaler at sikkerhetsnivået for disse systemene følger systemenes klasser, som i dag. Arbeidsgruppen har vurdert at det kan være behov for mindre endringer i ordlyden i kravene.

- Arbeidsgruppen mener videre at det bør lages en veileder på IKT-sikkerhet til beredskapsforskriften der NVE i større grad enn i dag henviser til og bruker begreper fra internasjonale standarder.

Del I Innledning og problembeskrivelse

1 Innledning

1.1 Bakgrunn

Vi har fra 2000-tallet og frem til i dag registrert en betydelig politisk interesse for sårbarhetsreduksjon innen IKT-sikkerhet. Sårbarhetsutvalget i 2000 (Willoch)[1] var først ut med en helhetlig analyse av samfunnets sårbarhet, deretter fulgte Infrastrukturutvalget i 2006 (Ullring)[2] med blant annet fokus på eierskap, og sist Digitalt sårbarhetsutvalg i 2015 (Lysne)[3]. NOU 2015:13 Digital sårbarhet – sikkert samfunn, trekker opp noen hovedtrekk hva angår framtidig utvikling i sårbarhetsbildet. Rapporten vektlegger sårbarhetsutfordringer som følger med lange digitale verdikjeder. Sikkerheten i selskapenes IT-systemer blir ikke bedre enn «det svakeste leddet» i verdikjeden.

Det er i Norge og Europa et økende politisk og kommersielt ønske om å ta i bruk og utnytte mulighetene som digitaliseringen gir. Politikerne har ambisjoner om å fornye, forenkle og forbedre samfunnet, samtidig som innbyggere og næringsliv har forventninger om en enklere hverdag og nye og bedre tjenester. IKT kan bidra til å oppnå disse ambisjonene, men da må tillit til teknologi være tilstede. Nøkkelen til tillit er sikkerhet.

Norges vassdrags- og energidirektorat (NVE) skal påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav[4]. Utvikling i EUs regelverk for IKT-sikkerhet i energisektoren, det nasjonale arbeidet med ny sikkerhetslov og IKT-politikk (Digital agenda for Norge) gir føringer for NVEs arbeid med IKT-sikkerhet i energisektoren. Parallelt med disse regulatoriske endringene går energisektoren igjennom et digitalt teknologiskifte som fører til at sektoren kan bli utsatt for nye typer trusler.[5] NVE etablerte derfor i 2016 et regelutviklingsprosjekt der en arbeidsgruppe og en styringsgruppe ble gitt i mandat å utrede behovet for regelverksendringer for å ivareta IKT-sikkerheten i energiforsyningen. Denne rapporten dokumenterer arbeidet og anbefalingene.

Arbeidsgruppen har bestått av Janne Hagen prosjektleder (TBB), Roger Steen (TBB) til 01.12.2016, Jon-Martin Pettersen, (TBB), Arne Venjum, (ETS), Heidi Kvalvåg, (ETS) til

---

[1] Et sårbart samfunn Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet, NOU 2000: 24. https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf besøkt 05.03.2017.

[2] Når sikkerheten er viktigst Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner NOU 2006:6, https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf besøkt 05.03.2017.

[3] Digital sårbarhet – sikkert samfunn Beskytte enkeltmennesker og samfunn i en digitalisert verden, nou Norges offentlige utredninger 2015: 13, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf besøkt 05.03.2017.

[4] Tildelingsbrev til Norges vassdrags- og energidirektorat, https://www.regjeringen.no/contentassets/98bccb1372ab47c99cc0a08e25752066/tildelingsbrev-til-norges-vassdrags--og-ernergidirektorat-for-2016.pdf, besøkt 13.02.2017.

[5] Hagen, J., Teknologiskifte i energiforsyningen. Studie om muligheter og sårbarheter, NVE-rapport 118 2015, http://publikasjoner.nve.no/rapport/2015/rapport2015_118.pdf besøkt 05.03.2017.

12.08. 2016, Øyvind A. Arntzen Toftegaard (ETS) fra 1. juli 2016 og til prosjektslutt, Synnøve Lill Paulen, (EK) og Ola Hermansen (AJ).

Styringsgruppen har bestått av Vassdrags- og energidirektør Per Sanderud, avdelingsdirektør Anne Vera Skrivarhaug, Energiavdelingen (E), avdelingsdirektør Ove Flataker, Elmarkedstilsynet (ET), avdelingsdirektør Ingunn Åsgard Bendiksen, Tilsyn og beredskap (TB) og seksjonsleder Anne Rogstad, Juridisk (AJ).

Prosjektarbeidet bygger på informasjon innhentet gjennom workshops og dialog med bransjen, bransjeforeninger og andre myndigheter, samt Nato og EU. Det vises til Del V, kapittel 12.1 for nærmere detaljer.

1.2 Mandat

Arbeidsgruppen skal utrede behovet for regelverksendringer for å ivareta IKT-sikkerheten i energiforsyningen.

Arbeidsgruppen skal beskrive hvilke forskrifter NVE forvalter som nå eller i nær framtid, gitt forventet teknologisk utvikling, vurderes som aktuelle for å målbære nye krav til IKT-sikkerhet.

Arbeidsgruppen skal, som bakteppe for arbeidet, redegjøre for prosesser og hovedstrømninger internasjonalt som viser utviklingen i andre land, herunder EU.

Arbeidsgruppen skal underveis i arbeidet ha dialog både med relevante aktører, bransjefora, leverandørindustri og bransjeforeninger og med relevante myndigheter slik som PST, NSM og E-tjenesten.

Et sentralt spørsmål er hvilke bestemmelser som bør inn og hvor de bør plasseres. NVE har i dag tre forskrifter som regulerer IKT-sikkerhet:

- Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften) FOR-2012-12-07-1157[6]
- Forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften) (FOR-2009-12-18-1600) § 7-8 Informasjonssikkerhet,[7]
- Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv (måle- og avregningsforskriften).[8]

Arbeidsgruppen skal vurdere:

- Beskyttelse av bryterfunksjonalitet i avanserte måle- og styringssystemer (AMS)

---

[6] Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften) FOR-2012-12-07-1157, https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157?q=beredskapsforskriften, besøkt 22.10.2016.

[7] Forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften), https://lovdata.no/dokument/SF/forskrift/2009-12-18-1600 besøkt 22.10.2016.

[8] Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. https://lovdata.no/dokument/SF/forskrift/1999-03-11-301 besøk 05.03.2017.

- Bruk av automatisk overvåkning og styring av ressurser i distribusjonsnettet
- Bruk av skytjenester og andre forhold som kan påvirke driftskontrollfunksjoner
- Fjernaksess for feilretting mv. av viktige system, særlig fra leverandører i utlandet
- Overvåkning, logging og analyse av datatrafikk i driftskontrollsystemer for å avdekke skadelig aktivitet (omfang, krav til oppbevaring, kompetanse til å lese logger)
- Foreta kostnyttevurderinger knyttet til de ulike sikkerhetskravene som drøftes

Arbeidsgruppen har tolket mandatet til å foreslå om det trengs endring, hvilke bestemmelser som må endres/fjernes/legges til og hvor endringen skal skje.

1.3 Avgrensninger

Selv om fysisk sikring og personellsikkerhet er viktige premisser for å beskytte også IKT og prosesskontrollsystemer, går arbeidsgruppen ikke inn og vurderer de detaljerte kravene til fysisk sikring av anlegg i beredskapsforskriften. Arbeidsgruppen legger til grunn for sine vurderinger at sikkerhetsregimet rundt fysisk sikring i beredskapsforskriften består som i dag.

KBO-enheter er virksomheter som ved vedtak i henhold til bfe §3-3 er utnevnt av NVE til å ha en spesiell rolle i krise og krig. De er valgt ut pga. sin viktige posisjon i sektoren. Arbeidsgruppen har tatt utgangspunkt i at KBO er en veletablert organisasjon med lang tradisjon, som fungerer som informasjonsdelings- og samhandlingsarena i bransjen og opp mot myndigheten. Denne samhandlingen er viktig også når det gjelder IKT-sikkerhet. NVE kan i dag gjennom vedtak bestemme at en virksomhet skal være en KBO-enhet. Hele beredskapsforskriften gjelder for KBO-enheter.

Arbeidsgruppen har ikke drøftet problemstillingen om formell utnevnelse av et sektorvis responsmiljø. Dette ivaretas i en egen prosess. Nasjonal strategi for informasjonssikkerhet, nasjonalt operativt rammeverk for digital hendelseshåndtering og NIS-direktivet legger opp til at det skal finnes et sektorvis responsmiljø også for energisektoren. Arbeidsgruppen har vurdert at dette er et viktig tema, men at en formalisering av et sektorvis responsmiljø for energisektoren, hva det skal gjøre og hvordan det skal organiseres, ligger utenfor dette prosjektmandatet. I dag ivaretar KraftCERT en responsfunksjon for energisektoren der medlemskap er frivillig. KraftCERT er KBO-enhet.

I dag er opprettholdelsen av forsyningssikkerhet indirekte regulert gjennom energilovens § 1-2 (Formål), § 9-1 (Kraftforsyningens beredskapsorganisasjon) og § 9-2 (Beredskapstiltak). Forsyningssikkerhet har alltid vært viktig i bransjen, både før og etter at energiloven ble innført.

Arbeidsgruppen har kun gjennomført overordnede vurderinger av kostnytte. Dette skyldes manglende datagrunnlag for tiltak og kostnader ved uønskede IKT-hendelser. Fordeler og ulemper er derimot kommentert.

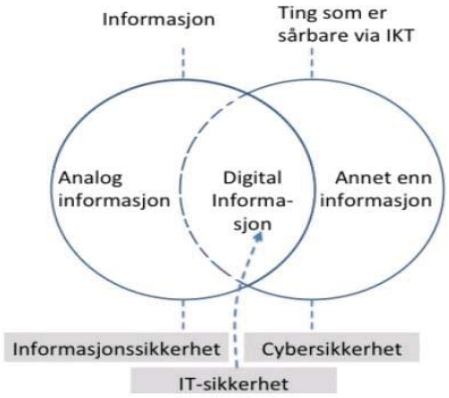
1.4 Viktige begreper

1.4.1 Informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet

Informasjonssikkerhet har med sikring av informasjon å gjøre, uavhengig av om den er lagret digitalt eller ikke. Det handler om å beskytte tilgjengelighet til informasjon, integriteten til informasjon (at ingen kan urettmessig endre innhold) og konfidensialiteten til informasjon (kun de med rettigheter kan få tilgang til informasjon).

IKT-sikkerhet har med sikring av informasjons- og kommunikasjonsteknologi å gjøre – altså maskinvare og programvare. Grunnen til at IKT-sikkerhet og informasjonssikkerhet ofte blir brukt om hverandre, er nok at mye informasjon er lagret og formidlet ved hjelp av IKT. For å beskytte slik informasjon, må man beskytte teknologien den er lagret og formidlet på. IT-sikkerhet har å gjøre med sikring av informasjonsteknologi. I praksis er det ingen forskjell på IKT-sikkerhet og IT-sikkerhet.

Cybersikkerhet handler om beskyttelse av ting som er sårbare gjennom IKT. En rekke fysiske komponenter er sårbare via IKT. Når styringssystemene til et kraftverk er IKT-basert, kan kraftverket fysisk skades via programvare. Med IKT kan man åpne vann-slusene i et vannkraftverk eller øke temperaturen i kjølesystemet til et kjernekraftanlegg.[9] God IKT-sikkerhet alene er ikke tilstrekkelig for å oppnå god cybersikkerhet. «Ikke-digitale» sikringstiltak som adgangskontroll, prosedyrer, konsekvensreduserende tiltak (f.eks. mekaniske vern) og økt kompetanse og bevisstgjøring vil også være viktige sikringstiltak.



Figur 1.1 Informasjonssikkerhet, IT-sikkerhet og cybersikkerhet[10]

Informasjonssystem er et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon.[11] Dette inkluderer alle organisatoriske, administrative og

---

[9] Informasjonssikkerhet, cybersikkerhet, datasikkerhet – hva er forskjellen?, CCIS, https://ccis.no/nb/informasjonssikkerhet-cybersikkerhet-datasikkerhet-hva-er-forskjellen/, besøkt 10.12.2016.

[10] Informasjonssikkerhet, cybersikkerhet, datasikkerhet – hva er forskjellen, NTNU CCIS, https://ccis.no/nb/informasjonssikkerhet-cybersikkerhet-datasikkerhet-hva-er-forskjellen/, publisert besøkt 21.02.2017

[11] Falkenberg, Eckhard D. (1998). *A framework of information systems concepts*. IFIP WG 8.1.
Langefors, Börje (1968). *Theoretical analysis of information systems*. Studentlitteratur.
Sølvberg, Arne (2012). *Information systems engineering: an introduction*. Springer Science & Business Media.

tekniske komponenter for at systemet skal fungere. Informasjonssystemsikkerhet handler om å beskytte informasjonssystemet. Dette omfavner derfor både IKT-sikkerhet der IT-systemer er en del av informasjonssystemet, men også alle organisatoriske og administrative deler av systemet.

1.4.2 Forsvarlig sikkerhetsnivå

Virksomhetene som NVE regulerer er ansvarlig for at egne systemer er sikret tilstrekkelig og at sikkerhetsnivået samsvarer med krav i lov og forskrift. Begrepet «forsvarlig sikkerhet» er brukt av både Nasjonal kommunikasjonsmyndighet og Tråvik-utvalget. Sikkerhetsnivået er ikke kun bestemt av regelverket, men av flere faktorer, herunder risikoanalysen til virksomheten og markedspraksis i bransjen. Tråvik-utvalget har også påpekt at ved vurderingen av hva som er forsvarlig sikkerhet, vil virksomhetene videre måtte se hen til gjensidige avhengigheter og virksomhetens støttende rolle.[12]

Arbeidsgruppen mener at dagens klassifiseringsregime og krav til driftskontrollsystemer samsvarer med forståelsen av begrepet forsvarlig sikkerhet. Arbeidsgruppen vurderer derfor at begrepet forsvarlig sikkerhet i denne rapporten kan forstås som en rettslig standard der sikkerhetsnivået i første rekke bygger på virksomhetenes risiko- og sårbarhets (ros)-analyser, utført i tråd med kravene til slike analyser, og markedspraksis i bransjen. Virksomheten kan ikke bruke ros-analyser til å senke eget sikkerhetsnivå. I tillegg vil regelverket sette en minstestandard. NVE vil kunne treffe vedtak om sikring eller vedtak om retting der virksomheten ikke har en praksis som tilfredsstiller regelverket, og på denne måten påvirke nivået på forsvarlig sikkerhet.

1.4.3 Prosesskontroll, driftskontrollsystem mv

Prosesskontrollsystemer er definert av ISO/IEC TR 22019 som systemer som støtter, kontrollerer og overvåker produksjon, overføring, lagring og distribusjon av elektrisk kraft og varme i kombinasjon med kontroll av eventuelle støtteprosesser. Dette inkluderer:

- Enhver IT-støttet sentral eller distribuert prosesskontrollsystem, overvåkning og automasjonsteknologi og IT-systemer brukt til drift, slik som programmering og parametersetting
- Digitale kontrollenheter og automasjonskomponenter, slik som kontroll- og feltkomponenter eller programmerbare logiske styringsenheter (PLC)er[13], inkludert digitale sensorer og aktuarer

---

[12] NOU 2016:19, *Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Kapittel 2.5 Beskyttelse av infrastruktur, https://www.regjeringen.no/contentassets/816d557c6ab24493a1101837cc2e1cf8/nou-2016-19-samhandling-for-sikkerhet.pdf, besøkt 03.11.2016.

[13] Programmable Logic Controller.

- Alle andre IT-system som er benyttet til prosesskontrollen, for eksempel til visualisering av oppgaver og for kontroll, overvåkning, data arkivering og dokumentasjon
- All kommunikasjonsteknologi brukt i prosesskontroll, inklusive nettverk, telemetri, telekontroll applikasjoner og fjernstyringsteknologi
- Digital måling og målekomponenter, for eksempel for å måle energiforbruk, produksjon og utslippsverdier
- Digitale sikringssystemer (for helse, miljø og sikkerhet), inklusive beskyttelse av relé og sikring av PLCer, og komponenter til framtidens smarte nett
- All programvare og fastvare installert på systemene nevnt ovenfor.Konvensjonelle, klassiske rene elektromekaniske komponenter og energistyringssystemer for private husholdninger faller utenfor definisjonen til ISO/IEC TR 27019.

Beredskapsforskriften opererer med begrepet driftskontrollsystem (DKS). Dette begrepet favner videre enn ISO/IEC TR 27019 sin definisjon av prosesskontrollsystem. Det tydeligste skillet er at elektromekaniske komponenter ikke er ekskludert slik som i standarden, og at alle støttesystemer som nødstrøm, ventilasjon, kjøling, samt driftssentraler, inklusive datarom er inkludert. I veilederen til beredskapsforskriften (2013), § 7-1. «*Generell plikt til å beskytte driftskontrollsystemet*» er det beskrevet at virksomheten selv er ansvarlig for å definere hva som inngår i driftskontrollsystemet.[14] Det betyr at dersom virksomheten etablerer nye koblinger mellom driftskontrollsystemet og andre typer system, eller innfører nye system som kan ha innvirkning på driftskontrollsystemets funksjonalitet, er det viktig å gjøre en vurdering av hvorvidt dette også skal inkluderes som en del av driftskontrollsystemet.

Videre skal driftskontrollsystemet opprettholde driftskontrollfunksjonen. I beredskapsforskriften er begrepet driftskontrollfunksjon benyttet flere steder. Dette forstås ifølge veilederen til bfe § 7-1 som følgende: *«Alle organisatoriske, administrative og tekniske tiltak for å overvåke og styre anlegg i energiforsyningen.»*

Lokalkontrollanlegg styrer og overvåker ett enkelt anlegg i energiforsyningen.

SCADA står for Supervisory Control And Data Acquisition systems, og er en annen benevnelse på et prosesskontrollsystem som strekker seg over store geografiske avstander.

DMS står for Distribution Management System, og kan forstås som et overvåkningssystem for distribusjonsnettet, og dersom det styrer fysiske prosesser, også som et prosesskontrollsystem.

KIS er forkortelse for kunde-informasjonssystem.

AMS er forkortelse for avanserte måle- og styringssystemer.

---

[14] *Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen*, Nr 1 2013, NVE, s 150, http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf besøkt 05.03.2017.

1.5 Rapportens oppbygging

Rapporten er inndelt i fem deler.

Del 1 gir innledning og bakgrunnsinformasjon for prosjektet, en beskrivelse av prosjektgruppen og definisjon av viktige begreper. I tillegg gis en overordnet introduksjon til sektorens digitale sårbarhet. Dette danner grunnlaget for vurderingen av behov for sikringstiltak og regulering.

I del 2 gis en oversikt over nasjonale og internasjonale føringer. Dette gjelder særlig EUs regelverk og beredskaps- og sikkerhetssamarbeid med andre nordiske land og med Nato. I tillegg omtales digitaliseringspolitikken i Norge.

Del 3 omhandler regelverk og normer. Det inkluderer gjeldende regulering av IKT-sikkerhet i energisektoren. I tillegg presenteres sektorovergripende regelverk og andre sektorers regulering av IKT-sikkerhet. Til slutt omtales viktige standarder og sentrale veiledere.

Del 4 inneholder arbeidsgruppens vurderinger og anbefalinger. Her drøftes ulike tema som bruk av standarder og funksjonskrav. Disse temaene er en oppfølging av Lysne-utvalgets rapport om digitale sårbarheter (2015). I tillegg drøftes en rekke tema, herunder om NVE bør regulere kompetansekrav. Mandatet peker på temaer som logging og logganalyse, skytjenester mv. Disse temaene er også drøftet. Kapittelet avsluttes med arbeidsgruppens anbefalinger om grunnsikring, om strengere sikring av avanserte målesystemer og om sikring av driftskontrollsystemer.

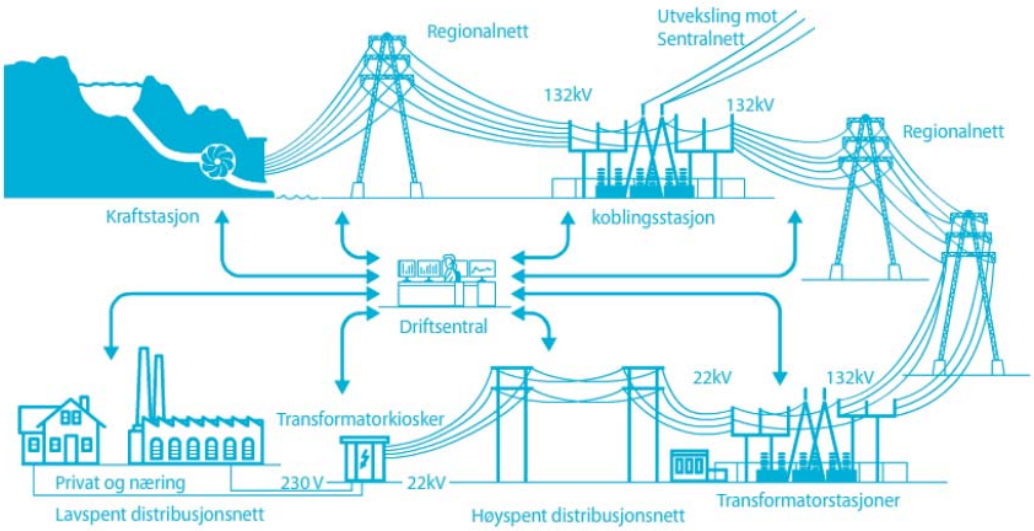
Del 5 er vedlegg til rapporten. Her gis informasjon om arbeidsgruppens arbeid, forkortelser og begreper, standarder og veiledere.

2 Digitale verdikjeder og systemer

2.1 Verdikjeden

2.1.1 Det fysiske systemet for elektrisk energi

Verdikjeden for elektrisk energi går fra vann i magasinet via turbin og nett til strøm i kontakten hos forbrukeren. Figur 2.1 illustrerer dette gjennom det elektriske energisystemet, også kalt kraftsystemet. Her vises den fysiske verdikjeden fra produksjon av energi gjennom overføring og til forbruk av energi. Videre vises hvilke deler av systemet som blir styrt av et kontroll- og styringssystem. Det som på figuren er beskrevet som sentralnett er det som nå regnes som transmisjonsnett.



Figur 2.1 Kraftsystemet (kilde: NOU 2015:13)

Nettet i Norge deles inn i tre nivåer: transmisjonsnett, regionalnett og distribusjonsnett. Transmisjonsnettet binder sammen produksjon og forbruk i ulike landsdeler, gir aktørene i alle landsdeler tilgang til en markedsplass og sørger for sentrale utvekslingspunkt i alle regioner. Transmisjonsnettet omfatter også utenlandsforbindelsene. Regionalnettene er bindeledd mellom transmisjonsnettet og distribusjonsnettene, og disse nettene består i hovedsak av kraftledninger med 66 kV og 132 kV spenning. Distribusjonsnettene er de lokale nettene som vanligvis sørger for distribusjon av kraft til sluttbrukerne, som husholdninger, tjenesteyting og industri. Når tredje energimarkedspakke implementeres, vil nettnivåene kun være transmisjonsnett og distribusjonsnett.

Store kraftproduksjonsanlegg knyttes til sentralnettet, mens mindre produksjonsenheter kan knyttes til enten regionalnettet (mindre vindkraftanlegg og småkraft) eller til distribusjonsnettet (mindre småkraft).

Små forbrukere er tilknyttet distribusjonsnettet, mens store forbrukere som kraftintensiv industri, kan være knyttet direkte til regional- eller sentralnettet.[15]

2.1.2 Kontrollsystemer og styringssystemer

Produksjon og forbruk av elektrisitet må til enhver tid være synkronisert for å unngå teknisk ubalanse i kraftnettet. Verdikjeden i kraftforsyningen har frem til nå blitt overvåket og styrt av driftskontrollsystemer for henholdsvis produksjonsanlegg, sentralnettnivå, regionalnettnivå og høyspent distribusjonsnivå. Etter utrullingen av digitale strømmålere (avanserte målesystemer - AMS) er det mulig å få bedre overvåking og styring på lavere distribusjonsnettnivå. AMS er i utgangspunktet et enveis målesystem der måledata hentes inn ved jevne tidsintervaller fra forbrukere og sendes over en kommunikasjonskanal til nettselskapets kundesystem og til en felles nasjonal database for slike måledata (Elhub). Med AMS vil nettselskapene kunne detektere og lokalisere

[15] Meld. St. 14 (2011–2012) Vi bygger Norge – om utbygging av strømnettet, https://www.regjeringen.no/no/dokumenter/meld-st-14-20112012/id673807/sec1, besøkt 07.01.2017.

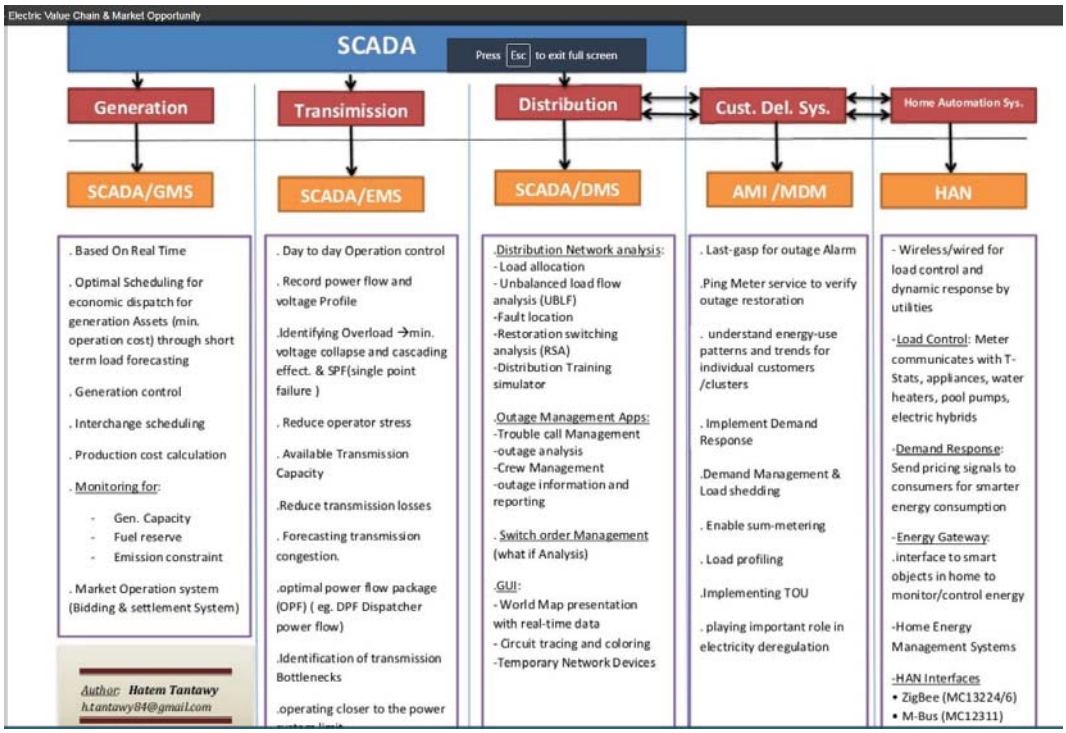
jordfeil, og overvåke spenning både i eget nett og hos forbrukere/sluttbruker, noe som gir økt personsikkerhet. De vil også kunne ha et enda bedre oversiktsbilde over energi- og effektsituasjonen i distribusjonsnettet, noe som også bidrar til forsyningssikkerheten.

NVE har stilt krav til at AMS skal inneha en brytefunksjon. Med brytefunksjonen kan AMS ansees som en del av et driftskontrollsystem. Med denne funksjonaliteten vil det være mulig å sette en øvre grense for effektuttaket for hver enkelt forbruker.

Automatisk timesmåling ved hjelp av AMS åpner for at tredjeparter (nye aktører) kan tilby å drifte husholdningers energiforbruk på en energioptimal og billig måte; ikke ulikt slik mobiloperatører kan selge mobiltjenester til kunder via en infrastruktureiers mobilnett. Tredjeparter som ender opp med å styre strømforbruket til mange sluttbrukere i et område kan, dersom de blir store nok, få betydning for beredskap og forsyningssikkerhet, uten at dette bør ses som en direkte konsekvens av AMS.

En annen trend man kan se er at ulike måleapparater som fjernvarme, vann-, strøm- og gassmålere benytter samme kommunikasjonskanal, og vil i noen grad kunne samkjøres eller integreres. Dessuten leverer samme leverandør produkter og tjenester til virksomheter i ulike bransjer. Samme tekniske sårbarhet vil derfor kunne treffe virksomheter på tvers av sektorer. Dette åpner opp for et behov for å tenke sikkerhet på tvers av sektormyndigheter for å unngå smitte av sårbarheter på tvers av ulike infrastrukturer.

Et eksempel på oversikt over kontroll- og styringssystemer fra generator til husholdning er vist i Figur 2.2. Norske løsninger kan fravike fra denne oversikten.



Figur 2.2 Eksempel på kontroll- og styringssystemer i den elektriske verdikjeden[16]

Et nettverk til en energivirksomhet deles opp i tre deler: 1) virksomhetens vanlige datanettverk (kontor/administrasjonsnettverk), 2) SCADA-nettverk (driftskontroll) og feltkomponenter / lokalkontroll (fjern-terminaler, sensorer, målere, brytere og lignende) og 3) lokalkontrollanlegg.

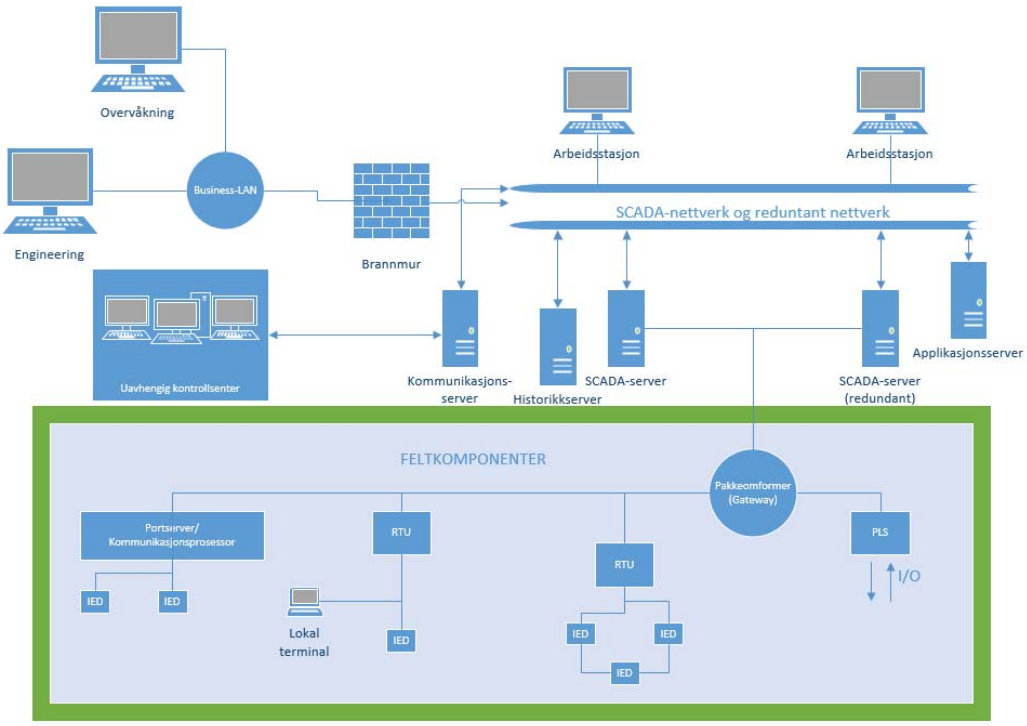
SCADA-servere sørger for kommunikasjon mellom SCADA-nettverket og lokalkontrollen. I tillegg finnes det flere servere med forskjellige funksjoner koblet på det samme nettverket. Feltkomponenter kommuniserer med nettverket via en datapakkeomformer. Datapakkeomformere gjør om de forskjellige industrielle kontrollsystem-protokollene til en protokoll som kan kommunisere via vanlige internettprotokoller og omvendt.[17]

Et eksempel på en prinsippskisse for et driftskontrollsystem er vist i Figur 2.3. Norske løsninger kan fravike fra dette oppsettet.

---

[16] Tantawy, H., *Smart Grid- Electric Value Chain & Market Opportunity*, 27. Desember 2014, http://www.slideshare.net/HatemTantawyBEngMBA/smart-grid-electric-value-chain-market-opportunity, besøkt 07.01.2017.

[17] Hovland, K. *Logging og logganalyse i energiforsyningen, studentrapport,* NVE rapport nr. 1, 2017, http://publikasjoner.nve.no/rapport/2017/rapport2017_01.pdf besøkt 11.01.2017.



Figur 2.3 Eksempel på prinsippskisse driftskontrollsystem

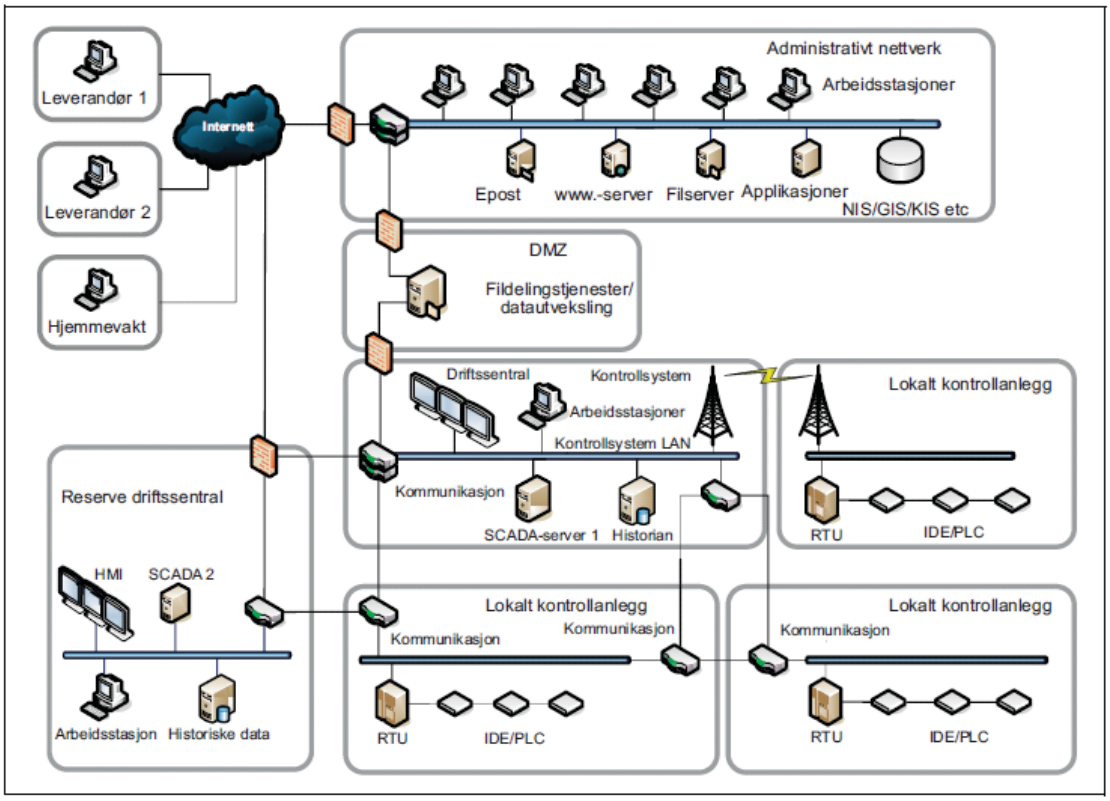
Et driftskontrollsystem inneholder som regel følgende elementer:[18] SCADA-server som samler inn prosessdata og sender kommandoer til feltkomponenter, Remote terminal units (RTUs) som utfører sensoraktivitet og driftsfunksjoner, Programmable logic controllers (PLCs) som virker på samme måte som RTUer, men er mer fleksible og avanserte med innebygget programmert logikk. I tillegg kommer kommunikasjons-infrastruktur (nett) som kobler SCADA-server til RTUs og PLCs og Human Machine Interface (HMI) som benyttes for at mennesker skal kunne betjene de kontrollerende datamaskinene. Engineering og overvåking utenfra prosessnett må sikres via VPN-oppkobling opp mot brannmur.

Feil i driftskontrollsystemet kan gi ulik effekt ut fra hvordan systemet er konfigurert. Det kan for eksempel være slik at produksjonen fortsetter som før selv etter at kommunikasjon har opphørt mellom kontrollerende datamaskin og RTU eller PLC, og at styring kan tas opp igjen når kommunikasjon gjenopptas. På den annen side kan feil få fatale følger dersom det gjelder kommunikasjonen til en viktig funksjon som krever kontinuerlig styring, hvor denne viktige funksjonen i ytterste konsekvens er avgjørende for energitilførsel for et større område. I slike tilfeller er det nødvendig med et redundant system dersom en kommunikasjonskanal faller ut.

Driftskontrollsystemer er koplet sammen med andre nettverk. I Figur 2.4 er det forenklet illustrert hvordan driftskontrollsystemer kan være delt inn i soner ved hjelp av brannmurteknologi med ulikt sikkerhetsnivå mot andre nettverk og mot internett. Soneinndeling filtrerer og begrenser datatrafikken mellom ulike soner, fra internettet og inn i driftskontrollsystemene.

---

[18]Se SCADA, Wikipedia https://en.wikipedia.org/wiki/SCADA, se også ISO/IEC TR 27019.



Figur 2.4 Soneinndeling i kontroll- og styringssystemer[19]

Når IKT-systemer som driftskontrollsystemer, administrasjonssystemer og andre nettbaserte systemer kobles sammen, vil det svakeste leddet i kjeden kunne være en inngangsport til tilknyttede systemer. I tillegg vil svakheter og feil i systemkonfigurasjon og programvare kunne medføre systemsvikt, eller gjøre systemene åpne for angrep fra opportunistiske angripere.

Mellom lokalt nett og internett vil det typisk være en brannmur som filtrerer og kontrollerer trafikk mellom nettene. Dette kalles et logisk skille. Så lenge driftskontrollsystemet er fysisk og logisk koblet sammen med administrativt nett, kan svakheter og skadevare i administrativt nett også potensielt påvirke driftskontrollsystemet. Det åpner eksempelvis for at et driftskontrollsystem kan angripes via administrativt nett. Direkte tilkoblingsmuligheter for elektronisk utstyr på driftskontrollsystem (for eksempel USB enheter) muliggjør videre direkte infisering av skadelig kode. Det samme gjør muligheter for fjerntilgang fra «hjemme-PCer», eller fjerntilgang fra leverandører. Dersom disse PCene er infisert, kan skadevaren potensielt smitte. Tilkobling via feltkomponenter/utestasjoner utgjør også en risiko.

[19] Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen, Nr 1 2013, NVE, http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf , besøkt 07.01.2017.

2.2 Markedet

2.2.1 Handelen

Handelen i kraftmarkedet skjer hovedsakelig hos markedsplasskonsesjonæren Nord Pool AS[20], hvor markedsaktører nominerer sine handelsbud om kjøp og/eller salg av kraft. Markedsaktørene er typisk kraftprodusenter og kraftleverandører som ønsker hhv. å selge og kjøpe kraft. Kundene har kun kontakt med kraftleverandørene. Etter at fristen for innsending av handelsbud er utløpt, beregner markedsplasskonsesjonæren markedsprisene og handelsvolumene for den enkelte kraftprodusent og leverandør. Beregningen er auksjonsbasert og gjennomføres hver kalenderdag. Den gjelder kun for påfølgende døgn. I tillegg til auksjonsmarkedet, tilbyr markedsplassen kontinuerlig handel, i det såkalte intradagsmarkedet.

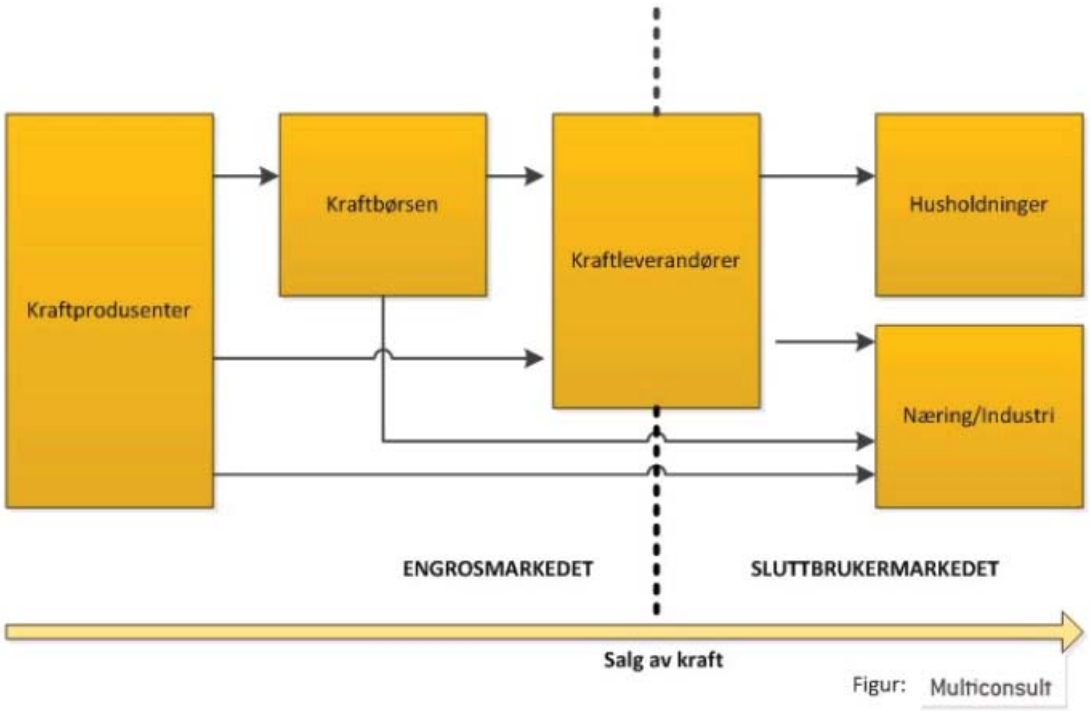
2.2.2 Markedsplassen

Kjøp og salg av kraft i Norge foregår digitalt og hovedsakelig på Nord Pool (kraftbørsen). Nord Pool tilbyr tjenester i ni europeiske land og gir oversikt over kraftprisen. Nord Pools datasystemer tar imot meldinger for kjøp og salg av kraft og kalkulerer kraftpriser for markedet. Dette er auksjonsmarkedet «day-ahead» og anses som primærmarkedet. Elbas, er en plattform som tilbyr kontinuerlig handel etter at auksjonsmarkedet er stengt, dvs. handel på markedet for inneværende dag.

Nord Pool eies av de nordiske transmisjonsnett system operatørene (TSOene): Statnett, Svenska kraftnät, Fingrid Oy, Energinet.dk and og de baltiske TSOene Elering, Litgrid og Augstsprieguma tikls (AST).

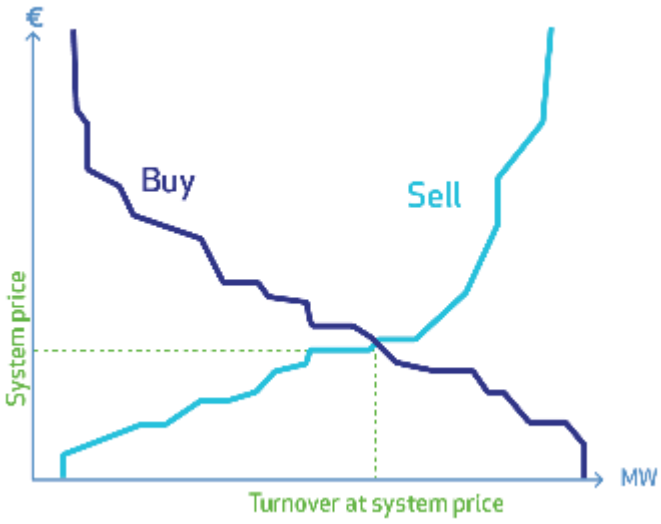
I tillegg til å handle på kraftbørsen er det mulig å handle bilateralt ved at kraftleverandørene handler fra kraftprodusentene direkte. Næringskunder handler i ulike sammenhenger både direkte fra kraftprodusent, fra Nord Pool og fra kraftleverandører (se Figur 2.5).

[20] I tillegg forekommer det noen handler hvor to parter, eksempelvis en kraftprodusent og en kraftleverandør, inngår en direkte kontrakt om fysisk levering av kraft. Dette omtales som en bilateral handel.



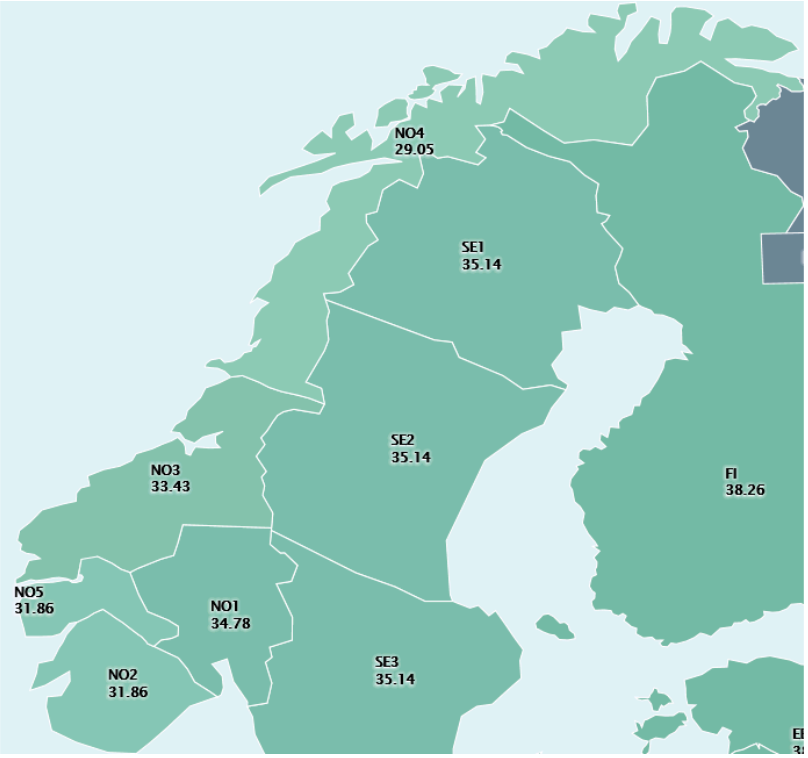
Figur 2.5 Forenklet illustrasjon av aktører i kraftmarkedet (Kilde: Multikonsult, gjengitt på fornybar.no)

På kraftbørsens day-ahead marked kjøpes og selges kraft for det neste døgnet. Her bestemmes en systempris etter at alle aktører har levert sine bud. Den finnes, ved at alle kjøps- og salgsordrene samles i to kurver for hver leveransetime, en etterspørselskurve og en tilbudskurve (Figur 2.6).



Figur 2.6 Bestemmelse av systempris (Kilde: nordpoolspot.com)

For at markedet skal ta hensyn til regionale forskjeller i nettkapasiteten, er det norske nettet delt inn i 5 elspot-områder, som har egne områdepriser (se Figur 2.7).



Figur 2.7 Prisområder i Norge (Kilde: nordpoolspot.com)

I tillegg til day-ahead markedet, administrerer Nord Pool et intradagsmarked hvor priser fastsettes løpende og handel foregår i nesten nå-tid (inntil 30 minutter før leveranse). På intradagsmarkedet er det mulig for aktørene å justere eventuelle feil eller uforutsette endringer av kraftmengde mot tilbudt mengde dagen før.

En annen mulighet for å justere misforhold mellom tilbydd og benyttet mengde kraft er gjennom regulerkraft. Regulerkraftmarkedet er en markedsplass administrert av Statnett, hvor tilbydere anmelder pris for å forandre produksjon eller forbruk. Budene havner i en felles nordisk liste, og aktiveres etter systemansvarliges behov med utgangspunkt i prisrekkefølge slik at den rimeligste reguleringsressursen benyttes først.[21]

En siste handelsplass er Nasdaq OMX Oslo ASA, som tilbyr det finansielle markedet med omsetning av kraft-derivater (finansielle kraftkontrakter). Slike derivater er gjerne avtaler som avregnes mot typisk systemprisen, og benyttes for å sikre seg mot finansiell risiko ved endringer av kraftpriser. Dette fordi prisen på kraft kan ha store prissvingninger av ulike årsaker som eksempelvis transport av kraften, forbruksmønstre, mengde nedbør, med mer.

2.2.3 Balanseavregning

Etter at handel er gjennomført vil det som regel være et avvik mellom solgt mengde strøm fra kraftprodusenter og faktisk forbrukt strøm av kundene. Avviket blir gjort opp mellom

[21] Statnett, Om regulerkraftmarkedet (RK), 2016, http://www.statnett.no/Kraftsystemet/Markedsinformasjon/RKOM1/Om-regulerkraftmarkedet-RKM/ besøkt 23.12.2016.

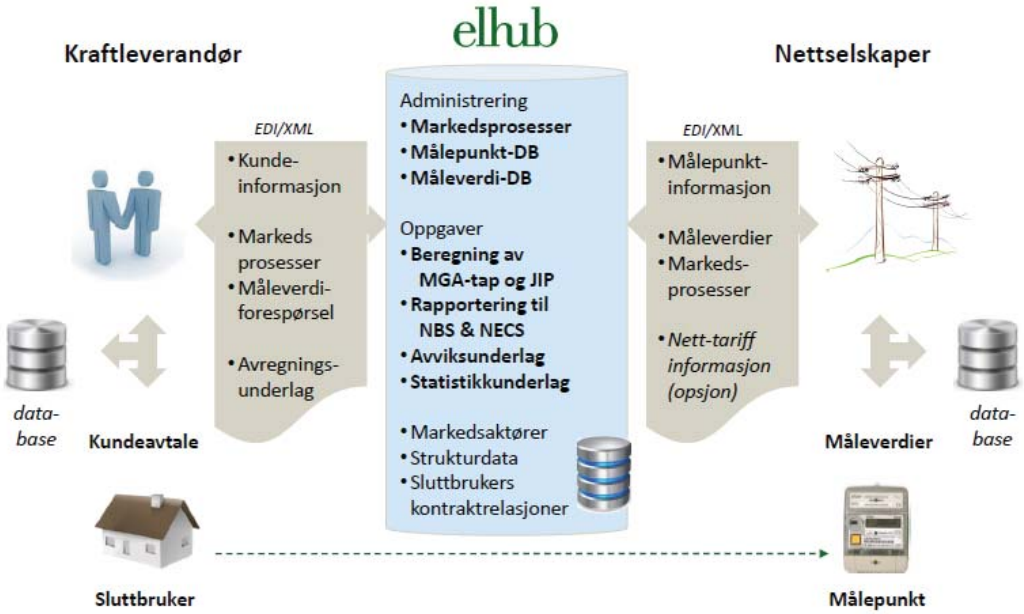
de involverte partene gjennom balanseavregningen foretatt av Statnett som avregningsansvarlig.

Våren 2017 skal det etableres en felles avregningssentral for Norge, Sverige og Finland, Nordisk balanseavregning (NBS), hvor denne type oppgjør etter handel og forbruk foretas. Dette vil bli basert på dataprogrammet til eSett Oy, som vil være eid av Transmission System Operators (TSO)ene og ha hovedsete i Finland. eSett Oy skal håndtere daglig drift for avregning og være en felles plattform for kommunikasjon. Innføring av eSett Oy skal skje før Elhub settes i drift (i løpet av 2017).

2.2.4 Distribusjon av måledata

Et felles nasjonalt oppsamlingspunkt for måledata vil bli satt i drift i løpet av 2017. Det vil bli administrert av et datterselskap av Statnett; Elhub AS. Elhub vil bli et kontaktpunkt mellom kraftleverandører og nettselskaper for deling av informasjon om kundene (inkludert måledata). Denne løsningen vil fremme konkurranse på like vilkår ettersom flere ulike prosesser (f.eks. strøm og nettleie på en faktura) ikke vil kunne resultere i uønsket innsyn i en konkurrents informasjon, slik som det er en mulighet for i dag når splittede kraftleverandør- og nettselskaper fortsatt bruker felles IT-systemer.

I tillegg vil Elhub bli et kontaktpunkt for tredjepartsleverandører som har fått tillatelse av kunder til å få tilgang til dennes måledata (timesoppløsning). Tredjepartene får måledataene fra Elhub, slik at de kan bruke dataene i forbindelse med for eksempel smarthustjenester.



Figur 2.8 Tjenester og kommunikasjons-prosesser i Elhub (Kilde: elhub.no)

2.2.5 Andre verdikjeder i markedet

Både kraftleverandører, kraftprodusenter, nettselskaper og Statnett benytter seg av felles kommunikasjonsløsning (Ediel), dagens avregningsprosess (operert av Statnett) og oppslag på målepunktID for kundeprosesser (NUBIX). Den nasjonale avregningsprosessen i regi av Statnett vil bli utfaset, i tillegg til at kundeprosessene tas over av Elhub. Systemstøtte for Ediel vil gjenstå da avregningsansvarlig vil forestå drift og vedlikehold og veiledning om Ediel-meldinger også i fremtiden.

Videre er det slik at alle virksomhetene på ulike måter benytter seg av underleverandører for IT. I tillegg er det enkelte kraftleverandører og nettselskaper som benytter seg av felles leverandører.

Flere nettselskaper har gått sammen om innkjøp og drift av AMS i en eller flere allianser. Dette gjør at slike allianser eller deres underleverandører gjerne blir mellomledd mellom AMS måler og/eller nettselskap og Elhub.

3 Energiforsyningens digitale sårbarhet

3.1 Farer og trusler mot digitale systemer i energisektoren

3.1.1 Et mangfoldig fare- og trusselbilde

Arbeidsgruppen har lagt til grunn en rekke rapporter og studier om trusler mot energiforsyningens digitale systemer. Noen sentrale rapporter er Lysne-utvalgets rapport NOU 2015:13 *Digital sårbarhet. Sikkert samfunn*, Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn, Samfunnssikkerhet*, *Mørketallundersøkelsen 2016*[22], NSMs rapport *Risiko 2016, Kan sikkerhet styre? En vurdering av sårbarheter og risiko i Norge*[23] og E- tjenestens rapport *Fokus 2016 Etterretningstjenestens vurderinger av aktuelle sikkerhetsutfordringer*. [24]

Fare- og trusselbildet er sammensatt. Dette er påpekt av Lysneutvalget som gir en samlet framstilling av tilfeldige feil og målrettede angrep. Arbeidsgruppen vurderer at

---

[22] *Mørketallsundersøkelsen 2016 - Informasjonssikkerhet, personvern og datakriminalitet,* Næringslivets sikkerhetsråd, http://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen_2016.pdf – besøkt 07.11.2016

[23] *RISIKO 2016 Kan sikkerhet styres? En vurdering av sårbarheter og risiko i Norge*, NSM, https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf besøkt 07.11.2016

[24] *Fokus 2016 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*, Forsvaret, https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus%202016.pdf besøkt 07.11.2016

det er viktig å ha et helhetsblikk som inkluderer menneskelige feil, organisatorisk svikt og systemsvikt i tillegg til trusler fra målrettede angrep fra mennesker. Fare- og trusselbildet endres som følge av teknologiutvikling, markedsdynamikk og politiske beslutninger.

3.1.2 Målrettede trusler fra mennesker

Mørketallsundersøkelsen 2016[25] viser blant annet risikobildet for norske virksomheter, og hvilke typer uønskede IKT-hendelser norske virksomheter opplever. 27% av virksomhetene oppgir at de har opplevd uønskede sikkerhetshendelser det siste året. Virksomhetene forteller at dette har ført til produktivitetstap i 4 av 10 tilfeller (i form av tapte arbeidstimer). Kun 2 av 10 oppgir at de har hatt kostnader som følge av slike hendelser. Dette viser at virksomhetene mangler oversikt over hva sikkerhetshendelsene koster dem, eller undervurderer disse kostnadene. Kun 9% av virksomhetene som utsettes for angrep tar saken videre til politiet. Det tilsier at det skjuler seg betydelige mørketall her, og at for kriminelle nettverk er denne typen angrep mot norske virksomheter i praksis straffefrie.

Markedet for skadevare er modent. På det kriminelle markedet kan en kjøpe både hackerverktøy og «konsulenttjenester». Markedet er stort, og de kriminelle tjenesteleverandørene tilbyr god ettersalg-service. De konkurrerer på god kvalitet og service, som i det åpne kommersielle markedet. Undersøkelser viser at de fleste angripere er opportunistiske. I en studie av Ponemon Institute, der forskerne spurte 306 sikkerhetseksperter i USA, UK og Tyskland, kom det fram at hackere går videre til neste mål dersom barrierene er sterke nok: 60% av alle hackerne går videre til neste mål dersom de ikke er innenfor i løpet av 40 timer. Rapporten[26] viser at inntjeningen fra kriminalitet er lavere enn ærlig IKT-arbeid.

Elektroniske komponenter til dagens IT-utstyr produseres i et globalt marked. Mikroprosessor kan produseres i ett land, mikro computer i ett annet og ulike sensorer i flere andre land igjen, før alt settes sammen i et tredje land. PST har i de siste årene åpent kritisert telekom-bransjen for å basere seg for mye på komponenter produsert i land vi ikke har sikkerhetssamarbeid med[27]. Det kan ikke utelukkes at fremmede makter vil kunne benytte seg av muligheten til å forsøke å implementere spionprogramvare i elektroniske komponenter de produserer: Enten til bruk for etterretning eller som hvilende destruktive script med tanke på eventuelle konfliktsituasjoner med Norge eller vesten. Det kan være svært utfordrende og tidkrevende å forsøke å finne denne typen skadevare dersom dette skulle være tilfelle.

---

[25] *Mørketallsundersøkelsen 2016 - Informasjonssikkerhet, personvern og datakriminalitet,* Næringslivets sikkerhetsråd, http://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen_2016.pdf besøkt 7.11.2016

[26] *2016 Ponemon Cost of Data Breach Study: Global Analysis*, tilgjengelig her: https://securityintelligence.com/media/2016-cost-data-breach-study/ besøkt 05.03.2017.

[27] «PST advarer mot telekom-spionasje», Dagbladet 2014, http://www.dagbladet.no/2014/02/09/nyheter/innenriks/overvaking/telekommunikasjon/31723971/ besøkt 23.12.2016.

Kanskje vil en i så fall ikke finne eventuell slik skadevare i det hele tatt da komponenter kanskje må ødelegges for å komme til koden, og dataene risikerer å bli ødelagt i prosessen.

NSM påpeker i sin rapport, «Risiko 2016. Kan sikkerhet styres? En vurdering av risiko og sårbarhet i Norge»[28] at det er lite sannsynlig at risikobildet vil endre seg i positiv retning i løpet av det neste året. Dagens trender vil fortsette og mest sannsynlig føre til økende sikkerhetsmessig risiko. Risikoen forbundet med IKT-angrep og annen spionasje i 2016 og årene fremover er stor. Etterretningstjenesten påpeker at etterretningsoperasjoner i det digitale rom, sosial manipulering og bruk av skadelig programvare øker i omfang. PST skriver at Norge og norske interesser vil i 2017 utsettes for fremmed etterretningsvirksomhet som kan ha et stort skadepotensial. Aktiviteten vil blant annet rettes mot mål innenfor norsk forsvars- og beredskapssektor, samt mot politiske beslutningsprosesser og kritisk infrastruktur. Systemer innenfor kraftsektoren og elektroniske kommunikasjonstjenester er å anse som spesielt etterretningsutsatt kritisk infrastruktur. Det norske samfunnet er i dag avhengig av sikker strømforsyning. I tillegg er norskprodusert kraft viktig for stabiliteten i kraftmarkedet i de nordiske landene og deler av Europa. Med et stadig tettere og mer europeisk samarbeid på kraftforsyningssiden er det viktig å se etterretnings- og sabotasjetrusselen mot norsk kritisk infrastruktur i en større europeisk sammenheng. Fremmede tjenester bruker både avanserte datanettverksoperasjoner og tradisjonelle metoder mot norske mål.[29]Etterretningstjenesten bekrefter dette bildet. Industrispionasje er forventet mot blant annet fornybar energi og grønn teknologi.[30]

SANS sin survey 2015 er gjort blant respondenter som vedlikeholder eller drifter eller tilbyr tjenester til virksomheter med industrikontrollsystemer. Surveyen viser at 32% har opplevd at kontrollsystemet eller nettverket ble infisert av skadevare eller infiltrert av hackere. Bare 12% var sikre på at systemene ikke hadde hatt noe innbrudd. Integrasjon av IT inn i industrikontrollsystemene er ansett av 19% blant de spurte som en av de store truslene.[31]

Globalt har energisektoren så langt få dokumenterte erfaringer med å håndtere store cyberhendelser, men det er eksempler der cyberangrep mot denne typen infrastruktur brukes bevisst i konflikter. En av de kjente hendelsene innenfor energiforsyningen er hendelsen i Ukraina 23. desember 2015 hvor totalt 225 000 kunder mistet strømforsyningen som følge av angrep hos tre nettselskap. Strømmen var borte i 1 til 6 timer for ulike regioner, men etter to måneder var fortsatt kontrollsystemet nede og

---

[28] *Risiko 2016. Kan sikkerhet styres? En vurdering av risiko og sårbarhet i Norge*, NSM, https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf, besøkt 27.02.2017.

[29] *Trusselvurdering 2017*, PST, http://www.pst.no/media/utgivelser/trusselvurdering-2017/, besøkt 06.02.2017.

[30] *Fokus 2017, Etterretningstenesta si vurdering av aktuelle tryggingsutfordringar*, Etterretningstjenesta, https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2017.pdf, besøkt 28.02.2017.

[31] Harp, D. and B-G. Brown, *The state of security in control systems today*, SANS, June 2015, https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042, besøkt 24.10.2016.

selskapet driftet nettet manuelt.[32] Det koordinerte angrepet mot tre selskap, som alle hadde ulike distribusjonsnettstyringssystemer, vitner om at dette var et planlagt og ikke et tilfeldig angrep. I følge en rapport fra SANS[33] om hendelsen foregikk angrepet ved at det i forkant ble levert skadevare via infiserte epost-vedlegg. Skadevaren i vedlegget koblet så maskinene hos nettselskapet sammen med en kommando- og kontroll-server som gjorde det mulig for angriperne å høste informasjon fra selskapene og skaffe ytterligere tilgang inn i systemene. Skadevaren inneholdt blant annet funksjon for tastaturavlesing hvilket muliggjorde tilgang til brukernavn og passord. Dermed kunne angriperne få tilgang til VPN (kryptert fjerntilgang) fra administrativt system over i driftskontrollsystem. Der kunne angriperen utforske driftsoppsettet over tid for å planlegge hovedangrepet med utkobling av kraftforsyningen. Under hovedangrepet tok angriperen kontroll over arbeidsstasjonene til operatørene i nettselskapet, og stengte dem ute fra sine systemer. Deretter ble strømmen brutt i distribusjonsnettet og UPS (nødstrøm) ble frakoblet. Nettselskapene ble på grunn av cyberangrepet tvunget over til manuell drift. Et fjernstyrt nektelsesangrep (overflod av automatiske oppringinger som gjorde at telefonsystemet ikke kunne ta imot flere samtaler) forhindret i tillegg kunder i å rapportere at de hadde mistet strømmen.

En annen fremtidig trussel er ubemannede droner. Droner kan bli nyttige tilleggsressurser for inspeksjon av energianlegg og infrastruktur.[34] Droner brukes til å inspisere dammer, ledninger, anlegg og miljø[35]. Det finnes droner som flyr, kryper på bakken, beveger seg på og i vann. For energibransjen vil slik bruk av teknologi kunne innebære et stort mulighetsrom knyttet til forebyggende vedlikehold og inspeksjon i vanskelig tilgjengelige områder. Fremmede droner, eller tap av egne droner, kan på en annen side bety utfordringer for sikkerheten. Samferdselsdepartementet har nedsatt en gruppe som skal se nærmere på reguleringen av bruk av droner i Norge.[36]

3.2 Administrative systemer

3.2.1 Digitale sårbarheter i administrative systemer

Administrative systemer og driftskontrollsystemer brukes av produksjonsselskap og nettselskap. Administrative systemer omfatter her alt som ikke er å betrakte som prosesskontrollsystemer. Driftskontrollsystemer overvåker, kontrollerer og styrer

---

[32] Zetter, K., "Inside the cunning, unprecedented hack of Ukraine's power grid", *Wired*, publisert 03.03.2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ besøkt 20.07.2016.

[33] *Analysis of the Cyber Attack on the Ukrainian Power Grid, Defence Use Case, TLP: White,* Sans Industrial Control Systems, Washington DC, March 18, 2016.

[34] "Real UAV / Drone Benefits for Energy Sector & Industry", Ascending technologies, 27 February 2015, http://www.asctec.de/en/real-uav-drone-benefits-for-energy-and-industry/, besøkt 07.01.2017.

[35] Kennedy, D., "The game of drones: Unmanned aerial vehicles by sector in Canada", Financial Post Tech Desk, 6 February 2016, http://business.financialpost.com/fp-tech-desk/the-game-of-drones-unmanned-aerial-vehicles-by-sector-in-canada?__lsa=31b8-355b, besøkt 07.01.2017.

[36] *Introduksjon av regelverk om droner/RPAS*, EØS-notat 06.06.2016, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2015/sep/a-npa-2015---regelverk-om-dronerrpas/id2458752/, besøkt 22.10.2016.

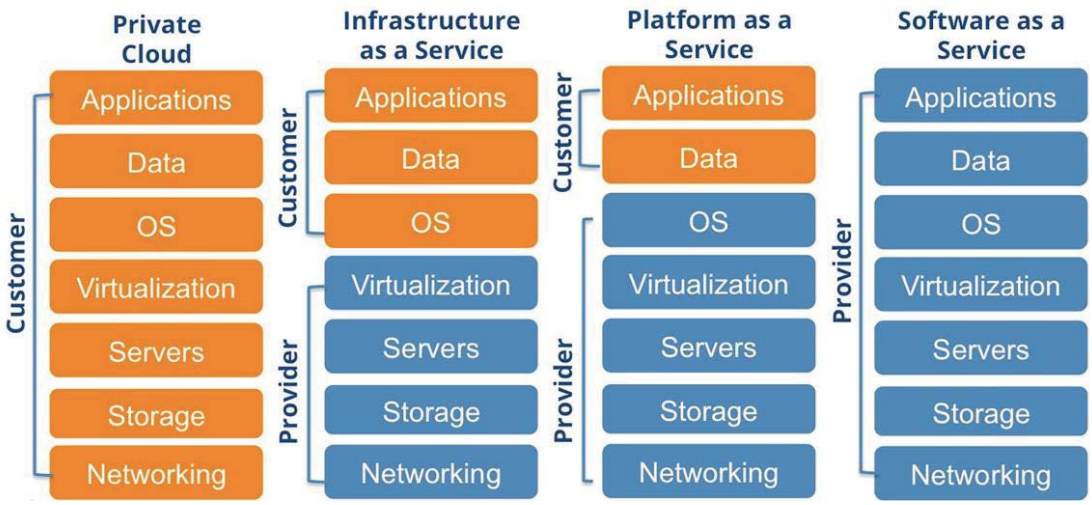
energiproduksjon og -overføring fra produsenter til forbrukere. Se for øvrig definisjoner i kapittel 1.4.3.

Et svært forenklet bilde av administrative systemer er følgende: For økonomistyring, handel og administrasjon av virksomheten kan virksomhetene bruke administrative systemer som inkluderer webservere, mailservere, filservere, skrivere og ulike klienter (laptoper, nettbrett, smarttelefoner mv.). Klientene er koplet til disse serverne via et lokalt nettverk. Det lokale nettverket består av trådløse forbindelser eller fiberlinjer. Rutere brukes for å rute trafikken i det lokale nettverket, og til videre tilkopling til internett. Internett (IP)-protokollen benyttes for å overføre informasjonen i nettverket. I tillegg til egne datamaskiner, kan ulike former for tjenesteutsetting av IT-tjenester (eksempelvis skyløsninger og andre eksterne digitale tjenester), gi systemer som er tilkoplet det lokale nettet eller være mulig å nå via en nettleser. Eksempler på tjenester en typisk kan kjøpe eksternt er personalstyringssystem, regnskap og fakturering, banktjenester, mailtjenester, IT-fjernsupport, databaser, markedsplass etc. I et slikt nettverk, eller system, vil sikkerhetsmekanismer som identitets- og tilgangsstyring, samt kryptering av data, bidra til forebyggende sikkerhet. Mellom lokalt nett og internett vil det typisk være en brannmur som filtrerer og kontrollerer trafikk mellom nettene, et logisk skille. Et logisk skille vil også typisk finnes mellom det administrative nettet og driftskontrollsystemet.

Markedet for kjøp og salg av elektrisitet der mange aktører deltar og der prisen på spotmarkedet styres av tilbud og etterspørsel har eksistert i ca 30 år. Nordpool er markedsplassen der disse aktørene handler. I fremtiden blir det flere markedsplasser tilgjengelig. Som andre virksomheter har også markedsplasser som Nordpool administrative systemer og dataregistre som er koplet til internett. Utviklingen går videre i retning av at flere digitale komponenter, sensorer og systemer koples sammen og til internett.

Utrullingen av AMS skaper muligheter for enda bedre overvåkning av distribusjonsnettet og styring av forbruket gjennom prismekanismer, samtidig som forbrukere gis mulighet til å bli plusskunder og få sterkere incentiver til å spare effekt og strøm i anstrengte situasjoner. Med AMS-utrullingen kommer også nye dataregistre som Elhub. Apper (programvare) på smarttelefoner for timeføring og avlesing av strømforbruk mv., er andre eksempler på digitale tjenester som kan bli integrerte inn i administrative systemer på en aller annen måte og representere en utvidelse av det administrative systemet. Med en slik utvidelse «av systemet» følger også flere sårbarheter og flere angrepsflater.

Skytjenester er en samlebetegnelse for ulike måter å drifte IT-systemene på. Skytjenester tilbyr en IT-driftsmodell som gjør det mulig å få tilgang til et sett konfigurerbare dataressurser (for eksempel nettverk, servere, lagring, applikasjoner og tjenester) som: er lett tilgjengelige overalt, blir levert og priset etter behov, og kan skaffes raskt og gjøres tilgjengelig med minimalt med administrasjon eller involvering fra tilbyderen. Avhengig av den praktiske løsninger, fordeles kontrollen mellom leverandør og kunde som vist i Figur 3.1.



Figur 3.1 Ulike modeller for skytjenester (Kilde: Ferc)

Skytjenester kom med internettets utvikling, der datalagringskapasiteten, dataprosesseringskapasiteten og internett sin gode dataoverføringskapasitet har muliggjort å hente data og digitale tjenester fra hvor-som-helst, så fremt man har en nettleser og internettilgang. Det å lagre noe i en skyen vil, avhengig av leverandør, kunne medføre at data i stor grad (helt/delvis) ligger fysisk utenfor Norge og blir overført gjennom infrastruktur i et tredjeland. En slik datalagring kan, dersom innholdet ikke er sikret tilstrekkelig, medføre at viktige data kan havne utenfor virksomhetens kontroll. Bruken av skytjenester er høy i Norge, og mange er ikke bevisste at de bruker skytjenester. Dersom en bruker CIM-verktøyet[37] til risikoanalyse og logg, bruker en i prinsippet en skytjeneste, samme gjelder dersom en konverterer til et Pdfdokument. I tråd med økt utbredelse og bruk av skytjenester har nå den største utfordringen for driftspersonell flyttet seg fra sikkerhet til management av skytjenester.[38]

Hva er så sårbarhetene i administrative systemer? Sårbarheter finnes i maskinvare, fastvare og programvare (operativsystem og applikasjoner). Med flere millioner kodelinjer bare i operativsystemet[39], skal det mye til for at enkeltfeil ikke oppstår i produksjonen av programvaren. Det skal bare en liten skrivefeil til for at programmet ikke fungerer som opprinnelig tenkt. At det er viktig å være første på markedet, øker risikoen for at produsenter av programvare slipper ut programvaren for tidlig. Slik vil det også være så lenge produsentene ikke bærer den økonomiske risikoen for kostnaden ved feil – den bærer kjøper av produktet. Det er normalt at brukere av programvare ved nedlasting må akseptere betingelser der produsenten fraskriver seg ansvar. I tillegg må

---

[37] CIM er verktøyet den sivile delen av forvaltningen bruker til krisehåndtering, og den mest utbredte løsningen for dem som jobber med sikkerhet og beredskap i Norge, se https://onevoice.no/no/ besøkt 05.03.2017.

[38] Weind, K, "Cloud Computing Trends: 2016 State of the Cloud Survey", Cloud management blog, 9 February 2016, http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey, besøkt 22.10.2016.

[39] «Microsoft Windows 8 er hevdet å ha ca 40 millioner kodelinjer», Quora, https://www.quora.com/How-many-lines-of-code-is-in-Microsoft-Windows-8 besøkt 05.03.2017.

kjøpere gjerne betale for oppgradering og feilretting som oppdages etter at produktet er sluppet på markedet og tatt i bruk.

Digitale sårbarheter kan oppstå ulike steder i lange forsyningskjeder. Som Lysne-utvalget (2015) pekte på, kan en sårbarhet eller svakhet i bunnen av en lang digital verdikjede forårsake store konsekvenser lenger opp i forsyningskjeden. Den leverandøren som befinner seg langt nede i forsyningskjeden, har ikke mulighet til å forutse konsekvensene for kundene lengre oppe i verdikjeden. Oppe i verdikjeder det tilsvarende vanskelig for kunder å forstå risiko og sårbarheter lenger nede i verdikjeden.

IT-utstyr som brukes i norsk energiforsyning er kjøpt fra en global IT-industri som leverer akkurat samme produkter og programvare til mange land. Samme utstyr leveres også til kunder i ulike samfunnssektorer. Derfor kan en også se lignende sårbarheter på tvers av samfunnssektorer. Samme trussel og sårbarhet kan med andre ord ramme på tvers av sektorer.

Får å få en god forståelse av sårbarhetene er det nyttig å se til det internasjonale sårbarhetsbildet, rapportering fra CERTer og leverandører. Databasen Common Vulnerabilities and Exposures (CVE) er driftet av amerikanske MITRE og oppdateres kontinuerlig med nye sårbarheter. Databasen gir et oversiktsbilde over sårbarheter. Databasen er viktig informasjonskilde for CERTene rundt om i verden, som varsler virksomheter om sårbarheter og hvordan disse kan fikses. Sårbarhetene kan være svakheter i autentisering, enkeltfeil som gjør at dataregistre kan overbelastes, feil som gjør det mulig i sette inn ekstra programkode som ikke var tiltenkt satt inn.

Grunnleggende sårbarheter som finnes i programvare og maskinvare finnes også i skytjenester uavhengig av IT-driftsmodell. Store leverandører har ofte et bedre regime på sikkerhetsforvaltning enn det små norske selskaper selv evner å ha. De har bedre kompetanse og mer ressurser til sikkerhetsarbeidet. Derfor vil bruk av skytjenester fra profesjonelle leverandører kunne gi lavere risiko for uønskede IKT-hendelser enn å drifte selv. Når det er sagt, er det «nye» sårbarheter som blir introdusert: Landsikkerhet inklusive jurisdiksjon og korrupsjon når data lagres og behandles på servere i utlandet, eierskap til data, mulighet til å skifte leverandør og mulighet til å holde kjernevirksomheten i gang dersom internettforbindelsen til IT-leverandøren går ned. I tillegg er det også knyttet sårbarheter til de digitale verdikjeder skyløsninger er avhengig av.

Sårbarhetsstatistikk kan belyse omfanget av problemet med digitale sårbarheter, men noe eksakt helhetlig verdensbilde eller bilde for Norge finnes ikke.[40] Flexera Software, som overvåker mer enn 50 000 applikasjoner og operativsystemer globalt, har gitt ut en oversikt og sårbarheter for 2016. 21% av sårbarhetene var i Microsoftapplikasjoner, [41] 87% av sårbarhetene var i andre applikasjoner. Nettlesere som Google Chrome, Mozilla Firefox, Internet Explorer, Opera og Safari hadde 1114 sårbarheter i 2015, en økning fra 1076 i 2014. Hvor alvorlige disse er framgår av CVE-databasen. I noen tilfeller kan

---

[40] *Flexera Software Vulnerability Review 2016, Key figures and facts on vulnerabilities from a global information security perspective*, http://resources.flexerasoftware.com/web/pdf/Research-SVM-Vulnerability-Review-2016.pdf?elqTrackId=a48c24bf4da04f5b95c4e95ed9024cb1&elqaid=1802&elqat=2, besøkt 21.11.2016.

[41] Windows 10 som kom i 2015, hadde for eksempel 256 identifiserte sårbarheter.

programmet miste funksjonalitet, i andre tilfeller kan en mulig angriper få store rettigheter, som igjen gir mulighet for misbruk av systemet, endring av systemets funksjonalitet og informasjonstyveri.

3.2.2 Sikring av administrative systemer

NSM har utgitt noen gode sikkerhetsråd og en god sikkerhetsløsning for oppdatering av programvare og operativsystem.[42] I følge Flexera Softwarehadde 85% av sårbarhetene hos de 50 mest vanlige applikasjonene en retting klar samme dag. Hos desom ikke hadde retting klar, manglet leverandøren ressurser. Frigivelse av sårbarheten var ikke koordinert, eller enda sjeldnere så var det snakk om nulldagssårbarhet, dvs. sårbarhet det ikke fantes en retting for. Dette forklarer også hvorfor oppdatering umiddelbart er viktig, og hvordan risiko kan reduseres. I 2015 var det 25 nulldagssårbarheter globalt i alle produkter som var overvåket av Flexera Software. Nulldagssårbarheter spiller en stor rolle når det kommer til avansert trusselaktører, som store organisasjoner og stater. Flexera Software-statistikken gir ett bilde på situasjonen, men ikke et komplett bilde.

I Norge ser vi avtrykk av de digitale sårbarhetene i Mørketallsundersøkelsen 2016: 27% av et tilfeldig utvalg på 1500 norske virksomheter har hatt uønskede hendelser i løpet av kalenderåret 2015. 20% av disse oppgir virus som den verste hendelsen. Analyser av datasettet i Mørketallsundersøkelsen viser ingen signifikante bransjeforskjeller. Vi kan som følge av dette, og som følge av det faktum at alle virksomheter bruker samme systemer fra globale leverandører, anta at risikoen for å få infisert administrative systemer er den samme for virksomheter i norsk energiforsyning.

Arbeidsgruppen viser til NSM når det gjelder sikring av administrative systemer. I Norge gikk NSM ut med fire råd – blant disse finner vi oppgradering av programvare og operativsystem så snart en oppdatering foreligger. Slik arbeidsgruppen ser det, vil de andre rådene – å redusere administratorrettigheter og kun tillate forhåndsgodkjent programvare, redusere risikoen ytterligere, men ikke til «null». Begrunnelsen for dette er blant annet at mennesket er en risikofaktor en må ta med i vurderingen. Brukernavn og passord gir tilgang til systemer. Med riktig brukernavn og passord kan en person som regel bevege seg på tvers av sikkerhetssoner. Det er mange eksempler på at angripere skaffer seg dette, for eksempel via utro tjenere eller phishing epost. Ved målrettede aksjoner sender angripere epost til ledere og personell med vide fullmakter og god tilgang. I neste omgang åpner mottakerne av eposten lenker og vedlegg og laster dermed ned programvare som fisker deres brukernavn og passord. I slike tilfeller vil flerfaktor-autentisering være et godt risikoreduserende tiltak. Eksempel på flerfaktor-autentisering er både passord og kode på mobil.

Arbeidsgruppen vurderer det slik at det er umulig å sikre systemene 100%, men risikoen kan reduseres betydelig gjennom god sikkerhetspraksis og god sikkerhetsforvaltning. Det er viktig å oppdage uønskede hendelser i systemene og viktig å ha evne til å håndtere hendelsene. I Mørketallsundersøkelsen 2014 rapporterte 5 % av store virksomheter at de

[42] Nasjonal sikkerhetsmyndighet, «Ti viktige tiltak mot dataangrep. Sjekkliste nr 2 (S-02)», Oppdatert 2016-03-03, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf, besøkt 13.02.2017.

var hacket. Blant kunder av NorCERT og mnemonic var andelen hackede store virksomheter mye høyere; en av to kunder av NorCERT og to av tre kunder av mnemonic.[43] Lærdommen fra denne sammenligningen var at logging, logganalyser og bruk av profesjonelle overvåkningssystemer bidrar til at virksomheter får et mye mer komplett bilde av hva som foregår i systemene. Over flere år har undersøkelsen vist at norske virksomheter ikke logger datatrafikken, og de analyserer heller ikke loggene sine. Derfor oppdager de også lite av uønskede hendelser i IT-systemene. De ser ikke hva som foregår.

Siden hendelser ikke kan unngås, er det nødvendig å ha beredskap for uønskede situasjoner som kan oppstå som følge av menneskelige og tekniske feil, og som følge av angrep mot systemene. Arbeidsgruppen vil understreke at selv om tekniske sikringsmekanismer kan gjøre mye, må likevel mennesker med kompetanse bidra både i drift og trå til når teknologien svikter. Det må lages beredskapsplaner og øves på å håndtere uønskede situasjoner. Backup må administreres og testes. På dette området lever menneske og teknologi i en slags symbiose, og begge er viktige for helhetlig sikkerhet.

3.3 Produksjonsanlegg, driftskontroll og nett

3.3.1 Digitale sårbarheter i lokalkontrollanlegg

Kraftverk kan driftes lokalt via lokalkontrollanlegget. I dag er mange lokalkontrollanlegg ubemannede, og trenden går mot mer automatisering. Kraftverk kan ha store utfordringer med å innføre prinsipper for god IKT-sikkerhet i kjernen av prosesskontrollsystemene, for eksempel regelmessig oppdatering av programvare. Automatisk oppdatering av programvare i for eksempel PLCer, som igjen er koplet til vern, kan få utilsiktede konsekvenser med fare for liv, miljø og økonomi dersom det oppstår feil og PLC ikke virker som forventet lenger.

NVE har fått opplyst fra et stort kraftselskap at mange feil har rot i at PLC er programmert til å virke under andre betingelser enn de som gjelder i virkeligheten. Tidligere kunne operatører se logikken i PLCene, men nå er PLC blitt sorte bokser. Det skaper også en utfordring når det gjelder automatisk oppgradering av programvare. Mangel på tilgang på kode i PLC gjør det vanskelig å finne feil og logiske brister. Ett kraftselskap opplyste at de brukte 1,5 år på å finne en enkel logisk feil i en PLC der selskapet ikke hadde tilgang til koden. Konsekvensen av denne hendelsen var problemer med lukestyringen.

Dette gir følgende dilemma. Med økende digitalisering, automasjon og integrasjon av systemer kan risikoen for utilsiktede feil øke. Samtidig vil automatisk oppdatering av programvare være vanskelig og forbundet med risiko. Oppdateringer må testes og oppdatering må skje kontrollert.

---

[43] *Mørketallsundersøkelsen - Informasjonssikkerhet, personvern og datakriminalitet, 2015,* Næringslivets sikkerhetsråd, http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014.pdf, besøkt 07.12.2017.

3.3.2 Digitale sårbarheter i driftskontrollsystemer

I korthet består driftskontrollsystemer (overvåknings- og prosesskontrollsystemene, SCADA) av kontrollenheter som koples til prosessenheter og sensorer for å innhente status og gjøre det mulig drifte systemet som helhet. Kontrollenhetene kommuniserer med en sentral server som bruker kommunikasjonsprotokoller (strukturert format for å pakke data for oversendelse). Ulike protokoller er i bruk, noen er utviklet kun for bruk i systemer levert av den enkelte leverandøren, dette er såkalte proprietære protokoller. I andre tilfeller brukes standardiserte protokoller. Internettprotokollen er velkjent, og det er forventet at framtidens systemer vil gjøre mer bruk av denne. Kommunikasjon mellom kontrollenhetene og serveren kan skje ved kabel eller trådløst (som for AMS og DMS), og gjøre bruk av ulike kommunikasjonsprotokoller. Noen protokoller har sikkerhet implementert, eksempelvis kryptering. Andre har ikke dette.

I prosesskontroll er samspillet mellom menneske og maskin viktig. Operatøren på driftssentralen overvåker og kontrollerer via et Human-Machine Interface (HMI) system. HMI tilbyr et grafisk skjermbilde og presenterer status på brytere og generatorer, alarmer og hendelser og annen relevant informasjon på en slik form at mennesker forstår dette bildet. Operatøren kan styre prosessene via HMI.

Systemdata blir innhentet fra sensorer og prosessenheter, prosessert og lagret i en server. Kritiske servere og systemkomponenter er typisk konfigurert i en fullt dublert arkitektur, som gjør det mulig å raskt få opp igjen drift dersom feil skulle oppstå og hovedserveren skulle feile. Reservedriftssentraler, som det iht. beredskapsforskriften er krav om for klasse 2 og klasse 3 anlegg, tilbyr tilsvarende alternativt driftssted dersom det skulle oppstå en situasjon der hovedsentralen er ute av drift.

Tidligere var SCADA systemene helt separert fra de administrative systemene,[44] men i dag er det vanlig at SCADA er lagt i et eget prosessnett og at kommunikasjonen går via protokoller med strenge krav til sikkerhet. Logiske skiller, som er laget ved hjelp av programvare, gir aldri 100% sikkerhet, men de reduserer risikoen. Brannmur og filtreringsteknikker brukes for å lage logiske skiller. Kontroll med brannmuroppsettet er derfor viktig for å ivareta den sikringen som gis gjennom logiske skiller. Det er heller ikke slik at fysisk skille garanterer 100% sikkerhet. I slike tilfeller kan minnepinner og bærbare digitale enheter bidra til å overføre skadevare på tvers av sikkerhetsgrenser når de koples sammen. Ettersom kompleksiteten og diversiteten i systemene øker, trenger en potensiell angriper en lang etterretningsperiode. Hjelp av innsidere vil være til stor hjelp for å få tilgang.

Økt bruk av passord for pålogging kan føre til at tilgangen til utstyr blir vanskeliggjort i en nødsituasjon. Personell som blir sendt ut til en stasjon for å gjøre en nødvendig jobb kan få problemer med å utføre jobben dersom vedkommende ikke kan passordet eller har eget passord som gir tilgang til viktige systemer. Virksomheten må ha rutiner for oppfølging av mange systemer over mange forskjellige plattformer og årganger, brukere,

[44] Overview of Cyber Vulnerabilities, Understanding Control System Cyber Vulnerabilities, ICS-CERT, https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities#under, besøkt 21.11.2016.

eksterne leverandører etc. Dette vil i praksis bli umulig å håndheve på en god måte inntil alle enheter da får sentralisert passord via domene.

I AMS samles måleverdier inn via en digital måler plassert i koplingsskapet hos kunden. Data fra flere målere i et geografisk område sendes trådløst til konsentratorer eller via andre målere (mesh-nettverk) videre til nettselskapet. Hos nettselskapet finnes overvåkningssystem (DMS) som viser status på distribusjonsnettet i sanntid, blant annet om kunder i et område har strømforsyning. Nettselskapet bruker dette systemet til overvåkning av aktiviteten i nettet, men nettselskapet har også programvare der operatører hos nettselskapet kan gå inn og frakople enkeltkunder.

AMS har fellestrekk med administrative systemer. AMS bruker åpne standarder og har tett kobling til kundeinformasjonssystemer. AMS har også likhetstrekk med driftskontrollsystemer: AMS bruker proprietære protokoller og vil i fremtiden kunne kobles logisk med SCADA gjennom DMS. Tett integrering av AMS-DMS-SCADA er ønsket av enkelte nettselskap samtidig som leverandører utvikler slike løsninger. Integrering av AMS, DMS og SCADA vil av hensyn til nettnytte kunne gi store fordeler, men en slik utvidelse vil kreve sterke sikkerhetsmekanismer.

3.3.3 Sikring av driftskontrollsystemer

SCADA og DMS har mange fellestrekk med administrative systemer – de bygger på samme type maskinvareteknologi, de inneholder fastvare og programvare som slippes tidlig på markedet og må i løpet av levertiden oppdateres flere ganger for å redusere sårbarheter. Systemene har servere, klienter og et grensesnitt mot operatører, som i administrative systemer, men de er i tillegg koplet til sensorer, brytere og styringsenheter, enten via digital eller analog kommunikasjon.Via kommandoer kan brytere og generatorer koples inn og ut, og det er denne digitale forbindelsen som gjør at sikring av SCADA og DMS (dersom det er et styringssystem) blir kritisk. Digitaliseringen og automatisering gjør det mulig å kjøre flere kommandoer automatisk, å kople sammen flere enheter og sensorer, og å sammenstille data fra ulike datakilder. Slik oppnås et bedre sanntids situasjonsbilde. Med et bedre sanntids situasjonsbilde kan driften i normalsituasjoner effektiviseres. Feil og utfall kan lokaliseres og repareres raskere.

For å forstå sårbarhetene må en forstå alle tilgangene til driftskontrollsystemet. I et typisk SCADA-system er det mange måter å kommunisere på, og det er mange enheter som skal kommunisere med SCADA-serveren. I tillegg kommer operatører som virker gjennom HMI. En angriper som ønsker å få kontroll over systemet må overvinne følgende utfordringer:

- Få tilgang til det lokale driftskontrollnettverket, som gjerne er beskyttet av flere brannmurer som kun tillater en viss form for trafikk, sesjoner og programvare å slippe igjennom. En annen mulighet er gjennom RTU (det kan for eksempel være en PLC). De fleste RTUer krever ingen autentisering eller passord for autentisering, men moderne RTU'er og IED'er støtter som regel passord/pålogging og rollebasert tilgang. Sårbarheter oppstår dersom bransjen ikke benytter de sikkerhetsmekanismene som ligger i produktene.

- Gjennom grundig etterretning få en forståelse for systemet. En angriper kan komme godt ut dersom vedkommende får tilgang via innsidere med vide fullmakter og tilgang. Insidere kan være både egne ansatte og innleide konsulenter eller leverandører. Det er viktig å ha kontrollordninger for personer med vide fullmakter slik at risiko for feil, misbruk og sabotasje blir redusert. Dagens beredskapsregelverk har krav om slik kontroll i kapittel 7. Kontrollen gjelder både mennesker og utstyr.

- Få kontroll over prosessen; dette krever at angriper forstår både IKT, prosesstyring og infrastrukturen, inklusivt hvordan alle systemer og komponenter er satt sammen og hva de heter. Kompetanse om prosesskontroll/automasjon er et eget fagfelt, og selv IKT-sikkerhet har mange spesialområder. Derfor kan en anta at det trengs et team av angripere med ulik kompetanse dersom utenforstående skal klare å bryte seg inn i driftskontrollsystemer og overta prosesstyringen. Det må antas at flere land i verden i dag, både vestlige og ikke vestlige, utvikler evne til å gjennomføre offensive cyberoperasjoner. Spor av slike ambisjoner finnes i flere nasjonale cyberstrategier.[45]

Angrepene mot industrikontrollsystemer er i vekst ifølge Dell Secure Works sin trusselrapport for 2015. Analysen fra Dell viser et skarpt hopp i antall rapporterte sårbarheter i industrikontrollsystemer etter at skadevaren Stuxnet[46] ble sluppet i 2011. Dell sier det har vært en dobling av angrep, og at angrepene synes å være politisk motivert. I NIST sin sårbarhetsdatabase (NIST National Vulnerability Database) kan en søke opp leverandør og tidsrom mm., og lete etter sårbarheter.[47] Recorded Future har gjort en analyse av sårbarhetene i industrikontrollsystemer (ICS) og SCADA ved å gjøre søk i denne databasen og andre datakilder. De fant totalt 400 sårbarheter. Recorded Future hevder også at ansatte bruker jobb-brukernavn og passord privat, og i praksis er dette ifølge Recorded Future dessverre et faktum også i kritisk infrastruktur. [48]

I følge analysen av Recorded Future dominerer Siemens og Schneider det globale sårbarhetsbildet, med 50% av de registrerte sårbarhetene. Dette henger sammen med at de har en dominerende markedsstilling, men også at de er flinke til å rapportere sårbarheter og jobbe med å sikre systemene sine. Skadepotensialet av manipulasjon av SCADA er stort med direkte konsekvens for liv og helse sammenlignet med manipulasjon av administrative systemer. I tillegg er risikoen høyere dersom en angriper først kommer innenfor brannmuren; dette har sammenheng med at sårbarheter eksisterer lengre i SCADA og prosesskontrollsystemer sammenlignet med administrative systemer. Dersom

---

[45] Se for eksempel HM Government National Cyber Security Strategy 2016-2021, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, besøkt 27.02.2017.

[46] Skadelig programvare oppdaget i 2010, designet for å angripe driftskontrollsystemer (SCADA).

[47] National Vulnerability Database, NIST https://web.nvd.nist.gov/view/vuln/search, besøkt 07.01.2017.

[48] Up and to the Right ICS/SCADA Vulnerabilities by the Numbers, Threat intelligence Report, Recorded Future, 2015, https://go.recordedfuture.com/hubfs/reports/ics-scada.pdf besøkt 05.03.2017.

et selskap skulle bli utsatt for et cyberangrep som påvirker fysiske prosesser og ødelegger fysiske komponenter, så er tidslinjen for å erstatte og reparere de fysiske komponentene lenger enn den er for rene programvarefeil som løses ved omformatering og nedlasting av ny programvare.[49]

Sikkerhetsfirmaet Kaspersky Lab har benyttet blant annet verktøyene Shodan og Censys search samt en «fingerprint» database til å identifisere leverandører og versjoner av komponenter til industrielle kontrollsystemer. Deres funn viser at:[50]

- 220558 industrikontrollkomponenter globalt er tilgjengelig via internett, flest i USA og Europa
- Usikre protokoller er brukt i 92% av de komponentene som er tilgjengelige via internett
- Mange sårbare komponenter er i stor utstrekning brukt, sårbarheter omfatter kjente sårbarheter som er kommunisert i en sårbarhetsdatabase tilgjengelig for alle og forhåndsprogrammerte (hardkodet) passord
- Mange industrier er rammet, hvilket henger samme med at samme leverandør leverer til flere industrier.

Sikring av SCADA-systemene trenger en helhetlig tilnærming der logisk sikring av systemene inngår, der fysisk sikring er en del av regimet og der en også tar inn over seg at også mennesket kan utgjøre en sikkerhetsrisiko.

For å løse sikkerhetsutfordringen i lokalkontrollanlegg må en risikobasert tilnærming anvendes og sikkerhetsmekanismer vurderes utfra hensynet til risiko. Aktuelle praktiske tiltak er fysisk skallsikring og adgangskontroll, interne sikkerhetsprosedyrer og retningslinjer, minimering av logiske tilganger til systemet og konsekvensreduserende tiltak som vern. Det finnes tekniker og løsninger som kan redusere risiko knyttet til informasjonsutveksling på tvers av sikkerhetsdomener betydelig, f.eks. bruk av idéer og tanker fra NATO-konseptet Information Exchange Gateways[52] kombinert med grensesetting, overvåking og fallback-løsninger. En annen sikkerhetsstrategi er å holde kontrollanlegget så reint som mulig, dvs. å fjerne unødig funksjonalitet og unødvendige logiske koplinger og tjenester. Dette kan komme i konflikt med leverandørers ønske om å overvåke egne komponenter for å i neste omgang utvikle bedre produkter.

---

[49] *Up and to the Right ICS/SCADA Vulnerabilities by the Numbers, Threat intelligence Report,* Recorded Future,2015, https://go.recordedfuture.com/hubfs/reports/ics-scada.pdf besøkt 05.03.2017.

[50] Andreeva, O., Gordeychik,S., Gritsai, G., Kochetova, O., Potseluevskaya, E. Sidorov, S. I. and A.A. Timorin, *Industrial control systems and their online availability*, Kaspersky, https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Availability_Statistics.pdf, besøkt 24.10.2016.

[51] *Control Systems Cyber Security: Defence in Depth Strategies*, May 2006, Prepared by Idaho Laboratory, US Departement of Homeland Security. External Report #IN/EXT-06-11478.

[52] *Information exchange gateways. The evolving story*. White paper, Nexor, April 2015, https://www.nexor.com/wp-content/uploads/2016/02/Information-Exchange-Gateways-The-Evolving-Story.pdf, besøkt 06.02.2016

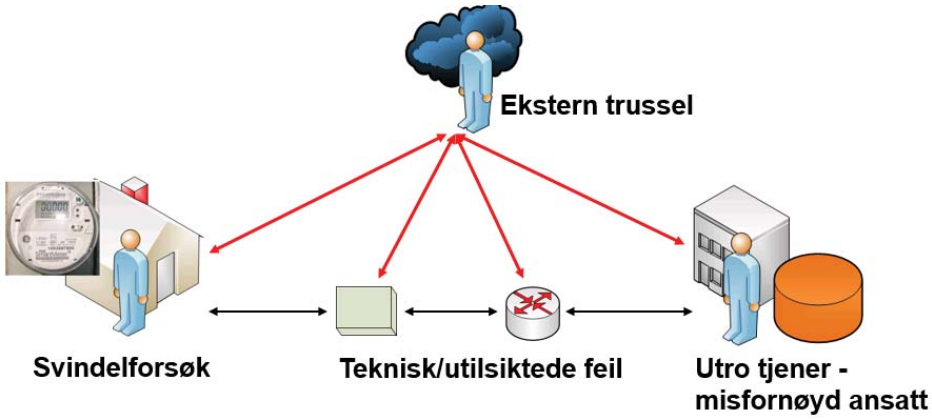
I kontrollanleggene er sikkerhetsfokuset i første rekke på personsikkerhet, miljøsikkerhet og tilgjengelighet. Å drifte kontrollanlegg krever i dag en annen type kompetanse enn å drifte IT-systemer eller samband, men på sikt kan dette bildet endre seg.

3.4 Endret risikobilde med innføring av ny teknologi

Trusler mot AMS kan i hovedsak oppsummeres som:

- Generelle og målrettede angrep fra eksterne aktører
- Svindelforsøk eller andre angrep utført av strømkunder
- Tekniske eller andre utilsiktede feil
- Utro tjenere eller ansatte i nettselskap (eller en av dets underleverandører) som ønsker å ramme nettselskapet eller selskapets kunder

Truslene er illustrert i Figur 3.2.



Figur 3.2 Trusler mot AMS

Trusler mot AMS kan innebære utbytting av ICer (Integrated Circuit) med en type som inneholder skadevare eller sosial manipulasjon av personell som produserer komponenter eller programvare for å få tilgang til å laste inn uønsket programkode. Andre trusler kan være tyveri av programvare for å klone smarte målere, utbytting av smarte målere med falske enheter, at ansatte eller samarbeidspartnere utfører uautorisert re-kalibrering (for eksempel for egen vinning mot å tilby kunden lavere rapportert strømforbruk). Hackere som ønsker å overvåke kommunikasjonskanaler, eller hackere som angriper fysisk smartmålere for å endre kode eller fange opp krypteringsnøkler er også eksempler på trusler.[53] Det smarte el-nettet har mange tekniske lag som hver for seg representerer potensielle inngangsporter for angrep.[54]

Dersom uvedkommende skulle få adgang til AMS, kan ødeleggelse eller endring av programvare i målere gjøre at målerne ikke oppfører seg som de skal. Dersom noen skulle

[53] "7 serious smart meter security threats", Smartgridnews, http://www.smartgridnews.com/story/7-serious-smart-meter-security-threats-do-not-involve-hacking-network/2014-07-28 besøkt 23.12.2016.

[54] Ghansah, I., *Smart Grid Cyber Security – Potential threats, vulnerabilities and risks*, 2012, http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf besøkt 23.12.2016

greie å skaffe seg uautorisert tilgang til en eller flere AMS-målere kan det også medføre tilgang til målerdata, hvilket er å anse som personopplysninger. Her vil kundens privatliv og nettselskapenes rykte først og fremst kunne stå på spill, og i mindre grad forsyningssikkerheten. I Elhub knyttes fødselsnummer til kundene, noe som vil gjøre en data-lekkasje fra Elhub eller nettselskap enda mer sensitivt. Elhub har innført flere tiltak for å unngå at måledata kan kobles direkte til personnummer, blant annet bruk av egne Elhub-identifikasjonsnummere. Elhub vil også inneholde en samlet historisk sammenstilling av det nasjonale energiforbruk.

Uautorisert endring av måledata er en annen type trussel. Slik endring kan være med vinningshensikt eller hevnønske. I følge NBC News hadde FBI i 2010 mistanke om at ansatte i et kraftselskap i Puerto Rico siden 2009 hadde tatt betalt av strømkunder for å justere ned deres AMS-måleres registrering av forbruk. Dette skal ha blitt gjort gjennom målernes infrarøde service port og/eller ved å benytte magneter for å manipulere ned målingene. FBI skal ha anslått årlig tap for dette forholdsvis store kraftselskapet på opptil 400 millioner dollar.[55]

Konsekvenser av en eventuell masseutkobling via AMS-måleres brytefunksjon vil stort sett kunne være de samme som ved bortfall av strømforsyning ellers. Imidlertid er sykehus og andre sentrale bygg og installasjoner som regel trafomålte og ikke AMS-målte, og disse får dermed en mindre risiko. Strømutfall kan vedvare over lang tid for store deler av befolkningen dersom noen skulle kunne klare å både slå av strømmen og deretter endre målerens programvare slik at måleren ikke kan benyttes for å slå på strømmen igjen. Dersom målerne eller enkelte komponenter i dem må fysisk byttes ut, kan det bli knapphet på målere (eller visse komponenter de er avhengige av). En vil da bli nødt til å finne andre løsninger enn å bytte ut målere for å få distribuert strøm inn i hjemmene igjen. Da vil det kunne bli snakk om å koble strøm på «gamlemåten» utenom AMS-målere for en periode før nye forsyninger av utstyr kommer på plass.

3.5 Utilsiktet risiko i markedet

3.5.1 Konsentrasjonsrisiko

I dagens samfunn bidrar kompleksitet og gjensidige avhengigheter til økt risiko. Teknologien utvikles for å håndtere stadig nye oppgaver, og gamle og nye systemer bygges sammen for å dra nytte av hverandre.

Sektoriell konsentrasjonsrisiko i denne sammenheng kan sees på som en situasjon hvor en spesiell type produkter eller tjenester øker risikoen i sektoren grunnet opphopning av avhengigheter. Konsekvens ved slik opphopning gjør seg spesielt gjeldende dersom det er snakk om essensielle produkter eller tjenester og i tillegg dersom det er betydelig dominans i markedet. Det finnes en rekke eksempler på at feil hos teknologiske virksomheter med markedsdominans har ført til alvorlige, og mer eller mindre nasjonale, konsekvenser.

---

[55] Liebowitz, M. "Smart meter hacks cost hundreds of millions annually, FBI says", NBC News, 2012. http://www.nbcnews.com/id/47003851/ns/technology_and_science-security/t/smart-meter-hacks-cost-hundreds-millions-annually-fbi-says/#.WFE8of7FCSQ besøkt 23.12.2016.

A) Telenor 6. mars 2014: En forstyrrelse i strømnettet i Telenors sentral i Ålesund på mindre enn et sekund gjør at en strømbryter går i stykker og et backup-aggregat starter opp. Det utløses en alarm i Telenors operasjonssenter på Fornebu, men den drukner i 30.000 andre små og store alarmmeldinger fra hele landet som strømmer inn. Etter nesten 4 timer er backup-batteriene ved Ålesund-sentralen tomme og nye alarmer går.[56] Feilen i bryteren gjør at også strøm fra aggregat blir hindret fra å komme frem til batterier og utstyr.[57] På dette tidspunktet går det opp for Telenor at telenettet er nede. Telenor på Fornebu forsøker da å få tak i entreprenører for å sjekke feilen, men klarer det ikke fordi mobil- og telenettet er nede. Når Telenor til slutt fås tak i mannskap, kommer de ikke inn i sentralen i Ålesund fordi kortleseren ikke virker som følge av mangel på strøm.

   Innbyggerne i Ålesund og 36 kommuner mellom Sognefjorden og Smøla ble rammet da telenettet brøt sammen.[56] Telenettet var nede ca. 5,5 timer, og som en konsekvens måtte eksempelvis politiet gå over til reserveløsning for 112. Anrop ble rutet til nødsentralen i et nabofylke, som var operativ. Imidlertid kunne ingen ringe likevel siden hele telenettet var nede.

B) Telenor 30. oktober 2014: Over en periode på 2,5 timer kunne ingen ringe eller sende sms i noen deler av Telenors nett. Over halve Norge ble rammet av sammenbruddet og over 3 millioner mobilkunder i Telenor mistet kontakten med omverdenen. Det omfattende sammenbruddet kom da det ble gjennomført planlagt arbeid i Telenors abonnements-database. Årsaken var en feil en kundebehandler la inn i en database, og når denne ble forsøkt fikset ved å slette feilaktige data som var lagt inn, ble feil data slettet og databasen slått ut. For å sikre redundans hadde Telenor flere kopier av databasen rundt om i landet, men feilen ble replisert også til disse databasene og dermed gikk disse ned i tillegg.[58]

C) Tieto 25. november 2011 (Sverige): Teknisk svikt hos driftsleverandøren Tieto førte til at både primær- og reservesystemet for lagring av data sviktet. Ny maskinvare var på plass etter kort tid, men prosessen med å gjenopprette dataene tok flere uker. En serie uhell forsterket av manglende beredskapsplanlegging førte til at cirka 50 virksomheter i Sverige, både offentlige og private, mistet datatjenester i opptil flere uker. Blant disse var 350 apotekfilialer, som ikke fikk delt ut resepter, og det svenske biltilsynet, som ikke fikk effektuert kjøretillatelser.[59]

---

[56] Johansen, P. A. (2014) «Mobilnettet svikter gang på gang», Aftenposten, http://www.aftenposten.no/norge/Mobilnettet-svikter-gang-pa-gang-78084b.html, 23.12.2016.

[57] Johansen, P. A., «Les hele rapporten fra Post- og teletilsynet her: Ekomutfall første halvår 2014», http://www.aftenposten.no/norge/Les-hele-rapporten-fra-Post--og-teletilsynet-herEkomutfall-forste-halvar-2014-78130b.html besøkt 23.12.2016.

[58] Johansen, P. A. (2015) «Slik mistet halve Norge mobilnettet», Aftenposten, http://www.aftenposten.no/norge/Slik-mistet-halve-Norge-mobilnettet-66022b.html besøkt 23.12.2016.

[59] NOU 2015:13, Digital sårbarhet – sikkert samfunn, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf besøkt 05.03.2017.

3.5.2 Komplekse interaksjoner og tette koblinger

Komplekse interaksjoner kan defineres som «interactions [..] of unfamiliar sequenses, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible».[60] Med andre ord er det snakk om samspill innad i avanserte og uoversiktlige sekvenser med innslag av usikkerhet. Teknologien utvikles stadig, og med det følger økende kompleksitet og risiko.[61] Målet er å øke mulighetene, effektiviteten og produksjonen i samfunnet, samt ofte også ett ønske om økt sikkerhet. Imidlertid er det slik at mange nye grupper som blir trukket med inn i teknologiens virkningsfelt, ikke har organisasjonsformer som passer til den økende kompleksiteten disse teknologiene har. Som ett resultat av dette øker risikoen for at alvorlige hendelser og ulykker kan inntreffe.

Tette koblinger beskrives som et system hvor det ikke finnes noe slakk eller buffer mellom to deler,[61] hvilket betyr at det som skjer på ett sted har direkte innvirkning på ett annet sted.[60] En feil ett sted i systemet vil altså nærmest umiddelbart kunne føre til en sekundærfeil som direkte årsak. Sekundærfeilen kan potensielt være en katastrofal feil i ett avansert system. Systemer som har tette koblinger og komplekse samspill vil være sårbare. Når disse inngår i systemer, som har potensiale for katastrofer, utgjør de den fremste utfordringen i samfunnet. Eksempler på slike virksomheter er kjernekraftverk, kjemisk industri, kjernevåpensystemer og damanlegg.[61] Problemet her er at det som regel ikke er mulig å fullstendig fjerne risiko-aspektet, med mindre en kvitter seg med hele systemet (hvilket som regel ikke er et reelt alternativ). Det vil alltid være en form for risiko forbundet med slike systemer uansett hvor mye sikkerhetstiltak en har. Den eneste gjenstående muligheten er da å redusere risikoen til ett nivå hvor det er mulig å leve med den.

3.5.3 Konsentrasjonsrisiko i energisektoren

Energisektoren utvikler stadig mer kompleksitet i sine systemer for fjernstyring og driftsoptimalisering. Et siste tilskudd blir nå innføring av AMS og de muligheter for innhenting av data dette medfører. Ved å integrere AMS med kunde- og administrasjons-systemer kan nettselskapene enklere får oversikt over alle kundeopplysninger på en gang. Ved å integrere AMS med DMS kan nettselskapene utnytte data fra sensorer i AMS om jordfeil, strømutfall og lignende til å trigge automatiserte handlinger som svar på slike hendelser. Dette sikrer effektiv drift. Ved å integrere AMS med driftskontrollsystemer kan en optimalisere nettdrift i samspill med andre sensor-systemer for optimalisering av kraftdistribusjonen. At mest mulig går automatisk uten menneskelige mellomledd vil være effektiv styring. Det eliminerer menneskelige feil, men det er likevel viktig å huske på kompleksiteten og den medfølgende risikoen dette vil kunne introdusere.

Ved høy kompleksitet vil en gjerne få et mindre antall aktører å velge mellom når det gjelder utvikling, drift og vedlikehold av IKT-løsninger. Dersom en ender opp med en eller svært få leverandører for nøkkelprodukter eller tjenester i deler av komplekse

[60] Perrow, C. *Normal Accidents.* USA: Princeton, 1999.

[61] Karlsen, J. E. *Ledelse av helse, miljø og sikkerhet.* Bergen: Fagbokforlaget, 2012.

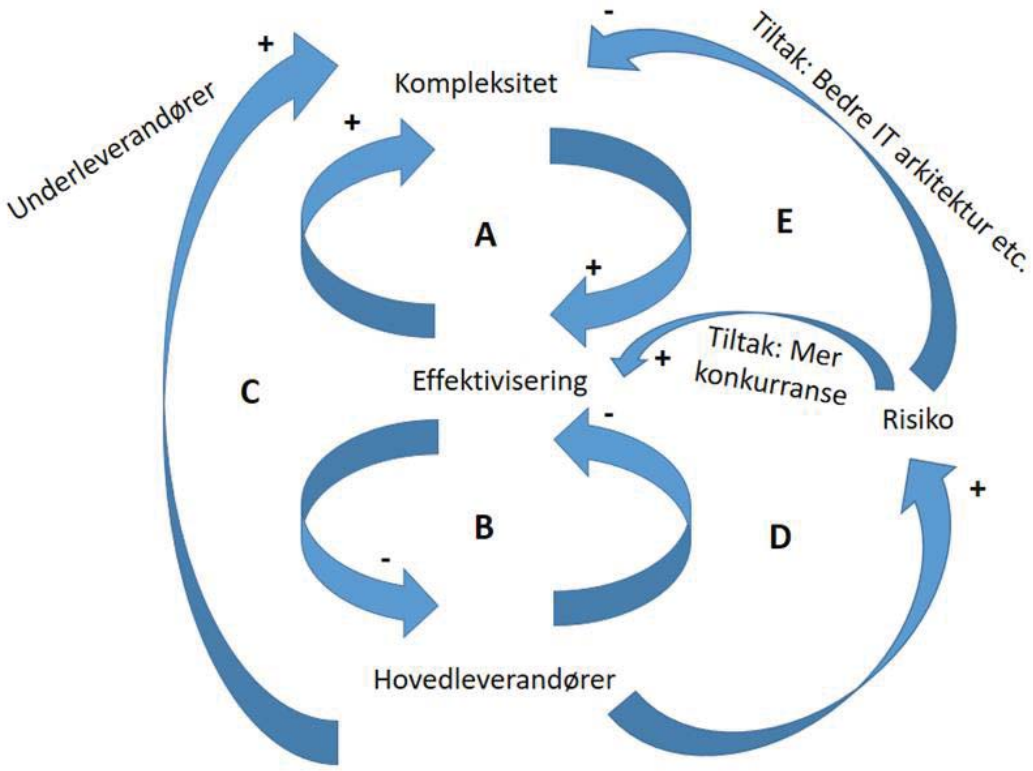
systemer, vil det skapes et avhengighetsforhold som kan være en risiko. Ulike typer risikoer kan vise seg på kan være:

1. Knapphet på ressurser (teknisk utstyr og personell) i forbindelse med større hendelser. Dette kan føre til at det tar unødvendig lang tid å rette feil eller skaffe reservedeler
2. Leverandørspesifikke feil som får konsekvenser for store deler av, eller for hele bransjen (kan være en feil i en komponent eller en oppdatering som slår feil)
3. Personavhengige forhold kan få konsekvenser (dersom kun to eller tre personer vet hvordan deler av et komplekst system virker, kan det bli problematisk om disse personene plutselig skulle bli utilgjengelige)
4. Når en først har valgt en leverandør i et komplekst terreng, kan det gjøre det vanskelig å bytte til en ny leverandør på et senere tidspunkt (dersom dette skulle bli nødvendig) fordi andre selskaper ikke har kompatible produkter
5. Selskapet en benytter som leverandør av en tjeneste kan bli kjøpt opp av et firma en ikke stoler på.

Figur 3.3 viser hvordan økt effektivisering i energisektoren typisk vil kunne påvirke områder som kompleksitet og antall tilgjengelige leverandører. En kan anse økt effektivitet på samme måte som økt automatisering. Dette vil som et resultat gi økt kompleksitet med tanke på at gamle systemer integreres med nye systemer og nye systemer bygges ut etc. Økt effektivitet og økt kompleksitet sees her som en forsterkende løkke hvor økt kompleksitet gir bedre utnyttelse av systemer og dermed økt effektivisering, mens økt effektivisering gir økt kompleksitet i systemer (loop A). Økt effektivisering vil igjen føre til at det blir færre leverandører som er i stand til å levere de stadig mer komplekse tjenestene (loop B). At en får færre leverandører å velge mellom vil sannsynligvis øke prisen på tjenester, og mangel på riktig kompetanse kan gjøre at en ikke vil klare å bringe ut så mye potensiale lenger. Altså vil økt effektivisering kunne virke negativt inn på antall tilgjengelige leverandører, som vil virke negativt inn på effektivisering.

Videre vil en kunne se at selv om en får færre hovedleverandører å velge mellom pga. økt kompleksitet, så vil det totale antallet underleverandører sannsynligvis gå opp fordi det er så mange ulike spesialkomponenter og spesialtjenester som vil være nødvendig i de komplekse systemene. Dette vil føre til økt kompleksitet igjen med tanke på utvikling, drift og vedlikehold. Den økte kompleksiteten antas likevel å ha en positiv virkning på effektiviteten dersom dette gjøres riktig (loop C).

At en får færre hovedleverandører og flere underleverandører vil imidlertid øke risikoen for at noe går galt (liten tue kan velte stort lass). For å minimere risikoen kan myndigheten regulere markedet slik at det ikke blir mulig for en hoved-leverandør å få totaldominans i markedet (loop D). Økt konkurranse vil gjerne virke positivt inn på effektiviteten. Et annet risikoreduserende tiltak kan i stedet være å satse på å bedre IT-arkitekturen, og på den måten ta høyde for sårbarhetene ved å kun ha tilgang på én hovedleverandør (loop E). Bedre IT arkitektur vil typisk skaffe bedre oversikt over systemer og hindre unødvendige ledd, og på den måten minske kompleksiteten i systemene. Ulike sikkerhetstiltak kan imidlertid også fort gi noe negativ effekt for effektiviteten i virksomheten.



Figur 3.3 Effektivisering, kompleksitet og konsentrasjonsrisiko

Selv om et foreslått virkemiddel i figuren over er å tvinge gjennom økt konkurranse (altså regulering av antall leverandører på markedet eller innblanding i valg av leverandører for bransjen) vil dette sannsynligvis være vanskelig å få til i praksis. NVE har per i dag ikke hjemmel som direkte kan benyttes for et slikt formål. Politiets sikkerhetstjeneste (PST) har kritisert ekom-bransjen i en årrekke uten at det har hatt signifikant effekt på valg av leverandør for infrastruktur.[62] Regelverket NVE forvalter åpner imidlertid for at en kan kreve høy sikkerhet i de løsninger som velges, og arbeidsgruppen vurderer at dess mer komplekse systemene blir, jo viktigere blir sikkerhetsarbeidet i virksomhetene.

3.6 Mangel på incentiver til å utvikle sikker programvare

Det kan stilles spørsmål om markedet alene, på bakgrunn av rene bedriftsøkonomiske kostnytte -vurderinger, vil klare å peile seg inn på et IKT-sikkerhetsnivå som ivaretar samfunnets krav til forsyningssikkerhet. I et tilbakeskuende perspektiv er det lite som tyder på at bedre tekniske tiltak alene vil løse problemene med digitale sårbarheter i framtida. Grunnen er blant annet manglende økonomiske incentiver for sikkerhet. I artikkelen «Why Information Security is Hard – An Economic Perspective» av professor

[62] Østby, L. (2014) «PST frykter kinesisk 4G-spionasje», TV2, http://www.tv2.no/a/5279820/ besøkt 23.12.2016.

Ross Anderson (2001) gis flere forklaringer med bakgrunn i økonomisk teori: "*Many of the problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons*."[63] Andersson henviser til viktigheten for programvareleverandører av å være først på markedet. Den som er tidlig ute og får markedsdominans, vinner alt. I følge Andersson avhenger verdien på produktet av hvor mange som bruker produktet. Sagt med andre ord, verdien av Facebook, Google og andre tjenester øker med antall brukere. Et annet moment er at programvare blir produsert med utilstrekkelig sikkerhet, produktet sendes på markedet med lavere pris og kostnadene for oppdatering av svakheter og retting av sårbarheter legges på kundene i ettertid. Kundene kan dessuten ikke se sårbarhetene i programvaren – det er tusenvis av kodelinjer. Kunden er prisgitt informasjon fra leverandøren. Fordi produktet eller programvaren ikke er feilfri, må brukere av programvare leve med ventetid og ekstra arbeid med å patche (rette) sine sårbare systemer.

Sikkerhetstjenester og -produkter kan kjøpes, og de kan ha prisdifferensiering i forhold til gratis versjon, kjøpt tjeneste og ekstra godt kjøpstilbud. Slike prisdifferensierte tilbud finnes hos antivirusleverandører. I denne verden vil også IT-leverandørene ha et incentiv til å hindre kundene å skifte leverandør. Det koster arbeidsinnsats for kundene å skifte leverandør. Et siste moment fra Andersson er plassering av ansvar, det er kundene som bærer ansvaret og den økonomiske byrden ved feil i programvare, selv om feilen skyldes svikt hos den som utviklet programvaren. Andersson konkluderer med at sikkerhetsutfordringene derfor ikke kan løses med teknologi og rasjonelle risikoanalyser alene. Her er heller ikke gode politiske intensjoner tilstrekkelig.

I EUs cybersecurity strategi av 2013 pekes det på det delte ansvaret for IKT-sikkerhet: *All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.*[64]

---

[63] Andersson, R., "Why Information Security is Hard - An Economic Perspective", University of Cambridge Computer Laboratory, 2001, https://www.acsac.org/2001/papers/110.pdf, besøkt 22.10.2016.

[64] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, s 4. http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf besøkt 05.03.2017.

Del II Internasjonale og nasjonale føringer

4 Internasjonale føringer for energisektoren

4.1 Initiativer og føringer fra EU

4.1.1 Europeisk program for beskyttelse av kritisk infrastruktur

Målet med *European Programme for Critical Infrastructure Protection* (EPCIP) er å tilrettelegge for en best mulig beskyttelse av kritisk infrastruktur. EPCIP retter seg mot både europeisk og nasjonal infrastruktur og har en helhetlig tilnærming til farer og trusler (all-hazards approach). Norge har sluttet seg til EPCIP-direktivet og forankret dette i norsk lovgivning.[65] EPCIP har sin forhistorie tilbake til 2005. Den europeiske union (EU)-kommisjonen har fastsatt prinsipper og virkemidler som trengs for å gjennomføre EPCIP. Rammeverket for EPCIP består av følgende:

- En prosedyre for å identifisere og utpeke (europeisk) kritisk infrastruktur og en felles tilnærming til å vurdere behovet for å forbedre beskyttelsen av slik infrastruktur. Dette vil bli gjennomført gjennom et direktiv
- Tiltak for å lette gjennomføringen av EPCIP, inkludert en EPCIP handlingsplan, Critical Infrastructure Warning Information Network (CIWIN), opprettelsen av Critical Infrastructure Protection (CIP) ekspertgrupper på EU-nivå, CIP informasjonsdeling prosesser, og identifisering og analyse av avhengigheter
- Støtte til EU-land innenfor området National Critical Infrastructures (NCIs) og beredskapsplanlegging
- En ekstern dimensjon knyttet til gjensidig avhengigheter der avbrudd i eller ødeleggelse av en bestemt infrastruktur kan ha konsekvenser for land utenfor unionen og vice versa. Det er derfor viktig å styrke det internasjonale samarbeidet på dette området gjennom sektoravtaler
- Økonomiske tiltak, særlig EU-program slik som «Forebygging, beredskap og konsekvenshåndtering av terrorisme og andre sikkerhetsrelaterte risiko»

ECPIP bygger på en handlingsplan bestående av tre hovedprosesser:[66]

- Den første er knyttet til de strategiske aspekter av EPCIP og utvikling av tiltak horisontalt som gjelder for alt arbeid med kritisk infrastruktur
- Det andre gjelder beskyttelse av europeiske kritiske infrastrukturer og har som mål å redusere sårbarheten for disse
- Den tredje er et nasjonalt rammeverk for å bistå EU-land i å beskytte sine nasjonale kritiske infrastrukturer

---

[65] *Lov om endringer i sivilbeskyttelsesloven (gjennomføring av EPCIP-direktivet),* https://lovdata.no/dokument/LTI/lov/2012-12-14-90

[66] European Programme for Critical Infrastructure Protection, EUR-Lex, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260 besøkt 05.03.2017.

EPCIP har fokus på resiliens (motstandsdyktighet)[67] og gjensidige avhengigheter mellom kritiske infrastrukturer i ulike sektorer, inklusive på tvers av ulike medlemsland. Som følge av transmisjonsnettets grenseoverskridende arkitektur, er energi en av sektorene arbeidet videre rettes mot. I piloten ligger planer for å utvikle verktøy for:

- Risikovurdering og –styring
- Beredskapsstrategier herunder stresstesting, kompetanseheving, øvelser og utveksling av personell
- Respons, ikke bare umiddelbar, og med også gjenoppretting av kritiske tjenester i et lengre perspektiv[68]

I *Prop. 129 L (2011-2012) Endringer i sivilbeskyttelsesloven* (gjennomføring av EPCIP-direktivet), blir Justis- og beredskapsdepartementet (JD) utpekt til kontaktpunkt for europeisk kritisk infrastruktur i Norge. JD vil være ansvarlig for å koordinere spørsmål knyttet til denne type infrastruktur innen Norge med medlemslandene og med Kommisjonen. Direktoratet for samfunnssikkerhet og beredskap (DSB) vil være ansvarlig for å samordne oppfølgingen av direktivet i Norge.

4.1.2 EUs cyber security strategi

I cyberstrategien for 2013 sier EU kommisjonen at cybersikkerhetshendelser øker raskt og at slike hendelser kan forstyrre tjenester vi tar for gitt, for eksempel energi, helse, vann mv. Samme lover og normer som gjelder i det virkelige livet gjelder også i cyber-domenet. Strategien omtaler noen tiltak for å løfte sikkerheten generelt: Etablere minstekrav gjennom lovgivning, dvs. NIS (The Directive on security of network and information systems), sette opp funksjonsdyktige CERTer, utvikle cybersikkerhetsstrategier, samarbeidsmodeller og heve kompetansenivået. Det blir også lagt vekt på samarbeid mellom myndigheter og privat sektor.[69]

EUs cyber-sikkerhetspolitikk for energiforsyningen tar utgangspunkt i utviklingen mot smarte nett og smarte byer og en desentralisert energiforsyning. Selv om det er mange fellestrekk både når det gjelder utfordringer og teknologibruk mellom ulike EU-land, er det store forskjeller i hvordan de ulike landene har implementert sikkerhetskrav. Skal smarte byer bli en realitet, kreves det en konvergens mellom driftskontrollsystemer og tradisjonell IT. Resultatet blir økt risiko i form av flere angrepsflater. Det er flere initiativer i EU for å adressere IKT-sikkerhet. Initiativene inkluderer å vurdere

---

[67] Resiliens er et mål på et systems evne til å tilpasse seg endrede betingelser og justere seg tilbake til normal tilstand.

[68] *Commission Staff Working Document. On a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure*, Brussels, 28.8.2013, http://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf, besøkt 26.10.2016.

[69] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint communication to the European Parliament, the council, the European economic and social committee and the commeettee of the regionas, Brussels, 7.2.2013, https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, besøkt 26.10.2016.

minimumsstandarder, bruk av revisjoner og sanksjoner, og oppmuntre til tverrsektoriell informasjonsdeling. En rapport til Europaparlamentet i 2016 anbefaler EU-regulering på følgende områder[70]:

- Utpeke en sentral nasjonal myndighet i energisektoren med ansvar for å sikre at virksomhetene driver i samsvar med cybersikkerhetspolitiske mål og regulering
- Pålegge aktører i energisektoren rapportering av uønskede hendelser
- Stille krav til relevant informasjonsdeling også på tvers av infrastrukturer og medlemsstater
- Samkjøre cyber-sikkerhetsaktiviteter på tvers av nasjonale infrastrukturer og inkludere kontrollsystemsikkerhet, i dette ligger også samkjøring mot nasjonale cyber sikkerhetsstrategier
- Utvikle sikkerhetsstandarder for minimumssikring av energisystemet, i dette inngår å kreve risikoanalyser, samsvar med sertifiseringskrav, etablere regulatoriske sanksjoner og publisere avvik etter revisjoner
- Etablere et sertifiseringsstyre som består av offentlig og private aktører som skal koordinere smarte nett og energi cyber-sikkerhet sertifisering og støtte nasjonalt sertifiseringsarbeid

I EUs Cyber Defence Policy Framework framheves blant annet samarbeid sivilt-militært, herunder mellom EU-Nato. Det sies videre at medlemsland, European External Action Services og European Defence Agency (EDA) bør samarbeide tettere for å utvikle evne til å forsvare seg mot cybertrusler.[71]

4.1.3 NIS-direktivet fra EU

EU-kommisjonen fremla 7. februar 2013 et forslag til direktiv om tiltak for å sikre et høyt felles nivå for nettverk- og informasjonssikkerhet i EU. NIS-direktivet (The Directive on security of network and information systems) har gjennomgått mange runder med tilbakemeldinger og ble endelig godkjent av EU-parlamentet og rådet 19.7.2016.[72] Bakgrunnen for forslaget til direktivet er at det i dag, innen EU, ikke er implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå god nok sikkerhet i nettverk og informasjonssystemer, som er særlig viktige for det indre markeds funksjon. Justisdepartementet har i sitt posisjonsnotat sett direktivet som EØS-relevant og akseptabelt. Norge har i stor grad allerede gjennomført de tiltak som kommisjonen foreslår.[73]

---

[70] *Cyber security strategy for the energy sector. Study for the ITRE Committee*, 2016, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf besøkt 05.03.2017.

[71] *EU Cyber Defence Policy Framework*, Council of the European Union, DG C 2B – Security, 22.10.2014.

[72] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, EUR-Lex, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148 besøkt 05.03.2017.

[73] *Europaparlamentets og råds direktiv (EU) 2016/1148 av 6. juli 2016 om tiltak som skal sikre et høyt felles sikkerhetsnivå I nettverks- og informasjonssystemer i EU.*

Direktivet vil gjelde for følgende innen energisektoren:

- Transmission System Operators (TSO)er
- Distribution System Operators (DSO)er
- Strømleverandører
- Markedsplasser for elektrisitet

Direktivet kan deles i tre hoveddeler, som setter krav til henholdsvis etablering av nasjonale rammeverk for IKT-sikkerhet, etablering av internasjonale samarbeidsfora og IKT-sikkerhet for virksomheter. Etablering av internasjonale samarbeidsfora medfører ingen relevante krav for sikkerheten i energisystemet.

Etter artikkel 8 i NIS skal medlemsstatene peke ut en eller flere nasjonale kompetente myndigheter for IKT-sikkerhet, som skal påse at direktivet implementeres nasjonalt. NVE og OED foreslo i sine høringsinnspill til JDs høring om NIS-direktivet 15. september 2016 at beredskapsmyndigheten utpekes som en av disse nasjonale kompetente myndighetene.

Etter artikkel 9 skal medlemsstatene peke ut et eller flere sektorvise responsmiljøer (CSIRT) for IKT-sikkerhet. Det er i dag ingen offisiell sektor-CSIRT for energiforsyningen, men NVE viste i sitt høringsinnspill til JDs høring om NIS-direktivet 15. september 2016 til etablering av KraftCERT.

NIS-direktivet stiller i art. 14 og art. 16 krav til at medlemslandene sørger for sikkerheten i nettverks- og informasjonssystemene tilhørende to kategorier av virksomheter - operatører av essensielle tjenester og tilbydere av digitale tjenester. Det stilles forskjellige sikkerhetskrav til de to kategoriene virksomheter. Felles for alle virksomheter uansett kategori, er at de skal beskytte de nettverk og informasjonssystemer som de benytter seg av i sin virksomhet. NIS-direktivet legger ikke begrensninger på medlemslandenes muligheter for å sikre kritiske samfunnsfunksjoner, særlig med henblikk på ivaretakelse av nasjonal sikkerhet, eller opprettholde lov og orden, herunder kriminalitetsbekjempelse, jf. art. 1(6). Det følger av art. 1(7) at dersom eksisterende sektorregelverk stiller krav om IKT-sikkerhet eller hendelsesvarsling, og reglene har minst like god effekt som NIS-direktivet, da skal sektorregelverket anvendes.

4.1.4 EUs tredje energimarkedspakke

The European Network of Transmission System Operators (ENTSO-E) representerer 42 systemoperatører (Transmission System Operators, TSO[74]). Med tredje energimarkedspakke får disse en enda viktigere rolle enn før. ENTSO-E arbeider sammen

[74] Transmission system operator' means a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity.

med Agency for the Cooperation of Energy Regulators (ACER)[75] med detaljerte regler for energiforsyningen, også kalt bindende retningslinjer og nettkoder.[76] [77] Målsettingen er økt konkurranse, diversifisering og optimering av bruken av eksisterende infrastruktur. Kodene er delt opp i tre forskjellige grupper.

- Markedskodene[78]
- Driftskodene[79]
- Tilknytningskodene[80]

For arbeidet med veilederen til beredskapsforskriften er driftskodene[81] mest relevant. I tillegg er nettkoden for ekstraordinære hendelser og gjenoppretting[82] som er under utarbeiding relevant. Markedskodene og tilknytningskodene er i mindre grad direkte relevant, men deler av markedskodene setter noen krav til deling av informasjon mellom TSOer som kan måtte vurderes opp mot kravene til sensitiv informasjon i kraftforsyningen i kapittel 6 i bfe.

Driftskodene (OS, OPS og LFC) er samlet i en bindende «retningslinje» for systemdrift (System Operations, SO). Disse innebærer krav til samarbeidet mellom TSOer som omfatter informasjonsutveksling og virkemidler for å ivareta driftssikkerhet, koordinert driftsstansplanlegging og frekvensregulering.

- Artikkel 26 i bindende retningslinje for systemdrift omhandler krav for TSOene til en sikkerhetsplan for beskyttelse av kritisk infrastruktur. Punkt (1) i denne spesifiserer at denne sikkerhetsplanen skal ta hensyn til alle store fysiske og digitale trusselbilder definert av medlemslandet

---

[75] ENTSO-E får oppdraget fra EC, jf. forordning (EF) nr. 714/2009 artikkel 6 nr. 6, jf. nr. 1, men da i utgangspunktet på bakgrunn av ACERs relevante «Framework Guideline» (FG), som er utarbeidet i henhold til artikkel 6 nr. 2-5.

[76] Både «netttkoder» («network codes») og bindende «retningslinjer» («Guidelines») er navn på det som til slutt blir bindende rettsakter vedtatt av EC, dog vedtatt etter forskjellige prosedyrer og hjemler, jf. særlig forordning (EF) nr. 714/2009 hhv. artikkel 6 nr. 11 hhv. artikkel 18 nr. 3 og nr. 5 (som er ECs vedtakshjemler). Den inngående formelle involvering av ENTSO-E og ACER knytter seg kun til forberedelse av Network Codes Cs/ «nettkoder», jf. forordning (EF) nr. 714/2009 artikkel 6, ikke til Guidelines/ «bindende retningslinjer» (GLs), jf. artikkel 18.

[77] Kodene er ennå ikke innlemmet i EØS-avtalen og norsk rett, men dette er et pågående arbeid (januar 2017).

[78] (CACM GL og FCA GL) vedtatt i EU.

[79] (SO GL og NC ER) begge er velsignet i komitologi, men ennå avventer Rådet og Parlamentets aksept, og deretter ECs vedtakelse.

[80] (NC RfG, NC DCC og NC HVDC) vedtatt i EU.

[81] *COMMISSION REGULATION (EU) …/… of XXX establishing a guideline on electricity transmission system operation*, Brussels, 2016, https://ec.europa.eu/energy/sites/ener/files/documents/SystemOperationGuideline%20final%28provisional%2904052016.pdf besøkt 05.03.2017.

[82] *ENTSO-E Network Code on Emergency and Restoration*, 25. March 2015, https://www.entsoe.eu/Documents/Network%20codes%20documents/NC%20ER/150325_ENTSO-E_NC%20ER_final.pdf besøkt 05.03.2017.

- Artikkel 33 til 35 omhandler beredskap, analyse og håndtering. Disse gir også krav om deling av informasjon knyttet til beredskap mellom Distribution System Operators (DSO)er[83] og TSOer i hvert land, og mellom TSOer i tilgrensende land
- Artikkel 40 til 53 omhandler krav til deling av drift og arkitekturdata mellom forskjellige aktører i energiforsyningen`
- Artikkel 61 setter krav til sertifisering av personell som sitter på driftssentraler for transmisjonsnettet[84]

Nettkoden for ekstraordinære hendelser og gjenoppretting[85] er under utarbeiding. Denne omhandler i hovedsak det samme som beredskapsforskriften, for eksempel krav til en plan for sikkerhetstiltak koplet opp mot en rekke forskjellige trusler og hendelser, krav til planer for gjenoppretting, re-synkronisering og informasjonsdeling, krav til kommunikasjonsverktøy og krav til rutiner for tilsyn og testing.

I vinterpakken for energimarkedet som kom vinteren 2016 fremmes også en endring i elmarkedsforordningen som gir Kommisjonen myndighet til å etablere en 'network code' om cybersikkerhet. Hva innholdet i en slik code er, er så langt ukjent.

4.1.5 EUs initiativ for elektrisitets- og gassmarkeder i Europa

Parlaments- og rådsforordning av 25. oktober 2011 om integritet og gjennomsiktighet i energimarkedet (EU) nr. 1227/2011 («REMIT») trådte i kraft i EU 28. desember 2011. Den er ennå ikke gjennomført i norsk rett, i påvente av gjennomføringen av den tredje energimarkedspakken, men skal gjennomføres i norsk rett.

REMIT har som overordnet formål å bidra til mer velfungerende elektrisitets- og gassmarkeder i Europa. Forordningen har bestemmelser som eksplisitt forbyr markedsmanipulasjon og utnyttelse av innsideinformasjon i engrosmarkedene for elektrisitet og gass. Forordningen pålegger også markedsaktørene å offentliggjøre innsideinformasjon.

Markesdaktørene skal rapportere data til den europeiske energimyndigheten, ACER, for å tilrettelegge for overvåkning av energimarkedene, jf. artikkel 8. I visse sammenhenger skal også informasjon rapporteres direkte til den nasjonale reguleringsmyndigheten (jf.

---

[83] Distribution system operator' means a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity

[84] *Commission regulation of establishing a guideline on electricity transmission system operation*, EU, draft, 2016, https://ec.europa.eu/energy/sites/ener/files/documents/SystemOperationGuideline%20final%28provisional%2904052016.pdf besøkt 05.03.2017.

[85] *ENTSO-E Network Code on Emergency and Restoration*, ENTSO-E, 25. March 2015, https://www.entsoe.eu/Documents/Network%20codes%20documents/NC%20ER/150325_ENTSO-E_NC%20ER_final.pdf besøkt 05.03.2017.

artikkel 4 (2), artikkel 7 (2) og artikkel 8 (5)). Informasjonen som rapporteres inn vil i mange tilfeller være kommersielt sett svært sensitiv.

Forordningen har bestemmelser om samarbeid og informasjonsutveksling, jf. artikkel 10. Videre stiller REMIT strenge krav til taushetsplikt knyttet til konfidensiell informasjon som mottas av den nasjonale reguleringsmyndigheten, jf. artikkel 17.

Artikkel 12 i REMIT om «operational reliability» er en helt sentral bestemmelse om datasikkerhet. Når REMIT blir gjennomført i norsk lov, pålegger denne bestemmelsen NVE som reguleringsmyndighet i Norge å sikre «the confidentiality, integrity and protection» av informasjonen som NVE mottar. Videre krever bestemmelsen at NVE aktivt må «take steps to prevent any misuse of such information».

En forutsetning for at ACER kan dele informasjonen som markedsaktørene rapporterer inn direkte til ACER med den nasjonale reguleringsmyndigheten, er at ACER etter en nærmere vurdering finner at reguleringsmyndigheten oppfyller kravet i artikkel 12. Å motta denne informasjonen fra ACER er viktig for at NVE etter hvert skal kunne drive så effektivt tilsyn som mulig med energimarkedene. ACER er i artikkel 12 (3) gitt ansvaret med å identifisere operasjonell risiko og minimere denne gjennom «the development of appropriate systems, controls and procedures». ACER har implementert et informasjonsdelingssystem som sørger for at nasjonal reguleringsmyndighet kan motta relevante data fra ACER. Deler av informasjonen er svært markedssensitiv, og nasjonal regulatormyndighet må oppfylle strenge krav for å få tilgang til systemet. Nasjonal reguleringsmyndighet må etablere IT-løsninger som sørger for at mottatt data blir håndtert på en sikker måte.

I REMIT artikkel 11 fremkommer det at krav til personvern som følger av Europaparlaments og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, gjelder i tillegg til kravene som følger av REMIT.

4.1.6 EUs tiltakspakke for ren energi

Europakommisjonen la den 30.11.2016 fram en «vinterpakke» for ren energi med et stort antall lovforslag og strategidokumenter. Forslagene inkluderer blant annet endringer av eksisterende regelverk for fornybar energi, energieffektivisering og kraftmarkedet, en revisjon av markedsregelverket og tredje energimarkedspakke, samt en ny elektrisitetsrisikoforordning. Kommisjonen foreslår også et nytt styringssystem for energiunionen.

Når det gjelder beredskap og forsyningssikkerhet, består pakken av mange elementer. Innenfor markedsdelen fremlegger Kommisjonen forslag til «risk preparedness» i kraftsektoren. Dette beskrives slik at det vil utfylle tredje pakke og de tekniske reglene som lages for driftsplanlegging mm.

Så vidt arbeidsgruppen kan se inneholder forslaget til forordning to deler: 1) en som går på overvåking av forsyningssikkerhet og 2) en som går på planer for risikohåndtering.

Det er medlemsstatene som er subjekt for forordningen og som skal utpeke en «national governmental or regulatory authority» som ansvarlig for oppgavene. Denne ses i

sammenheng med Network codes on emergency and restoration, NIS direktivet og direktiv 2008/114/EC om kritisk infrastruktur.

Det uttales videre at et velfungerende marked er den beste garanti for forsyningssikkerhet. Samtidig sier de også at en viss grad av samarbeid og koordinering er nødvendig for forsyningssikkerhet. I evalueringsrapporten på forsyningssikkerhet uttales det at tredje pakke bygger på at i særlige tilfeller vil markedsmekanismen og driftsregler kunne være utilstrekkelig, og det må derfor være åpning for at medlemsstatene kan treffe beskyttelsestiltak.

Arbeidsgruppen anser at dette er tiltak som også vil påvirke reguleringen av IKT-sikkerhet i kraftsektoren. Arbeidsgruppen mener erfaringer tilsier at det også vil ta lang tid før denne «vinterpakken» utkrystalliserer seg i konkrete regler for norske kraftaktører.

4.2 Beredskapssamarbeid i Norden

Både myndigheter og systemoperatører har et etablert beredskapssamarbeid. Nordisk Beredskaps og Krisehåndteringsforum (NordBER), består av de de fem nordiske landenes beredskapsmyndigheter innen elektrisitet (fra norsk side NVE) og de fem nasjonale systemansvarlige selskap (TSO), (fra norsk side Statnett). NordBER samarbeider om å sikre en målrettet nordisk beredskap innen elektrisitetssektoren. Samarbeidet har to hovedmål, som begge bidrar til å opprettholde et kontaktnett som er en sentral del av et beredskapsarbeid:

- Samarbeid om regelmessig utveksling av informasjon og erfaringer mellom partene om spørsmål av relevans for kraftsektoren, beredskapsplanlegging og om bestemte oppgaver og temaer i felles arbeidsgrupper, fora og temamøter
- Beredskap (herunder planlegging, ROS-analyser, øvelser mv) for den samlede nordiske kraftsektoren som et supplement til det nasjonale beredskapsarbeidet

Innen området IKT-sikkerhet har NordBER hatt aktiviteter på flere områder gjennom en rekke år:

- Arbeidsgruppe innen IKT-sikkerhetsom har fordypet seg i felles nordiske utfordringer og problemstillinger og fungert som arena for kunnskapsdeling
- ROS-analysegruppe som har arbeidet for å identifisere konkrete utfordringer som kan true sikkerhet og beredskap på selskapsnivå, nasjonalt nivå og nordisk nivå
- Beredskapsplangruppe for utvikling av felles planverk for å håndtere reparasjonsberedskap og ev. hjelpe nordiske naboer innen hele krisespekteret
- Øvelses samordningsgruppe, med formål å utvikle øvelseskonsept (også innen IKT-området), samt initiere øvelser som involverer noen eller alle nordiske land

4.3 Nato og energiforsyningssikkerhet

Nato er opptatt av forsyningssikkerhet på energikilder som petroleum, gass og elektrisitet. Forsyningssikkerhet forstås som pålitelighet, robusthet og leveringsevne også under anstrengte situasjoner. I Nato sin forståelse av forsyningssikkerhet inngår i tillegg

betalingsevne. I konflikter der krig truer, kan energiprisene svinge mye, og prisen på energi i et konfliktområde kan være mange ganger høyere enn utenfor konfliktområdet.

Nato har mobile løsninger som solcellepaneler, vindmøller og batteribanker slik at baser kan etableres med en viss selvforsyningsgrad på elektrisitet i områder der det ikke er mulig å kople seg til den nasjonale infrastrukturen. Disse anleggene kalles microgrid, men Nato vil også i en potensiell konfliktsituasjon ønske å kople seg til nasjonalt transmisjonsnett for å få tilgang til elektrisitet og energiforsyning.

Elektrisitetsforsyning er viktig for kommunikasjon og samarbeid med vertsnasjonen. Nato betrakter IKT og energiforsyning som kritiske og gjensidig avhengige innsatsfaktorer i militære operasjoner. I tråd med økt omfang av offensive cyberoperasjoner, er det blitt enda viktigere å beskytte energiforsyningens IKT-systemer og driftskontrollsystemer, som kan ha betydning for forsyningssikkerheten av energi. Nato etablerte 10. juli 2012 et eget Center of Excellence for Energy Security.[86]

Norge har signert avtalen om NATOs seven baseline requirement - North Atlantic Council in Warsaw 8-9 July 2016. [87] Nato sier her følgende om energiforsyningssikkerhet: *The disruption of energy supply could affect the security of their societies and have an impact on NATO's military operations. While these issues are primarily the responsibility of national governments, NATO continues to consult on energy security and further develops the capacity to contribute to energy security, concentrating on areas where it can add value. To this end, NATO seeks to enhance its strategic awareness of energy developments with security implications; develop its competence in supporting the protection of critical energy infrastructure; and work towards significantly improving the energy efficiency of the military*.[88]

4.4 The Federal Energy Regulatory Commission (USA)

The Federal Energy Regulatory Commission (Kommisjonen) har i varierende grad myndighet over infrastrukturer for energiforsyning og vannkraft. The Federal Power Act, the Natural Gas Act and the Interstate Commerce Act, er sentrale lover på området. Innenfor cyber-sikkerhet bygger gjeldende regime på regelverk og frivillighet. Krav brukes der dette er mulig og henvisning til beste praksis benyttes for de mest kritiske anleggene og systemene. Kommisjonen samarbeider tett med industrien og med andre myndigheter, og deler informasjon om både sårbarheter og trusler på tvers av sektorer.

---

[86] *Nato Center of Excellence*, https://enseccoe.org/en/about-us/centre-of-excellence.html, besøkt 26.10.2016.

[87] Warsaw Summit Communiqué – point 135 - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 http://www.nato.int/cps/en/natohq/official_texts_133169.htm –besøkt 07.11.2016

[88] "NATO's role in energy security", Nato 22. July 2016, http://www.nato.int/cps/en/natohq/topics_49208.htm besøkt 05.03.2017.

Kommisjonen har gjennom revisjon og godkjenning av NERC Reliability Standards (CIP-002-5.1[89]) gitt minimumsstandarder for beskyttelse av IKT-system i energisektoren, som dekker følgende:

- Driftssentraler og backup-driftssentraler
- Transformatorstasjoner
- Produksjonsanlegg
- Systemer og anlegg som er kritiske for gjenoppretting, inkludert oppstart fra svart nett og skadede linjer, og koplinger
- Sikkerhetssystemer som støtter og beskytter pålitelig drift og distribusjon

The Energy Independence and Security Act av 2007 (EISA) gir videre kommisjonen mulighet for å utvikle regelverk, som innebærer å ta i bruk standarder som eksempelvis er utviklet av National Institute of Standards and Technology (NIST) og regelverk relater til smarte nett. EISA krever imidlertid bred consensus. Kommisjonen har så langt ikke gått videre med å ta i bruk standarder og regelverk for smarte nett. Kommisjonen benytter videre følgende dokumenter for beste praksis:

- NIST – Cybersecurity Framework[90]
- NIST – 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations[91]
- NIST – 800-82 – Guide to Industrial Control Systems[92]
- NIST – 800-46 Rev. 2 – Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security[93]
- DOE – Energy Sector Cybersecurity Framework Implementation Guidance[94]
- Executive Order 13636 – Improving Critical Infrastructure Cybersecurity[95]
- Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing[96]

Regelverk for cybersikkerhet i energisektoren inkluderer videre:

---

[89] http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5_1.pdf besøkt 05.03.2017.

[90] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf besøkt 05.03.2017.

[91] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf besøkt 05.03.2017.

[92] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf besøkt 05.03.2017.

[93] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf besøkt 05.03.2017.

[94] http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf besøkt 05.03.2017.

[95] Executive Order -- Commission on Enhancing National Cybersecurity, White house, February 09. 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity besøkt 05.03.2017.

[96] Executive Order -- Promoting Private Sector Cybersecurity Information Sharing, White house, February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari, besøkt 05.03.2017.

- Fixing America's Surface Transportation Act Section 61003(d) som dekker beskyttelse, forebyggende sikring og deling av informasjon om kraftsystemet mellom virksomheter og kommisjonen[97]
- FERC Security Program for Hydropower Projects Rev. 3a (Section 9)[98]
- The North American Electric Reliability Corporation (NERC) sine pålitelighetsstandarder for energisektoren, som kommisjonen reviderer og godkjenner. Dagens standarder inkluderer the Critical Infrastructure Protection (CIP) cybersecurity Reliability Standards[99]
- Cybersecurity Information Sharing Act of 2015 (CISA), som dels har som mål å bidra til at selskaper overvåker systemene sine og beskytter informasjon mot cybertrusler, og å gi en viss beskyttelse for dem som deler informasjon om trusler og sårbarheter mot å bli stilt til ansvar/bli saksøkt i etterkant
- Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), som skisserer den nasjonale politikken for å beskytte kritisk infrastruktur mot cyberstrusler og bidra til at infrastrukturen er motstandsdyktig og samtidig gir muligheter for innovasjon og forretningsutvikling. Målene skal bli møtt gjennom partnerskap, informasjonsdeling, samarbeid og risikobaserte standarder. Executive Order 13636 inkluderer et mandat for å utvikle et rammeverk for å redusere cyber-risikoen for kritisk infrastruktur
- Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015) skal stimulere private selskap og ideelle organisasjoner til å dele informasjon om hendelser og cyber-risiko, og samarbeide for å håndtere hendelsene i sanntid

Kraftsensitiv informasjon omfatter informasjon om infrastruktur, produksjon og transmisjon som kan være nyttig for planlegging av sabotasje, gi detaljinformasjon om lokalisering eller er unntatt offentlig iht. the Freedom of Information Act. Code of Federal Regulations, 18 C.F.R. Part 388 – Information and Requests gir regler for beskyttelse av kraftsensitiv informasjon.[100] I vurderingen skal en balansere mottakers behov for informasjon mot sensitiviteten til informasjonen.

4.5 Danmark

Den 9. November 2016 kom det endringer til lov om elforsyning, og lov om naturgassforsyning. Disse endringene kom dels som et initiativ fra den danske nasjonale strategien for cyber- og informasjonssikkerhet (2014) som hadde som mål å styrke cyber-

---

[97] H.R. 22, 114th Cong. (1st Sess. 2015) Sec. 61003 (*Fixing America's Surface Transportation Act*) https://www.gpo.gov/fdsys/pkg/BILLS-114hr22enr/pdf/BILLS-114hr22enr.pdf besøkt 05.03.2017.

[98] *Federal Energy Regulatory Commission Division of Dam Safety and Inspections FERC Security Program for Hydropower Projects Revision 3A*, FERC, https://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf besøkt 05.03.2017.

[99] *Mandatory standards subject to enforcement*, NERC, http://www.nerc.net/standardsreports/standardssummary.aspx besøkt 05.03.2017.

[100] Code of Federal Regulations, 18 C.F.R. Part 388 – Information and Requests. 18 C.F.R. § 388.113 (*Accessing critical energy infrastructure information*), se https://www.ferc.gov/legal//maj-ord-reg/land-docs/ceii-rule.asp besøkt 05.03.2017.

og informasjonssikkerheten i energisektoren ved å stille krav til cyber- og informasjonssikkerhet. Lovforslaget er også relevant for oppfølging av NIS-direktivet.

Den tidligere beredskapsreguleringen av energisektoren i Danmark regulerte ikke spesifikt beredskap for forsyningskritiske IT-systemer. Gjennom endringene i loven stiller den nye loven krav til at virksomheter skal opprettholde IT-beredskap for forsyningskritiske systemer. De skal ha oversikt over egne systemer, vurdere risikoen for angrep eller svikt, samt motta relevante trusselvurderinger, slik at de kan iverksette tiltak for å begrense konsekvenser. Med lovforslaget gis ansvarlig minister myndighet til å fastsette regler, pålegge tiltak og innkreve gebyrer. Det er systemoperatøren Energinet som skal føre tilsyn med virksomhetene i sektoren, mens Energistyrelsen fører tilsyn med Energinet. Den foreslåtte tilsynspraksisen er lik det som er praksis på andre beredskapsområder og bidrar til helhet i tilsynsarbeidet.

Alle virksomheter pålegges å være tilknyttet en varslingstjeneste som varsler om farer og trusler. Noen virksomheter[101] vil være pålagt å utarbeide en avtale om mulighet for akutt bistand fra en IT-sikkerhetstjeneste. Lovforslaget innebærer i tillegg en hjemmel for økning av inntektsrammen for nettselskapene som følge av kravet om at nettselskapene skal være tilknyttet en IT-sikkerhetstjeneste.

5 Digitaliseringspolitikk i Norge

5.1 Nasjonal IKT-politikk

I stortingsmeldingen *Digital agenda for Norge* skisserer Regjeringen den nasjonale IKT-politikken.[102] En sentral målsetting i nasjonal strategi for informasjonssikkerhet er å sørge for at forvaltningen har en felles tilnærming til arbeidet med informasjonssikkerhet. Nøkkelen til å styrke beredskapen og redusere den digitale sårbarheten i samfunnet, er at det arbeides systematisk med IKT-sikkerhet i alle sektorer. Dette innebærer at det må settes tydelige mål og prioriteringer, med et klart definert ansvar for oppfølging hos alle involverte aktører. I *Digital agenda for Norge* sies det at alle sikkerhetstiltak skal være basert på en risikovurdering. I tråd med ansvarsprinsippet er det virksomhetene selv som skal vurdere om informasjon og systemer er godt nok sikret og som skal iverksette nødvendige tiltak. Flere regelverk pålegger virksomheter å ha et styringssystem for informasjonssikkerhet.[103]

I *Digital agenda for Norge* presiserer regjeringen at de aktivt vil sikre et godt personvern via IKT-politikken gjennom prinsipper for innebygd personvern (privacy by design) og ved å gjennomføre EUs nye personvernregelverk. I dette arbeidet må personvernhensyn

[101] Lovteksten snakker om kategori 1 og 2 virksomheter.

[102] Meld. St. 27 (2015–2016) *Digital agenda for Norge — IKT for en enklere hverdag og økt produktivitet,* https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/, besøkt 15.08.2016.

[103] Meld. St. 27 (2015–2016) *Digital agenda for Norge — IKT for en enklere hverdag og økt produktivitet*, https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/, besøkt 15.08.2016.

veies mot andre viktige samfunnsinteresser.[104] Her kan det også ligge grenseflater opp mot regelverket i energisektoren. Det finnes mye informasjon i IKT-systemer som kan være sensitiv og samfunnsviktig, i tillegg til at IKT-systemene i seg selv kan være viktige. Ekom-nettene er viktige for all verdiskapning. *Digital agenda for Norge* tegner ambisjoner om å sikre ekom-nettene blant annet ved å si at de skal være forsvarlig sikret mot uvær og feil og være forsvarlig sikret mot fysiske og logiske angrep.

I Stortingsmeldingen - *Risiko i et trygt samfunn*,[105] som kom etter *Digital agenda for Norge*, omtales en rekke oppfølgingspunkter av Lysne-utvalgets rapport. Følgende initiativer i meldingen antas å ha særlig relevans for arbeidet med IKT-sikkerhet i energisektoren:

- Vurdere etablering av et nasjonalt regelverk som gir enhetlig og tverrsektoriell regulering på IKT-sikkerhetsområdet. Arbeidet vil sees i sammenheng med EUs direktiv om tiltak for et felles sikkerhetsnivå i nettverks- og informasjonssystemer (NIS-direktivet), og vurderinger fra Sikkerhetsutvalget
- Utarbeide en ny nasjonal strategi for IKT-sikkerhet. Strategien skal angi regjeringens mål og strategiske prioriteringer innenfor IKT-sikkerhetsområdet. I tillegg skal det utarbeides en handlingsplan
- Heve IKT-sikkerhetskompetansen i sektortilsynene. Nasjonal sikkerhetsmyndighet (NSM) skal etablere en fellesarena hvor sektortilsynene kan samordne planlagte tilsynsaktiviteter og drive erfaringsutveksling innenfor IKT-sikkerhet
- Legge til rette for en langsiktig oppbygging av IKT-sikkerhetskompetanse, gjennom å utarbeide en nasjonal kompetansestrategi for IKT-sikkerhet. Tiltaket innebærer også bevisstgjøringsaktiviteter rettet mot befolkningen og virksomheter
- Videreutvikle den nasjonale evnen til å avdekke og håndtere digitale angrep, ved å videreutvikle varslingssystem for digital infrastruktur (VDI) og etablere et nasjonalt rammeverk for digital hendelseshåndtering

5.2 Nasjonal modell for håndtering av IKT-hendelser

Regjeringen har som målsetting at det skal finnes responsmiljøer i alle samfunnssektorer. Det er den enkelte sektor som skal etablere sektorCERT-er. Ambisjonen er at sektorCERT-ene skal ha oversikt over egen sektor, være informasjonsknutepunkt for alle relevante virksomheter og være sektorens bindeledd mot NSM NorCERT. Styrende dokumenter er *Nasjonal strategi for informasjonssikkerhet* og brev fra Justisdepartementet om modell for hendelseshåndtering. Justisdepartementet arbeider også med å utarbeide et nasjonal rammeverk for digital hendelseshåndtering i henhold til

---

[104] *Digital agenda for Norge*, s 148.

[105] Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn — Samfunnssikkerhet*, https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf besøkt 05.03.2017.

forslaget fra Lysneutvalget. Dette rammeverket er testet i den nasjonale cyberøvelsen *Øvelse IKT 2016*.

I *Nasjonal strategi for informasjonssikkerhet* (2014) og tilhørende handlingsplan er et viktig prioritert tiltak etablering av sektorvise responsmiljøer. NSM har utarbeidet en hovedmodell for dette som bygger på ansvarsprinsippet og nærhetsprinsippet.

De sektorvise responsmiljøene vil ha en nøkkelrolle i å sikre at alle relevante aktører mottar korrekt varslingsinformasjon raskt og på den måten settes i stand til å gjøre nødvendige tiltak. Innretningen av responsmiljøet skal vurderes av den enkelte departement.

De sektorvise responsmiljøene skal være NSM NorCERTs kontaktpunkt ved IT-sikkerhetshendelser. Den tenkte kjernen i det sektorvise responsmiljøet er at responsmiljøene har myndighet innenfor sektoren og kan pålegge tiltak både ved forebygging og håndtering, mens NSM NorCERT vil ha et overordnet varslings- og koordineringsansvar. Kommunikasjon med individuelle virksomheter skal ivaretas eller foregå koordinert med sektormyndigheter. Virksomhetene selv har et ansvar for å kunne ivareta sikkerhet og håndtere hendelser.

I tillegg vil regjeringen komme med en egen stortingsmelding om oppfølgingen av Lysne-utvalgets anbefalinger.

5.3 Nasjonal politikk for bruk av skytjenester

Skytjenester er en felles betegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet Internett.[106] [107] Det er vanlig å skille mellom følgende tjenestemodeller: programvare som tjeneste (Software as a Service, SaaS), plattform som tjeneste (Platform as a Service, PaaS) og infrastruktur som tjeneste (Infrastructure as a Service, IaaS). I en SaaS vil tjenesteleverandøren typisk tilby mer programvare og tjenester enn dersom man «kun» leverer en IaaS. Skytjenester kan leveres i form av ulike leveransemodeller: en offentlig tilgjengelig sky (Public Cloud), en privat tilgjengelig sky (Private Cloud, som benyttes innenfor en bedrift eller et konsern) eller en hybrid sky (Hybrid Cloud, som er en kombinasjon av de to alternativene). Tjenestene kan også leveres fra en server som er plassert hos kunden (On Premises). Hvordan dette organiseres, er i stadig endring[108] og kunden vil måtte vurdere hvilken modell som best dekker behovet.

Skytjenester markedsføres med mange fordeler: Skalering og betaling etter behov, sikkerhet (hos profesjonelle leverandører), energieffektivitet, fleksibilitet og

---

[106] NOU 2015:13, Digitalt sårbarhet, s 300.

[107] Se også: Peter Mell og Timothy Grace (2011): *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*. U.S. Department of Commerce, NIST Special Publication 800 145.

[108] NOU 2015:13, Digitalt sårbarhet, s 300.

innovasjon.[109] Sikkerhet og nasjonal kontroll oppgis ofte som en begrensende faktor for virksomheters bruk av skytjenester. Det er vanskelig for lovgiverne å holde tritt med denne teknologiutviklingen, og det skaper et behov for å tenke annerledes. Mange land har derfor utarbeidet strategier for bruk av skytjenester. Lovgivning skal ikke hindre konkurranse, men ivareta sikkerhet. Regjeringen nedsatte en arbeidsgruppe som gjorde et arbeid med kartlegging av hindringer i regelverk for bruk av skytjenester. Disse avga en rapport i 2015 som omtaler flere relevante regelverk som begrenser bruk av skytjenester.[110]

Kommunal- og moderniseringsdepartementet har i 2016 utarbeidet en nasjonal strategi for bruk av skytjenester. I digitaliseringsrundskrivet for 2016, som gjelder statlig sektor, har KMD lagt inn en anbefaling om at offentlige virksomheter skal vurdere skytjenester som et alternativ når de skal skaffe IKT-tjenester. Det er etablert noen prinsipper for bruk av skytjenester i offentlig sektor: Skytjenester skal vurderes på lik linje med andre løsninger når en står ovenfor større endringer eller omlegging av IKT-systemer eller – drift. Når skytjenester er den mest hensiktsmessige og kostnadseffektive løsningen, og det ikke er spesielle hindringer, skal skytjenester velges. Den valgte løsningen må tilfredsstille virksomhetens krav til informasjonssikkerhet. Dette krever at virksomheten kjenner verdien av egne systemer og data og gjør en risikovurdering av den valgte løsningen.[111]

Et særlig fenomen ved utsetting av IT-tjenester er at den eksterne tjenesteleverandøren kan befinne seg i et annet land og under en annen jurisdiksjon enn den som bestiller tjenesten. I denne sammenheng reises spørsmålet om hva som er konsekvensene av at en del av tjenesten utføres under et annet lands rett. Ofte benyttes også tredjepartsrevisjoner som dokumentasjon på at leverandøren har tilstrekkelig og adekvat sikkerhet. Slike revisjoner utføres normalt i henhold til en standard og ikke etter et nasjonalt lovverk, og det kan være forskjeller i reelt innhold mellom standarder og lovverk.

Noen leverandører tilbyr krypterte løsninger for å beskytte informasjonen. For å ha kontroll på kryptert informasjon må man imidlertid ha kontroll med hvem som har tilgang til krypteringsnøklene. Man må også vurdere om krypteringen er i kraft hele tiden, særlig om den er i kraft når opplysningene skal endres, og ikke bare når de lagres. Fordi mange skytjenester fakturerer i forhold til faktisk bruk, er det viktig å sikre at brukeren belastes for reell bruk, dvs. sikre integriteten. Avhengig av det tekniske oppsettet hos den enkelte leverandøren og den enkelte skytjenesten, kan skytjenester også være sårbare for nedetid og skifte av leverandør. Å få overført sine data hvis man ønsker å bytte tjenesteleverandør

---

[109] *Nasjonal strategi for bruk av Skytjenester,* Kommunal og – moderniseringsdepartementet, Strategi, ikke datert.

[110] Rapport fra interdepartemental arbeidsgruppe med deltakelse fra Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Kommunal- og moderniseringsdepartementet (KMD), Kunnskapsdepartementet (KD), Kulturdepartementet (KUD), Nærings- og fiskeridepartementet (NFD) og Samferdselsdepartementet (SD), Arbeidsgrupperapport 2015, *Kartlegging av hindringer i regelverk for bruk av skytjenester*, Overlevert Kommunal- og modermiseringsdepartementet (KMD) 13.mai 2015, https://www.regjeringen.no/contentassets/d48b5b5895e54d679fef76e0860140a8/skytjenester_arbeidsgrupperapport.pdf besøkt 05.03.2016.

[111] Nasjonal strategi for bruk av skytjenester.

kan videre være utfordrende. Det kan også være utfordringer knyttet til at signaler blir forsinket dersom det er lange fysiske strekk mellom brukere og datasentre og datasentre imellom.[112]

I *Nasjonal strategi for bruk av skytjenester* går en så langt at en sier at skytjenester skal vurderes. Bak dette «skal-kravet» ligger en bekymring for at gammel teknologi går ut på dato og at myndighetene ikke henger med. Kravet til lagring av data i Norge er i endring. Nå kan regnskapsdata lagres utenfor Norges grenser, og det jobbes med å revidere arkivloven. I den nasjonale strategien gis et råd om å vurdere strategi for utsetting av tjenester (dvs. hva skal settes bort til leverandører og hva skal virksomheten selv drifte), arkitektur (teknisk operabilitet, fleksibilitet og skalering) og informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet). Strategien anbefaler at en gjør en verdivurdering av informasjon og en risikoanalyse av det valgte løsningen – noen data (eksempelvis graderte etter sikkerhetsloven) bør kun lagres nasjonalt, en annen gruppe data kan lagres ute, men bør være mulig å hente hjem raskt ved behov, og en siste gruppe data kan fritt lagres utenfor Norges grenser.

KMD vurderer å lage en markedsplass for skytjenester lignede den som finnes i Storbritannia, der staten har kvalitets-sjekket leverandører. Strategien vil utvikle Difi til å bli en bedre rådgiver for virksomheter som vurderer skytjenester.[113]

5.4 Nasjonalt grenseforsvar

Diskusjonen om Digitalt grenseforsvar kom for fullt etter framleggingen av Lysneutvalgets rapport (NOU 2015:13). Regjeringen satte ned et utvalg (Lysne II-utvalget) for å utrede digitalt grenseforsvar. Digitalt grenseforsvar (DGF) er en innretning og en virksomhet som gir E-tjenesten[114] innsyn i digitale datastrømmer som krysser den norske landegrensen.

DGF vil kunne fange opp kommunikasjon mellom enkeltpersoner og datatrafikk som krysser landegrensene. DGF vil kunne virke inngripende i skybaserte lagringstjenester og i ekstern service fra leverandører som befinner seg utenfor Norges grenser, men som utfører service på systemer som tilhører energisektoren. I følge rapporten fra Lysne II-utvalget vil noe av denne trafikken maskinelt kunne filtreres bort før den tas vare på: Det vil kunne skje gjennom tre filtre, der første filter sorterer bort kommunikasjon som opplagt ikke er av interesse for e-tjenesten, filter 2 filtrerer bort innholdsdata og mest mulig metadata som ligger utenfor e-tjenestens oppdrag. Filter 3 slipper kun gjennom innholdsdata fra forhåndsgodkjente kommunikasjonsstrømmer.[115] Nøyaktig filtrering, slik

[112] Digitalt sårbarhetsutvalg 2015:13, s 301.

[113] Nasjonal strategi for bruk av skytjenester.

[114] Etterretningstjenesten skal fremskaffe informasjon om norske interesser sett i forhold til fremmede stater, organisasjoner og individer. Etterretningsinformasjonen benyttes til å varsle om trusler og til å understøtte politiske beslutningsprosesser knyttet til norsk utenriks-, sikkerhets-, og forsvarspolitikk.

[115] Skal være godkjent av en egen domstol for DGF.

at kun informasjon som er relevant for E-tjenestens oppdrag slipper gjennom, er likevel ikke mulig, og noe menneskelig behandling trengs.

En DGF-installasjon vil plukke opp en god del informasjon som E-tjenesten ikke skal ha innsyn i. Dette kan også berøre kraftsensitiv informasjon. I følge Lysene II-utvalget må en DGF-installasjon ligge under et strengt kontrollregime som består av både teknologiske og menneskelige kontrollmekanismer. Lysne II-utvalget har vurdert at DGF kan bli innført på en måte som kombinerer hensynene til teknisk gjennomførbarhet, juridisk gangbarhet, personvernmessige forhold, etterretningsmessig verdi og tillit i befolkningen.[116] Forslaget om DGF har i høringsrunden fått både juridisk og teknologisk kritikk: Juridisk dreier kritikken seg blant annet om at forslaget bryter med de grunnleggende krav til person- og kommunikasjonsvern som alle borgere har etter Grunnloven, Den europeiske menneskerettskonvensjon og EU-/EØS-retten. Domstolene som håndhever person- og kommunikasjonsvernet på øverste nivå i Europa, Den europeiske menneskerettsdomstol og EU-domstolen, har i en rekke avgjørelser slått fast at tvungen, statlig masselagring av personopplysninger er ulovlig. Teknologisk dreier kritikken seg dels om forslagets manglende effekt overfor DGFs anførte formål, kombinert med dets inngripende effekt på kommunikasjonsvernet samt potensielt skadelige effekt på samfunnets IKT-infrastruktur, dels om manglende utredning av en rekke relevante teknologiske problemstillinger, herunder stordataanalyse og kopling av dataregistre.[117]

5.5 Bruk av droner i Norge

Energisektoren i Norge har tatt i bruk droner til inspeksjon av kraftledningers faseliner, isolatorer/oppheng og master, særlig på vanskelig tilgjengelige steder. De brukes til termovisjonsfotografering for å oppdage unormal varmegang i komponenter og vil dermed kunne forhindre skade og havari. Videre brukes droner til å gi raskere og bedre grunnlagsinformasjon om havaristeder – i forbindelse med søk, planlegging og sikker og effektiv gjennomføring av reparasjonsarbeid. Statnett SF som eier og ansvarlig for drift av transmisjonsnettet, har i den senere tid drevet omfattende utprøving av ulike metoder og operasjoner med droner. Statnett har også søkt om operasjonstillatelse (sertifisert operatør) hos Luftfartstilsynet, og ønsker å lære opp egne ansatte som dronepiloter i sine ulike driftsområder landet rundt.[118]

Det stilles ingen spesifikke tekniske krav til droner som skal brukes til linjeinspeksjon, men selskapet må ta høyde for en del sikkerhetsregler, som for eksempel maksimal

---

[116] Lysne. O., Grytting, T., Jarbekk, E. og C. Reusch, *Digitalt grensforsvar (DGF), Lysne II-utvalget*, 26. august 2016., https://www.nito.no/contentassets/8c1777a704654255b563c89e543dc200/lysne-ii-utvalgets-rapport-2016.pdf, nedlastet 15. oktober 2016.

[117] Advokat Jon Wessel-Aas, «Digital grenseovervåkning utenfor lovlige grenser», NRK, 098.01.2017, https://nrkbeta.no/2017/01/08/advokat-jon-wessel-aas-digital-grenseovervakning-utenfor-lovlige-grenser/, besøkt 09.01.2017.

[118] *Høringssvar fra NVE - forslag til forskrift om kontroll med informasjon innhentet ved bruk av luftbårne sensorsystemer*, 201605338-4.

flyhøyde, ifølge Luftfartstilsynet.[119] Norge har en nasjonal forskrift som gjelder for alle luftfartøy uten fører om bord, forskrift 30. november 2015 nr. 1404 om luftfartøy som ikke har fører om bord mv. Det nasjonale regelverket vil gjelde inntil felleseuropeisk regelverk (forordning (EF) nr. 216/2008) vedtas og tas inn i EØS-avtalen. Når det felleseuropeiske regelverket er på plass, vil de nasjonale bestemmelsene bli overflødige og oppheves. Det vil være behov for nasjonal regulering inntil EU har kommet med regelverk for alle kategorier droner, noe som etter tidsplanen først kan være på plass i 2019. Det er sannsynlig at det vil kunne komme forskyvninger i tidsplanen.[120] Et forslag til ny forskrift fastsatt av Forsvarsdepartementet om kontroll med informasjon innhentet ved bruk av luftbårne sensorsystemer er for tiden til høring.[121]

---

[119] «Kraftselskapene kan bruke droner til linjeinspeksjon», E24, (2015), http://e24.no/energi/kraftselskapene-kan-bruke-droner-til-linjeinspeksjon/23490340 besøkt 19.03.2017.

[120] *Introduksjon av regelverk om droner/RPA*, Fakatnotat, Samferdselsdepartementet, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2015/sep/a-npa-2015---regelverk-om-dronerrpas/id2458752/ ,besøkt 23.10.2016

[121] «Forslag til ny forskrift om kontroll med informasjon innhentet ved bruk av luftbårne sensorsystemer er for tiden til høring», https://www.regjeringen.no/contentassets/4be33d96e43a42aeb878c7bdc39cb38e/forslag-til-forskrift.pdf, besøkt 28.02.2017.

Del III Regelverk og normer

6 Regelverk for IKT i energisektoren

6.1 Innledning

Arbeidsgruppen har gått igjennom eksisterende regelverk[122] for å kunne vurdere om det er behov for endringer. Dette kapitelet gjennomgår kort hvordan IKT-sikkerhet har blitt regulert før energiloven og beredskapsforskriften. Deretter presenterer det relevante bestemmelser i energiloven, beredskapsforskriften, damsikkerhetsforskriften og måle- og avregningsforskriften.

6.2 Sikkerhet- og beredskapsregler

6.2.1 Utviklingen

Dagens beredskapsregelverk går tilbake til 1948 og *lov om forsvarsmessig sikring av kraftforsyningen* med tilhørende retningslinjer, som klargjorde hvilke opplysninger som ikke burde gis til offentligheten både om dammer, vasskraftverk, kraftledninger/transformatorstasjoner etc. Opprinnelig var fokuset på fysisk beskyttelse av viktige kraftanlegg (inkludert kontrollrom og sambandsrom - jf. lokalkontroll). Formålet var å hindre at sabotører og en fiende kunne få tilgang til viktige opplysninger dersom det inntraff krig eller en krigslignende situasjon. Eksempler på slike opplysninger var kartdata, detaljplaner, et anleggs motstandskraft mot bomber og magasininnhold.

Konkrete bestemmelser om informasjonssikkerhet (opplysninger), adgang/besøk, ansettelser mv. går tilbake til begynnelsen av 50-tallet, fastsatt av daværende Industridepartement.

Kravene til sambandssikkerhet går tilbake til 60-tallet, med bl.a. krav/retningslinjer fra Totalforsvarets sambandsnemnd og tiltak innen den sivile beredskap. Dette inkluderte «Viktige Prioriterte Telefoner (VPT)» og «Sivil Hovedomleggingsplan (SHOP)». SHOP omfattet da også kraftforsyningen.

Energiloven ble vedtatt i 1990 i en tid hvor styringen av de fleste driftssystemer var mekanisk. Fokuset var på markedstilpasning og deregulering av tidligere statlige monopoler. Dette fremgår også av formålsbestemmelsen i energiloven som er å sikre at *produksjon, omforming, overføring, omsetning, fordeling og bruk av energi foregår på en samfunnsmessig rasjonell måte, herunder skal det tas hensyn til allmenne og private interesser som blir berørt*, jf. § 1-2.Ved vedtakelsen av energiloven ble det innført hjemler for både sikring av relevant «IKT» (elektronisk-/databasert) og fysisk sikring. Særtrykk «*Sikring av driftssentraler*» kom i mars 1991. Mer omfattende regelverk ble utviklet i *retningslinjer for sikring av kraftforsyningen (RSK)* fra 1995, og var basert på anbefalinger fra sambands- og datasikkerhetsutvalget for kraftforsyningen (1994).

[122] Avgrensning: Innenfor forskrifter NVE forvalter, jf. mandatet.

Forskrift om beredskap i kraftforsyningen (bfk), fastsatt av NVE 16. desember 2002 med hjemmel i energiloven, erstattet tidligere retningslinjer for sikring av kraftforsyningsanlegg[123] og beredskapshåndbok for kraftforsyningen.[124]

Da energilovens beredskapskapittel ble endret i 2011,[125] utløste det et behov for å endre eksisterende beredskapsforskrift.[126] *Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (bfe)* ble fastsatt av NVE 7. desember 2012 med hjemmel i energiloven §§ 9-1, 9-2, og 9-3. Veileder til bfe ble utgitt 1. juli 2013.[127]

IKT-sikkerhet regnes i loven i dag som et sikkerhet- og beredskapsspørsmål og er derfor regulert i kapitel 9 og hovedsakelig i §§ 9-1, 9-2 og 9-3. Det vil her bli gitt en kort presentasjon av bestemmelsene og kommentarer til innholdet.

6.2.2 Energiloven

6.2.2.1 Kraftforsyningens beredskapsorganisasjon

§ 9-1:

«Kraftforsyningens beredskapsorganisasjon (KBO) består av de enheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme. Beredskapsmyndigheten kan ved forskrift eller enkeltvedtak fastsette hvilke enheter som skal inngå i KBO.

Alle enheter i KBO skal sørge for at virksomheten er innrettet på en slik måte og med slike ressurser som er nødvendig for å ivareta ansvar og oppgaver etter dette kapittelet.

Beredskapsmyndigheten skal samordne beredskapsarbeid og utpeke den samlede ledelse i KBO.

I ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, kan KBO pålegges oppgaver og plikter. Det samme gjelder i ekstraordinære situasjoner hvor skade eller hindring som nevnt i første punktum har oppstått.

---

[123] *Sikring av kraftforsyningsanlegg – RSK*. Revidert utgåve. NVE 1997. U.off. § 6.1.

[124] Grunnlaget for endringen ble lagt i et forskningsprosjekt ved Forsvarets forskningsinstitutt og flere offentlige utredninger som pekte på kraftforsyningens betydning i det moderne samfunnet og på NVEs beredskapsstrategier. Se: *NVEs strategier for beredskap – Strategi for BAS3*, brev datert 4.5.2006. U.off. §6.1.1.

[125] *Endringer i energiloven og i enkelte andre lover,* Prop. 112 L (2010-2011). https://www.regjeringen.no/no/dokumenter/prop-112-l-20102011/id642213/ besøkt 05.03.2017.

[126] *Prosjekt informasjonssikkerhet. En vurdering av kravene til informasjonssikkerhet i bfk er riktig dimensjonert*, NVE juli 2016, ikke publisert.

[127] *Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen*, nr. 1 2013. NVE, 1. juli 2013.

Beredskapsmyndigheten kan under beredskap og i krig underlegge kraftforsyningen KBO. Kraftforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves.»

§ 9-1 angir hvem og hva Kraftforsyningens beredskapsorganisasjon (KBO) er. Første ledd første punktum angir hvilke enheter KBO skal bestå av. Det er verdt å merke seg at det ikke bare er konsesjonærer etter energiloven som er medlem av KBO, men alle som *«eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme».* I forarbeidene ble dette begrunnet med at det er viktig å ha styring med, og rask tilgang til de personer, virksomheter og ressurser for øvrig, som er av reell betydning for kraftforsyningen. [128] Departementet understreket at det som hovedregel er de som har konsesjon etter energiloven som skal inngå i KBO, men at det likevel kan være aktuelt for myndighetene å bestemme at også andre kan inngå.[129]

I normal drift består norsk energiforsyning av over 200 selvstendige enheter (selskaper o.l.) som, i medhold av lover, forskrifter, regelverk, enkeltvedtak og vilkår nedfelt i de enkelte konsesjoner, eier, bygger og driver det fysiske energisystemet (kraft, fjernvarme mv) helt fra produksjons- til sluttbrukerleddet. Virksomhetene som utgjør energiforsyningen inngår i Kraftforsyningens beredskapsorganisasjon (KBO). Den mest korrekte måten å forstå KBOs rolle, er at den utgjør en organisatorisk struktur som definerer fordelingen av beredskapsoppgaver og ansvar mellom enhetene som inngår i KBO.

Det er også verdt å merke seg fjerde ledd som omhandler kravet til «ekstraordinære situasjoner». Hva som kvalifiserer som en ekstraordinær situasjon vil bero på en skjønnsmessig vurdering i det enkelte tilfelle. Eksempler på situasjoner hvor det kan være nødvendig å pålegge KBO-enheter oppgaver og plikter er kraftig uvær med påfølgende betydelige skader over større områder, ved langvarige strømavbrudd, ved terror mot kraftforsyningens personell eller ressurser, ved manipulering av kraftforsyningssystemet via urettmessig inntrengning eller overtakelse av driftskontrollsystemer, mv.[130]

§ 9-1 gir NVE hjemmel til å pålegge relevante aktører å være medlem av KBO, og deretter stille IKT-sikkerhetskrav til KBO'ene i §§ 9-2 og 9-3.

6.2.2.2 § 9-2 Beredskapstiltak

«Den som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, plikter å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner som nevnt i § 9-1 fjerde eller femte ledd og for å gjenopprette normal situasjon.

---

[128] *Endringer i energiloven og i enkelte andre lover*, Prop. 112 L (2010-2011) s 14. https://www.regjeringen.no/no/dokumenter/prop-112-l-20102011/id642213/ besøkt 05.03.2017.

[129] ibid, s. 14

[130] ibid, s. 23

Beredskapsmyndigheten kan gi forskrift eller treffe enkeltvedtak om beredskapstiltak for å forebygge, håndtere eller begrense virkningene av ekstraordinære situasjoner som nevnt i § 9-1 fjerde eller femte ledd eller for å gjenopprette normal situasjon. Beredskapstiltak kan pålegges den som eier eller driver anlegg eller systemer som nevnt i første ledd. Beredskapstiltak kan gjelde for eksisterende og planlagte anlegg eller systemer som nevnt i første ledd.

Vedtak om beredskapstiltak kan blant annet omfatte krav til organisering, planlegging, forebygging, sikkerhets- eller sikringstiltak, utførelse, gjennomføring, gjenopprettingsevne, ledelse eller drift. Beredskapsmyndigheten kan treffe vedtak om at drift i ekstraordinære situasjoner og gjennomføring av tiltak etter dette kapittel skal kunne skje fra norsk territorium.

Den som pålegges beredskapstiltak plikter å gjennomføre tiltaket for egen regning og risiko.

Når det anses nødvendig kan beredskapsmyndigheten uten hensyn til tidligere pålegg treffe vedtak om at nye eller endrede beredskapstiltak skal settes i verk.»

Bestemmelsen innebærer at de som eier eller driver anlegg og systemer som er kritiske for kraftforsyningen får en selvstendig plikt til å iverksette tiltak, uavhengig av beredskapsmyndighetens myndighet til å kunne vedta iverksettelse av beredskapstiltak etter § 9-2 annet ledd. Med system forstås eksempelvis driftskontrollsystemer og nødvendige hjelpesystemer for kraftforsyningen.[131]

Forskriftskompetanse er hjemlet i annet ledd. Vedtak etter denne bestemmelsen skal fokusere på en totalvurdering av hvordan kraftforsyningens vitale funksjoner opprettholdes, og betydningen av disse for samfunnssikkerheten. Tiltak er opplistet i tredje ledd. Merk at denne opplistingen ikke er uttømmende.[132] Pålegg skal som før gjennomføres for eiers eller drivers regning og risiko.

6.2.2.3 § 9-3 Informasjonssikkerhet

«Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming og beskyttelse av sensitiv informasjon.

Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen.

Departementet kan gi nærmere forskrifter om informasjonssikkerhet i kraftforsyningen og om taushetsplikten.»

§ 9-3 er det rettslige grunnlaget for reglene om informasjonssikkerhet som i dag i det vesentligste er fastsatt i beredskapsforskriften.

---

[131] *Endringer i energiloven og i enkelte andre lover*, Prop. 112 L (2010-2011) punkt 5.1.3. https://www.regjeringen.no/no/dokumenter/prop-112-l-20102011/id642213/ besøkt 05.03.2017. pkt 5.1.3.

[132] ibid

Første ledd første punktum innebærer at alle enheter i KBO til enhver tid skal foreta en helhetlig vurdering av sikkerheten ved all behandling av informasjon om kraftforsyningen. Informasjon er i sikkerhetsloven definert som enhver form for opplysninger i materiell eller immateriell form. Tilsvarende forståelse av begrepet ble lagt til grunn av departementet i utarbeidelsen av lovforslaget.[133]

Første ledd annet punktum innebærer at alle enheter i KBO har plikt til å kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den.

Første ledd tredje punktum stiller krav til å etablere effektiv avskjerming og beskyttelse av sensitiv informasjon. I dette ligger også krav til beskyttelse mot avlytting og manipulasjon fra uvedkommende og gjennomføring av tilgangskontroll slik at kun rettmessige brukere får tilgang.

Som sensitiv informasjon regnes spesifikke og inngående opplysninger om kraftsystemet, herunder det enkelte anlegg, som kan være egnet til å skade anlegg eller påvirke funksjoner som har betydning for kraftforsyningen. Slik informasjon er underlagt taushetsplikten i annet ledd. For KBO-enheter som er omfattet av offentleglova innebærer dette at slik informasjon er unntatt fra innsyn i medhold av offentleglova § 13.

KBO-enhetenes plikter etter første ledd er nødvendige for enhetenes oppfyllelse av taushetsplikten etter annet ledd.

Annet ledd er en taushetspliktregel. Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen. Bestemmelsen er ikke begrenset til KBO-enheter, men påligger enhver. Med enhver menes alle som kommer i kontakt med sensitiv informasjon om kraftforsyningen, for eksempel netteiere, kontraktører og tilsynsmyndigheter. Rettmessige brukere vil primært være selskapets egne ansatte, innleide leverandører og myndigheter med tilsynsansvar på området.

Tredje ledd gir departementet myndighet til å fastsette nærmere forskrifter om informasjonssikkerhet i kraftforsyningen og taushetsplikten.

6.2.3 Beredskapsforskriften

6.2.3.1 Forskriftens virkeområde og oppbygning

Formålet med *forskrift om forebyggende sikkerhet og beredskap i kraftforsyningen (beredskapsforskriften, bfe)* er å sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en sikker og effektiv måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene, jf. § 1-1.

Dette innebærer at det stilles en rekke minimumskrav til alle enheter i kraftforsyningens beredskapsorganisasjon (KBO) om forebygging og håndtering av ekstraordinære

[133] *Endringer i energiloven og i enkelte andre lover*, Prop. 112 L (2010-2011) s. 26. https://www.regjeringen.no/no/dokumenter/prop-112-l-20102011/id642213/ besøkt 05.03.2017.

hendelser som kan skade eller hindre produksjon, overføring eller fordeling av elektrisk kraft og fjernvarme, jf. § 1-2

Forskriften har en kombinasjon av funksjonskrav og mer detaljerte krav. NVE utgav i juli 2013 en veileder som utdyper og forklarer forskriftsteksten.

Forskriften retter seg i første rekke mot de virksomheter som er KBO-enheter. Kravene i kapittel 5 gjelder for de virksomheter som eier eller driver anlegg, system eller annet som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme, også for virksomheter som ikke er KBO-enheter. § 6-1 om taushetsplikt for sensitiv informasjon gjelder for enhver, det vil si alle som måtte få tilgang til sensitiv informasjon om energiforsyningen. Dette har selvstendig hjemmel i *energiloven* § 9-3.

§ 8-2 i forskriften gir Beredskapsmyndigheten myndighet til å gi de pålegg som er nødvendige for gjennomføring av bestemmelser gitt i eller i medhold av denne forskrift. Arbeidsgruppen anser at bestemmelsen gir en vid hjemmel som bl.a. kan brukes til å fatte vedtak om IKT-sikkert.

Forskriften gjelder også for informasjonssikkerhet. Det vil si sikkerhet for at ikke andre enn rettmessige brukere får tilgang til sensitiv informasjonen om energiforsyningen. Kapittel 6 i forskriften og veiledning til kapittel 6 utdyper hvordan dette skal forstås. Arbeidsgruppen vil gi en kort gjennomgang av kapitel 6. I tillegg vil vi kort gjennomgå relevante bestemmelser i forskriftens generelle krav i kapitel 2, klassifisering i kapittel 5 og beskyttelse av driftskontrollsystem i kapitel 7.

6.2.3.2 Kapittel 2 Generelle krav

Kapittel 2 beskriver grunnleggende krav til virksomhetene som er omfattet av forskriften, for å sikre at beredskapsarbeidet er helhetlig og funksjonelt, kontinuerlig og forankret i ledelsen, jf. § 2-1 (Ansvar), § 2-2 (Organisasjon og funksjon) og § 2-3 (Beredskapsplikt).

KBO-enhetene skal bruke ROS-analyser, jf. § 2-4, som planverktøy for å skaffe seg grunnlag for å utarbeide gode beredskapsplaner og kunne prioritere ressursene til de viktigste tiltakene. Disse analysene skal sette virksomhetene i stand til å vurdere hvilke hendelser som kan forebygges, og hvilke sikringstiltak som kan iverksettes for å forhindre, eller begrense skadevirkningene av ekstraordinære hendelser. Hendelser som ikke kan forebygges, eller hvor det gjenstår en restrisiko, skal omtales i beredskapsplanverket. Slike hendelser skal håndteres i henhold til beredskapsplanverket, og håndteringen skal øves jevnlig av virksomheten. Håndtering av ekstraordinære hendelser og øvelser skal evalueres. Sammen med nye trusselvurderinger, tilsyn fra beredskapsmyndigheten med videre, skal virksomheten vurdere om det er nødvendig med en oppdatering av ROS-analysene. Dette gjelder også for IKT-sikkerhet.

§ 2-2 bokstav c, stiller krav om at virksomheter omfattet av forskriften skal ha en IKT-sikkerhetskoordinator. I veilederen til bfe har NVE skrevet at man forventer at vedkommende:

- Har inngående kunnskap til gjeldende lover og forskrifter innenfor IKT-sikkerhet og beredskap i energiforsyningen, inkludert kravene i beredskapsforskriften

- Har god oversikt over interne krav til KBO-enhetenes IKT-sikkerhets- og beredskapsarbeid
- Koordinerer formidling av informasjon, henvendelser og vedtak fra beredskapsmyndigheten med betydning for IKT-sikkerhet internt i virksomheten
- Bidrar til at henvendelser fra beredskapsmyndigheten om IKT-sikkerhetstema blir fulgt opp av virksomheten
- Kan koordinere planlegging, gjennomføring og oppfølging av virksomhetens arbeid med beskyttelse av driftskontrollsystem og virksomhetens øvrige IKT-system, som inneholder sensitiv informasjon om energiforsyningen
- Har god kunnskap om enhetens driftskontrollfunksjoner og administrative datasystemer, deres funksjonalitet, og hvordan de skal beskyttes
- Har god kjennskap til IKT-trusselbildet

Kapitel 2 inneholder for øvrig krav til beredskapsplanlegging (§ 2-5), varsling og rapportering (§ 2-6), øvelser (§ 2-7), informasjonsberedskap (§ 2-8), evaluering (§ 2-9) og internkontrollsystem (§ 2-10).

6.2.3.3 Kapittel 5 Klassifiserings- og sikringstiltak

Bfe kapittel 5 oppstiller en sikringsplikt for eier eller driver av anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, herunder adgang for uvedkommende, jf. § 5-1.

§ 5-1 oppstiller minstekravet til sikring, mens § 5-2 viser til at anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme, skal sikres i henhold til en opplisting i bestemmelsen til henholdsvis Klasse 1-3. Alle klassifiserte anlegg skal prosjekteres, plasseres, utføres, utrustes, sikres, driftes og holdes i slik stand at risiko for skade, havari og funksjonssvikt og andre uønskede hendelser og handlinger blir minst mulig, jf. § 5-3.

Hvilke sikringstiltak som skal utføres i de ulike klassene er beskrevet i §§ 5-4 - 5-6 og i vedlegg 1-4.

Beredskapsmyndigheten kan fatte vedtak om andre eller ytterligere sikringstiltak i medhold av energiloven § 9-2 annet ledd, jf. tredje ledd og om at anlegg eller system skal klassifiseres i en annen klasse enn det som følger av § 5-2 dersom det anses nødvendig, jf. § 5-7.

Kapitelet inneholder videre krav til analyse (§ 5-8), meldeplikt (§ 5-9), vakthold (§ 5-10 og besøksrestriksjoner (§ 5-11).

6.2.3.4 Kapittel 6 Informasjonssikkerhet

Bfe kapittel seks utdyper energiloven § 9-3, og konkretiserer hvordan plikten til å beskytte sensitiv informasjon om energiforsyningen kan etterleves av KBO-enhetene. Samtidig gjelder plikten til å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen. Plikten gjelder for enhver, det vil si ikke bare begrenset til KBO-enhetene.

Bfe kapittel 6 har kriterier for hva som regnes som kraftsensitiv informasjon (§ 6-2), og krav til at virksomhetene skal identifisere den sensitive informasjonen, vite hvor den befinner seg, og vite hvem som har tilgang til den (§ 6-1).

§ 6-3 oppstiller en generell regel om system og rutiner for sensitiv informasjon hos KBO-enhetene. Bestemmelsen sikrer bl.a. at sensitiv informasjon beskyttes i alle faser av informasjonens livsløp. § 6-4 stiller krav til at alle KBO-enheter skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas, og som beskriver identifiseringen som er foretatt i henhold til § 6-1 og hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.

Kapittel 6 har også bestemmelser om taushetsbelagt personkontroll og anskaffelser. § 6-7 henviser til gjeldende sikkerhetslov og dens regler for sikkerhetsklarering og autorisasjon. §§ 6-5 og 6-6 omfatter anskaffelser og beskyttelse av informasjon.

6.2.3.5 Kapittel 7 Sikring av driftskontrollsystemer

Den raske utviklingen av teknologi og økt krav til effektivitet har ført til at man i stadig større grad kobler sammen driftskontrollsystemet med andre IKT-systemer og nettverk. Dette krever at virksomhetene må ha kontinuerlig fokus på å sikre driftskontrollsystemet mot alle typer hendelser, også uautorisert inntrengning. Bfe kapittel 7 gir en generell plikt til å beskytte systemet og sørge for at det virker etter sin hensikt. Beredskapsforskriften mangler en entydig definisjon av hva et driftskontrollsystem er, men en beskrivelse finnes i NVEs veileder til beredskapsforskriften.

Alle virksomheter i energiforsyningen som har etablert et driftskontrollsystem, har en eksplisitt plikt til å beskytte systemet og dokumentere hvordan det er gjort. Dokumentasjonskravene framgår av § 2-10 Internkontrollsystem, jf § 7-1.

Videre må den enkelte virksomhet blant annet fastsette sikkerhetskrav, ha oppdatert dokumentasjon om systemet, kontrollere brukertilgangen og sørge for effektiv håndtering av feil, sårbarhet og sikkerhetsbrudd, samt ha beredskap og forberedte tiltak for fortsatt drift av anlegg ved svikt i driftskontrollsystemet.

Bfe kapittel 7 gir krav om at virksomheten skal sette sikkerhetskrav, men dette er ikke basert på risikovurdering, slik som det ofte er i andre regelverk og standarder. Det er dokumentasjonsplikt, krav til kontroll med brukertilgang og med utstyr som koples til driftskontrollsystemet, krav til håndtering av feil og sikkerhetsbrudd og krav til beredskap. I tillegg har Bfe kapittel 7 detaljerte krav til sikring avhengig av klassifisering, slik at jo høyere klassifisering, desto strengere sikringskrav.

6.2.4 Energilovforskriften

6.2.4.1 Innledning

Energilovforskiftens formål er likt som energiloven. Forskriften inneholder mer detaljerte krav til reglene i loven. Den omtales her fordi den har krav til kompetanse hos nettselskap og alle som har konsesjon.

6.2.4.2 Krav til kompetanse

§ 3-6.Tilgang til personell

Nettselskap med inntektsramme skal til enhver tid ha tilgang til personell med kompetanse innenfor nettforvaltning, driftskontroll, tilstandskontroll og feilretting, behandling av henvendelser om tekniske forhold, samt nybygging og ombygging av elektriske anlegg. Det kreves tilstrekkelig egenbemanning til å lede virksomheten i enhver situasjon, vurdere hvilke tiltak som må iverksettes for å utføre oppgavene nevnt i første punktum, og til å følge opp innhold og utførelse dersom disse oppgavene er satt bort til andre.

Alle med konsesjon etter energiloven § 3-1 for kraftproduksjon skal til enhver tid ha tilgang til personell med kompetanse til å ivareta ledelse, kontroll og praktisk drift.

Den som omfattes av første eller annet ledd skal til enhver tid kunne fremvise dokumentasjon for at kravene er oppfylt. Avtaler og beskrivelser av kontrollrutiner ved kjøp av tjenester skal fremlegges for Norges vassdrags- og energidirektorat eller departementet på forespørsel.

Kravene i første og annet ledd fritar ikke konsesjonæren fra forpliktelser gitt i eller i medhold av lov.

Denne bestemmelsen ble vedtatt i forbindelse med opphevelsen av kompetanseforskriften.

6.2.4.3 Kompetansekrav

Energilovforskriften setter krav til tilgang til personell med kompetanse. Selskapene kan velge utsetting av tjenester om dette blir vurdert som mest lønnsomt for selskapet. I energilovforskriften er det ikke spesifisert hvilke tjenester som kan overlates til andre. Det betyr at hele verdikjeden, dvs. drift av måling og sending av data til nettselskap og elhub kan outsources til tredjepart. Det finnes heller ikke eksplisitte EU-krav til dette.

6.2.5 Måle- og avregningsforskriften

6.2.5.1 Innledning

Formålet med *forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. (Forskrift om kraftomsetning og nettjenester, maf)* er å sikre kraftleverandører tilgang til overføringsnettet og legge til rette for at sluttbrukere av elektrisk energi enkelt kan bytte kraftleverandør, jf. § 1-1. Gjennom forskriften stilles det krav til at nettselskap, som en nøytral aktør, sørger for en effektiv

informasjonsutveksling ved leverandørskifter, måling og avregning, slik at konkurransen i kraftmarkedet blir mest mulig effektiv. Reglene skal også sikre en effektiv regulerkraftavregning. Det er en målsetning at reglene for fakturering av nettjenester skal bevisstgjøre husholdningene om sitt strømforbruk.

- Maf setter krav til AMS og Elhub. Begge deler er relevant for IKT-sikkerheten
- NVE har pålagt Statnett å utvikle en felles IKT-løsning (Elhub) for informasjonsutveksling mellom aktørene i kraftmarkedet. Løsningen skal legge til rette for utveksling av måleverdier og kundeinformasjon som benyttes til avregning og fakturering. Løsningen skal også håndtere leverandørskifter i sluttbrukermarkedet
- I § 1-4 stilles det tekniske krav til elektronisk informasjonsutveksling, mens i § 1-6 er det krav til kvalitetssikring og migrering av data til Elhub
- I forskriften § 4-2 stilles det funksjonskrav til AMS, i bokstav *g* er det et eget krav om å gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner. Ansvaret for sikkerhet i AMS påligger nettselskapene. Det er laget en veileder til forskriftens krav til sikkerhet.[134]

6.2.5.2 Styringsfunksjonalitet og sikkerhet

Som det fremgår av benevnelsen «avanserte måle- og styringssystemer (AMS)», har AMS to hovedfunksjoner: måling og styring. Målefunksjonaliteten i AMS gjør det mulig med kommunikasjon mellom måleren plassert hos sluttbrukeren og en innsamlingssentral hos nettselskapet. Dette er grunnpakken i AMS som gjør det mulig å registrere energiforbruk, spenningsavvik, avbrudd mm. og overføre dataene til nettselskapet gjennom valgt kommunikasjonsløsning.

Styringsfunksjonaliteten i AMS innebærer i dag at nettselskapet har mulighet til å kople ut den enkelte kunde. I tillegg vil AMS gi nettselskapene økt mulighet for mer effektiv overvåkning av energiflyt og tilstand i distribusjonsnettet. AMS har ingen styringsfunksjonalitet ut over brytefunksjonen, men etter hvert vil kunden kunne, om han ønsker, installere teknisk utstyr som kan reagere på forbruksinformasjon. Dette gir likevel ikke nettselskapet noen direkte styringsmulighet.

Nettselskapene har ansvar for å innføre og drifte AMS-systemet i sitt forsyningsområde. Sikkerheten i AMS-systemet er primært regulert gjennom bestemmelsene i måle- og avregningsforskriften og beredskapsforskriften. AMS-løsningene vil bli et komplekst system med en omfattende infrastruktur for overføring av kunde- og målerdata, med mer.[135] Infrastrukturen vil ha knutepunkter for overføring til databaser, som igjen skal håndtere og behandle målerdata. I

---

[134] Skapalen, F. og B. Jonassen, *Veileder til sikkerhet i avanserte måle- og styringssystem*, Rapport 7 2012, NVE, tilgjengelig: http://webby.nve.no/publikasjoner/veileder/2012/veileder2012_07.pdf, besøkt 25.07.2016.

[135] Det er enda usikkert i hvilken grad styring vil bli utført gjennom AMS. En annen sak er at AMS gir masse nye data som åpner for nye styringsmuligheter utenfor AMS, slik som eksempelvis aggregator-tjenester.

tillegg til egne tjenester skal nettselskapene legge til rette for at ulike tilleggstjenester kan tilknyttes AMS i fremtiden. Sikkerhet i AMS omfatter beskyttelse mot alle typer uautorisert tilgang for å hindre misbruk, tyveri av data, spredning av skadevare, utførelse av uautoriserte kommandoer og liknende.[136] Mål for beskyttelse av AMS kan være:

i) God drift av energiproduksjon, overføring og distribusjon i el-nettet, uten brudd på tilgjengeligheten pga. cyberangrep via AMS[137]
ii) Legitim kraftlevering og –forbruk gjennom å motvirke elektrisitetstyveri og sikre riktig mål på forbruk
iii) Personvern for forbrukere[138,139,] ved å sikre håndtering av forbrukerdata, inkludert overføring og lagring
iv) Sikring av bryte- og strupefunksjonen, spesielt med tanke på masseutkobling av målepunkter
v) Sikker sammenkobling av AMS-infrastruktur, eksisterende styringssystemer og eksisterende administrative systemer
vi) Ikke-benekting[140] [141]

§ 6-21. Sikkerhet i Elhub

«Elhub skal ikke inneha funksjoner som kan påvirke, utføre eller overta overvåking og styring av elektriske anlegg i energiforsyningen, jf. energiloven § 1-3 første ledd og energilovforskriften § 1-1.

Elhub skal ikke inneha funksjoner for å kunne strupe eller bryte effektuttaket i noen målepunkt. Avregningsansvarlig skal sørge for at Elhub til enhver tid fungerer etter sin hensikt og beskytte Elhub mot alle typer uønskede hendelser, herunder omfattende teknisk svikt, alle typer uautorisert tilgang for å hindre tyveri eller misbruk av måleverdier og kundeinformasjon, spredning av skadelig programvare og liknende.

Avregningsansvarlig skal sørge for at all informasjonsutveksling i henhold til Ediel er kryptert.

---

[136] Skapalen, F. og B. Jonassen, *NVE veileder til sikkerhet i AMS*, http://webby.nve.no/publikasjoner/veileder/2012/veileder2012_07.pdf besøkt 05.03.2017.

[137] Skopika, F., Maa, Z., Bleiera, T. and H. Grüneisb, "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures Survey on Threats and Vulnerabilities", *International Journal of Smart Grid and Clean Energy*, http://www.infosys.tuwien.ac.at/staff/skopik/ait/2012_ijsgce_b.pdf besøkt 05.03.2017.

[138] «Informasjonssikkerhet og personvern i AMS, Hvordan bruke AMS opplysninger innenfor juridiske rammer med tilfredsstillende informasjonssikkerhet?» Evry, http://www.ey.com/Publication/vwLUAssets/EY-Temaark-Advisory-AMS/$FILE/EY-Temaark-Advisory-AMS.pdf besøkt 05.03.2017.

[139] « Støtte til risikoanalyse av AMS og tilgrensende systemer », Sintef 24. September 2014, http://infosec.sintef.no/stikkord/ams/ besøkt 05.03.2017.

[140] Ikke-benekting betyr at en ikke kan nekte for å ha mottatt en melding.

[141] *Smart Grid Cyber Security, potential threats, vulnerabilities and risks.* Public Interest Energy Research (PIER) Program INTERIM PROJECT REPORT, Sacramento to State opposed for California Energy Commission, http://www.energy.ca.gov/2012publications/CEC-500-20, 12-047/CEC-500-2012-047.pdf besøkt 05.03.2017.

Avregningsansvarlig skal etablere et dokumentert styringssystem for sikkerhet som kontinuerlig skal ivareta en helhetlig risikostyring av Elhub. Styringssystemet skal som minimum omfatte følgende områder:

a) Risikovurdering med gjennomgang og oppfølging av denne,
b) sikkerhetskrav for utvikling, drift, bruk, systemvedlikehold av Elhub,
c) fysisk beskyttelse og kontroll med fysisk tilgang til sentralt teknisk utstyr knyttet til Elhub,
d) tekniske ordninger og prosedyrer for tildeling, endring, sletting og autentisering av korrekt tilgang til Elhub,
e) automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i Elhub,
f) beredskapsplaner eller prosedyrer for å håndtere alle typer hendelser eller feil som medfører svikt i funksjonen til Elhub og
g) prosedyrer eller rutiner for å registrere, gjennomgå og evaluere hendelser eller feil som har medført svikt i funksjonen til Elhub.»[142]

6.2.6 Damsikkerhetsforskriften

6.2.6.1 Innledning

Damsikkerhetsforskriften omfatter både planlegging, bygging, drift og nedlegging av vassdragsanlegg, og dekker ulike damtyper med tilhørende anlegg. Samlet sett vurderes regelverket i Norge å være godt gjennomarbeidet, enhetlig og dekker hele livssyklusen til en dam fra planlegging til drift og nedlegging.

Damsikkerhetsforskriften regulerer i kapittel 7 drift,[143] herunder driftsprosedyrer, overvåkning, sikringstiltak og beredskap.

6.2.6.2 § 7-8 Informasjonssikkerhet

§ 7-8 i forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften) (FOR-2009-12-18-1600) omhandler informasjonssikkerhet.

«For vassdragsanlegg i konsekvensklasse 2, 3 og 4 skal det foretas en helhetlig risikovurdering knyttet til all behandling av informasjon om vassdragsanlegget. Som sensitiv informasjon regnes spesifikk informasjon og inngående kjennskap om vassdragsanlegget som kan brukes til å skade anlegget eller påvirke funksjoner som har betydning for sikkerheten. Det skal identifiseres hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming av sensitiv informasjon og gjennomføres tilgangskontroll slik at kun rettmessige brukere får tilgang. Enhver som omfattes av forskriften her plikter å hindre at andre enn

---

[142] Tilføyes ved forskrift 12 juni 2015 nr. 705 som endret ved forskrift 3 feb 2017 nr. 120 (i kraft 23. okt 2017).

[143] Forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften), https://lovdata.no/dokument/SF/forskrift/2009-12-18-1600/KAPITTEL_7#KAPITTEL_7 besøkt 05.03.2017.

rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om vassdragsanlegget. Slik informasjon er å anse som taushetsbelagt informasjon unntatt fra innsyn etter offentleglova § 13. All kommunikasjon og behandling av sensitiv informasjon skal beskyttes mot avlytting og manipulering fra uvedkommende.

En sikkerhetsinstruks for å ivareta informasjonssikkerheten skal utarbeides. Det skal gjennomføres tiltak for å ivareta krav etter instruksen.

NVE kan treffe vedtak om at informasjon om vassdragsanlegg skal behandles i henhold til bestemmelsene i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).»

I første ledd angis at bestemmelsen gjelder vassdragsanlegg i konsekvensklasse 2, 3 og 4. For disse anleggene skal det foretas en helhetlig risikovurdering knyttet til all behandling av informasjon som angår vassdragsanlegget. Med sensitiv informasjon menes spesifikk informasjon og inngående kjennskap om vassdragsanlegget som kan brukes til å skade anlegget eller påvirke funksjoner som har betydning for sikkerheten. Det skal identifiseres hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming av sensitiv informasjon og gjennomføres tilgangskontroll slik at kun rettmessige brukere får tilgang. Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om vassdragsanlegget. Det presiseres i siste punktum at all kommunikasjon og behandling av sensitiv informasjon skal beskyttes mot avlytting og manipulering fra uvedkommende.

I annet ledd angis at det skal utarbeides en sikkerhetsinstruks som beskriver hvordan informasjonssikkerheten skal ivaretas og at det skal gjennomføres tiltak for å ivareta kravene i instruksen. Ifølge første ledd må innholdet i en sikkerhetsinstruks omfatte klargjøring og merking av sensitive dokument, angivelse av begrensning i tilgang til og taushetsplikt om sensitive forhold, oppbevaring og distribusjon av sensitive dokument, fjerning/svartsladding av sensitive opplysninger i dokumenter før skanning/kopiering ved tilgjengeliggjøring for andre enn rettmessige brukere, beskyttelse av sensitiv informasjon mot avlytting og manipulering, og at eksterne som skal forholde seg til sensitivt materiale må ha sikkerhetsavtale.

I tredje ledd gis NVE hjemmel til å treffe vedtak om at informasjon om vassdragsanlegg skal behandles i henhold til bestemmelser i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

6.2.7 Systemansvarsforskriften

6.2.7.1 Innledning

Statnett har i dag systemansvaret i det norske kraftsystemet. Systemansvarlig skal legge til rette for et effektivt kraftmarked og en tilfredsstillende leveringskvalitet i kraftsystemet, som igjen fører til en rasjonell utnyttelse av kraftressursene for samfunnet som helhet. Statnett har også fått tildelt myndighet til å koordinere måling og avregning av kraftomsetning i henhold til måle- og avregningsforskriften. Som avregningsansvarlig har Statnett videre ansvar for utviklingen av Elhub. Prinsipper for utøvelse av

systemansvaret i henhold til forskrift om systemansvaret i kraftsystemet (fos) sier at systemansvarlig skal:

- Sørge for frekvensreguleringen og sikre momentan balanse i kraftsystemet til enhver tid
- Opptre nøytralt og ikke-diskriminerende i forhold til alle som omfattes av fos
- Utvikle markedsløsninger som bidrar til å sikre en effektiv utvikling og utnyttelse av kraftsystemet
- I størst mulig utstrekning gjøre bruk av virkemidler som er basert på markedsmessige prinsipper
- Samordne og følge opp konsesjonærer og sluttbrukeres disposisjoner med sikte på å oppnå tilfredsstillende leveringskvalitet og en effektiv utnyttelse av kraftsystemet
- Utarbeide og distribuere informasjon om forhold i kraftsystemet som er av betydning for kraftmarkedet, samt om forhold som er av betydning for den generelle leveringskvaliteten

6.2.7.2 Myndighet og kontrollansvar knyttet til systemansvaret

I forbindelse med utøvelsen av systemansvaret er systemansvarlig delegert myndighet på flere områder. For å utøve systemansvaret har systemansvarlig myndighet til å fatte vedtak til andre konsesjonærer, blant annet gjelder dette pålegg om tilpasning av produksjonsplaner (§8) og rekvirering av effekttilgang i vanskelige driftssituasjoner (§12). Muligheten til å fatte ovennevnte vedtak er et viktige verktøy for systemansvarlig i driften av kraftsystemet. Det griper inn i andre aktørers beslutninger om kjøp og salg i markedet. Systemansvarlig har derfor et helt spesielt ansvar for å koordinere, og nøytralitet er helt sentralt. Samtidig er systemansvarlig også tildelt myndighet på områder som ikke er like tidskritisk. For eksempel gjelder dette godkjenning av idriftsettelse av endringer eller nye anlegg i kraftsystemet (§14). For alle disse vedtakene har konsesjonærene klagemulighet, men det ligger likevel en plikt til å gjennomføre pålegg fra systemansvarlig, uavhengig av en mulig klage.

Videre er systemansvarlig pålagt å samle inn og kontrollere data, både data som er nødvendig for driften av kraftsystemet og data som NVE har behov for (§7, § 14a). Utover å samle inn data i henhold til disse paragrafene er systemansvarlig tillagt kontrolloppgaver i forbindelse med systemansvaret; for eksempel skal systemansvarlig varsle NVE dersom konsesjonærer ikke oppfyller plikter i henhold til §7, §12, §13 og §14. Denne metoden å følge opp krav på letter NVEs tilsynsarbeid på disse områdene betraktelig. Det er fremdeles NVE som har mulighet for reaksjoner, men systemansvarlig, som uansett har behov for dataene får byrden å kontrollere at de har tilstrekkelig data.

6.2.7.3 Konsekvenser av et mer digitalisert kraftmarked

Utviklingen vi ser i dag og fremover vil ha påvirkning på utøvelsen av systemansvaret, blant annet mer fokus på lokale og distribuerte løsninger og håndtering av store mengder data. I kjølvannet av etableringen av Elhub, større mengder registrerte data, bruk av skytjenester, droner og enda flere sensorer på komponenter, kan nye markeder og nye typer tjenester for forbrukere og for leverandører bli utviklet. Det er like vanskelig å

forutse i dag hvordan dette vil se ut som det var å forutse utviklingen av Google og Facebook i tiden da fasttelefoni var den dominerende kommunikasjonsformen.

På det organisatoriske planet er det et spørsmål også hvordan lokale og regionale driftsutfordringer blir håndtert, og hvordan samhandlingen mellom DSO og TSO vil utvikle seg i Europa.

7 Sektorovergripende regelverk for IKT-sikkerhet

7.1 Innledning

Det er flere regelverk som har sektorovergripende regler som kan gi føringer for reguleringen av IKT-sikkerhet i energiforsyningen.

7.2 Sikkerhetsloven

7.2.1 Gjeldende lov

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)[144] er rettet mot forvaltningsorganer og skal legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet, og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste.

Sikkerhetsloven og dens forskrifter angir minimumskravene for beskyttelse av informasjon og objekter av betydning for rikets eller alliertes sikkerhet, eller andre vitale nasjonale sikkerhetsinteresser. Regelverket fastsetter forebyggende tiltak mot forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger. Loven gjelder for alle forvaltningsorganer som er i besittelse av skjermingsverdig informasjon eller objekter etter sikkerhetsloven. I tillegg gjelder loven for leverandører til forvaltningsorganer når leverandøren kan få tilgang til skjermingsverdig informasjon eller objekt. Loven har en rekke forskrifter:

- Forskrift om personellsikkerhet
- Forskrift om sikkerhetsadministrasjon
- Forskrift om informasjonssikkerhet
- Forskrift om sikkerhetsgraderte anskaffelser
- Forskrift om objektsikkerhet

NSM har en rekke veiledere til loven og forskriftene som beskriver krav til systemteknisk sikkerhet. Disse veiledningene tar for seg forskjellig typer sikring av IT-systemer:

---

[144] *Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven),* LOV-2015-06-19-65 fra 01.10.2015, https://lovdata.no/dokument/NL/lov/1998-03-20-10/KAPITTEL_1#KAPITTEL_1, besøkt 22.10.2016.

servere, klienter, nettverk, krypto, mm.[145] Energisektorens ansatte klareres i henhold til forskrift om personellsikkerhet. Ingen virksomheter i energisektoren har objekter utpekt etter sikkerhetsloven.

7.2.2 Forslaget til ny lov om forebyggende nasjonal sikkerhet

Den 12.oktober 2016 presenterte Tråvik-utvalget forslag til ny sikkerhetslov.[146] Lovforslaget, i nåværende form, vil kreve omfattende endring av forskriftene til dagens sikkerhetslov, forskriftene omtales derfor ikke nærmere i denne rapporten. Nedenfor presenteres lovforslaget i korthet slik det foreligger per dags dato.

Virkeområdet som er foreslått i den nye sikkerhetsloven er videre enn eksisterende sikkerhetslov, som primært gjelder forvaltningen. Den foreslåtte utvidede sikkerhetsloven skal være en helhetlig sektorovergripende rammelov for samhandling, og bygger på beredskapsprinsippene ansvar, nærhet, likhet og samvirke. Lovens sikkerhetsbegrep er likevel fremdeles kort sagt avgrenset til: tilsiktede uønskede hendelser - rettet mot grunnleggende nasjonale funksjoner som er nærmere angitt §1.3 *a) de øverste statsorganers virksomhet, sikkerhet eller handlefrihet b) forsvars-, sikkerhets- og beredskapsmessige forhold, c) forholdet til andre stater, d) landets økonomiske trygghet og velferd, e) befolkningens grunnleggende sikkerhet og overlevelse.* Energiforsyning er viktig som understøttende tjeneste for alle disse grunnleggende nasjonale funksjonene.

Dagens energilov angir til sammenligning ekstraordinære situasjoner, m.a.o. alle uønskede hendelser og handlinger som kan skade eller hindre, osv. Dagens energilov har dermed et langt videre siktemål (all-hazard approach).

I lovforslaget snakkes det om sikkerhetsmyndighet, klareringsmyndighet, sektormyndighet og tilsynsmyndighet. Slik lovforslaget leses, vil det med eksisterende organisering være NSM som er sikkerhetsmyndighet og klareringsmyndighet, mens NVE er sektormyndighet og tilsynsmyndighet for sektoren. Etter lovforslaget vil NSM kunne føre tilsyn med andre departementer/sektormyndigheters sikkerhetsarbeid, samt gi rammer/føringer for deres tilsynsarbeid. NSM kan videre selv føre tilsyn på områder/i sektorer hvor dette ikke er forsvarlig ivaretatt. Dette stiller krav til et sektorregelverk som er minst like godt som det som følger av sikkerhetsloven.

Sikkerhetsloven operer også med begrepet *forsvarlig* i forhold til sikkerhetsnivå. Dette er et begrep som også finnes i EKOM-loven.[147] Forsvarlig sikkerhet er en rettslig standard

---

[145] *Veiledning for systemteknisk sikkerhet,* NSM, https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet besøkt 05.03.3017.

[146] *Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*, NOU 2016: 19, Forsvarsdepartementet.

[147] Se EKOM-loven § 2-10.Sikkerhet og beredskap, 1.ledd: Tilbyder skal tilby elektronisk kommunikasjonsnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig. Tilbyder skal opprettholde nødvendig beredskap, og viktige samfunnsaktører skal prioriteres ved behov. Tilbyder skal formidle viktig melding fra statsmyndighet. Myndigheten kan treffe enkeltvedtak for å sikre at tilbyder iverksetter tiltak som gir forsvarlig sikkerhet og nødvendig beredskap. Tilbyder skal dekke kostnadene ved oppfyllelsen av dette. https://lovdata.no/dokument/NL/lov/2003-07-04-83?q=ekomloven, besøkt 23.10.2016.

som vil kunne variere over tid, avhengig av sikkerhetsarbeidet i virksomhetene og vedtak etter tilsyn. Loven legger også opp til at virksomhetene skal gjøre risikovurderinger og sikre egne systemer deretter, iht. ansvarsprinsippet. Virksomhetene gis en tydelig sikringsplikt. En slik plikt finnes også i energiloven.

Forslaget til ny sikkerhetslov kapittel 4 stiller generelt krav til forebyggende sikkerhet: Plikt til å gjennomføre sikkerhetstiltak, krav til sikkerhetsstyring der ansvar plasseres på ledelsen, bruk av risikoanalyse som grunnlag for å vurdere og prioritere sikkerhetstiltak, krav til dokumentasjon, øvelser, varsling til tilsynsmyndighet og sikkerhetsmyndighet, og behandling av personopplysninger.

Kapittel 6 i forslaget til ny sikkerhetslov definerer skjermingsverdige informasjonssystemer som a) informasjonssystemer som er av *kritisk* betydning for grunnleggende nasjonale funksjoner og b) informasjonssystemer som behandler sikkerhetsgradert informasjon. Slike systemer skal godkjennes av en ansvarlig godkjenningsmyndighet. I dag ivaretar NSM denne rollen. Det stilles strengere kontrollkrav til disse systemene enn til systemer av lavere klasse.

§ 7-2 Klassifisering sier at skjermingsverdige objekter og infrastruktur skal klassifiseres i en av følgende klassifiseringsgrader:

- MEGET KRITISK nyttes dersom det kan få helt avgjørende skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet
- KRITISK nyttes dersom det kan få alvorlige skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet
- VIKTIG nyttes dersom det kan få skadefølger for grunnleggende nasjonale funksjoner, jf.§ 1-2, om objektet eller infrastrukturen får redusert funksjonalitet.

Klassifiseringen skal skje på grunnlag av virksomhetens risiko- og sårbarhetsanalyse, jf. § 4-3, og skal begrunnes ut ifra hvilke grunnleggende nasjonale funksjoner objektet eller infrastrukturen understøtter og konsekvensene av redusert funksjonalitet.

Det enkelte departement (myndighet) skal velge ut virksomheter og kritiske/viktige skjermingsverdige objekter og nå også systemer. Men, NSM skal ha en samlet tverrsektoriell oversikt over slike objekter og systemer og kan selv foreslå nye. Systemfokus skal tillegges langt større vekt enn til nå.[148]

Loven legger videre opp til at underlagte virksomheter, ut fra overordnede harmoniserte krav og ROS-analyser, selv skal konkretisere, planlegge og utføre sikringstiltakene, mens sektormyndighetene skal være pådrivere, føre tilsyn, og eventuelt gi pålegg om dette måtte anses nødvendig. Dersom det er hensiktsmessig kan det henvises til standarder, for eksempel bruk av standarder for risikoanalyse og sikkerhetsstyring. Dette er ikke helt i tråd med NVEs praksis på IKT-sikkerhet. På andre områder enn IKT-sikkerhet henviser

[148] Dagens beredskapsforskrift har til sammenligning også tre klasser, som gjelder alle som eier og driver anlegg i energiforsyningen. Beredskapsforskriftens klasser er konkretisert i forhold til anleggenes samlede betydning og ytelse i sektoren i form av konkrete elektro-tekniske målbare kriterier, kriterier på kundemasse og samfunnsviktige kunder, jf. sikkerhetslovens funksjonsfokus.

veilederen til standarder. Når det er sagt, så har dagens beredskapsforskrift klare spor av for eksempel ISO 27001, og vi finner også igjen en rekke tiltak fra ISO 27002.

Om loven blir vedtatt omtrent som utvalget (enstemmig) har foreslått, vil kraftforsyningen bli dekket både som understøttende tjeneste, som andre kritiske samfunnsfunksjoner, og som sentrale objekter i seg selv.

7.3 Personopplysningsloven

Lov om behandling av personopplysninger (personopplysningsloven) gjelder i utgangspunktet for all behandling av personopplysninger, både i privat og offentlig sektor, forutsatt at det benyttes elektroniske hjelpemidler eller at opplysningene skal inngå i et personregister. Behandling for rent personlige formål er unntatt fra loven. Det samme gjelder behandling av hensyn til rikets sikkerhet og behandling knyttet til sivile og strafferettslige saker. Det er også visse unntak av hensyn til ytringsfriheten. Personopplysningsloven gjelder heller ikke dersom annen lov regulerer behandlingsmåten, jf. personopplysningsloven § 5. Altså er personopplysningsloven en generell lov som gjelder om ikke annet er særskilt regulert. Eksempler på særskilt regulering er politiregisterloven, pasientjournalloven og helseregisterloven.

Loven stiller noen grunnkrav til all behandling av personopplysninger:

- Behandling av personopplysninger skal være formålsbestemt (grunnkravet om formålsbestemt bruk av personopplysninger). Behandling av personopplysninger skal også være relevant og tilstrekkelig for formålet (grunnkravet om nødvendighet)
- Behandling av personopplysninger skal også være relevant og tilstrekkelig for formålet (grunnkravet om nødvendighet)
- Den behandlingsansvarlige må ha rettslig grunnlag for behandlingen, dvs. enten samtykke fra den registrerte, hjemmel i lov eller behandlingen må være nødvendig av hensyn til et av formålene som er nevnt i § 8
- Opplysningene skal ha tilfredsstillende kvalitet
- Opplysningene skal ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker
- Opplysningene skal ikke lagres lengre enn det som er nødvendige for behandlingen

I Stortingsmeldingen om personvern, Meld. St. 11 (2012–2013), ble det satt et prinsipielt mål om innebygd personvern i alle sektorer. Offentlige myndigheter har et særlig ansvar og må sørge for personvernutredninger i forkant av regelverksarbeid, og de må stille strenge krav til personvern ved anskaffelser av IKT-løsninger.[149] Økt ønske om forskning

[149] *Digital agenda for Norge*, s 141-142, https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/ besøkt 05.03.2017.

på registerdata kan komme i konflikt med den enkeltes råderett over egne data. Ved forskning på data som inneholder personopplysninger, må personvernhensyn ivaretas.[150]

Personopplysningsloven har følgende forskrifter:

- Personopplysningsforskriften[151]
- Instruks om sikkerhetstjeneste i Forsvaret[152]
- Kommunikasjonskontrollforskriften[153]

7.4 Forvaltningsloven

I *Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)* § 13 første ledd har «enhver som utfører tjeneste eller arbeid for et forvaltningsorgan» taushetsplikt for opplysninger om noens personlige forhold og forretningsrelaterte opplysninger som det vil være av konkurransemessig betydning å hemmeligholde.

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) gir konkrete føringer ved bruk av elektronisk kommunikasjon i et forvaltningsorgan, blant annet i forskriftens § 5. Det vises her til at risiko for uberettiget innsyn i opplysningene, ved bruk av elektronisk kommunikasjon, må «være forebygget på tilfredsstillende måte», jf. § 5, første ledd.

7.5 Arkivloven

Alle offentlige organ er underlagt en plikt til å ha arkiv. Fordi arkivloven inneholder en begrensning på å føre arkiv ut av landet, er denne bestemmelsen en hindring for offentlige virksomheter som ønsker å ta i bruk skyløsninger med utenlandske servere for arkivering. Nesten alle fagsystemer i stat og kommune produserer arkivdokumenter. Alle har dermed arkiv som vesentlig del av sin IKT-løsning.

Etater og kommuner har etterlyst verktøy som kan gjøre det enklere å finne de rette tjenestene og ta stilling til hvilke leverandører man bør velge. Kommunal- og moderiniseringsdepartementet (KMD) har signalisert at det offentlige trenger en form for markedsplass for skytjenester – inspirert av Storbritannias Digital marketplace.[154]

---

[150] Digital Agenda s 146.

[151] Forskrift om behandling av personopplysninger (personopplysningsforskriften), https://lovdata.no/dokument/SF/forskrift/2000-12-15-1265 besøkt 05.03.2017.

[152] *Instruks om sikkerhetstjeneste i Forsvaret*, https://lovdata.no/dokument/INS/forskrift/2010-04-29-695?q=Instruks om sikkerhetstjeneste i Forsvaret, besøkt 05.03.2017.

[153] Kommunikasjonskontrollforskriften, https://lovdata.no/dokument/SF/forskrift/2016-09-09-1047?q=Kommunikasjonskontrollforskriften besøkt 05.03.2017.

[154] Chaffey, P., «Skytjenester i det offentlige ikke lenger i det blå», Tale/innlegg 09.06.2016, https://www.regjeringen.no/no/aktuelt/skytjenester-i-det-offentlige-ikke-lenger-i-det-bla/id2503734/, besøkt 23.10.2016.

Kulturdepartementet har startet et arbeid med å revidere arkivforskriften, og vil vurdere endringer i loven som kan åpne for å lagre arkiv utenfor Norge. Den 26.10.2016 sendte departementet et forslag til forskrift på høring.[155] Departementet foreslår at de eksisterende detaljerte regler for offentlige arkiv blir erstattet av mer overordnede og funksjonelle krav. Forslaget innebærer at offentlige institusjoner selv kan velge hvordan de ønsker å organisere arkivet, så lenge dokumentene er ordnet og lagret i samsvar med arkivansvaret i arkivloven.

Kulturdepartementet foreslår i ny § 22 at offentlige organ kan lagre digitalt arkivmateriale utenfor Norge dersom pliktene i arkivloven med forskrifter er regulerte i avtalen mellom organet og eieren av arkivlageret. Organet skal beholde tilgang til, kontroll med og eiendomsretten til sitt arkivmateriale. Dette åpner bl.a. for at kommunale, fylkeskommunale og statlige institusjoner kan kjøpe skytjenester.

En forutsetning er at system og leverandør kan sikre forsvarlig håndtering av arkivmaterialet. KMD har gitt Difi i oppdrag å tilby veiledning som vil kunne omfatte verktøy for risikovurdering, kost-nytte analyser, kontraktsoppfølging og databehandleravtaler.

7.6 Bokføringsloven

Bokføringsloven § 13 stiller krav om oppbevaring av regnskapsmateriale, og det følger at regnskapsmateriale som hovedregel skal oppbevares i Norge. Etter 5.ledd kan det i forskrift gjøres unntak fra bestemmelsene om oppbevaring.

Etter bokføringsforskriften § 7-5 kan bokføringspliktige «oppbevare elektronisk regnskapsmateriale i et annet EØS-land dersom avtale eller overenskomst med det aktuelle landet sikrer norske skatte- og avgiftsmyndigheter tilfredsstillende adgang til regnskapsinformasjonen for kontrollformål i oppbevaringstiden, og slik oppbevaring ikke vil være til hinder for effektiv norsk politietterforskning.» De må videre «skriftlig informere Skattedirektoratet om hvilket regnskapsmateriale som oppbevares i utlandet, hvor regnskapsmaterialet oppbevares, og hvordan kontrollmyndighetene til enhver tid kan få adgang til regnskapsmateriale»".

[155] «Forslag om ny arkivforskrift opnar for bruk av skytenester», 24.20.2016., https://www.regjeringen.no/no/aktuelt/forslag-om-ny-arkivforskrift-opnar-for-bruk-av-skytenester/id2517014/ besøkt 18.11.2016.

8 Regler for IKT-sikkerhet i andre sektorer

8.1 El-tilsyn

I *Lov om tilsyn med elektriske anlegg og elektrisk utstyr (el-tilsynsloven)* § 5 fjerde ledd heter det at «Enhver som er underlagt tilsyn etter denne lov, skal når tilsynsmyndigheten krever det og uten hinder av taushetsplikt fremlegge opplysninger som anses nødvendige for utøvelsen av tilsynet. Tilsynsmyndigheten kan bestemme i hvilken form opplysningene skal gis.» Tilsyn etter denne loven foretas av Direktoratet for samfunnssikkerhet og beredskap (DSB).

Det er i forarbeidene påpekt at det er viktig at «tilsynsmyndighetene ikke utestenges fra steder hvor dokumentasjon befinner seg», altså det som kan kalles «stedlig tilsyn». Lovteksten er ment å skulle ivareta dette hensynet, men DSB opplyser at bruk av skytjenester i seg selv ikke er i direkte strid med ordlyden i bestemmelsen. Bruken av skytjenester behøver ikke medføre at tilgangen på opplysninger blir dårligere for tilsynsmyndigheter, men det oppstår en utfordring når opplysninger er lagret på servere som er plasser i utlandet slik at ikke tilsynsmyndigheten får ført tilsyn med dem. Eventuelle begrensninger på bakgrunn av denne loven følger av praktiseringen av tilsynet, og de premisser tilsynsmyndigheten krever foreligger for å tilfredsstille et stedlig tilsyn.

8.2 Olje- og gass

Olje- og gassindustrien har et funksjonsbasert regelverk innenfor helse, miljø og sikkerhet (HMS). Regelverket har lagt til grunn at selskapene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak. Dette gjøres gjennom risiko- og beredskapsanalyser i de enkelte selskapene. Bransjens egenutviklede standarder legges til grunn for arbeidet. Næringen har selv, gjennom Norsk olje og gass, utarbeidet spesifikke retningslinjer for informasjonssikkerhet i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer. Retningslinjene er basert på ISO 270001/2-standarden.

Olje- og gassektoren har et omfattende regime for dokumentasjon og styring. Næringen selv viser til at mengden av dokumentasjon som produseres i forbindelse med utbygging og drift av felt og innretninger på norsk sokkel har økt vesentlig de senere årene, selv om selskapene forsøker å redusere dokumentasjonsmengden gjennom økt standardisering og mer effektive metoder. Utstyrsleverandørene og hovedleverandørene har tradisjonelt lite direkte kontakt med Petroleumstilsynet. De forholder seg til kravene gitt i en kontrakt, og de har normalt en forventning om at operatørens opplistede krav tilfredsstiller kravene i det funksjonsbaserte regelverket. Hovedleverandørene erfarer at operatørene bruker «påse»-plikten i regelverket som begrunnelse for detaljoppfølging i kontrakter.[156]

---

[156] *Dokumentasjonsprosjektet, Kartlegging av dokumentasjonsomfanget i petroleumsnæringen*, Ptil, http://www.ptil.no/getfile.php/1340598/PDF/Dokumentasjonsprosjektet%20-%20Endelig.pdf besøkt

8.3 Elektronisk kommunikasjon

De sikkerhets- og beredskapsplikter som er pålagt tilbydere av elektroniske kommunikasjonsnett og -tjenester i Norge er i hovedsak nedfelt i ekomloven, ekomforskriften, klassifiseringsforskriften og forskrift om prioritet i mobilnett. Nasjonal kommunikasjonsmyndighet (Nkom) har også fattet vedtak om minstekrav til reservestrømkapasitet i mobilnett.

Ekomloven § 2-10 sier at tilbyder skal tilby ekomnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig, og opprettholde nødvendig beredskap. Med dette menes at nett og tjenester skal være tilgjengelige, og at integritet og konfidensialitet skal beskyttes. Dette gjelder også i situasjoner med ekstraordinære påkjenninger. Hva som anses forsvarlig vil fremkomme gjennom markedspraksis, tilgjengelig teknologi og internasjonale krav. Tilbyder skal selv dekke kostnadene med dette. Myndigheten kan gjennom vedtak eller forskrift presisere hva som er forsvarlig sikkerhet og nødvendig beredskap.

Videre kan myndigheten treffe enkeltvedtak, inngå avtale eller gi forskrift om at tilbyder skal gjennomføre tiltak for å oppfylle nasjonale behov for sikkerhet, beredskap og funksjonalitet. Dette er ment å sikre tiltak som går utover forsvarlighetsnivået nevnt ovenfor. Merkostnadene knyttet til slike tiltak kompenseres av staten.

Klassifiseringsforskriften skal sikre nettutstyr i anlegg mot uønsket ytre fysisk påvirkning, og retter seg mot tilbydere av elektroniske kommunikasjonsnett som benyttes til offentlig elektronisk kommunikasjonstjeneste (nettilbydere). Nettilbydere skal klassifisere alle anlegg ut i fra hvor viktig eget nettutstyr i anleggene er for offentlige elektroniske kommunikasjonstjenester. Anleggene skal klassifiseres i klassene A, B, C og D. Sentralt i klassifiseringsforskriften er bestemmelsen som krever at nettilbyderne gjennomfører en helhetlig risiko- og sårbarhetsvurdering knyttet til sine anlegg, og sørger for at anlegg i de ulike klassene er forsvarlig sikret i samsvar med denne vurderingen. Nkom har utarbeidet egen veiledning for klassifiseringsforskriften og skjema/mal for rapportering.

I ekomforskriften § 8-2 har tilbydere en plikt til å utarbeide og vedlikeholde beredskapsplaner. Det forutsettes at det ligger dokumenterte risiko- og sårbarhetsvurderinger til grunn for disse beredskapsplanene. Det fremkommer også av § 8-2 at tilbyder på forespørsel skal delta på beredskapsøvelser arrangert av myndigheten.

I gjenopprettingsfasen etter utfall plikter tilbydere, etter ekomforskriften § 8-4, å prioritere hensynet til sluttbrukere med ansvar for liv og helse, foran kommersielle hensyn. Myndigheten kan i særlige tilfeller pålegge tilbyder å prioritere andre viktige samfunnsaktører. Dette er situasjoner hvor offentlige interesser tilsier en annen rekkefølge i gjenopprettingen enn det som fremkommer ovenfor. Tilbydere skal uten

---

26.10.2016. «Olje- og gassindustrien går sammen i kampen mot cyberkriminalitet», DNV, https://www.dnvgl.no/news/olje-og-gassindustrien-gar-sammen-i-kampen-mot-cyberkriminalitet-77263, besøkt 13.02.2017

ubegrunnet opphold varsle Nkom om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til ekomtjenester.

Ekomforskriften inneholder også krav om konkursvern, og nasjonal autonomi (i kraft når departementet bestemmer).[157]

Nkom har også skrevet veiledningsbrev til aktørene i bransjen som spesifiserer nærmere risikoakseptkriterier knyttet til krav om kommunikasjonsvern, integritet og tilgjengelighet i forhold til logiske angrep.

8.4 Finans

IKT-forskriften[158] skal sikre at IKT-virksomheten leverer de tjenester som er avtalt, også der hele eller deler av IKT-virksomheten er utkontraktert til andre aktører. IKT-forskriften omfatter IKT-systemer som er av betydning for foretakets virksomhet. Den stiller krav til: planlegging og organisering av sikkerhetsarbeidet, risikoanalyse, å fastsette kvalitetsmål for de deler av IKT-virksomheten som er knyttet opp mot foretakets øvrige mål, sikkerhet (beskyttelse), utvikling og anskaffelse, systemvedlikehold, drift, avviks- og endringshåndtering, utkontraktering og dokumentasjon av organisasjon, utstyr, IKT-systemer og andre vesentlige forhold i IKT-virksomheten. *Sikkerhet er rettet mot målrettede trusler, og oppfyllelse av kravet til beskyttelse av personopplysninger*[159] *skal anses være oppfylt i §5.*

For å vurdere om finansforetakene etterlever kravene i IKT-forskriften, benytter Finanstilsynet såkalt egenevaluering. Spørsmålene er basert på Cobit, ITIL, ISO og andre kilder, tilpasset av Finanstilsynet for det norske finansmarkedet. Finanstilsynet har utarbeidet veiledere for etterleving av IKT-forskriftens bestemmelser §5 sikkerhet,[160] samt risiko- og sårbarhetsanalyser. I tillegg har de to veiledninger som er tilpasset spesielle foretak, mindre sparebanker og eiendomsmeglingsforetak.[161]

Finanstilsynet er ansvarlig leder og sekretariat for Beredskapsutvalget for finansiell infrastruktur (BFI).

---

[157] *Forskrift om prioritet i mobilnett*, https://lovdata.no/dokument/SF/forskrift/2013-10-21-1241?q=forskrift om prioritet i mobilnett, mer informasjon her: http://www.nkom.no/teknisk/sikkerhet-og-beredskap/prioritet-i-mobilnettet/prioritet-i-mobilnettet - Om vedtak om minstekrav til reservestrømkapasitet i mobilnett se http://www.nkom.no/teknisk/sikkerhet-og-beredskap/ekomsikkerhet/tilbyders-sikkerhets-og-beredskapsplikter, under kapittel 8, og selve vedtaket og departementets vedtak i klagebehandlingen som lenke på høyresiden på samme nettside.

[158] *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT),* https://lovdata.no/dokument/SF/forskrift/2003-05-21-630, besøkt 26.10.2016.

[159] Jf. forskrift av 15. desember 2000 nr. 1265 til personopplysningsloven.

[160] *Veiledning til IKT-forskriftens § 5 "Sikkerhet",* Finanstilsynet, august 2013, http://www.finanstilsynet.no/Global/Temasider/IT-tilsyn/Veiledning_IKT_forskrift_5_sikkerhet.pdf, besøkt 26.10.2016.

[161] «IT-tilsyn», Finanstilsynet, http://www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/, besøkt 26.10.2016.

9 Standarder og veiledninger

9.1 Innledning

Dette kapittelet knytter noen kommentarer til sikkerhetsstandardene ISO 27001 og 27002 for informasjonssikkerhetsledelse, samt utvalgte internasjonale veiledere for sikring av driftskontrollsystemer og AMS fra National Institute for Standards and Technology (NIST). Grunnen til at vi framhever spesielt disse standardene er at Difi har anvendt ISO 27001 som grunnlag i sin veileder til offentlig forvaltning. For driftskontrollsystemer har vi valgt å framheve Myndigheten för Samhällsskydd och beredskap (MSB)s veileder, siden denne referer til andre internasjonale standarder. I tillegg har vi valgt å kommentere NIST sine to standarder for henholdsvis industrikontrollsystemer og AMS. Disse NIST-standardene er konkrete mht. tekniske tiltak, sikkerhetsarkitektur og beskyttelse.

9.2 Internasjonale standarder og veiledere

9.2.1 Generell IKT-sikkerhet

Det er mange ulike standarder og veiledere innen internkontroll for informasjonssikkerhet tilgjengelig, også kalt styringssystem for informasjonssikkerhet, Information Security Management System (ISMS), informasjonssikkerhetsledelse, med mer. I EU er bruken av ISO 27001 og ISO 27002 utbredt.

I kapittel 12.3 er det listet opp standarder og veiledninger som kan være aktuelle for IKT-sikkerhet i energisektoren. Dette er på ingen måte en uttømmende liste. Det kan oppleves å være en nærmest uendelig tilgang på ulike standardversjoner og tilgjengelige veiledere på mange områder, spesielt om en har et internasjonalt perspektiv. Det er vanskelig å si om en standard eller veileder er bedre enn en annen, og hva som bør benyttes kan være fornuftig å overlate til den enkelte virksomhet. Det viktige er at standarden eller veilederen ikke er utdatert, og at den fungerer slik at virksomheten når sine mål og myndighetenes krav til sikkerhet. Generelt er standarder fornuftig å bruke. Bak arbeidet med en standard ligger det ofte mye arbeid, og et stort fagnettverk av eksperter har bidratt i utviklingen. Ofte er også mye av lovmessige krav innebygd.

9.2.2 Driftskontrollsystemer

Som for generell IKT-sikkerhet og sikkerhetsledelse, finnes det flere standarder og veiledninger for sikring av industrikontrollsystemer. ISO/IEC TR 27019:2013 *Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry* bygger på ISO/IEC 27002 *Information security management*. ISO 27019 utvider ISO/IEC 27000 standardene til prosesskontrollsystem og automasjonsteknologi, og standarden bistår energiselskaper med å innføre et styringssystem for

informasjonssikkerhetsledelse i samsvar med ISO/IEC 27001. Dette gjør det mulig å utvide styringssystemet fra forretningsnivå til prosesskontrollnivå.

Konvensjonell eller analog kontrollteknologi er utenfor rekkevidden til ISO/IEC TR 27019:2013. Det er også kontrollsystemer for husholdninger (smarte hjem) og telekom-komponenter som er brukt i kontrollsystemet. Disse er dekket av en annen standard i ISO-serien, ISO/IEC 27011:2008.

I Europa har rådgivnings- og veiledningsorganet ENISA så langt kommet fram til to anbefalinger når det gjelder å sikre IKT og SCADA-systemer:

- For det første har ENISA utviklet et rammeverk for å vurdere modenhetsgrad i sikkerhet i industrielle prosesskontrollsystemer og SCADA. Rammeverket gjør det mulig å klassifisere sikring av SCADA-systemer i fire modningsnivåer for sikkerhet. I dette rammeverket inngår regelverk og revisjon av kriteriene som blir vurdert for modenhet. Mange land har ikke regelverk på plass og havner lavt på modningsskalaen. Tyskland og Frankrike arbeider med å implementere en revisjons- og sertifiseringsprosess for sikring av SCADA-systemer. Det er henholdsvis BSI og ANSII som står bak disse initiativene
- ENISA anbefaler å koordinere sikring av SCADA med nasjonale IKT-sikkerhetsstrategier. ENISA anbefaler videre å utvikle god praksis for beskyttelse av prosesskontrollsystemer, standardisere informasjonsdeling på tvers av sektorer og land, styrke kunnskap hos virksomhetene, satse på utdanningsprogram og forskning,[162] og sertifisering av kompetanse hos operatører som arbeider med prosesskontroll.[163] Sertifisering av driftspersonell er også et tema i NIS.

Myndigheten för samhällsskydd och beredskap (MSB) har laget en veileder for SCADA-sikkerhet som kopler rådene opp mot en rekke internasjonale standarder. De gir fire grunnleggende råd i arbeidet med å sikre SCADA:[164]

- Øk bevisstheten i hele organisasjonen om behovet for sikkerhet i industrielle informasjons- og styringssystemer
- Gjennomfør grunnleggende utdanning om sikkerhet i industrielle kontrollsystem
- Arbeid aktivt med sikkerhetsarkitektur i industrielle informasjons- og styresystemer og i tilknyttede IT-systemer
- Still sikkerhetskrav i forhandlinger med leverandører og i serviceavtaler

NIST har utviklet en veiledning til sikring av industrikontrollsystemer, *Guide to Industrial Control Systems (ICS) Security*.[165] Veilederen dekker teknologi som SCADA,

---

[162] Mattioli, R og M. Konstantinos, *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*, ENISA, 2015, tilgjengelig her: https://www.enisa.europa.eu/publications/maturity-levels, besøkt 21.07.2016.

[163] *Certification of Cyber Security skills of ICS/SCADA professionals, Good practices and recommendations for developing harmonised certification schemes*, ENISA, December 2014.

[164] *Vägledning till ökad säkerhet i industriella informations och styrsystem,* Myndigheten för samhällsskydd och beredskap MSB, 2014, https://www.msb.se/RibData/Filer/pdf/27425.pdf, besøkt 23.10.2016.

[165] Stouffer, K., Pillettiri, V. Lightman, S., Abrams, M. and A. Hahn,

DMS, PLC og retter oppmerksomheten mot pålitelighet og sikkerhet. Veilederen gir også en oversikt over topologier, og identifiserer typiske sårbarheter og trusler mot slike systemer. Veilederen gir råd om hvordan en skaper en sikker arkitektur for industrikontrollsystemet. Den er teknisk i sin natur, men tilbyr også nødvendig bakgrunnsinformasjon for å forstå temaet som er omtalt.

NIST har også en veileder for sikring av AMS, *Guidelines for Smart Grid Cybersecurity*.[166] Veilederen gir tekniske råd om arkitektur og beskyttelse av grensesnitt.

9.3 Nasjonale standarder og veiledere

9.3.1 Generell IKT-sikkerhet

Standarder og veiledere kan være gode verktøy for virksomheter i forbindelse med å følge opp informasjonssikkerhetskrav. Disse hjelpemidlene finnes tilgjengelig både nasjonalt og internasjonalt, og de kan benyttes både på overordnet organisatorisk nivå, og på detaljnivå i tekniske løsninger. Standard Norge bidrar i internasjonalt standardiseringsarbeid og utarbeider veiledere for IKT-sikkerhet på norsk.[167]

I norske virksomheter virker veilederne fra Datatilsynet, NSM og Difi å være mest brukt:

- Difis veileder for internkontroll gjelder for alle virksomheter i offentlig sektor, men kan også benyttes av virksomheter i privat sektor. Difis veileder er basert på ISO 27001 og forsøker i tillegg å ivareta krav fra norsk personvernregelverk og sikkerhetsregelverk[168]
- NSMs sikkerhetsveiledere for systemteknisk sikkerhet gjelder for alle virksomheter som er underlagt sikkerhetsloven. Veilederne er temabaserte, og to relevante forhold til forebyggende sikkerhet og nettverkssikkerhet er *Ti viktige tiltak mot dataangrep* og *Ti grunnleggende tiltak for sikring av egne nettverk* [169] [170]

Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, NIST, May 2015, Revision 2,

[166] *Guidelines for Smart Grid Cybersecurity, Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*, NISTIR 7628 Revision 1, NIST, 2014, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf, besøkt 26.10.2016.

[167] *Standard Online AS (2016) IT-sikkerhet - ISO/IEC 27000*, https://www.standard.no/fagomrader/ikt/it-sikkerhet/

[168] «Internkontroll i praksis – informasjonssikkerhet», Difi, http://internkontroll.infosikkerhet.difi.no/ besøkt 11.01.2017.

[169] «Ti viktige tiltak mot dataangrep, Sjekkliste nr 2 (S02)», Oppdatert 2016-03-03, NSM, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf, besøkt 11.01.2017.

[170] «Ti grunnleggende tiltak for sikring av egne nettverk, Sjekkliste nr 3 (S03)», Oppdatert 2016-11-15, NSM, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-03.pdf, besøkt 11.01.2017. Flere veiledere finnes her: https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet

- Datatilsynet har flere veiledere på personvern og internkontroll[171]

I tillegg til disse sektorovergripende veilederne kommer sektorspesifikke veiledere. NVE har veileder til beredskapsforskriften. I 2012 laget NVE en veileder til sikkerhet i avanserte måle- og styringssystemer. Denne har krav av både styringsmessig og teknisk art. I tillegg anbefaler NVE å følge NEK sine anbefalinger for AMS, som fremkommer av konklusjon i deres rapport AMS + HAN[172], samt NVEs rundskriv fra 2016 vedrørende HAN-grensesnittet og OBIS koder.[173]

9.3.2 Sikkerhet i driftskontrollsystemer

NSM har utgitt en *veileder for sikring av industrikontrollsystemer* (2014). Veilederen gir råd om perimetersikring, sikkerhetsmessig herding, brukerhåndtering og passord, samt deteksjon. Det er en overordnet teknisk veiledning for sikring av industrielle automatiserte kontrollsystemer basert på sikkerhet i dybden. Veilederen er ikke ment å erstatte veiledere fra leverandører.[174]

---

[171] *Veileder i sikkerhetsarkitektur. For virksomheter som behandler personopplysninger og sensitive personopplysninger*. August 2011. Datatilsynet. Veileder om internkontroll og informasjonssikkerhet, Datatilsynet, 2009, https://www.datatilsynet.no/globalassets/global/04_veiledere/internkontroll_veil.pdf, besøkt 11.01.2017.
https://www.datatilsynet.no/globalassets/global/04_veiledere/sikkerhetsarkitektur_veil.pdf, besøkt 11.01.2017.

[172] Aanesen, L. T., Fines, S. og Ek, R. (2015), A»MS + HAN – Om å gjøre sanntid måledata tilgjengelig for forbruker», http://www.enova.no/upload_images/3C6882F6519248C2BA24B53E6A96A395.pdf besøkt 23.12.2016.

[173] Venjum, A., «Informasjon til kundene via HAN-grensesnittet i AMS-måleren. OBIS-koder», NVE, 2016, https://www.nve.no/Media/4307/201603186-1-informasjon-til-kundene-via-han-grensesnittet-i-ams-m%C3%A5leren-obis-koder-1772408_1124902_0.pdf besøkt 23.12.2016.

[174] *Sikring av industrielle automatiserte kontrollsystemer, Veiledning,* sist oppdatert 2014-03-26, Nasjonal sikkerhetsmyndighet, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/sikring-av-industrielle-automatiserte-kontrollsystemer.pdf, besøkt 26.10.2016.

Del IV Vurderinger og anbefalinger til endringer i regelverk

10 Vurderinger til endringer i regelverket

10.1 Innledning

Behovet for økt bruk av digitale verktøy og informasjonssystemer med tilhørende sårbarheter, internasjonale og nasjonale føringer og eksisterende standarder og regelverk danner grunnlaget for vurderingene som arbeidsgruppen har gjennomført. Den sentrale problemstillingen som er håndtert, er om eksisterende regelverk legger til rette for bruk av nye effektive digitale verktøy og informasjonssystemer i energiforsyningen, samtidig som det sørger for at eventuell økt risiko for forsyningssikkerheten blir redusert.

- Arbeidsgruppen har vurdert om krav til sikring av informasjonssystemer gjøres mest hensiktsmessig gjennom funksjonskrav eller spesifikke krav. De generelle begrunnelsene for funksjonsbasert regelverk – ansvarliggjøring, handlefrihet, fleksibilitet og endringstilpasning – er avveid mot generelle rettssikkerhetshensyn når det gjelder utforming av rettsregler, slik som klarhet, tydelighet og forutsigbarhet. Arbeidsgruppen vurderer at et funksjonsbasert regelverk, hvor noen tema har mer spesifikke krav ivaretar behovene for krav til sikkerhet i informasjonssystemer i energiforsyningen.
- Arbeidsgruppen har vurdert om krav til sikring av informasjonssystemer gjøres mest hensiktsmessig gjennom krav til bruk av standarder eller direkte i forskriftskrav. Arbeidsgruppen mener at bruk av standarder vanligvis ikke bør erstatte forskrifter. Standarder er et verktøy for å oppnå det som er fastsatt av krav i lover og forskrifter, og som eventuelt er utdypet i veiledere.
- Arbeidsgruppen har vurdert behovet for krav til kompetanse, krav til utdanning og økt bruk av veiledning. Arbeidsgruppen vurderer det slik at kompetanseløft bør skje ved andre virkemidler enn nye forskriftskrav. Dagens krav til kompetanse er tilstrekkelig, men må i større grad følges opp. Arbeidsgruppen mener at NVE i veilederen bør tydeliggjøre eksisterende krav til kompetanse.
- Arbeidsgruppen har vurdert utfordringene og sårbarhetene i tjenesteutsetting, leverandørkjeder og fjernaksess. Arbeidsgruppen vurderer at det kan være behov for å tydeliggjøre regelverket slik at det ikke hindrer innovasjon og utvikling og samtidig setter krav til et forsvarlig sikkerhetsnivå.
- Arbeidsgruppen har vurdert behovet for krav til systemovervåkning, rapportering og hendelseshåndtering. Arbeidsgruppen vurderer det slik at det bør stilles tydeligere krav til logging, logganalyse og hendelseshåndtering for alle virksomheter i energisektoren og deres IKT-systemer og nettverk.
- Arbeidsgruppen anser at beredskapsforskriftens kapittel 2 har viktige krav for å få på plass et styringssystem for også informasjonssikkerhet. Samtidig vurderer arbeidsgruppen at det er behov for en forenkling og tydeliggjøring i bfe kapittel 6 og 7. I dette ligger det en mulighet til å i større grad bruke begreper fra internasjonale standarder fordi begreper bør tolkes likt. Arbeidsgruppen har vurdert særlig ISO-standardene 27001/2 og den tekniske rapporten ISO TR

27019. Samsvaret mot beredskapsforskriften slik den er i dag, er god, men ikke fullstendig. Særnorske krav i beredskapsforskriften, gir blant annet NVE fullmakter til å utnevne KBO-enheter, jf. bfe § 3-3 *«KBO-enheter»* og bfe § 8-2 *«Pålegg»,* og til å fatte vedtak om sikringstiltak.

- Arbeidsgruppen mener videre at det bør lages en veileder på IKT-sikkerhet til beredskapsforskriften der NVE i større grad enn i dag henviser til og bruker begreper fra internasjonale standarder.
- Arbeidsgruppen har vurdert virkeområdet til regelverket, og anbefaler at virkeområdet utvides på området IKT-sikkerhet til å omfatte det som i dag er klasse 1 selskap

10.2 Vurdering av funksjonskrav eller spesifikke krav

10.2.1 Innledning

Et viktig spørsmål ved utformingen av regler er hvor detaljerte skal de være. Er det praksis eller lovgiver som skal stå på for den nærmere presisjon og konkretisering av reglene?[175] I norsk rettskultur er det i dag en tendens til å beskrive funksjonen som kreves i lov, og at forskrifter, veiledere og standarder beskriver kravene mer i detalj. Begrepet funksjonsbasert regelverk har ikke et helt entydig innhold. Funksjonskrav retter i større grad seg mot mål og resultater og i mindre grad mot bestemte metoder eller løsninger.[176] Funksjonskrav kan forstås som generelle krav rettet mot et formål eks. bfe § 7-1 *Generell plikt til å beskytte driftskontrollsystemet*. Men det kan også tenkes andre kombinasjoner, der man har generelle krav rettet mot prosesser og ikke mot resultater, eksempelvis bfe § 2-9 sitt krav om evaluering etter ekstraordinære situasjoner og øvelser. Kravene til internkontroll i virksomheter (jf. Bfe § 2-10) er et annet eksempel. Begrunnelsene for bruk av funksjonskrav er at slike regler antas å gi fleksibilitet til å følge den teknologiske utviklingen av innen forskjellige fagområder. Virksomhetene får handlefrihet og kan utnytte lokal og situasjonsspesifikk kunnskap til å finne egnede løsninger innenfor regelverkets rammer. Videre blir det opp til virksomheten å vurdere og velge løsning.

10.2.2 Eksempel på bruk av funksjonsbasert regelverk

Både elektronisk kommunikasjon og petroleumsindustrien har et funksjonsbasert regelverk. Olje- og gassindustrien har et funksjonsbasert regelverk innenfor helse, miljø og sikkerhet (HMS). Regelverket har lagt til grunn at selskapene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak. Dette gjøres gjennom risiko- og sårbarhetsanalyser i de enkelte selskapene. Bransjens egenutviklede standarder innenfor informasjonssikkerhet legges til grunn for arbeidet. Disse standardene bygger på ISO

---

[175] Sunde, J.Ø., *Speculum legale*, 2004, s. 309.

[176] I *St.meld. nr. 17 (2002–2003) Om statlige tilsyn,* https://www.regjeringen.no/no/dokumenter/stmeld-nr-17-2002-2003-/id134860/ besøkt 05.03.2017.

27000-serien.[177] Å bruke standarder for risikostyring av IKT-systemer er nyttig for å sikre at analyser er mest mulig komplette og tar med alle relevante områder. Henvisning til standarder er også nyttig for å oppnå effektive sikkerhetstiltak. Standardiseringen kan omfatte både organisering av sikkerhetsarbeidet, kompetansetiltak og konkrete tekniske sikkerhetsløsninger.

Den store friheten i løsningene ved funksjonskrav gjør det imidlertid mer krevende for myndigheten å angi hva som konkret ligger i et krav og eventuelt kunne gi pålegg om retting innenfor sikkerhet. Det er også krevende for en aktør å velge et sikkerhetsnivå som er i tråd med regelverket. Bruk av standarder gir heller ingen garanti for at ikke feil og svikt kan oppstå. Det fikk Statoil, som har lang erfaring innen tjenesteutsetting, erfare natt til 21. mai 2014. I mai 2014 ble det utført vedlikeholdsarbeid på en server i produksjonsmiljøet på Mongstad som medførte forstyrrelser for den pågående lasteoperasjonen. I følge Synergi-rapporten er dette arbeidet utført på en måte som ikke er i samsvar med prosedyre for arbeid på automasjonssystemer. Hendelsen førte til at den gjenværende delen av lasteoperasjonen måtte gjennomføres med manuell styring i samsvar med etablert prosedyre for dette. Manuell styring innebærer at kvaliteten på leveransen er «off spec», noe som innebærer et begrenset økonomisk tap for Statoil. Den aktuelle serveren påvirket ikke øvrige deler av anlegget på Mongstad og hendelsen påvirker ikke anleggets integritet.[178]

NSM har uttalt at kravene til styringssystem i ISO 27001 sammenfaller i stor grad med kravene gitt i forskrift om sikkerhetsadministrasjon, Standarden kan derfor benyttes så lenge tilleggskravene til sikkerhetsadministrasjon etterleves.[179] Difi har gjort en vurdering av om statlige virksomheter bør bli pålagt å bruke standarden ISO 27001 (Informasjonsteknologi, *Sikringsteknikker, styringssystemer for informasjonssikkerhet, krav*). Difi konkluderte med at dette ikke er hensiktsmessig. På ene siden er standarden fleksibel, men på en annen side vil det bli kostbart å innføre et slikt *krav* og sikre etterlevelse. Dessuten kan det føre til at dette blir normen, og at virksomheter blir mer opptatt av å etterleve krav enn å jobbe aktivt med å forbedre sikkerheten. Difi har derfor lagt seg på en linje der de veileder og rådgir basert på ISO-standarden 27001 og 27002. Difi har utviklet en rekke veiledere, herunder veileder for internkontroll i praksis og veileder for overgang til NS-ISO 27001.

10.2.3 Arbeidsgruppens vurderinger

I energisektoren er mange selskaper små. Selskapsstrukturen gjenspeiler i så måte den generelle næringsstrukturen i Norge. De små virksomhetene har begrensede ressurser tilgjengelige til sikkerhetsarbeidet. Denne utfordringen var også påpekt av Lysne-utvalget, som anbefalte større fagmiljøer. Å beskytte og sikre IKT-systemene er krevende. Det trengs både kompetanse og kapasitet (mennesker). NVE har fått tilbakemelding fra små selskaper at de ønsker et tydelig regelverk innen IKT-sikkerhet

---

[177] Se NOU Digital sårbarhet – sikkert samfunn (2015:13).

[178] *Tilsyn med IKT-sikkerhet i Statoil*, PTIL 31.01.2017, http://www.ptil.no/tilsynsrapporter/tilsyn-med-ikt-sikkerhet-i-statoil-article12576-713.html, besøkt 13.02.2017.

[179] *Styringssystem for informasjonssikkerhet. Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002.* Rapport 2012:15. Direktoratet for forvaltning og IKT (Difi).

med konkrete krav slik at de kan kjøpe ressurser for å svare ut kravene. Et for detaljert regelverk kan på den annen side innebære fare for en «huke-av-kultur» hos virksomhetene.

De generelle begrunnelsene for funksjonsbasert regelverk – ansvarliggjøring, handlefrihet, fleksibilitet og endringstilpasning – må avveies mot generelle rettssikkerhetshensyn når det gjelder utforming av rettsregler, slik som klarhet, tydelighet og forutberegnelighet. I tillegg vil reguleringsmyndigheten i mange sammenhenger ha kunnskap som kan formidles gjennom forståelige og praktisk anvendbare regler som dermed bidrar til mer forutsigbare og forsvarlige resultater. For vage regler kan gi stor variasjon i resultater i form av etterlevelse og håndhevingspraksis fra myndighetene. Forståelse av de regulerte virksomhetenes forutsetninger for å etterleve de overordnede reguleringshensynene vil måtte spille inn i valget av reguleringsstrategi. Dersom det er stor variasjon i målgruppen, vil avveiingen mellom klare regler og funksjonsbaserte regler være særlig utfordrende.

Valget bør videre basere seg på de regulerte virksomhetenes ressurser, kapasitet, motivasjon og behov, og myndighetenes evne og kapasitet til å tilby tilstrekkelig veiledning i regelverksforståelse, samt til kontinuerlig å vurdere om etterlevelsesmønstre reflekterer kravene til tilstrekkelige og forsvarlige løsninger.[180] Det kan være en utfordring for både tilsynsmyndighet og pliktsubjekt å vite når krav er tilfredsstilt. Veiledningen bør kunne gi noen råd.

Oppsummert har de ulike reguleringsregimene følgende fordeler og ulemper:

Fordeler med funksjonsbasert regelverk:

- Mulighet for virksomheter å selv bestemme på en fleksibel måte eget oppsett for informasjonssikkerhetsstyring (innenfor gjeldende lover og regler)
- Ulike standarder kan benyttes etter hva som passer best for den enkelte virksomhet
- En kan benytte en risikobasert tilnærming for informasjonssikkerhetsoppsettet slik ISO/IEC 27001 anbefaler

Ulemper med funksjonsbasert regelverk:

- Ingen tydelige felles krav til sikring, annet enn rammeverk og anbefaling om å kontrollere egne tiltak opp mot de mest typiske/vanligste tiltakene (ISO/IEC 2700)
- Risikoanalysen blir svært viktig, og en må kontrollere tiltakene som er valgt opp mot tiltakslisten som følger av risikoanalysen
- Virksomheter kan gå seg vill i jungelen av veiledere (ISO, NVE, NSM, Difi, Datatilsynet, med flere), og ikke makte å finne frem til egne egnede sikkerhetstiltak

Fordeler med detaljregulering:

- Myndigheten kan angi krav som er tilstrekkelige, det gir klarhet og forutsigbarhet

[180] NOU 2015:13 Digital sårbarhet – sikkert samfunn, s 294-205 https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf besøkt 05.03.2017.

- Prediktere løsninger eller krav som gjør det enkelt å føre tilsyn og oppnå kontroll på felles sikkerhets-nivå
- Det kan bli billigere og sikrere løsninger når flere er nødt til å bruke like løsninger (stordriftsfordeler)

Ulemper med detaljregulering:

- Mindre fleksibilitet for virksomhetene
- Det kan bli utfordrende for mindre virksomheter økonomisk å etterleve en felles tiltakspakke som myndigheten vurderer at de trenger, men som de selv ikke har kompetanse til å forstå behovet for
- Stiller strengere krav til myndighetene om et helhetlig og fullstendig regelverk
- Regelverket kan raskere gå ut på dato, særlig ved raske teknologiendringer

Det er viktig at NVE i arbeidet med forskriftskrav utformer enkle og tydelige funksjonskrav. Kravene bør ikke hindre utvikling og innovasjon i et marked i rask endring og med stor teknologisk utvikling, og samtidig sikrer likebehandling av aktørene. Arbeidsgruppen mener at bruk av standarder er nyttige tillegg til forskrift. Arbeidsgruppen anbefaler på dette grunnlaget å beholde krav til IKT-sikkerhet i forskrift, men se til formuleringer og begrepsbruk i internasjonale standarder når forskriftstekst skal reformuleres.

Arbeidsgruppen vurderer det slik at beredskapsforskriften fortsatt bør ha funksjonskrav om IKT-sikkerhet. Samtidig er det under noen temaer behov for mer detaljerte krav. Små selskap etterspør mer detaljerte regler og råd.

Dagens beredskapsforskrift har i stor grad funksjonskrav til IKT-sikkerhet. Gjennom KILE, tilsyn og veiledning har NVE muligheter til å stimulere til et godt sikkerhetsnivå og bidra til at forsvarlig sikkerhet finner sin form. Et funksjonsbasert regelverk kan bidra til risikoreduksjon på sikt, mens kostnadene i stort er uendret. I vurderingen av hvor detaljert et regelverk skal være må man også tenke på hvordan NVE skal føre tilsyn med regelverket. Funksjonskravene må være av en slik art at de kan brytes ned i praktiske spørsmål der svaret kan verifiseres, slik at NVE kan vurdere om regelverkets krav er tilfredsstilt eller ikke.

10.3 Vurdering av bruk av standarder eller forskriftskrav

10.3.1 Innledning

Arbeidsgruppen har gjort vurderinger knyttet til bruk av standarder. Det finnes en rekke standarder. En oversikt over noen viktige standarder er vist i kapittel 12.3.

10.3.2 Arbeidsgruppens vurdering

Arbeidsgruppen har vurdert beredskapsforskriftens kapittel 7, opp mot ISO 27001/2[181] og ISO TR 27019 og funnet at det er mye samsvar i sikringstiltak mellom standardene og dagens forskrift. Både beredskapsforskriften og ISO-standeren legger til grunn forsvar-i-dybden som prinsipp. Arbeidsgruppen mener at dette er et nødvendig prinsipp for sikring av SCADA og driftskontrollsystemer. Arbeidsgruppen har også sett til Difi som har gjort en vurdering om statlige virksomheter bør bli pålagt å bruke standarden ISO 27001. Difi har lagt seg på en linje der de veileder og rådgir basert på ISO-standarden 27001 og 27002. Difi har utviklet en rekke veiledere, herunder veileder for internkontroll i praksis og veileder for overgang til NS-ISO 27001.

Fordelene med å bruke standarder er at de lettere enn forskrifter kan reflektere teknologisk utvikling på grunn av jevnlige oppdateringer, og at de forenkler regelverket fordi lover og forskrifter kan begrense seg til overordnede målsetninger/funksjonskrav. Forutsetningen må være at standarder benyttes for områder der det er egnet, og at betingelsene er vurdert som akseptable.

Arbeidsgruppen mener at bruk av standarder er nyttige i tillegg til forskrifter. Standarder er et verktøy for å oppnå det som er fastsatt av krav i lover og forskrifter, og som eventuelt er utdypet i veiledere. Standarder brukes vanligvis ikke som krav på hvilken løsning man *må* følge, men angivelse av løsning man *kan* følge for å oppfylle de kravene som er fastsatt i lov og forskrift. De gir dermed forutsigbarhet for aktørene på at man oppfyller krav. Arbeidsgruppen vurderer på dette grunnlaget at det er mest hensiktsmessige å se til formuleringer og begrepsbruk i internasjonale standarder når forskriftstekst skal reformuleres.

Arbeidsgruppen vurderer det som fornuftig å henvise til internasjonale standarder på IKT-sikkerhet i veilederen i større utstrekning enn det er gjort i dag. I denne vurderingen har arbeidsgruppen lagt vekt på følgende argumenter:

- Beredskapsforskriften har stort samsvar med ISO/IEC 27001/2 og tilbyr et helhetlig sikkerhetsregime tilpasset norske behov
- Bransjen har tilpasset sine systemer og rutiner til krav i beredskapsforskriften
- NVE har et utviklet og utprøvd tilsynsregime for beredskapsforskriften
- NVE fått tilbakemelding på at flere land arbeider med å få på plass regelverk. Fra møter i EU og Danmark har NVE fått tilbakemelding på at Norge har et godt regelverk for å ivareta IKT-sikkerhet i energisektoren

Arbeidsgruppen mener videre at det bør lages en veileder på IKT-sikkerhet til beredskapsforskriften der NVE i større grad enn i dag henviser til og bruker begreper fra internasjonale standarder.

[181] Det går flere år mellom hver gang en standard eller forskriftstekst oppdateres. ISO 27001 kom i 2005 og ble oppdatert i 2013, COBIT hadde 5 oppdateringer mellom 1996 og 2012 pluss noen tillegg som kom underveis, men COBIT dekker mer enn bare informasjonssikkerhet.

10.4 Vurdering av kompetansekrav, utdanning og veiledning

10.4.1 Innledning

Norge har en generell kompetanseutfordring innenfor IKT-sikkerhet. Lysne-utvalget pekte på denne sikkerhetsutfordringen, som følger i kjølvannet av digitaliseringen av Norge. Kompetanseutfordringen var også tatt opp av Sofie Nystrøm, direktør NTNU CCIS, som sa i en ytring på NRK: «*Det er et stort underskudd i det norske samfunnet på kompetanse rundt IT, og spesielt innenfor cyber- og informasjonssikkerhet. Skal vi ikke bare la utenlandske eksperter ta seg av det da? Fornuftig sett fra bunnlinja. Effektivt og økonomisk lønnsomt, på kort sikt. Hvorfor er det så farlig? Det er ikke praktisk mulig å drifte IT-løsninger uten vide tilganger som gir innsyn i data på systemene som kan utgjøre kritisk informasjon som helsedata, data om kritiske infrastrukturer og konti-opplysninger.*»[182]

10.4.2 Eksempler på internasjonale krav til kompetanse

I energisektoren er det, i tillegg til den allmenne utfordringen på IT-sikkerhetskompetanse, en ekstra utfordring når det gjelder sikring av driftskontrollsystemer. ENISA har sett nærmere på denne problemstillingen i en rapport og vurdert behovet for sertifisering av operatører av industrikontrollsystemer og SCADA. I sin rapport peker de på utfordringen med konvergens mellom industrikontrollsystemer, SCADA og IT, og at dette har konsekvenser for sikkerheten. I rapporten konkluderer forfatterne med å anbefale at det utvikles en sertifiseringsordning for personell som arbeider med industrikontrollsystem/SCADA.[183]

I EUs tredje markedspakke setter artikkel 61 i driftskoden for Systems Operations krav til sertifisering av personell som sitter på driftssentraler.[184] Sertifiseringen skal gjennomføres av TSO, for Norge blir dette Statnett: Artikkel 61. punkt 1. «*An individual may become a system operator employee in charge of real-time operation provided he or she is trained and subsequently certified by a nominated representative from his or her TSO for the concerned tasks within the timescale defined in the training programme. A system operator employee in charge of real-time operation shall not work unsupervised in the control room unless he or she is certified*».

---

[182] Sofie Nystrøm, «Hvem skal sitte med «atomkodene» våre?,»Ytring NRK, 20. november 2016.

[183] Adrian Pauna (ENISA), Contributors, Samuel Linares (CCI), Ignacio Paredes (CCI), José Valiente (CCI), María Pilar Torres Bruna (everis Aeroespacial y Defensa), Sara García-Mina Martínez (everis Aeroespacial y Defensa), Auke Huistra (Suver), *Certification of Cyber Security skills of ICS/SCADA professionals Good practices and recommendations for developing harmonised certification schemes*, ENISA, December 2014, tilgjengelig: https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals, besøkt 21.11.2016.

[184] *Commssion Regulation EU, establishing a guideline on electricity transmission system operation*, Bryssel 2016, draft, https://ec.europa.eu/energy/sites/ener/files/documents/SystemOperationGuideline%20final%28provisional%2904052016.pdf besøkt 05.03.2017.

10.4.3 Eksisterende nasjonale kompetansekrav for energiforsyningen

I dag stilles det ingen krav til formell kompetanse til IKT-sikkerhet i energiforsyningen i Norge, men det er flere bestemmelser som indirekte sier noe om kompetanse og bemanning.

Energilovforskriften § 3-6 stiller krav å «ha tilgang til personell med kompetanse» til å gjøre en rekke oppgaver innenfor henholdsvis nettforvaltning (første ledd) og kraftproduksjon (andre ledd). Bestemmelsen kom etter at OED i 2015 opphevet forskrift 10. mars 2011 nr. 263 om krav til kompetanse mv. hos anleggs- og områdekonsesjonærer (kompetanseforskriften) og innførte istedenfor energilovforskriften § 3-6 som omtalt ovenfor. OED sin begrunnelse for endringen var at kompetanseforskriften kan ha hatt uønskede effekter for selskapenes muligheter til selv å avgjøre optimal organisering av sin virksomhet. Departementet ønsket å gi selskapene mer fleksibilitet for egen organisering av virksomheten. Samtidig forutsatte OED at beredskapsforskriften har krav til kompetanse som fortsatt gjelder.

I bfe § 2-1 (Ansvar) legges ansvaret for å ha tilstrekkelig ressurser på leder for virksomheten *«Leder for virksomhet som er omfattet av denne forskrift har ansvar for at: Virksomheten er innrettet på en slik måte og med slike ressurser som er nødvendig for å ivareta ansvar og oppgaver i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift.»*

I beredskapsforskriften § 2-2c *(Organisasjon og funksjon)* stilles det krav til at alle KBO-enheter skal ha en IKT-sikkerhetskoordinator. Denne skal være faglig kontaktpunkt til beredskapsmyndigheten vedrørende IKT-sikkerhet. I utgangspunktet betyr det at IKT-sikkerhetsansvarlig kan ha denne rollen uten å ha formell IKT-sikkerhetskompetanse, men det vil det måtte ansees som et brudd på forskriften dersom IKT-sikkerhetskoordinatoren ansatt i virksomheten ikke har nok kompetanse eller forståelse på feltet til å ivareta koordineringsoppgaven.

Videre stiller § 7-9. *(Bemanning av driftssentral)* i bfe krav om «nødvendig kompetanse»: Virksomheten skal til enhver tid ha tilstrekkelig og tilgjengelig autorisert personell med nødvendig kompetanse, slik at driftskontrollfunksjonen kan utøves uten ugrunnet opphold. Virksomhetens risiko- og sårbarhetsanalyse skal ligge til grunn for valg av bemanningens størrelse, samt omfang av ordninger for påkalling av ekstra personell ved behov, jf. § 2-4 og § 5-8. I veilederen til beredskapsforskriften gis det eksempel på hva personellet på driftssentralen skal ha av kompetanse:

- Kompetanse i krisemestring
- Inngående kjennskap til virksomhetens risiko- og sårbarhetsanalyser og beredskapsplanverk
- Ha deltatt på øvelser i håndtering av ekstraordinære hendelser
- God oversikt over sitt forsyningsområde
- Førstehånds kjennskap til anleggene de styrer
- Trening i håndtering av kompliserte feilsituasjoner
- Etablert kontakt med nødvendig personell og hensiktsmessige språkkunnskaper
- Omfattende kunnskaper om driftskontroll

Beredskapsforskriften stiller videre krav til at driftssentralen bemannes i *7-14e Bemanning av driftssentral* for klasse 2 anlegg *og § 7-15b Bemanning av driftssentral* for klasse 3 anlegg. Hovedforskjellen ligger i responstid og at klasse 3 anlegg skal ha døgnkontinuerlig bemanning. Det er ikke ytterligere krav til kompetanse i bemanningsbestemmelsene i disse bestemmelsene.

Funksjonskrav til kompetanse er stilt i bfe § 7-17c *Mobile radionett – driftsradio: Kunne betjenes av personell med nødvendig kompetanse til bruk*. I veiledning til bfe skriver NVE at «Når virksomhetene skal vurdere bemanningens størrelse, bør det tas utgangspunkt i evalueringer etter hendelser, ROS-analyser etc. for å vurdere hvorvidt bemanningen har vært tilstrekkelig til å kunne håndtere de hendelsene som har vært. Følgende spørsmål kan være aktuelle å stille seg ved vurderingen: Kunne hendelsene vært håndtert raskere/bedre med større grunnbemanning i driftssentralen? Hadde operatørene god nok kompetanse og evne til å håndtere hendelsene, og vil de kunne håndtere hendelser som kan forventes å oppstå i henhold til ROS-analysen? Har virksomheten planer for å utvide nettet eller driftskontrollsystemet som kan tilsi at man trenger større grunnbemanning? Selv dersom virksomheten finner ut at det ikke er nødvendig med økt bemanning, anbefales det sterkt at man med jevne mellomrom øver operatørene i å håndtere feilsituasjoner.»

10.4.4 Eksisterende kompetansekrav i damsikkerhetsforskriften

Når det gjelder andre områder som NVE regulerer kan det være av interesse å sammenligne med damsikkerhetsforskriften som i § 3-1 har detaljerte kvalifikasjonskrav: Det stilles kvalifikasjonskrav til:

a) leder, vassdragsteknisk ansvarlig (VTA), stedfortredende VTA og tilsynspersonell, jf. § 3-2, § 3-3 og § 3-4
b) fagansvarlig, jf. § 3-5
c) utførende foretak og anleggsleder, jf. § 3-8
d) kontrollør, jf. § 3-9.

NVE bestemmer hva som er spesifikk teoretisk opplæring i henhold til § 3-2 til § 3-4.

For kvalifikasjonskrav og godkjenning av personell fra annen EØS-stat skal direktiv 2005/36/EF om godkjenning av yrkeskvalifikasjoner følges. Damsikkerhetsforskriftens kapittel 3 regulerer videre konkret hvilken kompetanse og formell utdanning som kreves til de ulike rollene. NVE treffer vedtak for godkjenning av selskap og enkeltpersoner for alle disse funksjonene.[185]

10.4.5 Arbeidsgruppens vurdering om kompetansekrav

Arbeidsgruppen ser at det er et stort sprik i bransjen om selskapene besitter nødvendig IKT-sikkerhetskompetanse eller ikke. Arbeidsgruppen anser at det er vel så viktig å

[185] Også Eltilsynslovens § 12 og tilhørende forskrift om elektroforetak og kvalifikasjonskrav for arbeid har kvalifikasjonskrav til driftsleder og montør, https://lovdata.no/dokument/SF/forskrift/2013-06-19-739#KAPITTEL_3 besøkt 08-01.2017.

tydeliggjøre ledelsens og forretningssidens ansvar på dette området, og at dette ikke bare er et ansvar som kan løses av IT-avdelingen.

Det er flere selskaper, spesielt de største, som har svært god kompetanse innenfor IKT og informasjonssikkerhet. Samtidig er det er flere selskaper som ikke innehar tilstrekkelig kompetanse på informasjonssystemsikkerhet.

NVE har så langt prioritert tilsyn på IKT-sikkerhet hos virksomheter der konsekvensene ved svikt er store, og har følgelig ikke ført tilsyn med små selskap. NVE møter allikevel representanter for disse i andre fora. Disse selskapene har der gitt utrykk for at det er utfordrende å håndtere temaer rundt informasjonssystemsikkerhet på grunn av manglende kompetanse. Arbeidsgruppen mener det vil være hensiktsmessig at NVE også fører tilsyn med IKT-sikkerhet hos små virksomheter. Tilsyn kan bidra til å lukke sikkerhetshull og bidra til kompetanseheving hos tilsynsobjektet.

NVE har heller ikke ført tilsyn med kravene til kompetanse i dagens regulering. Arbeidsgruppen har vurdert alternative løsninger på kompetanseutfordringen i energisektoren, herunder å stille kompetansekrav til profesjoner i sektoren. Samtidig er arbeidsgruppen kjent med at det i Stortingsmeldingen om Samfunnssikkerhet[186] er skissert et tiltak for å legge til rette for en langsiktig oppbygging av IKT-sikkerhetskompetanse, gjennom å utarbeide en nasjonal kompetansestrategi for IKT-sikkerhet. Tiltaket innebærer også bevisstgjøringsaktiviteter rettet mot befolkningen og virksomheter.

På europeisk nivå har ENISA utredet sertifisering for operativt personell på driftskontrollsystemer, og artikkel 61 i driftskodene for System Operators setter krav til kompetanse for operatører. Denne reguleringen anses av arbeidsgruppen som tilstrekkelig for tydeliggjøring av kompetansekravet. Arbeidsgruppen vurderer at kompetanseløft for hele bransjen (både monopolister og markedsaktører) kan skje ved andre midler enn strengere forskriftskrav, for eksempel ved veiledning, og henviser til Stortingsmeldingen om *Samfunnssikkerhet*, der et tiltak spesielt går på å heve det nasjonale kompetansenivået på IKT-sikkerhet. Det vil på sikt komme energiforsyningen til nytte. Arbeidsgruppen mener at NVE bør tydeliggjøre i veilederen til beredskapsforskriften eksisterende krav til kompetanse.

Arbeidsgruppen vurderer at NVE i tillegg kan iverksette og samkjører kompetansehevende aktiviteter i energisektoren opp mot nasjonal strategi og nasjonale initiativer. Her mener arbeidsgruppen at NVE i samarbeid med relevante aktører i bransjen kan utvikle egne tiltak for sektoren. Med stor variasjon i kompetanse på IKT-sikkerhet i bransjen, vil det være fornuftig for NVE å være med på å gi bransjen, dvs. både monopolister og markedsaktører, et kompetanseløft. Et kompetanseløft vil komme til nytte i både egen drift og i forholdet til leverandører (innkjøperkompetanse). Det ligger allerede generelle krav til kompetanse i nettvirksomhetenes omsetningskonsesjon, og arbeidsgruppen mener at disse kravene bør tydeliggjøres gjennom veiledning.

---

[186] Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn, Samfunnssikkerhet,* https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/ besøkt 05.03.2017.

10.5 Vurdering av tjenesteutsetting, leverandørkjeder og fjernaksess

10.5.1 Innledning

For virksomheter med lite kunnskap om systemforvaltning og sikkerhet, kan det være et kostnadseffektivt tiltak å sette ut IT-drift til eksterne leverandører.

Skyteknologi tilbyr ulike driftsmodeller, og blir ofte framstilt som rimeligere enn å drifte egne systemer. Samtidig kan bruk av skytjenester på den ene siden gi en bedre teknologisk sikkerhet så lenge tjenesten kjøpes fra kompetente leverandører, men på den andre siden representere driftsmodellene en endring i risiko i forhold til blant annet kontroll med data lagret utenfor Norges grenser.

10.5.2 Problemstillinger knyttet til tjenesteutsetting

Når anskaffelsesprosessen skal igangsettes må virksomheten vurdere hvilke kompetanseområde som skal dekkes av virksomheten og hva som best kan dekkes av en leverandør. Deretter bør virksomheten utvikle en forvaltningsstrategi som blant annet definerer tjenestene en trenger å kjøpe fra leverandøren og hvordan risiko skal deles. Neste trinn er å velge ulike IT-driftsmodeller og tjenester.[187] Skytjenestenes ulike driftsmodeller fordeler ansvar mellom kunde og leverandør avhengig av valgt modell, se for øvrig kapittel 3.2 om administrative systemer der leveranse- og tjenestemodeller for skytjenester er forklart nærmere.

Videre er det viktig å selv ha en organisasjon som kan ivareta leverandørsamarbeidet. Til sist kommer kontraktene med leverandørene. For store komplekse systemer er gjerne flere leverandører involvert. Både Den norske dataforening[188] og IKT-Norge har maler for IT-kontrakter.[189] Dataforeningen har også utviklet en veileder for skytjenesteavtale.[190]

Selv der virksomheten skulle velge å drifte egne systemer, vil virksomheten være avhengig av støtte fra leverandører av programvare, maskinvare og kjøp av eksterne tjenester. Ved feilsituasjoner som virksomheten selv ikke klarer å løse, er det nødvendig at servicepersonell hos leverandøren av utstyret får tilgang for å gjennomføre reparasjoner og utviklingsarbeid. Servicepersonell fra leverandøren kan komme på anlegget og utføre service, eller servicepersonell kan utføre arbeid via fjerntilgang.

Uavhengig av drift og servicemodell, er IKT-sikkerhet og forvaltning av systemene viktig, særlig viktig er tilgangskontroll og overvåkning av systemet. Det krever igjen at

---

[187] Dataforeningen, Software 2012, *Konkurranseutsetting av systemforvaltning,* https://www.youtube.com/watch?v=vklIRJWtMgs, besøkt 21.02.2017.

[188] Dataforeningens IT-kontraktsstandarder, *IT-kontrakter, en hel familie av standarder*, https://www.dataforeningen.no/it-kontrakter.160152.no.html, besøkt 21.02.2017.

[189] IT-driftsytelser (outsourcing) – Standardavtale – Norsk – Årslisens, https://www.ikt-norge.no/butikk/it-driftsytelser-outsourcing-standardavtale-norsk-arslisens/ besøkt 21.02.2017.

[190] *Cloud 2100 Skytjenesteavtale, Veiledning for skytjenesteavtale,* Den norske dataforening, versjon 0.9, 13.12.2016.

virksomhetene har tilstrekkelig oversikt og forståelse av systemenes oppbygging og sammenkoplinger, samt hvem som har tilgang når, og til hvilke tjenester og data.

Selv om virksomheter kan ha fordel av å sette ut informasjonstjenester til eksterne leverandører, er det flere vurderinger som bør gjøres før en beslutter tjenesteutsetting. Det første er typen data som skal lagres og/eller behandles og eierskap til dataene. Deretter bør virksomheten vurdere om regelverket tillater at denne typen data sendes ut av virksomheten, og hvor i verden det er lov å lagre dataene. Videre vil tjenesteleverandørens sikring av innhold (lagrede data) ha betydning, og hvor dataene vil befinne seg i verden hvis tjenester settes ut til en ekstern leverandør.

Skytjenester gir mulighet til å flytte data til den fysiske lokasjonen (serveren) med best kapasitet på ethvert tidspunkt. Data kan derfor skyfles rundt på ulike geografiske lokasjoner og på ulike servere. I tillegg kan data sikkerhetskopieres til flere lokasjoner. Servicepersonell kan videre være ansatt andre steder enn der sky-leverandørens hovedkontor befinner seg slik. Dersom dette er en virksomhet med aktivitet i mange land kan data fort bli gjort tilgjengelig i land hvor jurisdiksjonen er ganske annerledes enn i Norge. Derfor er kryptering av innhold og kontroll på krypteringsnøklene viktige tema.

Et velbenyttet argument mot bruk av skytjenester er at norske myndigheter mister muligheten til å gjennomføre direkte revisjon eller tilsyn med sikringen av norske virksomheters data. Spørsmålet er da om innsyn i tredjeparts revisjonsrapporter er godt nok for myndigheten? KMD arbeider med regelverk på skytjenester, og dette er et område der andre sektorers praksis og teknologiutvikling kan få betydning for regelverket også i energiforsyningen.

Verdens IT-brukere er blitt mer mobile, og tjenester er utviklet der brukerne kan få tilgang via mobile enheter. Denne utviklingen treffer også energisektoren, og kan bidra til raskere og mer effektiv drift. Men, en annen side av dette er at koplingene mot internett blir flere, og det blir derfor viktig å også sikre slike mobile enheter og begrense rettigheter når de koples til mer sentraliserte tjenester.

10.5.3 Eksisterende regulering av tjenesteutsetting i energiforsyningen

I tillegg til beredskapsforskriften, kommer bestemmelser i forvaltningsloven, lov om offentlige anskaffelser, personopplysningsloven, sikkerhetsloven, bokføringsloven, arkivloven og avtalen om offentlige innkjøp (GPA)-avtalen.[191] De største juridiske utfordringene er knyttet til arkivloven, bokføringsloven og personopplysningsloven (NOU 2015: 13). KMD og NSM arbeider med å se på begrensningene i norsk lovverk og mulighetene for bruk av skytjenester.

Når det gjelder de administrative informasjonssystemene til et selskap, er det ikke i dag direkte krav i beredskapsforskriften knyttet til fjernaksessløsninger. Dersom en tredjepart

[191] Avtalen om offentlige innkjøp (GPA), som ble inngått i 1994 og trådte i kraft i 1996, er en plurilateral avtale og omfatter 41 av WTOs medlemmer, se Offentlige anskaffelser i WTO. GPA-avtalen, 28.11.2012, https://www.regjeringen.no/no/tema/naringsliv/handel/ud---innsiktsartikler/innsikt/wto---doha-runden/offentlige-anskaffelser-i-wto-gpa-avta-2/id708717/ besøkt 10.01.2017.

kan komme i kontakt med kraftsensitiv informasjon, så er det krav i § 6-5 til KBO-enheter som setter ut oppdrag til leverandører, å påse at disse er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for sensitiv informasjon. Det betyr at det er et minimumskrav om beskyttelse, avskjerming og tilgangskontroll dersom for eksempel de administrative informasjonssystemene inneholder kraftsensitiv informasjon.

Bfe §§ 7-10, 7-14 og 7-15 regulerer direkte fjernaksess til driftskontrollsystemer, både fra interne ansatte og leverandører.

Bfe § 7-10 sier:

«Virksomheten skal ha kontrollordninger for å godkjenne, vedlikeholde og avvikle ordninger for ekstern tilkobling til driftskontrollsystemet, samt funksjoner for innstiling av vern. En særskilt vurdering skal ligge til grunn for godkjenning av løsning.

Kun autorisert personell kan gis adgang til driftskontrollsystemet gjennom ekstern tilgang. Virksomheten skal ha kontrollordninger for vurdering, tildeling, endring og tilbaketrekking av autorisasjon. Virksomheten skal ha en oppdatert liste over alle som er autorisert.

Det skal foreligge en egen forhåndsavtalt prosedyre for ekstern tilkobling til driftskontrollsystemet.

Det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg.

For fjernvarmeanlegg der hele eller deler av driftskontrollfunksjonen utføres av selskap som ikke er KBO-enhet, må vedkommende KBO-enhet påse at hele driftskontrollsystemet beskyttes etter relevante bestemmelser i denne forskrift.»

Det tillates ikke at eksterne leverandører, som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg. Det betyr at kun eier av anlegg eller andre KBO-enheter kan drifte transmisjonsnettet gjennom fjerntilgang.

For klasse 2 og klasse 3 systemer er det krav til at ved tilkobling fra leverandører skal driftssentralen være bemannet. Virksomheten skal ha kontrollordning for korrekt autentisering av de personene som er autorisert til å benytte ekstern tilkobling for adgang til driftskontrollsystemet. Virksomheten må sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser. Virksomheten skal utarbeide interne regler for hva som er et sikkert sted. Dette skal skrives i avtalen med leverandøren.

Den eksterne tilkoblingen skal kun åpnes når det er behov for å få tilgang til driftskontrollsystemet. Tilkoblingen skal være lukket når den ikke er i bruk. Det skal foreligge en egen skriftlig prosedyre for ekstern tilkobling. Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.

For klasse 3 anlegg er det direkte forbud mot styring av anlegg gjennom ekstern tilkobling.

10.5.4 Arbeidsgruppens vurdering

Arbeidsgruppen har observert at det kan være behov for å tydeliggjøre regelverket slik at det ikke hindrer innovasjon og utvikling. Arbeidsgruppen mener at det ikke er eksplisitte forbud mot bruk av skytjenester eller bortsetting av IT-drift i regelverket, men at regelverket i dag setter strenge krav til beskyttelse av kraftsensitiv og taushetsbelagt informasjon og til redundans i kritiske systemer. For driftskontrollsystemer settes det krav til hvem som kan få koble i anleggene, og at det skal skje fra et sikkert sted, slik som det er definert av den enkelte virksomhet. Reglene er satt slik fordi service og oppdatering av programvare skal skje kontrollert. En IT-leverandør skal ikke kunne fjernstyre nettet gjennom sin tilgang.

Det finnes ikke en nasjonal sertifiserings- eller godkjenningsordning for tilbydere av skytjenester, hvor disse kan få rangert tjenestene sine etter sikkerhetsnivå (vil typisk inkludere forhold som hvor informasjon lagres, fysisk sikkerhet, teknisk sikkerhet, virksomhetens sikkerhetsrutiner/internkontrollsystem og lignende). Å få til dette avhenger ikke bare av NVE, men avhenger av koordinering med andre myndigheter slik at regelverk kan forenkles og harmoniseres.

Sintef laget en rapport «Cloud security requirements»[192] som beskriver viktige sikkerhetstiltak i forbindelse med skytjenester. Denne rapporten nevner en rekke forhold: Sikkerhetskopiering, kryptering, geografisk lokalisering av servere, hvem eier dataene, revisjoner, logging, rutiner ved sikkerhetsbrudd, beredskap og at leverandørbytte senere er mulig mv. Sintef peker videre på at skytjenesteleverandør ikke bør benytte seg av flere underleverandører.

Arbeidsgruppen mener at fordelen ved bruk av skytjenester må vurderes opp mot risikokostnaden. Noe av risikokostnadene må kunne dekkes og, for selskapet, reduseres gjennom en god Service-Level Agreement (SLA) med leverandøren. Her vil gode veiledere fra myndighetene og fra interesseorganisasjoner kunne være til hjelp.[193] Tjenesteutsetting av IT-drift og fjerntilgang bør reguleres i krav med tilhørende mer detaljerte anbefalinger, og eventuelt også henvise til andres veiledninger i NVE-veileder. Spesifikt for skytjenester vurderer arbeidsgruppen at følgende bør reguleres gjennom regelverket:

1. *Virksomheten må gjøre verdivurdering av informasjonen.* Jo høyere verdi på informasjon, desto strengere krav til redundans. Informasjon kan være kritisk for drift og beredskap, herunder for gjenoppretting fra «svart nett».[194] I slike tilfeller kan det være viktig å ha lokal kopi, og redundans. Informasjon kan også være spesielt viktig utfra en hensyn til rikets sikkerhet. Slik informasjon må lagres kun nasjonalt. Eksempel på informasjon kan være planer for energibruk ved mottak av Natoforsterkninger eller beredskapsplaner for terror og sabotasje. Merk at leverandørens grad av ansvar er forskjellig i ulike skytjenestemodeller. Noen

---

[192] Bernsmed, K., Meland, P.H. og M. G. Jaatun, *Cloud Security Requirements, A checklist with security and privacy requirements for public cloud services*, SINTEF 2015, https://www.sintef.no/en/publications/publication/?pubid=SINTEF+A27131, besøkt 11.01.2017.

[193] Se for eksempel Uninett sin veileder på skytjenester, https://www.uninett.no/skytjenester/juridisk-veileder-skytjenester, besøkt 11.01.2017. Se også Den norske dataforening og IKT-Norges veiledere.

[194] Svart nett er dødt nett, dvs. ikke funksjonerende nett.

leverandører tilbyr for eksempel redundans der de har ansvar. Dette skjer ved duplisering og kopiering til andre datasentre. Det kan også være er mulig å velge hvilken region data skal lagres og i etterkant å flytte data mellom regioner.

2. *Virksomheten må kontraktfeste minimum følgende:*
    - Eierskap til data gjennom et tydelig avtaleverk. Sertifisering som ISO 27018 stiller krav til skyleverandøren og har krav til dette forholdet
    - Krav til at skyleverandøren har sertifisering, som for eksempel ISO 27018. Virksomheten bør se til standarder som ISO 27001, SOC1, SSA, PCI, HIPH – helse m.fl. I den grad norske myndigheter kommer opp med en «liste» over gode skyleverandører, som en har gjort i UK og USA, bør virksomheten sjekke denne lista. Det finnes også digitale tjenester for salg som kan kartlegge den samlede risikoen hos ulike skyleverandører og presentere bildet grafisk
    - Krav til økonomi og konkursbeskyttelse. Service Organization Control report (SOC)1 og SOC2 er revisjonsstandarder. Kundene må ha rett til å flytte sine data hjem dersom leverandøren skulle gå konkurs.
    - En exit-strategi for hvordan data kan tas tilbake i eget eller annet datasenter dersom det skulle være ønsket, for eksempel dersom leverandøren blir kjøpt opp og tjenestetilbudet endres. Kontrakten må avklare økonomi og praktiske forhold
    - Kontrakten bør sikre virksomheten tilgang til tredjeparts revisjonsrapport for tilsyn med leverandøren
    - Kontrakten bør også ha krav om at virksomheten skal varsles dersom uønskede hendelser har oppstått og kundens data er kompromittert

Arbeidsgruppen har forhørt seg med det amerikanske Federal Energy Regulatory Commission Office of Energy Infrastructure Security, som sier at sanntids programvare slik som prosesstyring og automasjon som krever umiddelbar respons bør unngå IT-løsninger som kan medføre unødige signalforsinkelser. Også systemer som krever spesialisert maskinvare er uhensiktsmessig å legge i skyen. De peker videre på typisk kraftsensitiv informasjon som et område som bør vurderes spesielt. Overføring av kraftsensitive data krever kryptering, validering og verifisering av mottakere.

På dette grunnlaget vurderer arbeidsgruppen at kontroll- og styringssystemer i energiforsyningen ikke bør tillates lagt i «skyen». SCADA skal dermed ikke legges i skyen. Dette betyr videre at DMS, så lenge det bare er et overvåkningssystem uten styringsfunksjonalitet, vil kunne legges i en skyløsning forutsatt at data sikres. Det betyr at en DMS-løsning som representerer kun et oversiktsbilde uten styringsfunksjonalitet, kan benytte skytjenester, men virksomheten må vurdere verdien av denne informasjonen i forhold til beskyttelse og lokal backup.

10.6 Vurdering av overvåkning, rapportering og hendelseshåndtering

10.6.1 Innledning

Ethvert IT-system som er koplet til internett er utsatt for trusler. Statistikk fra US CERT og US ICS CERT på driftskontrollsystemer viser at det stadig oppdages nye sårbarheter i systemer som brukes energisektoren. Dette har sammenheng med karakteristikker og svakheter i markedet. Produktene kommer på markedet med innebygde svakheter som må rettes etter at kundene har kjøpt og installert systemene, og kundene bærer kostnadene i form av tid, plunder og heft.

10.6.2 Problemstillinger

Driftskontrollsystemer i energisektoren var tidligere fysisk ikke tilkoplet internett. I dag er det logiske skiller som sikrer driftskontrollsystemene. Systemene er med andre ord koplet til internett, fysisk. Disse logiske skillene utgjøres av brannmurer som blant annet filtrerer trafikk og åpner og stenger porter, hvitelister trafikk mv. I tillegg kommer autorisasjon av personell, regimer for tilgangsadministrasjon mv. Selv med gode forebyggende sikkerhetsmekanismer kan skadevare bli transportert inn i systemene. Erfaring viser at angripere gjerne går via ansatte gjennom sosial manipulasjon. Når de tekniske tiltakene blir gode, er mennesket det svakeste leddet. Det er derfor viktig å ha evne til å se og oppdage hva som skjer i IT-systemene. Denne evnen er blitt gradvis viktigere både av hensyn til forebyggende sikkerhet, av hensyn til effektiv håndtering av uønskede hendelser for å minimere skade og tap, og i etterkant for etterforskning og eventuell anmeldelse. Den er blitt gradvis viktigere som følge av at 100% beskyttelse ikke er mulig. Det vil finnes en restrisiko.

Slik kravene er formulert i dag gjelder kravene til logging og hendelseshåndtering for driftskontrollsystemer hos KBO-enheter. Så lenge krav til logging kun gjelder driftskontrollsystem i klasse 2 og 3, så har en ikke et heldekkende sikkerhetsregime i hele virksomheten, som også tar inn i seg risikoen for at uønskede hendelser kan oppstå utenfor driftskontrollsystemet og forplante seg inn i systemet. Denne risikoen er relevant, jf. Mørketallsundersøkelsen 2016, som viser at 27% av norske virksomheter har vært utsatt for en uønsket IKT-hendelse i 2015. Opportunistiske angripere tar svakeste leddet først, for så å ta seg videre inn i mer beskyttede systemer.

10.6.3 Eksisterende regulering

Beredskapsforskriften stiller krav til håndtering av feil, sårbarheter og sikkerhetsbrudd i driftskontrollsystem (§ 7-7), videre overvåkning og logging i klasse 2 og 3 driftskontrollsystem. Logging og logganalyse er viktig for å ha informasjon til å ivareta kravet som NVE stiller til hendelsesrapportering, jf § 2-6 h. I 2015 ble IKT-sikkerhet fulgt opp gjennom tre revisjoner av driftskontrollsystem. NVE fulgte opp enkelthendelser gjennom skriftlig tilsyn og IKT-sikkerhet ble et tema i de fleste revisjonene som ble

gjennomført i selskapene.[195] Statistikken for resultat av skriftlig tilsyn med driftskontrollsystemer (2015)[196] viser blant annet at de fleste avvikene kom på beredskapsforskriftens § 7-7 og § 7-14c, som omhandler logging, logganalyse og hendelseshåndtering. Disse avvikene skal være lukket for klasse 2 og 3 nå.

Kapittel 2 i beredskapsforskriften stiller generelle krav til varsling og rapportering hos KBO-enheter. Følgende punkter i § 2-6 har relevans for IKT-sikkerhetshendelser:

§ 2-6.Varsling og rapportering

Alle KBO-enheter skal uten ugrunnet opphold varsle beredskapsmyndigheten om ekstraordinære situasjoner. Varslet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson.

Alle KBO-enheter skal uten ugrunnet opphold og senest innen tre uker skriftlig innrapportere følgende uønskede hendelser til beredskapsmyndigheten:

a. *Forsøk på inntrengning og/eller manipulasjon av hele eller deler av driftskontrollsystemet og avanserte måle- og styringssystem (AMS).*

d. Situasjoner hvor sensitiv informasjon om kraftforsyningen er blitt kjent for andre enn rettmessige brukere, eller mistanke om dette.

h. Omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer.

Kapittel 7 i beredskapsforskriften stiller krav til driftskontrollsystemer.

§ 7-7.Håndtering av feil, sårbarheter og sikkerhetsbrudd
Virksomheten skal etablere kontrollordninger for å sikre effektiv håndtering av feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemets funksjon.

Virksomheten skal ha tilgang til tilstrekkelig personell med nødvendig kompetanse som uten unødig opphold kan håndtere forhold angitt i første ledd.

Alle sikkerhetsbrudd og hendelser skal registreres.

Forhold som kan utgjøre en umiddelbar risiko for driftskontrollsystemets funksjon, skal varsles og rapporteres til beredskapsmyndigheten, jf. også § 2-6.

Kapittel 7 i beredskapsforskriften stiller i tillegg følgende krav til klasse 2 og klasse 3 driftskontrollanlegg:

§ 7-14 Overvåking og logging

c) Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.

---

[195] *Årsrapport for tilsyn NVE rapport 2015,* Oslo april 2015.

[196] Abel, C. G., *Statistikk for resultat skriftlig tilsyn. Driftskontroll 2015*, NVE, 11.11. 2015, journalnummer 201505525.

10.6.4 Arbeidsgruppens vurdering

Et godt sikkerhetsregime bygger på følgende prinsipper:

- Forsvar i dybden (barrierer og sikringstiltak hele vegen inn til kjernen av systemet)
- Forsvar i bredden (beskytte alle endepunkter)
- Minimering av rettigheter og tilganger (redusere brukernes frihet slik at nødvendige oppgaver kan utføres men heller ikke mer)
- Splittet ansvar når kritiske operasjoner skal gjennomføres (to brukere med ulike oppgaver må begge utføre sine oppgaver før det skjer en handling).

Logging, logganalyse, rapportering og hendelseshåndtering kommer inn under forsvar-i-dybden kategorien. I Mørketallsundersøkelsen 2014 og tidligere undersøkelser framgår det at få virksomheter logger, og de leser heller ikke loggene sine. Mørketallsundersøkelsen 2014 konkluderer dermed med at få virksomheter ser at de er utsatt for hendelser. I 2014 undersøkelsen ble dette forholdet fulgt opp, og innsamlede data i undersøkelsen ble sammenlignet med data innhentet fra profesjonelle overvåkningssystemer, i denne sammenheng fra NSM NorCERT og mnemonic. I 2014 viste undersøkelsen at 5% av store virksomheter rapporterte at de var hacket. Data fra overvåkningssystemene til NSM NorCERT og mnemonic viste til sammenligning at mer enn halvparten av virksomhetene var hacket. Det NSM NorCERT og mnemonics kunder hadde, var tilgang til tjenester og sensorer som logget aktiviteten, trafikken ble analysert av kompetente personer, og slik sett kunne en trekke konklusjoner. Resultatet viste dermed «mørketall på mørketallene». (De opprinnelige mørketallene var avvik mellom hendelser som skjer og de som blir anmeldt til politiet.)

Bfe stiller krav til logging hos klasse 2 og 3 anlegg hos KBO-enheter. Som Næringslivets sikkerhetsråd har anbefalt, så bør alle virksomheter skru på loggene sine og undersøke hva som skjer i systemene sine.[197]

Det er nødvendig med kompetanse for å sette opp logger og analysere varsler og hendelser. Et problem med «varsler» er falske alarmer (falske positive). Automatiserte systemer for overvåkning bør innstilles slik at andelen falske alarmer blir lavest mulig, men samtidig fanger opp reelle hendelser i størst mulig grad. Falske alarmer reduserer årvåkenheten i organisasjonen.

I tillegg til den sikkerhetsmessige behovsvurderingen kommer føringer fra EU og nasjonalt regelverk, for eksempel NIS-direktivet. Her er NVEs oppfatning at bransjen er godt dekket på logging og hendelseshåndtering.

I forslaget til ny sikkerhetslov§ 4-6 pålegges virksomheten en varslingsplikt til tilsynsmyndigheten. I sektorer der tilsynsmyndigheten er sektormyndigheten, skal det varsles både til sikkerhetsmyndigheten og til tilsynsmyndigheten. I praksis i dag vil dette for enkelte selskaper i energiforsyningen kunne bety parallell varsling til NSM og NVE, alternativt at selskapene varsler NVE og NVE varsler videre til NSM.

---

[197] Se Mørketallsundersøkelsen 2012 og 2014, Næringslivets sikkerhetsråd.

Lovforslaget har også krav i § 6-4 til overvåkning av skjermingsverdige informasjonssystemer. Det er en risiko for at skjermingsverdige informasjonssystemer fort kan gjenfinnes i energisektoren, hvilket betyr at disse systemene vil kunne bli underlagt sikkerhetsregimet som loven gir. I så fall blir enkelte av virksomhetene i energisektoren uansett underlagt et regime med krav til overvåkning av systemene sine.

Å stille tydeligere krav til administrative systemer gir en helhetlig styrking av sikkerheten. Det å drifte systemene med for høy risiko har også en kostnad når hendelsen inntreffer. Evne til å detektere og håndtere hendelser er spesielt viktig for å finne skadevare som er kommet seg inn i systemer.

Arbeidsgruppen har vurdert at logging og logganalyse er viktig for å oppdage og forebygge feil i IT-systemene og i driftskontrollsystemene. Logging bør settes opp og gjennomføres slik at driftskontrollsystemenes og kraftverkenes autonomi og funksjonalitet ikke blir berørt. Arbeidsgruppen vurderer at uten logging og logganalyse, er det vanskelig å undersøke hendelser. Det er viktig å undersøke hendelser for feilretting, læring og etterforskning. Logging vil også være grunnlag for å kontrollere om krav etterleves. Logging og logganalyse er viktig fordi en uansett aldri kan garantere 100% sikkerhet, og loggene gir informasjon om aktiviteten i systemene. Arbeidsgruppen vurderer at et slikt krav gir en risikoreduksjon i form av læring fra hendelser slik at tilsvarende uønskede hendelser kan forhindres senere, samt mer presis rapportering til myndighetene.

Basert på vurderingen ovenfor vurderer arbeidsgruppen at det bør stilles krav til logging, logganalyse og hendelseshåndtering for alle virksomheter i energisektoren og deres IKT-systemer og nettverk. Hva som skal logges og omfanget av loggingsaktiviteten må vurderes av den enkelte virksomhet, men NVE bør kunne gi råd i en veileder. NSM har utarbeidet en veileder for systemovervåkning. [198] NVE har også i et sommerstudentprosjekt og i et konsulentoppdrag sett nærmere på logging og logganalyse i energiforsyningens driftskontrollsystemer.[199] [200] Disse dokumentene gir et grunnlag for å utarbeide råd til bransjen på logging og logganalyse, samt hendelseshåndtering.

---

[198] Nasjonal sikkerhetsmyndighet, *Systemovervåkning ved bruk av ELK-stakken*, IT-veiledning for ugradert nr 11 (U-11), oppdatert 2016-04-04.https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-11_systemovervaking_ved_bruk_av_elk-stakken.pdf, besøkt 13.02.2017.

[199] Kristoffer Hovland, *Logging og logganalyse i energiforsyningen, studentrapport,* NVE rapport nr 1., 2017, http://publikasjoner.nve.no/rapport/2017/rapport2017_01.pdf besøkt 11.01.2017.

[200] *Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem*. Rapport utarbeidet for Norges vassdrags- og energidirektorat, BDO, 31.10.2016.

11 Anbefalinger til endringer i regelverket

11.1 Innledning

På bakgrunn av de vurderingene arbeidsgruppen har gjort har arbeidsgruppen kommet med anbefalinger som tar vurderingene inn i en overordnet struktur som tydeliggjør forventingene til å sikre informasjonssystemer samtidig som det passer inn i eksisterende regulering.

- Arbeidsgruppens anser et overordnet sikkerhetsregime som en anbefaling i seg selv da forsyningssikkerhet er et stort og komplisert tema å forvalte. Det underliggende temaet om sikkerhet og beredskap skal sørge for en helhetlig forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner i energiforsyningen. Krav til sikring av informasjonssystemer må derfor kunne passe inn i et sett av krav som omfatter blant annet helhetlig sikkerhetsstyring, sikring av informasjon og fysisk sikring av anlegg.

- Arbeidsgruppen anbefaler en tydeliggjøring av den generelle sikringsplikten i dagens krav om at alle system som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger. Arbeidsgruppen anbefaler at dette gjøres ved å etablere tilsvarende generelle krav for informasjonssystemer som sørger for et minstenivå på informasjonssystemsikkerhet.

- Arbeidsgruppen anbefaler at systemer hvor avbrudd har større konsekvens har noe strengere sikringskrav enn den anbefalte generelle grunnsikringen. Arbeidsgruppen mener dette gjelder systemer som er direkte knyttet til overvåking av energiforsyningen slik som AMS. Arbeidsgruppen anbefaler derfor en tydeliggjøring av den generelle sikringsplikten i dagens krav til alle system som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner. Arbeidsgruppen anbefaler at risiko og sårbarhetsvurderinger skal ligge til grunn for sikringsnivået for disse systemene.

- Arbeidsgruppen anbefaler at systemer som overvåker og styrer energiforsyningen, for eksempel dagens driftskontrollsystemer, beholder dagens sikkerhetsnivå for driftskontrollsystemer. Arbeidsgruppen anbefaler at sikkerhetsnivået for disse systemene følger systemenes klasser, som i dag. Arbeidsgruppen vurderer at det kan være behov for mindre endringer i ordlyden i kravene, og anbefaler en gjennomgang av teksten.

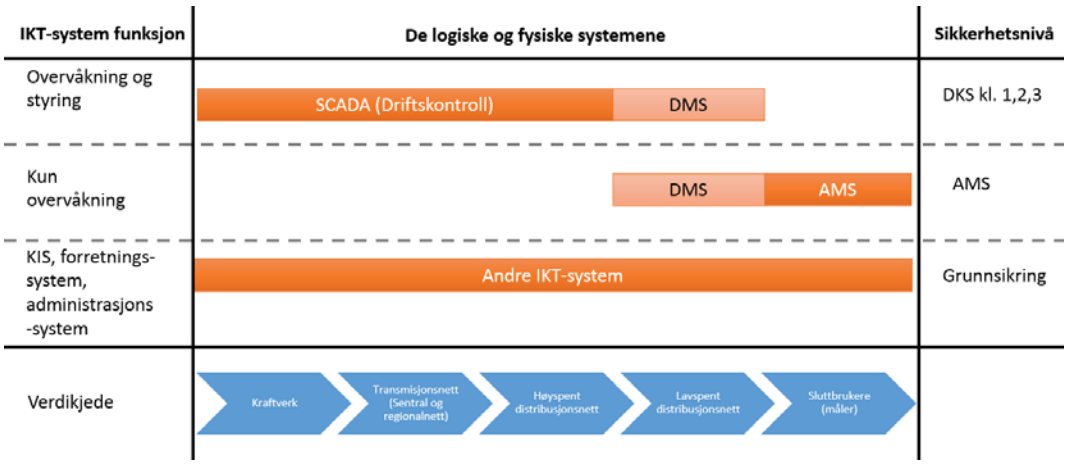
11.2 Anbefaling om overordnet sikkerhetsregime

11.2.1 Innledning

Dagens krav til forebyggende sikkerhet og beredskap i energiforsyningen skal sørge for en helhetlig forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner i energiforsyningen. Krav til sikring av informasjonssystemer bør derfor kunne passe inn i et sett av krav som omfatter blant annet helhetlig sikkerhetsstyring, sikring av informasjon og fysisk sikring av anlegg. Arbeidsgruppen anbefaler derfor at en endring av kravene til forebyggende sikkerhet og beredskap for informasjonssystemer i energiforsyningen følger en overordnet struktur som tydeliggjør behovet for å sikre informasjonssystem, samtidig som det passer inn i eksisterende regulering.

11.2.2 Arbeidsgruppens anbefaling

Figur 11.1 gir et forenklet bilde av hvilke systemer som benyttes i energiforsyningen, og hvordan arbeidsgruppen ser for seg et fremtidig sikkerhetsregime.



Figur 11.1 Forslag til reguleringsregime for IKT-systemer i energisektoren.

Dagens sikkerhetsnivå relaterer seg til dagens beredskapsforskrift der energiloven stiller generelle krav til sikring, og klassifiseringssystemet, som gjelder for driftskontrollsystemer hos virksomheter som eier eller driver anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner. Figuren viser blant annet at sikringsnivået til overvåknings- og styringssystemer på distribusjonsnettnivå (DMS) bestemmes av hvor vidt dette systemet har styringsfunksjonalitet eller er et rent overvåkningssystem som ikke er knyttet sammen med SCADA.

Arbeidsgruppen anbefaler at det stilles krav til grunnsikring for alle digitale informasjonssystemer hos aktører som har anlegg eller system av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme i energiforsyningen. Støttesystemene til virksomheten i energiforsyningen får økt betydning for driften. En større grad av automasjon og økt integrasjon mellom digitale systemer fører til tettere koplinger mellom flere systemer. Det betyr at dersom det oppstår én feil, som gir svikt i ett system, kan det føre til at flere tilknyttede systemer feiler. Arbeidsgruppen anbefaler derfor at det stilles krav til grunnsikring for alle digitale

informasjonssystemer i energiforsyningen. Dette innebærer at virksomhetene først må etablere et tilstrekkelig sikkert system. Så må virksomheten kunne drifte og forvalte systemet, inkl. ha oversikt over systemet og tilknyttede systemer og enheter. I tillegg må virksomheten kunne oppdage og håndtere hendelser. Arbeidsgruppen anslår at kravet bør gjelde alle nettselskaper, og i tillegg omsettere, produsenter og andre aktører som til sammen kontrollerer produksjon på over 25 MW. Arbeidsgruppen anbefaler videre at grunnsikringen bør skaleres i forhold til forsvarlig sikkerhet. Forsvarlig sikkerhet er en rettslig standard der sikkerhetsnivået i første rekke bygger på virksomhetenes risiko- og sårbarhets (ros)-analyser utført i tråd med kravene til slike analyser. Virksomheten kan ikke bruke ros-analyser til å senke eget eller anbefalt sikkerhetsnivå. NVE kan blant annet treffe vedtak om sikring eller vedtak om retting der virksomheten ikke opprettholder et forsvarlig sikkerhetsnivå. Arbeidsgruppen viser til NSM, til Nkom og til NIS-direktivet, og anbefaler grunnsikring fordi noen sentrale tiltak kan gi stor effekt i form av risikoreduksjon. Arbeidsgruppen anbefaler at NVE presiserer i veilederen hva som er god sikkerhet og henviser til internasjonale standarder og gode veiledere der det er hensiktsmessig.

Arbeidsgruppen anbefaler at det som en del av grunnsikringen stilles krav til sikring av informasjon i tjenesteutsetting. Arbeidsgruppen anbefaler at dekningsområdet for kravet er tilsvarende som for grunnsikring. Tjenesteutsetting dekker ulike IT-driftsmodeller, inklusive skytjenester. Kompleksiteten i maskede og sammenkoplede IT-systemer gjør at det er vanskelig å ha full kontroll og tilstrekkelige teknisk kompetanse selv. Tjenesteutsetting og bruk av skytjenester vil kunne bøte på dette forholdet, men introduserer samtidig nye utfordringer som må reguleres. Arbeidsgruppen vurderer derfor at det kan settes et generelt krav til sikring og at sikkerheten reguleres gjennom driftsavtalen med leverandør. NVE bør i veilederen vise til gode eksempler eller veiledere på IT-kontrakter. Arbeidsgruppen vurderer dette som svært viktig gitt utviklingen at stadig flere virksomheter setter ut deler eller hele IT-driften sin. Tiltaket har kostnader knyttet til reforhandling av kontrakter for virksomheter der kontraktene bør forbedres. Det er kun oppgaver som kan settes ut til en leverandør, ikke ansvaret.

Arbeidsgruppen anbefaler at det som en del av grunnsikringen stilles krav til logging og logganalyse i alle informasjonssystemene i energiforsyningen. Arbeidsgruppen mener at logging og logganalyse er viktig for å oppdage hva som pågår i IT-systemene, og i driftskontrollsystemene. Arbeidsgruppen vurderer at uten logging og logganalyse, er det vanskelig å undersøke hendelser. Det er også umulig å sikre bevis ved eventuell anmeldelse. Logging og logganalyse er viktig fordi en uansett aldri kan garantere 100% sikkerhet. Arbeidsgruppen vurderer at et slikt krav gir en risikoreduksjon i form av læring fra hendelser slik at tilsvarende uønskede hendelser kan forhindres senere, samt mer presis rapportering til myndighetene. Arbeidsgruppen anbefaler at dette kravet får samme dekningsområde som kravet til grunnsikring. Tiltaket medfører ekstra kostnader i form av analyseverktøy og behov for kompetanse for selskap som ikke allerede har dette. NVE har fått oppgitt estimat på kostnader til systemovervåkning tilsvarende 50 000 NOK/år for små virksomheter, 100 000 NOK/år for mellomstore virksomheter og enda høyere kostnader for store virksomheter.

Arbeidsgruppen anbefaler at NVE i forskrift stiller krav til at bryterfunksjonen i digitale strømmålere sikres særskilt med tiltak som begrenser uautorisert tilgang og manipuleringsmuligheter. Digitale strømmålere koples til overvåknings- og

styringssystemer for distribusjonsnettet i dag. Så fremt systemene da benyttes til styring, og til å kople inn og ut forbruk via bryterfunksjonen, bør det da vurderes å underlegge systemet samme regulering som driftskontrollsystemer. Det bør videre tas hensyn til kritikaliteten av systemene på samme måte som det er gjort for driftskontrollsystemer i dag.

NVE har et funksjonskrav til sikring av måleverdikjeden og mot uønsket tilgang til styrefunksjoner i måle- og avregningsforskriften. Ny veileder for dette forskriftskravet kommer i 2017. Anbefalingen gjelder for nettselskaper. Kravet medfører ikke vesentlige endringer i kostnadsbildet i forhold til i dag, med mindre AMS underlegges samme regulering som driftskontrollsystemer.

Arbeidsgruppen anbefaler at driftskontrollsystemer har strengere sikringskrav enn grunnsikring, og at det tas hensyn til driftskontrollsystemenes særegenhet med krav til særlig integritet og tilgjengelighet. Driftskontrollsystemene til virksomhetene styrer viktige komponenter i energisystemet som har direkte betydning for forsyningssikkerheten. Arbeidsgruppen vurderer at konsekvensen for forsyningssikkerheten av at driftskontrollsystemer svikter er mer alvorlige enn dersom administrative støttesystemer svikter. Tilfeldig feil, manipulasjon, svikt eller skadevare i driftskontrollsystemet kan få fysiske konsekvenser for materiell og personell. Arbeidsgruppen vurderer at dagens beredskapsforskrift gir det dekningsområde og sikringsnivå som er nødvendig. Anbefalingen medfører ikke ekstra kostnader i forhold til i dag for dem som allerede faller inn under regelverket.

11.3 Anbefaling om sikringsplikt for informasjonssystemer

11.3.1 Innledning

Som tidligere påpekt i denne rapporten kan den samme leverandøren levere programvare, IT-produkter og IT-tjenester til virksomheter i ulike sektorer. Virksomheter i ulike sektorer kan derfor være eksponert for samme digitale sårbarheter. De digitale verdikjedene spenner over landegrensene. I tråd med digitaliseringen blir det vanskelig for kjøpere av digitale tjenester å oppdage sårbarheter dypt i verdikjeden. Samtidig er det vanskelig for leverandører dypt i verdikjeden å forutse de samfunnsmessige konsekvensene av en programvare- eller maskinvarefeil i deres produkt eller tjeneste.[201] Disse forholdene gjør det vanskelig å lage presise risikoanalyser. Likevel, risikoanalyser og risikobasert tilnærming til sikkerhet er toneangivende når det gjelder IKT-sikkerhet, i internasjonale standarder og i nasjonalt lovverk. Arbeidsgruppen har valgt å forholde seg til det.

[201] NOU Digital sårbarhet – sikkert samfunn 2015:13, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf nedlastet 05.03.2017.

Mørketallsundersøkelsen er den eneste nasjonale kartleggingen av IT-sikkerhetstilstanden hos norske virksomheter. Undersøkelsen har over flere år vist at små norske virksomheter har generelt svakere sikkerhet enn de store. Analyse av datagrunnlaget i Mørketallsundersøkelsen har ikke gitt signifikante utslag på forskjell mellom bransjer når det gjelder sikkerhetspraksis,[202] og siden det ikke finnes tilsvarende undersøkelse for virksomheter i energisektoren, legger vi til grunn at funnene fra mørketallsundersøkelsen kan gjøres gjeldende også i energisektoren. I korthet betyr det at små virksomheter er dårligere på sikkerhet enn store.

11.3.2 Problemstilling

Dagens IKT-regelverk for energisektoren fanger ikke tydelig opp alle virksomheter i energisektoren. Regelverket har mange funksjonskrav, dekker internasjonale sikkerhetsstandarder på mange områder, men ikke alle, og legger slik arbeidsgruppen ser det, for lite vekt på generell grunnleggende IKT-sikkerhet.

En større grad av automasjon og økt integrasjon mellom digitale systemer fører til tettere koplinger. Det betyr at dersom det oppstår én feil, som gir svikt i ett system, kan det føre til at flere tilknyttede systemer feiler.

Store mengder informasjon er lagret i administrative systemer, databaser og andre tilknyttede IT-systemer. Dette er informasjon som er viktig for driften av virksomhetene. I «hendene på en sabotør» kan denne informasjonen være nyttig for å kunne komme seg videre inn i driftskontrollsystemet. Administrative støttesystemer er fysisk koplet sammen med industrikontrollsystemer, men separert logisk. Ulik praksis og kompetanse hos virksomhetene og deres leverandører gjør at virksomhetene i ulik grad er eksponert for truslene fra internett, som for eksempel nektelsesangrep (DDoS) og skadevare gjennom eksempelvis phishing-angrep. Samtidig vil enkle sikringstiltak kunne stoppe flere av disse truslene. Spørsmålet, som arbeidsgruppen har vurdert, er hvilken grunnsikring alle virksomheter i energisektoren bør ha?

11.3.3 Eksisterende regulering

Energiloven § 9-3, 2. ledd har et generelt krav til informasjonssikkerhet: *Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen*. Energiloven § 9-3 *(Informasjonssikkerhet)* gjelder KBO-enheter: «*Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming og beskyttelse av sensitiv informasjon*.»

Dagens beredskapsforskrift, kapittel 6 har hovedfokus på beskyttelse av sensitiv informasjon og gjelder for KBO-enheter. Bestemmelsen i bfe § 6-1 om taushetsbelagt informasjon gjelder alle og enhver. Kravet til beskyttelse av informasjon og hva som utgjør sensitiv informasjon i beredskapsforskriften er angitt i bfe kapittel 6. Det er en presisering som knytter seg til konfidensialitetsaspektet av informasjon.

---

[202] Fra analysen av Mørketallsundersøkelsen 2014.

Beredskapsforskriften setter i dag ikke krav til geografisk lokalisering av kraftsensitiv informasjon, men til at denne informasjonen skal beskyttes uansett lokalisering. Dagens regelverk legger et stort ansvar på virksomhetene ved at de selv må vurdere risiko og sikre informasjonen mot uautorisert tilgang. Selv om kraftsensitiv informasjon kan deles ved behov, så er det ikke tydelig hvordan dette skal gjøres når det er behov for automatisert deling. Dette fører til utfordringer når det gjelder innføring av nye systemer som DMS. Kraftsensitiv informasjon er beskrevet i detalj i bfe § 6-2.

I energiloven § 9-2 ligger den generelle plikten til å sørge for effektiv sikring for virksomheter som eier eller driver anlegg som er eller kan bli av vesentlig betydning for energiforsyningen. Dette er fulgt opp i beredskapsforskriften, der kapittel 5 gjelder for disse virksomhetene jfr. bfe § 1-3 andre ledd. I bfe § 5-1 sies det at alle som eier eller driver plikter å sikre anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, herunder adgang for uvedkommende. Med anlegg menes her også bygg og andre ressurser som personell og reservedeler.

Dette betyr at virksomheter som eier eller driver anlegg som er av vesentlig betydning for energiforsyningen plikter å sikre IKT-system som er nødvendige for driften. Dagens regulering er likevel ikke tydelig på hvordan dette skal sikres, da anlegg først må bli klassifisert og virksomheten bli KBO-enhet for at resten av forskriftene skal gjelde. Det generelle sikringsnivået for IKT-sikkerhet i energiforsyningen kan derfor gjøres mer presist.

Kravene til sikring av AMS ligger i maf § 4-2 g) «*AMS skal gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner*». Damsikkerhetsforskriften § 7-8 har krav til beskyttelse av sensitiv informasjon.

Virksomheter som eier eller driver klassifiserte anlegg og som har konsesjon etter energiloven er KBO-enheter. For disse gjelder hele beredskapsforskriften. Kapittel 2 stiller krav om sikkerhetsorganisering, herunder IKT-sikkerhetskoordinator. De generelle kravene inneholder også krav til beredskapsplikt, risiko- og sårbarhetsanalyser, varsling og rapportering og internkontrollsystem.

11.3.4 Arbeidsgruppens anbefaling

11.3.4.1 Behov for generelle krav til IKT-sikkerhet i energibransjen

Det er behov for generelle krav til IKT-sikkerhet i energibransjen. Det er over tid dokumentert at markedsmekanismene alene ikke er tilstrekkelig for å redusere risikoen. Avhengigheten av IKT-systemer er stor. Svikt i systemene kan oppstå som følge av naturhendelser, teknisk eller menneskelig svikt, eller som følge av trusler gjennom internett.

Alle virksomheter bør ha et minimumsnivå av sikkerhet for å beskytte tilgjengelighet til informasjon, integritet i informasjonen og konfidensialitet for sensitiv informasjon. Minimumskravet bør bygge på gode prinsipper for sikkerhet, slik som forsvar i dybden, minimere brukerrettigheter mv. I arbeidsgruppens vurdering for grunnsikring har arbeidsgruppen blant annet vurdert truslene, NIS-direktivets krav til grunnsikring og varsling, og sett hen til IKT-forskriften, som forvaltes av Finanstilsynet.

De mest vanlige dataangrep skjer i dag via infiserte e-poster, nettsider, eller USB-minnepinner. De fleste av disse angrepene er teknisk sett relativt enkle å stoppe. NSMs fire råd gir en god start for grunnleggende beskyttelse mot trusler som kommer fra internett.[203] I følge den australske signaletterretningsorganisasjonen kan en ved disse tiltakene stoppe 85% av datainnbrudd.[204] For ytterligere teknisk sikring av generelle IKT-systemer, har NSM en sjekkliste med 10 tiltak totalt, der de fire også inngår.[205]

Lysne-utvalget har videre påpekt at NVE bør se på hele verdikjeden og identifisere hvilken informasjon, som gitt de teknologiske endringene og organisatoriske rammene, er så kritisk at den ikke kan lagres utenfor Norges grenser. Arbeidsgruppen vurderer at EU kan være en mulig grense når det gjelder lagring av kraftsensitiv informasjon i utlandet. Dette følger av den stadig tettere sammenkoplingen av energiinfrastrukturen i Europa. Arbeidsgruppen vurderer at lagring av data utenfor Norges grenser kan være både en styrke (backup) og en økt risiko (landrisiko og tilgang til data).

Arbeidsgruppen mener at virksomhetene fortsatt må gjøre en verdivurdering av informasjon og en risikoanalyse av valgt løsning for lagring, overføring og deling av kraftsensitiv informasjon.

Arbeidsgruppen har sett til annet nasjonalt regelverk og vil anbefale å benytte begrepet forsvarlig sikkerhet i utformingen av krav til grunnsikring i ny forskriftstekst:

Hva som anses forsvarlig sikkerhet i energiforsyningens IKT-systemer vil fremkomme gjennom markedspraksis, tilgjengelig teknologi og internasjonale og nasjonale krav. Det er virksomhetens ansvar at tjenestene som benyttes holder et forsvarlighetsnivå, at en systemtilnærming og risikovurdering legges til grunn i vurderingen av forsvarlig sikkerhet, og at tiltakenes kostnader står i et rimelig forhold for til den sikkerhetsmessige effekten som oppnås.[206]

11.3.4.2 Hvem skal kravene være rettet mot?

Slik det er nå er det kun KBO-enheter som har tydelige funksjonskrav til sikring av viktige systemer, herunder informasjonssystemer. Ved klassifisering av anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme benyttes klasse 1 til 3. Nivået for å automatisk bli KBO-enhet er å få et anlegg i klasse 1 etter bfe § 5-2. Det betyr at nivået er lagt til selskaper som har:

a) Kraftstasjon med samlet installert generatorytelse på minst 25 MVA.

---

[203] «Fire effektive tiltak mot dataangrep. Nasjonal sikkerhetsmyndighet NSM, Sjekkliste nr 1 (S01)» Oppdatert 2016-03-03 og «Strategies to mitigate cyber intrusion systems», Australian Government Department of Defence, , http://www.asd.gov.au/infosec/mitigationstrategies.htm, besøkt 28.10.2016

[204] Strategies to Mitigate Targeted Cyber Intrusions, Defence Signals Directorate, February 2014, http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf, nedlastet 28.10.2016.

[205]«Ti viktige tiltak mot dataangrep, Sjekkliste nr 2 (s-02)», oppdatert 2016-03-03, Nasjonal sikkerhetsmyndighet NSM, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf, besøkt 28.10.2016.

[206] Forslaget bygger på Nkom og Traavik-utvalgets definisjoner.

b) Transformatorstasjon med samlet hovedtransformatorytelse på minst 10 MVA.
c) Omformerstasjon med samlet installert ytelse for omforming på minst 10 MVA.
d) Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 30 kV.
e) Kraftledning bygget for et spenningsnivå på minst 5 kV.
f) Fjernvarmesentral med samlet installert ytelse på minst 50 MW. I ytelsen skal medregnes effekt i ekstern varmeleveranse.
g) Driftskontrollsystem som styrer eller overvåker anlegg som omfattet av bokstav a til d og f.

Arbeidsgruppen ser at det er en rekke selskaper som kommer under dette nivået. Det var hensikten slik at kun virksomheter som har anlegg eller annet av vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i energiforsyningen er medlemmer av KBO.

Arbeidsgruppen mener det er nødvendig å etablere et minimumsnivå av IKT-sikkerhet også for selskaper som er utenfor KBO, selskaper som indirekte kan få betydning for drift eller gjenoppretting av eller sikkerhet i energiforsyningen. Dette for å sikre at ikke disse selskapene utgjør en risiko for energiforsyningen. Dette gjelder blant annet markedsplassen og selskaper som eier AMS, men ikke har driftskontrollsystemer i klasse 1.

Virksomheter som er eller kan bli viktig i forhold til forsyningssikkerheten har en sikringsplikt for egne informasjonssystemer, i den grad disse er kritisk for opprettholdelse av egen drift, jf. bfe § 5-1. NVE kan ved enkeltvedtak (jf. bfe§5-7) innlemme andre virksomheter i KBO, men det er ikke hensiktsmessig å innlemme alle aktuelle leverandører i KBO.

Energiloven § 9-2 første ledd kan forstås som et krav til sikring av vesentlige informasjonssystem: «*Den som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, plikter å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner*» som nevnt i § 9-1 fjerde eller femte ledd og for å gjenopprette normal situasjon.

Nye aktører kan komme på markedet i framtiden, og nye avhengigheter og kritiske tjenester kan oppstå. Nye tjenester kan dermed få betydning for forsyningssikkerheten, indirekte. Eksempler kan være leverandører som tar over styring av deler av infrastrukturen på distribusjonsnettet, eller blir svært tunge aktører i det økonomiske segmentet.

På denne bakgrunnen anbefaler arbeidsgruppen at energiloven § 9-3 *(informasjonssikkerhet)* gjøres gjeldende for alle, jf. energiloven § 1-2, og ikke begrenset til KBO-enheter. Dette vil bl.a. innebære at essensielle digitale tjenestetilbydere, kraftleverandører og andre viktige aktører, som kan defineres inn under NIS-direktivet blir regulert i sektorlovverket. Ansvar kan presiseres eksempelvis etter modell av IKT-forskriften til finanstilsynet, som nevner hvilke type aktører som kommer inn under regelverket.

Arbeidsgruppen anbefaler derfor følgende endring energiloven § 9-3 (informasjonssikkerhet):

§ 9-3 (informasjonssikkerhet)

*Alle **virksomheter i energiforsyningen** ~~[enheter i KBO]~~ skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den.*

Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen.

Departementet kan gi nærmere forskrifter om informasjonssikkerhet i kraftforsyningen og om taushetsplikten.

11.3.4.3 Grunnsikring IKT-sikkerhet

Arbeidsgruppen har vurdert at det i beredskapsforskriften bør stilles krav til generell IKT-sikkerhet og beskyttelse av sensitiv informasjon i informasjonssystemer. Virksomhetene skal sikre tilgjengelighet, integritet og konfidensialitet til sensitiv og kritisk informasjon om energisystemet. Tiltakene bør gi et forsvarlig sikkerhetsnivå, jf. Tråvik-utvalgets innstilling, § 4-1. Dette innebærer at virksomhetene først må etablere et tilstrekkelig sikkert system, så kunne drifte og forvalte systemet, inkl. ha oversikt over systemet og tilknyttede systemer og enheter, samt kunne oppdage og håndtere hendelser. Forskriften bør henvise til NVEs veileder, som igjen viser til anerkjente relevante anerkjente standarder og relevante veiledere. Slik kan virksomheten nivåtilpasse IKT-sikringen til sin risikovurdering.

For å tilfredsstille kravet må virksomheten ha et styringssystem for informasjonssikkerhet som revideres årlig. Krav til internkontroll er i dag dekket gjennom kapittel 2 i beredskapsforskriften. Kravene i beredskapsforskriften bør tydeliggjøres slik at det er klart at dette også dekker IKT-sikkerhet. NVE-veileder bør gi råd, med tydelig effekt (jf. NSMs råd), og for øvrig henvise virksomheter med mer komplekse systemer til relevante standarder og veiledere (eks. Difi, NSM) som grunnlag for sikkerhetsarbeidet. Forslaget kan for eksempel lyde som:

> *Eier eller driver plikter å sikre informasjonssystemer som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, herunder adgang for uvedkommende.*

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter informasjonssystemets type, oppbygging og funksjon. Virksomheten skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll av og i informasjonssystemene som nevnt i enl § 9-3 første ledd.

Alle informasjonssystemer, som nevnt i enl §9-3 første ledd, skal holdes i funksjonsdyktig stand og skal så langt som mulig virke etter sin hensikt under ekstraordinære forhold.

Virksomheten skal sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges.

11.3.4.4 Logging og overvåking

Arbeidsgruppen anbefaler at NVE, som en del av grunnsikringen, i forskrift stiller krav til logging og logganalyse i alle informasjonssystemene i energiforsyningen. Arbeidsgruppen anbefaler at dette kravet skal gjelde de samme virksomhetene som er dekket av kravet til grunnsikring. Anbefalingen medfører ekstra kostnader i form av analyseverktøy og behov for kompetanse for selskap som ikke allerede har dette på plass. Arbeidsgruppen vurderer at NVE i veilederen bør kunne gi råd om nivå på logging og logganalyse. Anbefalingen medfører ekstra kostnader knyttet til logging sammenlignet med i dag. En enkel overvåkningstjeneste kan for en liten virksomhet koste anslagsvis 50 000 NOK pr. år. For en middel stor virksomhet kan overvåkningstjenester koste 100 000 NOK, og for en stor virksomhet kan kostnadene bli enda høyere. Dersom en virksomhet utsettes for en alvorlig IKT-hendelse, og ikke evner å oppdage årsaker eller lære, kan det medføre merutgifter og økonomiske tap. Det finnes dessverre ikke gode data på tap som følge av uønskede IKT-hendelser.

11.3.4.5 Tjenesteutsetting

Tjenesteutsetting omfatter utsetting av IT-drift og -tjenester, herunder skytjenester. Kravene i bfe § 6-5. *Anskaffelser i energiforsyningen* er problematisk ved bruk av utenlandske IT-leverandører. Myndigheten får ikke tilgang ved stedlig tilsyn hos disse, og norsk jurisdiksjon gjelder heller ikke utenfor Norges grenser. Arbeidsgruppen anbefaler at en bør heller vurdere et krav lignende det Finanstilsynet har til finansielle virksomheter. I Finanstilsynets IKT-forskrift § 12 klargjøres at ansvaret for IKT-sikkerheten uansett påhviler virksomheten. Finanstilsynet krever at det skal foreligge en skriftlig avtale som sikrer at foretak under tilsyn også gis rett til å kontrollere, herunder revidere de av leverandørens aktiviteter som er knyttet til avtalen, og at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Finanstilsynet finner det nødvendig, som et ledd i tilsynet med foretaket. Virksomheten må sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte tjenesteutsettingsavtalen. Tjenesteutsetting gjelder alle virksomheter.

Virksomheter som setter ut tjenester til underleverandører skal påse at disse er forpliktet til å etterleve bestemmelsene om informasjonssystemsikkerhet og at dette dokumenteres. Det skal også i avtalen med leverandøren opplyses at virksomheten kan føre tilsyn med etterlevelsen av disse bestemmelsene hos leverandøren.

11.3.4.6 Dokumentasjon

Et generelt krav til alle virksomheter om dokumentasjon er viktig for å ha nødvendig orden og oversikt over informasjonssystemene og styringssystemer. Dokumentasjonskrav henger tett sammen med kravet om internkontroll i bfe § 2-10. Bfe § 6-4.*Sikkerhetsinstruks,* og bfe § 7-3.*Dokumentasjon av driftskontrollsystemet*.

Det skal foreligge en samlet oppdatert oversikt over informasjonssystemet til virksomheten. Det skal foreligge oppdatert dokumentasjon av det enkelte informasjonssystem, som er av betydning for foretakets virksomhet og som dokumenterer at forskriftens krav er oppfylt til enhver tid. Virksomheten skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssystemsikkerhet ivaretas og som beskriver hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssystemsikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.

11.3.4.7 Varsling og rapportering

I bfe § 2-6 er det stilt krav til KBO-enheter om varsling. Arbeidsgruppen anbefaler at en bør vurdere krav til alle virksomheter om å rapportere uønskede IT-hendelser til sektorCERT, (eller den NVE utpeker), slik at sektorCERTen kan lage et oversiktsbilde over sikkerhetssituasjonen i sektoren. Alvorlige sikkerhetsbrudd må i tillegg rapporteres til NVE og NSM der det er relevant. Dette kravet følger også Tråvik-utvalgets forslag til ny sikkerhetslov. Skal kravet være reelt, kreves det også at virksomhetene logger datatrafikk og analyserer loggene sine. Veilederen bør presisere hvilke type hendelser som bør logges og rapporteres.

Arbeidsgruppen viser til varslingspliktens bestemmelser bfe § 2-6 om varsling og rapportering og anbefaler at denne gis en dekning utover KBO-enhetene.

11.3.4.8 Hendelseshåndtering og beredskap

Alle virksomheter må ha beredskap for håndtering av uønskede IKT-hendelser. Beredskapsplanen skal bygge på risikovurderingen. Planverket bør øves, og rutiner bør gjennomgås regelmessig. I bfe § 2-2 og bfe § 2-3. er det stilt krav om beredskapsorganisering og beredskapsplikt til KBO. Internasjonale standarder dekker også dette forholdet gjennom kontinuitetsplanlegging, backup mv.

11.3.4.9 Hvordan bør kravene implementeres?

Arbeidsgruppen ser at det mest hensiktsmessige vil være å tydeliggjøre kravene til sikring av anlegg, system eller annet etter bfe § 5-1. Det gjelder alle som eier eller driver anlegg, system eller annet, som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner, mot uønskede hendelser og handlinger.

Arbeidsgruppen har vurdert at det kan det utarbeides en søsterparagraf til bfe § 5-1 som nettopp tar for seg grunnleggende IKT-sikkerhet. Denne gjelder for de samme selskapene som bfe § 1-3 andre ledd og bfe § 5-1 første ledd. Den nye paragrafen for grunnleggende IKT-sikkerhet kan presisere grundigere hva som er grunnleggende nivå for IKT-sikkerhet.

En slik endring må sees opp mot markedssituasjonen, spesielt i forhold til et intra-europeisk marked og europeisk regelverk for øvrig. Kravene bør gis som funksjonelle krav og et forsvarlig sikringsnivå bør legges til grunn. Dette anses særlig viktig i de

markedsnære delene av energiforsyningen der endringene skjer raskt. Det er viktig at regelverket ikke blir til hinder for innovasjon og utvikling.

Forslaget om å stille krav til informasjonssikkerhet til alle virksomheter i energiforsyningen må ses sammen med tilsvarende utvidelser av virkeområde for andre deler av loven med forskrifter. Nye aktører vil kunne komme inn på styringssiden hos den enkelte kunde gjennom f.eks. smarthus-løsninger og forbruker fleks. Aktører som kontrollerer flere kunder i et område kan gjennom dette påvirke strømleveranse på samme måte som styring i distribusjonsnettet (og delvis som i regionalnettet for dominerende aktører).

11.3.4.10 Økonomiske og administrative konsekvenser av forslaget

Forslaget er basert på god sikkerhetspraksis. Endringene vil medføre at det kan stilles tydeligere krav til IKT-sikkerhet til aktører som i dag ikke er KBO-enheter og likevel er en viktig del av energisystemet. Arbeidsgruppen vurderer at tydeliggjøring av krav til grunnsikring slik det her er skissert, kan medføre kostnader til kompetanse og personell hos virksomheter som i dag ikke er underlagt noe regelverk. Kostnadene vil måtte vurderes mot muligheten til å unngå framtidig økonomisk tap som følge av utilstrekkelig IKT-sikkerhet. På sikt vil grunnsikringskrav føre til at alle aktører i energisystemet må ha kompetanse, rutiner og teknologi som gjør at de har en tilfredsstillende IKT-sikkerhet. Arbeidsgruppen mener at et slikt krav ikke er uforholdsmessig i et digitalt samfunn, og viser blant annet til økt satsting på digital kompetanse og IKT-sikkerhetskompetanse i Norge.

Forslaget bygger på eksisterende regulering og er basert på å trygge forsyningssikkerheten og å sikre at en fremtidig digitalisering av energiforsyningen ikke skaper unødig risiko med store økonomiske tap som følge.

11.4 Anbefaling om AMS- og målekjeden

11.4.1 Innledning

Avanserte måle- og styringssystemer (AMS) består av både målere (også kalt smarte-målere), nettselskapets sentrale IT-system for AMS og kommunikasjons-infrastrukturen mellom disse. Dette inkluderer både den logiske systembiten og fysiske enheter med infrastruktur. Det er vanlig å omtale AMS internasjonalt som advanced metering infrastructure (AMI) eller advanced metering management (AMM). I Norge er det slik at dersom AMS med bryte- eller strupe-funksjonalitet integreres med driftskontrollsystemer (SCADA), vil de deler av AMS som er sammenkoblet med SCADA defineres som et driftskontrollsystem. Det er imidlertid ikke spesielt vanlig i dag å administrere AMS og SCADA i samme system.

Flere nettselskap har aktivert brytefunksjonen. Brytefunksjonen vil blant annet kunne brukes som et virkemiddel overfor dårlige betalere eller ved rasjonering. De nettselskap som har tatt i bruk brytefunksjonen, har kun etablert funksjon for utkobling av en måler av gangen. At system ikke er klargjort for masseutkobling eller at brytefunksjon ikke er

tatt i bruk, gir likevel ingen garanti for at ikke avanserte og kompetente trussel-aktører kan utnytte funksjonen gjennom digitale angrep.

11.4.2 Problemstilling

I Norge er det et funksjonskrav for AMS at effektuttaket i hvert enkelt målepunkt skal kunne brytes med mindre det er snakk om trafomålte anlegg. Det skal være mulig for kunder å få tilgang til sine forbruksdata fra den enkelte AMS-måler via en dedikert port på måleren. Denne HAN porten vil i første omgang gjøre det mulig å strømme måledata til både PCer, nettbrett og mobiltelefoner via kundens hjemmenettverk. Kunden kan, etter hvert som markedet utvikles, på sikt også koble sammen ting som smarte termostater, el-billadere og kjøleskap til et system som kan bruke informasjon fra HAN-porten som input til styring. Dette fordi det for eksempel kan være gunstig å justere ned varmen i gulv og varmtvannstanker, vente med å lade bilen, eller justere temperaturen i fryserdelen av kjøleskapet, når strømmen er på sitt mest kostbare. En kan se for seg at for eksempel kjøleskapsprodusenter ikke vil ønske å benytte mye ressurser på å sikre oppdateringsmuligheter for kjøleskapenes digitale funksjoner. Det samme vil kunne være tilfelle for produsenter av eksempelvis smarte termostater. Dermed vil denne typen digitale funksjoner i fremtiden kunne bli forsøkt benyttet som potensielle angrepsverktøy for aktører som ønsker å skaffe seg tilgang til AMS. Disse vil likevel møte vanskeligheter med å gå inn i måleren via HAN-porten, som kun er satt opp for å strømme informasjon ut og ikke motta signaler. I dag er det ingen nettselskaper som har åpnet HAN-porten for bruk i hjemmet.

Dersom sikkerheten i AMS ikke er godt nok ivaretatt, kan det potensielt oppnås tilgang til brytefunksjon, og/eller utføres rekonfigurering av måler for å gjøre den ubrukelig. Ellers kan det ved for lav sikkerhet potensielt utføres uønskede handlinger som tyveri av personopplysninger i form av måledata, og/eller rekonfigurering av måler for å la den vise feilaktig forbruk. Et annet tenkt trussel-scenario kan være å sette opp AMS-målere i Botnett for å utføre ulike typer synkroniserte digitale angrep mot AMS system eller helt andre typer systemer. 21. oktober 2016 ble Regjeringens nettsider utilgjengelige som resultat av et hackerangrep i USA mot nettsteder som Twitter, Netflix og Spotify, men som også påvirket en av Regjeringens nettsteds-underleverandører. Ifølge NRK ble det i angrepet benyttet et botnett som inkluderte rutere og webkameraer.[207] Det er viktig at sikkerheten i AMS er god slik at ikke systemet kan misbrukes til uønsket aktivitet.

11.4.3 Eksisterende regulering

Sikkerhet i AMS er i dag regulert gjennom måle- og avregningsforskriften. Ut over dette stilles det en del krav til AMS av ulike myndigheter innenfor sikkerhet; Justervesenet (målenøyaktighet), Statens strålevern (stråling fra apparatur), DSB (el-/personsikkerhet), Nkom (kommunikasjon) og Datatilsynet (personopplysninger).

---

[207] Olsson, S. V., Hackere lammet internett på fredag – anbefaler å dekke til webkameraer, NRK 22.10.2016, URL: https://www.nrk.no/urix/hackere-lammet-internett-pa-fredag-_-anbefaler-a-dekke-til-webkameraer-1.13190974 besøkt 23.12.2016.

Maf § 4-2g stiller krav om sikkerhet mot uautorisert tilgang til AMS sine styrefunksjoner og sikkerhet mot misbruk av måledata/personopplysninger og andre data det er nødvendig å beskytte. Energiloven stiller også krav om effektiv sikring og beredskap for AMS gjennom § 9-2 da denne gjelder både system av betydning for omsetning, og for fordeling og overføring av elektrisk energi (hvorav de to siste punktene kan bli mer aktuelle i fremtiden). I tillegg stiller beredskapsforskriften krav til AMS med tanke på varsling av forsøk på inntrenging eller manipulasjon, samt at det stilles tilleggskrav for sikkerhet dersom AMS med bryterfunksjon integreres med et eller flere driftskontrollsystemer.

AMS kan også være å anse som et system som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, og vil derfor også være underlagt den generelle sikringsplikten i bfe § 5-1.

NVEs ansvarsområde ligger innenfor målerens anvendelse, funksjon og generelle sikkerhet. For å følge opp sikkerhetsbiten her har NVE blant annet utgitt en veileder til sikkerheten i avanserte måle- og styringssystemer.[208] Ny revidert veileder kommer i 2017.

11.4.4 Arbeidsgruppens anbefaling

11.4.4.1 Behov for ny regulering

I dag er reguleringen av sikkerhet i AMS generell, ved at det hovedsakelig kun stilles krav gjennom måle- og avregningsforskriften § 4-2 g: *[AMS skal] gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner.*

Detaljmål for sikkerhet gis i NVEs veileder til sikkerhet i avanserte måle- og styringssystemer, men disse fungerer i dag kun som veiledende krav til bransjen. NVEs veileder til sikkerhet i AMS setter generelle krav til beredskap, men har ingen spesifikke krav om reserveløsninger (fall-back). En slik reserveløsning er en løsning for gjenoppretting av normal drift dersom en får problemer under utrulling av nye systemer eller system-oppdateringer.

Riktig konfigurasjon av AMS er en sentral faktor for å lykkes med forebyggende sikkerhet. Dersom sikkerheten i systemet er godt nok implementert og det ikke er mulig å bryte seg inn i systemet via noen deler av nettverket, er en kommet langt på vei i beskyttelsen av det. For å få til dette må det stilles krav i lov eller forskrift. Eksempler er benyttelse av sikre autentiseringsmekanismer, alltid oppdaterte krypteringsstandarder, at det er mulig å lukke sikkerhetshull og svakheter løpende i alle deler av systemet, samt krav om jevnlig utførelse av sikkerhetstester.

Under workshop hos Sintef om AMS sikkerhet og NVEs veileder (avholdt 31. oktober 2016) ble det gitt noen kommentarer fra kraftbransjen med tanke på regulering. Det ble hovedsakelig nevnt at veilederen ikke beskriver hva som bør anses som ufravikelige krav og hva som kun kan anses som anbefalinger. Dette kan tyde på at en forskriftsfesting av krav vil kunne være tydeligere overfor bransjen. En annen måte å løse dette på kan være å

[208] Skapalen, F og B. Jonassen, *Veileder til sikkerhet i avanserte måle- og styringssystemer,* NVE, 2012, http://webby.nve.no/publikasjoner/veileder/2012/veileder2012_07.pdf besøkt 23.12.2016.

uttrykke eksplisitt i veilederen de deler som ansees av NVE som direkte krav for å oppfylle maf § 4-2 g.

Digitale strømmålere har innebygd bryterfunksjonalitet. I fremtiden vil AMS kunne koples til overvåknings- og styringssystemer for distribusjonsnettet. Så fremt systemene da benyttes til styring, og til å kople inn og ut forbruk via bryterfunksjonen, bør det da vurderes å underlegge systemet samme regulering som driftskontrollsystemer. Det bør videre tas hensyn til kritikaliteten av systemene på samme måte som det er gjort for driftskontrollsystemer i dag.

NVE har et funksjonskrav til sikring av måleverdikjeden og mot uønsket tilgang til styrefunksjoner i måle- og avregningsforskriften. Ny veileder for dette forskriftskravet kommer i 2017. Anbefalingen gjelder for nettselskaper. Kravet medfører ikke vesentlige endringer i kostnadsbildet i forhold til i dag med mindre AMS underlegges samme regulering som driftskontrollsystemer.

11.4.4.2 Konkret forslag til regulering

Arbeidsgruppen har kommet opp med to ulike forslag til regulering.

1. Samle sikkerhetskrav til AMS i en forskrift: I dag er sikkerhetskrav til AMS fordelt på både beredskapsforskriften og måle- og avregningsforskriften. Det kan være en fordel for kraftbransjen at regelverk forenkles ved å samle alle sikkerhetskrav - inkludert AMS - i en enkelt forskrift. Integrasjon av AMS med driftskontrollsystem kan bli vanlig i fremtiden, og sikkerhetskrav til driftskontrollsystemer også vil kunne bli gjeldende for AMS. Det ville da typisk vært beredskapsforskriften som ville vært en naturlig plass å samle sikkerhetskrav.

   Videre vil det sannsynligvis medføre fordeler ved å samle IKT-sikkerhet kompetansen på ett sted. En ulempe vil derimot kunne være mangel på kunnskap om markedsprosessene og tilpasning av sikkerhetstiltak til dette når det gjelder AMS-sikkerhet spesifikt. Sintef anbefalte i sin risikovurdering fra 2012[209] at beredskapsforskriften bør gjelde for AMS fordi uønskede hendelser med AMS kan få konsekvenser for kraftforsyningen. Sintef mente blant annet at flere av kravene til informasjonssikkerhet i kapittel 6 i beredskapsforskriften også bør gjelde for AMS. I tillegg mente Sintef at AMS (med bryter/strupefunksjonalitet inkludert) bør inngå i veiledningen til beredskapsforskriften i § 6-4 og klassifiseres på samme måte som driftssentraler, slik at kravene også kan gjelde for AMS, for eksempel med tanke på fjerntilgang.

2. Fortsette med sikkerhetskrav til AMS i to forskrifter: Ved å fortsette slik det er i dag, altså med sikkerhetskrav til AMS i 2 ulike forskrifter, er det større

[209] Bartnes, M., Johansen, G. og Sæle, H. (2012). *Rapport – risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS*, SINTEF, 2012, https://brage.bibsys.no/xmlui/bitstream/handle/11250/2380394/SINTEF%2bA22318.pdf?sequence=3&isAllowed=y nedlastet 05.03.2017.

sannsynlighet for at nettselskapene som har ansvaret for sikkerheten får med seg at de har et sikkerhetsansvar. I tillegg er måleverdikjeden en struktur hvor sikkerheten for hele kjeden i dag er innlemmet i måle- og avregningsforskriften. Det kan derfor være en fordel at de som har ansvar for oppfølging av måle- og avregningsprosessen, også kan føre tilsyn med sikringen av disse prosessene. Det kan gi en verdifull oversikt for å sette prosesser i sammenheng (og forstå kravene til sikkerhet i et kost/nytte perspektiv). Dette er spesielt viktig i en utrullingsperiode og frem til systemet er «stabilisert». I tillegg er det viktig at Elmarkedstilsynet har mulighet og kompetanse til å foreta helhetsvurderinger, som inkluderer IKT sikkerhet i forbindelse med innføring av nye prosesser og funksjoner i markedet.

Forskriftsrelatert sikkerhetsarbeid i Elmarkedstilsynet kan også være fornuftig både i dag og i et fremtidsperspektiv. EU-regelverk stiller i dag uavhengig regulator ansvarlig for at også sikkerhet følges opp i målekjeden.

Krav til sikkerhet i AMS i dag er meget overordnet regulert. Det gjør det utfordrende å velge ut et forslag som bedre enn et annet. Det kan være en ide å undersøke mer nøyaktig hvilke konkrete krav som bør stilles til AMS sikkerhet før en setter seg opp en mening om hvilken forskrift og hvilket miljø hos NVE som dette skal legges til. I tillegg er oppsett og bruk av bryterfunksjon, oppsett og bruk av HAN-port, samt oppsett og bruk av M-bus port ikke avklart. Mens en venter på avklaringer for overstående anbefaler arbeidsgruppen å ikke innføre endringer i forskrifter gjeldende AMS, men heller la regelverket ha det oppsettet det har i dag. Dette for å hindre unødig forvirring i bransjen og unødvendig arbeid i NVE.

Uansett hvilket forslag som fremstår mest hensiktsmessig, er det enkelte andre forslag som gjelder for begge. Arbeidsgruppen anbefaler at:

- Så lenge HAN-porten er åpen (i prinsippet kun for push fra systemet), utgjør den en potensiell sikkerhetstrussel. Det bør fjernes fra regelverket at annen informasjon enn måledata skal kunne gjøres tilgjengelig via HAN port, da dette ikke er nødvendig og kun bidrar til en mindre sikker løsning. Prisinformasjon kan på en enkel måte i stedet sendes over vanlig internett til enheter som mobiltelefoner, PCer og annet internett-tilkoblet utstyr.
- For å utføre et effektivt tilsyn med sikkerhet i AMS er det behov for konkrete krav om sikkerhetstiltak som nettselskapene må følge opp. Dette kan løses gjennom å klargjøre i veilederen hva NVE anser som minimumskrav til sikkerhet i AMS.

11.4.4.3 Økonomiske og administrative konsekvenser av forslaget

Forslaget medfører ingen endringer i kostnadsbildet eller administrative konsekvenser sammenlignet med i dag.

11.5 Anbefaling om industrielle kontrollsystemer og driftskontrollsystemer

11.5.1 Innledning

Et driftskontrollsystem er et industrielt kontrollsystem som styrer enheter over flere forskjellige geografiske steder, ofte langt fra hverandre. Energiforsyningen kan fungere uten et fungerende driftskontrollsystem, men det er veldig utfordrende og krever bemanning av stasjonene døgnet rundt. Dette betyr at for å ha en sikker og samfunnsmessig rasjonell drift av energiforsyningen, må driftskontrollsystemene sikres.

Det er kjent fra internasjonale undersøkelser at sårbarheten i industrikontrollsystemer øker, og at antall identifiserte SCADA-sårbarheter økte kraftig etter at Stuxnet-viruset ble oppdaget. Hendelsen i Ukraina i desember 2015 ga en ytterligere pekepinn på hvor sårbare slike systemer kan være. Dagens beredskapsforskrift kapittel 7 om beskyttelse av driftskontrollsystemer har mange funksjonskrav som inkluderer lagdelt sikring avhengig av kritikalitet.

Arbeidsgruppen har sammenlignet kravene i beredskapsforskriftens kapittel 7 med ISO/IEC TR 27019, og finner her et stort samsvar. Det betyr at mange av kravene har relevans dersom en sammenligner med standardiseringsarbeidet i ISO.

11.5.2 Problemstilling

Driftskontrollsystemene til virksomhetene styrer viktige komponenter i energisystemet som har direkte betydning for forsyningssikkerheten. Arbeidsgruppen vurderer at konsekvensen for forsyningssikkerheten av at driftskontrollsystemer svikter, er mer alvorlige enn dersom administrative støttesystemer svikter. Tilfeldig feil, svikt eller skadevare i driftskontrollsystemet kan få fysiske konsekvenser for materiell og personell. Konsekvensen for skade er størst i anstrengte situasjoner. Arbeidsgruppen har forhørt seg med det amerikanske Federal Energy Regulatory Commission Office of Energy Infrastructure Security, som sier at sanntids programvare slik som prosesstyring og automasjon, som krever umiddelbar respons, bør unngå IT-løsninger som kan medføre unødige signalforsinkelser. Også systemer som krever spesialisert maskinvare er uhensiktsmessig å legge i skyen. De peker videre på typisk kraftsensitiv informasjon som et område som bør vurderes spesielt. Overføring av kraftsensitive data krever kryptering og validering og verifisering av mottakere.

Det eksiterer en konflikt mellom sikkerhetsregimene innenfor tradisjonell IKT-sikkerhet og industrikontrollsikkerhet. I mange tilfeller er sikkerhetsmålene forskjellig. Generelt er driftskontroll avhengig av tilgjengelighet til styringssystemer og sårbare for signalforsinkelser. Integritet og tilgjengelighet er viktigere enn konfidensialitet. I praktisk sikkerhetsarbeid er driftskontrollsystemer beskyttet bak sterke sikringsmekanismer og tilgangskontroll, mens systemene har sårbarheter som patches med vesentlig sjeldnere frekvens enn administrative systemer. I tillegg er patche-regimet mye mer rigid og kontrollert for driftskontrollsystemer enn for administrative systemer, og

sikkerhetsregimet er i mer varierende grad basert på deteksjon og logganalyse. Et felles sikkerhetsregime er derfor utfordrende å få til.[210]

Høyere klasse driftssentralsentraler i dag er tilknyttet administrative systemer og adskilt med logisk seperasjon. Administrative systemer kan være kritiske for rask gjenoppretting etter feil og skade. Samtidig kan administrative systemer inneholde kraftsensitiv informasjon og være en inngangsport til kritiske industrikontrollsystemer og driftskontrollsystemer. Sikring av IKT-systemer, som er knyttet logisk til driftskontrollsystemer i klasse 2 og 3 og ev. andre kritiske industrikontrollsystemer, er nødvendig for å beskytte disse industrikontrollsystemene og driftskontrollsystemene. Sikring av administrative systemer vil være dekket i grunnsikringen.

Verdikjeden i kraftforsyningen har frem til nå blitt overvåket og styrt av driftskontrollsystemer for henholdsvis produksjonsanlegg, sentralnettnivå, regionalnettnivå og høyspent distribusjonsnettnivå. Etter utrullingen av smarte målere har mange selskap også etablert mer overvåkning og styring på distribusjonsnettnivå.

11.5.3 Eksisterende regulering

I dag er mange sikkerhetstiltak implementert for å beskytte driftskontrollsystemene. Driftskontrollsystemer i klasse 1 til 3 er som følge av et strengt reguleringsregime over mange år redundante og sikret i bredden mot mange ulike typer trusler. Sikringen gjelder ikke bare forebyggende logisk sikring, men også krav til logging, hendelseshåndtering, øving og beredskap mv. I tillegg er det særkrav til redundant samband, eget samband uavhengig av offentlig kommunikasjonsnett, og strenge krav til fysisk sikkerhet, herunder elektromagnetisk puls (EMP) beskyttelse av servere og annet IT-utstyr. Siste skanse er krav til evne til manuell drift – dette gjelder klasse 2 og 3 anlegg.

Dagens beredskapsforskrift setter krav til både fysisk og logisk sikring av driftskontrollsystemene gjennom henholdsvis kapittel 5 og 7. Begge kapitlene opererer med forskjellige nivåer på kravene etter hvor viktige et driftskontrollsystem er for forsyningssikkerheten i samfunnet. Et driftskontrollsystem blir automatisk klassifisert som klasse 1 dersom det styrer anlegg som har klasse 1. Det er NVE som klassifiserer anlegg og systemer. Høyere klasse blir klassifisert etter enkeltvedtak av NVE. Høyere klasse krever ekstra sikringstiltak som gjør at barrierene blir sterkere. I beredskapsforskriftens kapittel 7 er dette veldig tydelig når det gjelder fysisk sikkerhet og også når det gjelder logisk sikring av driftskontrollsystemer. Et prinsipp som går igjen i dagens regulering er at når systemer er koplet sammen (systems of systems), så skal tilknyttede systemer sikres i henhold til høyeste klasse. Denne problemstillingen gjelder for eksempel dersom AMS og DMS eller andre systemer koples sammen med et klassifisert driftskontrollsystem.

Eksisterende regulering bygger på standarder og dokumentasjon fra NERC-CIP, NIST og ENISA, og inneholder noen krav innledningsvis i kapittel 7 til driftskontrollsystemer:

§ 7-1.Generell plikt til å beskytte driftskontrollsystemet
§ 7-2.Overordnede sikkerhetsregler

[210] Smart grid security – Annex 1 General Concepts and Dependencies with ICT, ENISA 2012.

§ 7-3.Dokumentasjon av driftskontrollsystemet
§ 7-4.Kontroll med brukertilgang
§ 7-5.Kontroll ved endringer i driftskontrollsystemet
§ 7-6.Kontroll med utstyr i driftskontrollsystemet
§ 7-7.Håndtering av feil, sårbarheter og sikkerhetsbrudd
§ 7-8.Beredskap ved svikt i driftskontrollsystemet
§ 7-9.Bemanning av driftssentral
§ 7-10.Ekstern tilkobling til driftskontrollsystem
§ 7-11.Systemredundans i driftskontrollsystemet
§ 7-12.Sammenkobling mellom avanserte måle- og styringssystem (AMS) og driftskontrollsystem

§ 7-13.Beskyttelse mot elektromagnetisk puls og interferens

Videre er regelverket delt i to nivåer – klasse 2 og klasse 3 driftskontrollsystemer, slik at høyere klasse bygger på lavere klassekrav:

Tabell 11.1 viser en oppsummering av nivådelte sikkerhetskrav avhengig av klassifisering.

Tabell 11.1 Nivådeling på sikringstiltak for driftskontrollsystemer.

Klasse 2 tilleggskrav § 7-14	Klasse 3 tilleggskrav § 7-15
a. Sikkerhetskopier	a. Reservedriftssentral
b. Sikkerhetsrevisjon	b. Bemanning av driftssentral
c. Overvåking og logging	c. Ekstern tilkobling til driftskontrollsystemet
d. Utilgjengelig driftssentral	d. Systemredundans
e. Bemanning av driftssentral	f. Fastsettelse av særlige krav til bemanning
f. Ekstern tilkobling til driftskontrollsystemet	
g. Systemredundans	
h. Særskilt om dublering	
i. Beskyttelse mot EMP og EMI	
j. Sikker tidsreferanse	

11.5.4 Arbeidsgruppens anbefaling

11.5.4.1 Behov for regulering

Dagens regulering av driftskontrollsystemer har sin bakgrunn i beskyttelse av kritisk infrastruktur i situasjoner der krig truer og er utviklet over tid. Norges geopolitiske stilling, endringer i det sikkerhetspolitiske landskapet gjennom de siste 20 årene – fra kald krig, til terror, til en ny øst-vest spent situasjon og uro i Europa med terror og sabotasje, viser at en i et lengre tidsperspektiv ikke kan ta fred for gitt. Arbeidsgruppen vurderer at dette tilsier at det eksisterende reguleringsregimet fortsatt er relevant, gitt infrastrukturens kritikalitet for både samfunnsfunksjoner og for forsvaret av Norge i en potensiell konfliktsituasjon.

Arbeidsgruppen har observert at trenden internasjonalt er en innstramning i reguleringen. Tyskland og Frankrike er eksempler på land som jobber med regelutvikling på området. I møte med representanter fra EU og Danmark har arbeidsgruppen fått høre at norsk regelverk på området er godt, og at få land kan måle seg mot dette. I Europa er det Tyskland og Frankrike som er kommet lengst på området.

Arbeidsgruppen vurderer at krav fra EU og ny norsk sikkerhetslovgivning kan få betydning for norsk energisektor. Dagens regelverk bygger allerede på internasjonale standarder og veiledninger

Arbeidsgruppen har vurdert at en uløst utfordring, som ikke er godt dekket i dagens regelverk, er fjern-vedlikehold fra leverandører som ønsker å vedlikeholde systemene fra utlandet i større grad enn i dag. I dag dekker regelverket krav som hindrer at eksterne som ikke er KBO-enhet utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg, men drift av IT-systemene og komponenter er ikke dekket. Vi vil her henvise til forslag til grunnsikring og forslag til regulering vedrørende tjenesteutsetting.

Arbeidsgruppen har gått igjennom alle kravene i beredskapsforskriftens kapittel 7 og vurdert dem opp mot ISO/IEC TR 27019. Arbeidsgruppen vurderer at eksisterende regelverk er dekkende for å sikre forsyningssikkerheten, med unntak av overvåking, rapportering og hendelseshåndtering. Arbeidsgruppen vurderer at det kan være behov for mindre endringer i ordlyden i paragrafene, for eksempel endre ordlyd fra «person» til «bruker», for å tydeliggjøre at kravet gjelder også applikasjoner og ikke bare mennesker. Videre anbefaler arbeidsgruppen en grundigere gjennomgang i forhold til ordlyd i forskriften, slik at ordlyden er harmonisert med internasjonale standarder (ISO/IEC) i den grad det er hensiktsmessig.

Arbeidsgruppen vurderer at den største utfordringen knyttet til kapittel 7 er at den er begrenset til KBO-enheter på grunn av begrensningene i bfe § 1-3. For at kapittel 7 og skal sette krav til viktige driftskontrollsystem som ikke kommer i klasse 1, mener arbeidsgruppa at det er behov for å endre bfe § 1-3. Dette fører også til et større behov for å gå igjennom bfe §§ 7-1 til 7-15 og se om det er mulig å slå sammen og sløyfe deler av disse paragrafene.

11.5.4.2 Konkret forslag til regulering

Arbeidsgruppen foreslår ny ordlyd i beredskapsforskriften § 1-3 om Hvem forskriften er rettet mot:

Forskriften gjelder for de virksomheter som etter § 3-3 er enheter i Kraftforsyningens beredskapsorganisasjon (KBO). Forskriften gjelder også for de virksomheter som etter vedtak blir KBO-enheter.

Forskriftens kapittel 5 ***og 7*** *gjelder for de virksomheter som eier eller driver anlegg, system eller annet som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme.*

Forskriftens § 6-2 om taushetsplikt for sensitiv informasjon gjelder for enhver.

Arbeidsgruppen har også vurdert om det er behov for strengere krav til driftskontrollsystemene med bakgrunn i krav til ny sikkerhetslov som er foreslått i NOU2016 :19 Samvirke for sikkerhet. Denne vurderingen er ikke fullstendig da det avhenger av detaljene i nye forskrifter knyttet til ny sikkerhetslov. Arbeidsgruppen mener at kravene til Klasse 3 anleggene dekker i stort kravene til informasjonssystemsikkerhet for skjermingsverdige informasjonssystemer slik det foreslås i ny sikkerhetslov.

11.5.4.3 Økonomiske og administrative konsekvenser av forslaget

Forslaget innebærer en mulig kostnadsøkning for virksomheter som ikke faller inn under regelverket allerede. Økt kostnad må imidlertid sees opp mot forventet tap som følge av utilstrekkelig sikkerhet og uønskede hendelser.

Del V Vedlegg

12 Vedlegg

12.1 Arbeidsmetode og informasjonsgrunnlag

Prosjektet ble etablert i april 2016 og sluttført i mars 2017.

Prosjektet har innsamlet data fra en rekke skriftlige kilder i løpet av prosjektperioden, som er listet fortløpende i fotnotater. I tillegg har prosjektet gjennomført flere workshops med bransjen:

- Teknisk workshop om logging 15 juni 2016
- Workshop on Cyber Safety, Security and Resilience of Critical Energy Infrastructures, Oslo Norway, June 21-22, 2016, organisert av New Strains of Society (SAMRISK-II) project sponsored by the Norwegian Research Council, in collaboration with IFIP WG 11.10 on Critical Infrastructure Protection (http://ifip1110.org/)
- NVE intern workshop 6. september 2016 med inviterte gjester fra Sintef og University of Tulsa – Hvordan kan lovverk bidra til robuste infrastrukturer?
- Workshop om bryterfunksjon og AMS 9. september 2016
- Workshop om skytjenester og sikkerhet 12.september 2016
- Gjennomgang av rapporten og innspill fra bransjen, interesseorganisasjoner og leverandørindustrien 20.01.2017
- FSK har fått presentert resultatene (februar 2017) og prosjektet har hatt en representant på FSKs workshops med tema hva inngår i driftskontrollsystem 9 februar 2017

Prosjektet har hatt møter med en rekke IT-leverandører og nettselskaper i løpet av prosjektperioden, og dessuten benyttet foredragsaktivitet til å invitere bransjen til å gi synspunkter og komme med problemstillinger underveis i arbeidet. Det har kommet noen innspill som følge av dette initiativet.

Prosjektet har hatt møter med Nkom, Datatilsynet, PTIL, PST og NSM om prosjektet.

Prosjektet har videre gjennomført møter 8. -9. november 2016 med den norske delegasjonen i Bryssel, representanter fra European External Action Services (EEAS), Nato, DG Energy og EU-kommisjonen. Kontakt med amerikanske myndigheter (FERC) har foregått på epost.

Arbeidet har vært forankret internt i NVE gjennom en styringsgruppe som har deltatt med synspunkter og innspill i arbeidet. Totalt har det vært holdt 4 styringsgruppemøter i 2016 og ett styringsgruppemøte i 2017. Arbeidet er gjennomført av en intern arbeidsgruppe hos NVE.

12.2 Forkortelser og ordliste

Forkortelser	
ACER	Agency for the Cooperation of Energy Regulators (ACER)
AMS	Avenserte Måle- og Styringssystemer
bfe	Beredskapsforskriften
CERT	Computer Emergency Response Team
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DGF	Digitalt grenseforsvar
Difi	Direktoratet for forvaltning og IKT
DMS	Distribution Management System
DSO	Distribusjonsnett system Operatør
EMI	Elektromagnetisk forstyrrelse
EMK	Den europeiske menneskerettskonvensjon
EMP	Elektromagnetisk puls
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
HAN	Home Area Network
HMI	Human-Machine Interface
ICT	Information and Communications Technology (IKT på norsk)
IKT	Informasjons- og kommunikasjonsteknologi
IT	Informasjons-Teknologi
KBO	Kraftforsyningens beredskapsorganisasjon
LFCR	Load Frequency Control and Reserves
maf	Måle- og avregningsforskriften
MSB	Myndigheten för samhällsskydd och beredskap
NBS	Nordisk balanseavregning
NEK	Norsk Elektroteknisk Komite
NIST	National Institute of Standards and Technology (USA)
NKOM	Nasjonal kommunikasjonsmyndighet
NSM	Nasjonal sikkerhetsmyndighet
OPS	Operational Planning and Security
OS	Operational Security
PLC	Programmable Logic Controller
PLC	Programmerbar logisk styring (engelsk: PLC)
REMIT	Regulation on wholesale Energy Market Integrity and Transparency

RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
TSO	Transmisjonsnett system Operatør
Ordliste	
CIM	Krisehåndteringsverktøy
Cybersikkerhet	Sikkerhet knyttet til verdenen av sammenkoblede datasystemer og informasjonsressurser
Distributed Denial of Service	Angrepsform hvor flere enheter benyttes i et koordinert angrep for å hindre legitim tilgang, eksempelvis tilgang til en nettside
Distribution Management System	Programvare designet for å overvåke og styre elektriske distribusjonsnett
Driftskontrollsystem	IT system som brukes til overvåking og styring av driftsfunksjoner i infrastrukturen (SCADA på engelsk)
Elektromagnetisk forstyrrelse	Forstyrrelser som påvirker en elektrisk krets på grunn av elektromagnetisk stråling fra en ekstern kilde
Elektromagnetisk puls	Elektromagnetisk utladning som kan forårsake skader på elektroniske komponenter
Elhub	Database som skal omfatte alle måledata for strøm i Norge
Forsvar i bredden	Forsvarsprinsipp hvor et helhetlig design skal sørge for at alle ulike deler av systemet har forsvarsmekanismer mot angrep
Forsvar i dybden	Forsvarsprinsipp hvor et design med flere adskilte lag skal gradvis kunne absorbere et angrep
Fysisk kobling	Fysisk sammenkoblet
Fysisk skille	Fysisk adskilt
GPA-avtalen	Avtalen om offentlige innkjøp (WTO)
HAN port	Grensesnitt for å strømme måledata fra el-måler til hjemme-nettverk
Hvitelisting	Funksjon for forhåndsgodkjenning av for eksempel dataprogrammer eller epostadresser, ved å plassere de i en liste over pålitelige kilder

Ikke-benekting	En mekanisme knyttet til elektronisk samhandling, og som fungerer slik at de deltakende partene ikke kan benekte å ha deltatt i deler av eller hele samhandlingen
IKT-sikkerhet	Sikkerhet knyttet til skjæringspunktet mellom cyberverdenen og egne datasystemer og informasjonsressurser
IT-systemer	Teknologiske systemer for behandling av informasjon og data
KBO-enheter	De enheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme
Logisk kobling	Sammenkoblet gjennom regeloppsett (programvare)
Logisk skille	Adskillelse gjennom regeloppsett (programware)
Lysneutvalget	Et digitalt sårbarhetsutvalg ledet av professor Olav Lysne
M-bus port	Grensesnitt som gir mulighet for kommunikasjon over AMS infrastruktur for eksterne målere som vann og gass med mer
NIS-direktivet	EU direktiv om tiltak for å sikre et høyt felles nivå for nettverk- og informasjonssikkerhet i EU
Patch	En liten programvareoppdatering for å fikse en feil eller en svakhet i en allerede ferdig programvare levert til brukeren
Programmable Locig Controller	Del av et driftskontrollsystem. Utfører sensoraktivitet og driftsfunksjoner, er fleksible og avanserte med egne kontrollsystemer
Remote Terminal Unit	Del av et driftskontrollsystem. Utfører sensoraktivitet og driftsfunksjoner
ROS-analyse	Risiko- og sårbarhetsanalyse
SANS	Privat virksomhet med tilhold i USA med hovedfelt informasjons- og cybersikkerhet
SCADA-sikkerhet	Sikkerhet knyttet til Supervisory Control And Data Acquisition systemer

Service level agreement	En tjenestenivåavtale som beskriver og regulerer ytelsesnivået på en løpende tjeneste (for eksempel skytjeneste)
Skytjeneste	Samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett
Sosial manipulering	Å utnytte menneskelig kontakt og sosiale evner for å få tilgang
Stuxnet	Avansert skadevare oppdaget i 2010, som var målrettet mot driftskontrollsystemer
Supervisory Control And Data Acquisition	Se driftskontrollsystem
Tredje energimarkedspakke	Inneholder et direktiv og en forordning som omhandler kraftmarkedet, samt et direktiv og en forordning som omhandler gassmarkedet

12.3 Standarder og veiledere

12.3.1 Kvalitetsledelse generelt

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
ISO 9000	Internasjonal standard	Overordnede prinsipper innen kvalitetsstyring	Kjøpes hos Standard Norge https://www.standard.no/
ISO 9001	Internasjonal standard	Standard for kvalitetsledelse	Kjøpes hos Standard Norge https://www.standard.no/
DFØ (Internkontroll)	Norsk veileder for offentlig sektor	Etablering, forbedring og oppfølging av internkontroll	http://dfo.no/styring/internkontroll/

ISO 9000 standarden beskriver de overordnede prinsippene og terminologien som gjelder for hele ISO 9000 familien. Det er vanlig å referere til ISO 9000 standarden som hele samlingen av 9000 standarder.

ISO 9001 gir kriterier for et system for kvalitetsledelse og er den standarden i 9000 rekken som benyttes til underlag for sertifisering. Standarden setter kunde/bruker i fokus, samt legger vekt på toppledelsens motivasjon og forståelse. I tillegg legges det vekt på prosess-styring og kontinuerlig forbedring.

DFØ [Direktoratet for Forvaltning og Økonomi] sin veileder i internkontroll gir veiledning i etablering, forbedring og oppfølging av internkontroll. Veilederen kan benyttes både for enkeltområder i virksomheten og for virksomheten samlet sett. Denne veilederen har av åpenbare årsaker noe fokus på økonomiske prosesser.

12.3.2 IKT-ledelse/styringssystemer

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
COBIT (ISACA)	Internasjonalt rammeverk	IT-styrings rammeverk for IT-ledere	Kjøpes hos ISACA https://cobitonline.isaca.org/publications
ITIL	Internasjonalt rammeverk	Rammeverk for IT Service Management	Kjøpes hos blant annet TSO https://www.tsoshop.co.uk/
ISO 20000	Internasjonal standard	Standard for IT Service Management	Kjøpes hos Standard Norge https://www.standard.no/

COBIT står for Control Objects for IT og skal hjelpe til med å identifisere og tette gapene mellom IT-tekniske utfordringer og forretningens risiko. Forretningsorienteringen består i å koble forretningsmål til IT-mål, måltall og modenhetstabeller for å kunne måle resultater og identifisere ansvarsdeling mellom forretningen og IT-prosesseiere.[211]

ITIL består av 5 hoved-publikasjoner og definerer organisatorisk struktur og krav til kvalifikasjoner for IT-virksomheter. I tillegg gir den et sett av administrative prosedyrer for å fasilitere IT drift med tilknyttet infrastruktur. ITIL rammeverket tilsvarer ISO 20000.

ISO 20000 spesifiserer krav til tjenesteytere for å planlegge, etablere, implementere, drifte, overvåke, kontrollere, vedlikeholde og forbedre et Service Management System (SMS). Et SMS kan bli integrert med styringssystem for kvalitetsledelse basert på ISO 9001 eller informasjonssikkerhetsledelse basert på ISO 27001. ISO 20000 er samkjørt/synkronisert med ITIL.

12.3.3 Informasjonssikkerhetsledelse

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
ISO 27001	Internasjonal standard	Standard for informasjonssikkerhets-ledelse	Kjøpes hos Standard Norge https://www.standard.no/
ISO 27002	Internasjonal standard	Veiledning til 27001	Kjøpes hos Standard Norge https://www.standard.no/
Difi (Internkontroll for informasjons-sikkerhet)	Norsk veileder for offentlig sektor	Etablering og vedlikehold av internkontroll for informasjonssikkerhet	http://internkontroll.infosikkerhet.difi.no

[211] COBIT, ASP Norge, http://www.aspnorge.no/strategy_governance/cobit besøkt 05.03.2017.

		(inkludert risikostyring og avvikshåndtering)	
Datatilsynet	Veileder for Norske virksomheter	Veileder for internkontroll og informasjonssikkerhet	https://www.datatilsynet.no/Sikkerhet-internkontroll/internkontroll_informasjonssikkerhet/
Direktoratet for eHelse	Norsk veileder	Veileder for informasjonssikkerhets-ledelse (inkludert risikostyring og avvikshåndtering)	https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen
NSM (Veileder i sikkerhets-styring)	Norsk veileder for organisasjoner underlagt sikkerhetsloven	Råd til virksomheter om hvordan et styringssystem for sikkerhet kan etableres og videreutvikles	https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf
IASME	UK-basert standard for informasjons-sikring	Enklere versjon av ISO 27001 tilpasset mindre og mellomstore virksomheter	https://www.iasme.co.uk/wp-content/PDFs/IASMEStandardv4.pdf

ISO 27001 spesifiserer krav til et styringssystem for informasjonssikkerhet (eller internkontroll for informasjonssikkerhet) og er grunnlag for sertifisering. Målet med standarden er å fasilitere etablering, implementering og kontinuerlig forbedring av internkontroll for informasjonssikkerhet.

ISO 27002 utdyper tiltak foreslått i ISO 27001, Annex A. Tiltakene er ment å adressere krav identifisert via gjennomførte risikovurderinger.

Difi sin veileder er særdeles grundig og gir veiledning for etablering og vedlikehold av fullstendig internkontroll for informasjonssikkerhet (som kan likestilles med et styringssystem for informasjonssikkerhet). Denne veilederen er hovedsakelig basert på ISO 27001 og er ment å veilede offentlige virksomheter i deres informasjonssikkerhetsarbeid.

Datatilsynets veileder for internkontroll og informasjonssikkerhet skal hjelpe virksomheter gjennom prosessen med å innføre internkontroll og informasjonssikkerhet, med fokus på sikring av personopplysninger.

Direktoratet for eHelse sin norm for informasjonssikkerhet setter i system oppfølging av krav til informasjonssikkerhet basert på lovverket. Normen er først og fremst rettet mot helse og omsorgssektoren, men er tidligere anbefalt av Difi for virksomheter som generelt forholder seg til personopplysninger.

NSMs veileder for sikkerhetsstyring gir råd til virksomheter om hvordan et styringssystem for sikkerhet kan etableres og videreutvikles. NSM hevder veilederen er generell og aktuell for alle som jobber helhetlig med sikkerhet. Hovedfokus i veilederen er på tilsiktede uønskede hendelser. Veilederen kan sees på som et supplement til for eksempel DFØ sin veileder og andre relaterte verktøy for internkontroll, samt DIFI sin veileder for informasjonssikkerhet. I tillegg skriver NSM at terminologi og innhold er søkt harmonisert med sentrale standarder innen sikkerhet som ISO/IEC 2700x-serien og NS 583x-serien.

IASME er utarbeidet som en raskere og mer kostnadseffektiv standard enn ISO 27001 og er spesielt tiltenkt mindre og mellomstore virksomheter som synes ISO 27001 blir for omfattende. Standarden er basert på internasjonal best practice, er risikobasert og inkluderer aspekter som fysisk sikkerhet, oppfølging av ansatte og data backup. Det er også mulig å bli sertifisert etter IASME standarden.

12.3.4 Risikostyring

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
ISO 27005	Internasjonal standard	Standard for risikovurdering av informasjonssikkerhet	Kjøpes hos Standard Norge https://www.standard.no/
ISO 31000	Internasjonal standard	Standard for risikostyring	Kjøpes hos Standard Norge https://www.standard.no/
ISO 31010	Internasjonal standard	Metoder for risikovurdering	Kjøpes hos Standard Norge https://www.standard.no/
ISO 5814	Internasjonal standard	Omhandler krav til risikovurderinger	Kjøpes hos Standard Norge https://www.standard.no/
NVE	Norsk veileder for kraftsektoren	Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen	http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf
Datatilsynet	Veileder for Norske virksomheter	Risikovurdering av informasjonssystem	https://www.datatilsynet.no/sikkerhet-internkontroll/risikovurdering/
NIST Special Publication 800-39	Publisering av U.S. Dep. of Commerce	Risikostyring innen informasjonssikkerhet	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
ISACA The Risk IT Framework	Internasjonalt rammeverk	Rammeverk for å identifisere, administrere og håndtere IT relaterte risikoer	http://www.isaca.org/knowledge-center/research/documents/risk-it-framework-excerpt_fmk_eng_0109.pdf
FAIR	Internasjonalt rammeverk	En metode for å kvantifisere og analysere informasjons-risiko i virksomheter	ftp://mail.im.tku.edu.tw/Prof_Liang/IRM/10%20An%20Introduction%20to%20Factor%20Analysis%20of%20Information%20Risk.pdf (whitepaper)
OCTAVE (CERT)	Internasjonal guide	Metode for å undersøke en organisasjons behov innen informasjonssikkerhet	www.cert.org/octave
NSM	Norsk håndbok	Risikovurdering for sikring	https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf
Difi (Internkontroll for informasjons-sikkerhet)	Norsk veileder for offentlig sektor	Etablering og vedlikehold av internkontroll for informasjonssikkerhet (inkludert risikostyring og avvikshåndtering)	http://internkontroll.infosikkerhet.difi.no
Direktoratet for eHelse	Norsk veileder	Veileder for informasjonssikkerhets-ledelse (inkludert	https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen

		risikostyring og avvikshåndtering)	
ENISA	Europeisk rammeverk	Metoder for å identifisere voksende og kommende risikoer	https://www.enisa.europa.eu/publications/emerging-and-future-risks-framework-introductory-manual
CMS	Håndbok for risikostyring for helsesektoren	Risikostyring	https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VI_Risk_Management_XLC.pdf
Department of Homeland Security	Amerikansk "Risk management fundamentals" og "Strategic national risk assessment"	Overordnet guide for risikostyring i henhold til Amerikanske reguleringer og forhold	https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf and https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
British Standard 7799 part 3	Britisk standard	Inneholder generelle retningslinjer for informasjonssikkerhets risikostyring	Kjøpes hos BSI http://www.bsigroup.com/en-GB/
ISF	International standard of good practice	Virksomhets-fokusert guide for å identifisere og håndtere informasjonssikkerhets-relaterte risikoer	Kjøpes hos ISF https://www.securityforum.org/

ISO 27005 standarden gir en oversikt over aktiviteter som kan inkluderes i en risikovurdering innen informasjonssikkerhet. Dokumentet bygger på generelle prinsipper fra ISO 27001.

ISO 31000 beskriver prinsipper, rammeverk og en prosess for risikohåndtering. Standarden kan hjelpe organisasjoner å nå mål, identifisere muligheter samt trusler, og effektivt fordele ressurser for risikohåndtering.

ISO 31010 fokuserer på risikovurderingskonsepter, prosesser og valg av risikovurderingsteknikker. Standarden bygger på ISO 31000. NB: ISO 31010 er ikke designet spesielt for sikkerhet.

ISO 5814 stiller krav til de elementene som kan inngå i en risikovurderingsprosess, samt beskriver risikovurderingens plass i risikostyring samt de faktorer som påvirker planlegging og gjennomføring av risikovurderinger, for eksempel rammebetingelser og etablering av risikoakseptkriterier.

NVEs veileder i risiko- og sårbarhetsanalyser for kraftforsyningen gir en innføring i hvordan denne type analyse skal benyttes for å tilfredsstille kravene gitt av Forskrift om beredskap i kraftforsyningen.

Datatilsynets veileder for risikovurdering av informasjonssystem forklarer hvordan virksomheter bør gjennomføre en risikovurdering (med fokus på virksomhetene som behandlere av personopplysninger).

NIST [National Institute of Standards and Technology] utarbeidet Special Publication 800-39 for å følge opp Amerikansk lovgivning innen informasjonssikkerhet. Offentlige virksomheter er i målgruppen, men også private organisasjoner oppfordres til å følge innholdet på frivillig basis.

ISACA The Risk IT Framework er designet som en opplæringsressurs for fagpersoner, for å hjelpe virksomheter i å håndtere IT relaterte risikoer. Rammeverket er spesielt egnet for virksomheter som vil benytte COBIT som styringssystem for informasjonssikkerhet. Mens COBIT presenterer tiltak for å redusere risiko, gir Risk IT et rammeverk for å identifisere, administrere og håndtere IT relaterte risikoer.

FAIR [Factor Analysis of Information Risk] inneholder konsepter for å håndtere risiko: Risikoforståelse og risikoanalyse, risikolandskapet og dens komponenter, risikokvantifisering, konsepter for risikoreduserende tiltak, samt måling av risikofaktorer.

OCTAVE beskriver metodeverk innen vurdering av trusler, verdier og sårbarhet. Metodeverket søker å optimere vurderingsprosessen av informasjonssikkerhetsrisiko slik at organisasjoner kan oppnå tilfredsstillende resultater med mindre benyttelse av tid, arbeidskraft og andre begrensede ressurser.

NSMs risikovurdering for sikring beskriver en gjennomføring av risikovurdering med fokus på tilsiktede uønskede handlinger. Håndboken gir råd til virksomheter om hvordan slike risikovurderinger kan planlegges og gjennomføres.

Difi sin online veileder for internkontroll for informasjonssikkerhet inkluderer risikostyring. Det er en grundig veileder for norske offentlige virksomheter, og den er basert på ISO 27001.

Direktoratet for eHelse sin norm for informasjonssikkerhet setter i system oppfølging av krav til informasjonssikkerhet basert på lovverket. Normen er først og fremst rettet mot helse og omsorgssektoren, men er tidligere anbefalt av Difi for virksomheter som generelt forholder seg til personopplysninger.

ENISA [European Network and Information Security Agency] sitt rammeverk for å identifisere voksende og kommende trusler ble laget for å dekke eget krav til identifisering av risikoer som kan få konsekvenser for tilgjengeligheten for elektroniske systemer og nettverk. ENISA mener i tillegg at rammeverket kan benyttes av andre organisasjoner som en veiledning under utvikling av egne prosesser for vurdering av voksende og kommende risikoer.

CMS Risk management handbook kommer i tre opplag, hvor 1 er referansematerialet, 2 inneholder prosedyrer for risikostyring og 3 inneholder gjeldende standarder, krav, direktiver og praksiser. Håndboken er utviklet for helse- og omsorgsvirksomheter.

Department of Homeland Security sin oversikt/strategi for risikostyring/vurdering ble utarbeidet for samkjøring av risikostyring/vurdering for indre sikkerhet innen USA. Det er ikke ment som sjekkliste men heller å illustrere et ambisjonsnivå for gjennomføring av risikostyring. I tillegg vises i «Strategic national risk assessment» faktiske resultater og metode for gjennomføring.

British Standard 7799 part 3 veileder nøkkelprosesser som å identifisere, evaluere, behandle og håndtere informasjonssikkerhetsrisikoer. Standarden utfyller ISO

27001:2005 gjeldende risikohåndtering og hvordan sette dem i kontekst med andre virksomhetsrisikoer.

ISF [Information Security Forum] sin standard inneholder omfattende tiltak og veiledning for nåværende og kommende informasjonssikkerhetsområder som lar organisasjoner respondere på den raske utviklingen av trusler, teknologi og risikoer.

12.3.5 Kriseledelse

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
ISO 22320	Internasjonal standard	Standard for kriseledelse – krav til hendelsesrespons	Kjøpes hos Standard Norge https://www.standard.no/

ISO 22320 «Kriseledelse – Krav til hendelsesrespons» har som mål å minimere virkningen av katastrofer, terrorangrep og andre store hendelser. Standarden skal bidra til å redde liv, redusere skade og sikre kontinuitet i grunnleggende tjenester som for eksempel helse, vann- og matforsyning, og elektrisitet.

12.3.6 Skytjenester

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
Nasjonal strategi for bruk av skytjenester	Norsk nasjonal strategi for både offentlig og privat sektor	Strategien beskriver skytjenester og regelverket for bruk	https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal_strategi_for_bruk_av_skyteneste r.pdf
Datatilsynet	Veileder for bruk av skytjenester	Veileder for bruk av skytjenester med utgangspunkt i personopplysningsloven	https://www.datatilsynet.no/globalassets/global/04_veiledere/skytjenester-2016.pdf
Legal guide to public cloud sourcing	Nordisk veiledning	Tar for seg EU relaterte lover og regler, ansvar, risikovurdering og avtaler relatert til skytjenester	http://norden.diva-portal.org/smash/get/diva2:701093/FULLTEXT01.pdf
Cloud service level agreement standardization guidelines	Europeiske retningslinjer	Retningslinjer for kontraktvilkår for skytjenester	https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines
NIST Special Publication 500-292	Amerikansk referanse-arkitektur	Verktøy for å beskrive, diskutere og utvikle systemspesifikk skytjeneste arkitektur	http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

Nasjonal strategi for bruk av skytjenester er utarbeidet for å effektivisere IKT bruken nasjonalt ved å stimulere til å også vurdere bruk av skytjenester. Strategien beskriver skytjenester og utfordringer ved disse, samt hvilke vurderinger som bør gjøres når en tenker på å kjøpe skytjenester. I tillegg er det fokusert på tydeliggjøring av hva regelverket rundt bruk av skytjenester sier slik at dette ikke skal oppleves som en hindring.

Datatilsynet har laget en veiledning for skytjenester med fokus på personvern. Veilederen er ment for alle typer virksomheter og også privatpersoner som ønsker å bruke skytjenester. Innholdet omfatter relevante områder ved anskaffelse av skytjenester slik som internkontroll, risikovurdering, spesielle problemstillinger, samt sjekkliste for relevante oppgaver underveis og anbefalinger til privat bruk av skytjenester.

Legal guide to public cloud sourcing er en veiledning som tar for seg spesielt skytjenester hvor personlige data blir behandlet. Men veiledningen hevdes å også kunne benyttes med tanke på annen type informasjon. Veiledningen tar for seg EU relaterte lover og regler, ansvar, risikovurdering og avtaler relatert til skytjenester.

Cloud service level agreement standardization guidelines gir veiledning med tanke på SLA avtaler mellom tilbydere av skytjenester og kjøpere (som ikke er privatpersoner), og standardisering av dette. Innholdet er spesielt tilpasset europeiske behov for marked og tilbydere.

NIST Special Publication 500-292 gir råd vedrørende forståelse av hva skytjenester medfører av krav, og bruk av generelt rammeverk for å utvikle systemspesifikk skytjeneste arkitektur.

12.3.7 Sikkerhet i SCADA og kritisk infrastruktur

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
IEC 62443	Cyber sikkerhet standard rekke	Sikkerhet for industrielle automatiserings og kontrollsystemer	Kjøpes hos Standard Norge https://www.standard.no/
ETSI	Internasjonal standard rekke	Standarder som omhandler cyber sikkerhet	http://www.etsi.org/technologies-clusters/technologies/cyber-security
MSB	Svensk veiledning	Veiledning til økt sikkerhet i industrielle kontrollsystemer	https://www.msb.se/ribdata/filer/pdf/25548.pdf
NERC (CIP)	Internasjonal pålitelighets-standard	Pålitelighets-standard utviklet for det Nord-Amerikanske hoved-nettsystemet	http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf
NIST CSF	Amerikansk rammeverk	Bruk av virksomhets-prosesser for å styre cyber sikkerhet aktivitet for kritisk infrastruktur	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
NIST Special publication 800-82	Amerikansk veiledning	Sikkerhet i SCADA, DCS, og andre kontroll-	http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

		system konfigurasjoner som PLC	
NESCOR Failure scenarios	Amerikansk støtteverktøy for risikovurdering	Trusselscenarier for energi-forsyningen	Alle: http://smartgrid.epri.com/doc/NESCOR%20failure%20scenarios09-13%20finalc.pdf Høyrisiko utvalg: http://smartgrid.epri.com/doc/nescor%20detailed%20failure%20scenarios%2009-13%20final.pdf
Roadmap to achieve energy delivery systems cybersecurity	Amerikansk veileder	Definerer krav til cyber sikkerhet i energisystemer	http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf
ISO/IEC TR 27019	Industrikontrollsystemer	Tilleggskrav til industrikontrollsystemer der sikkerhetsregimet fra før bygger på ISO 27001/2	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759

IEC 62443 er en sikkerhetsstandard rekke for sikkerhet for industrielle automatiserings og kontrollsystemer. Standardrekken inkluderer blant annet patch management, sikkerhet i trådløse systemer, samt samspill mellom sikkerhet og tekniske krav i system og komponenter.

ETSI opprettet i 2014 en komite ved navn TC CYBER for å organisere internasjonal standardisering innen cyber sikkerhet. I tillegg skal denne gruppen arbeide for å møte det voksende behovet for standarder for å beskytte internett og kommunikasjonen og prosessene som foregår der.

MSB [Myndigheten för samhällsskydd och beredskap] sin veileder gir grunnleggende anbefalinger for sikring av SCADA systemer, som å øke kunnskapsnivået om sikkerhet i virksomheten, gjennomføre undersøkelse av systemsikkerheteten, holde SCADA system separat fra administrative system og å stille sikkerhetskrav i alle anskaffelsesprosesser for SCADA systemer og serviceavtaler.

NERC [North American Electric Reliability Corporation] sin standard rekke er utviklet for drift av hovednettet i Nord Amerika, men kan også i stor grad benyttes andre steder innenfor samme bransje. Det er CIP serien som er spesielt interessant og omtaler identifisering av aktiva, sikkerhetsledelse, trening, sikkerhetsteknologi, fysisk sikkerhet, systemsikkerhet, hendelseshåndtering og gjenoppretting/ beredskap/kontinuitet.

NIST CSF [Cyber Security Framework] fokuserer på å sikre robust funksjon i kritisk infrastruktur, gjennom å inkludere cyber sikkerhet aktiviteter i virksomhetsaktiviteter innenfor risikostyring. Rammeverket inkluderer også metode for personvern og borgerrettigheter i cyber sikringsprosesser. Rammeverket henviser til ulike internasjonale standarder, rammeverk og veiledninger og skal kunne benyttes også utenfor USA.

NIST Special publication 800-82 veileder etablering av sikre industrielle kontrollsystemer. Dokumentet er spesielt oppmerksom på at kontrollsystemer endres fra

skjermet drift til å kjøres over IP [Internet Protocol], og den økte risikoen som følger med dette.

NESCOR Failure scenarios oversikten gir et sett av prioriterte trusselscenarier med konsekvens-vurdering for energisektoren. Informasjonen er tenkt benyttet for blant annet risikovurdering, planlegging, øving og sikkerhetstesting.

Roadmap to achieve energy delivery systems cybersecurity veilederen gir en plan for å forbedre cybersikkerheten i energisektoren. Det er et strategisk rammeverk for det neste tiåret for å etablere, operere, og vedlikeholde et forutsigbart energiforsyningssystem robust nok til å overleve cyber hendelser og opprettholde kritiske funksjoner.

ISO/IEC TR 27019:2013 dekker industrikontrollsystemer og utvider dermed ISO 27000 serien. Den dekker digitale systemer men ikke analoge, og heller ikke styringssystemer som blir benyttet i husholninger (eks. smarte hjem).

12.3.8 Kommunikasjon generelt

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
TCP	Internasjonal standard	Grunnleggende standard for å styre trafikken i nettverk basert på IP	https://tools.ietf.org/html/rfc793
FTP	Internasjonal standard	Protokoll for filoverføring i et TCP/IP basert nettverk	https://www.ietf.org/rfc/rfc959.txt
HTTP 1.1	Internasjonal standard	Protokoll for overføring av informasjon på web	https://datatracker.ietf.org/doc/rfc2616/
IPv4 og IPv6	Internasjonal standard	Protokoller for kommunikasjon på internett	https://tools.ietf.org/html/rfc791 og https://tools.ietf.org/html/rfc2460
UDP	Internasjonal standard	Grunnleggende protokoll for å styre trafikken i nettverk basert på IP	https://www.ietf.org/rfc/rfc768.txt
TLS	Internasjonal standard	Kryptografisk protokoll for kommunikasjon på nett	https://tools.ietf.org/html/rfc5246
SSH	Internasjonal standard	Kryptografisk nettverks-protokoll for å styre nettverkstjenester over usikre nettverk	https://tools.ietf.org/html/rfc4253
TOR	Verdens-omspennende frivillig nettverk	Gratis software for anonym kommunikasjon	https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt
IEC 60870-5-101	Internasjonal standard	SCADA protokoll standard for seriell kommunikasjon	Kjøpes hos Standard Norge https://www.standard.no/
IEC 60870-5-104	Internasjonal standard	SCADA protokoll standard for seriell kommunikasjon	Kjøpes hos Standard Norge https://www.standard.no/
IEC 61850	Internasjonal standard	SCADA protokoll standard for kontroll og vern av transformator- og bryterstasjoner	Kjøpes hos Standard Norge https://www.standard.no/

DNP 3.0	Internasjonal standard mye brukt i Nord Amerika	Sett av kommunikasjons-protokoller benyttet mellom komponenter i prosesskontrollsystemer	http://www.dnp.org/pages/aboutdefault.aspx
IEC 60870-6	Internasjonal standard	SCADA protokoll standard for inter-kontroll senter kommunikasjon	Kjøpes hos Standard Norge https://www.standard.no/
OPC	Internasjonal standard	Serie av standarder og spesifikasjoner for industriell telekommunikasjon	https://opcfoundation.org/

TCP er den mest brukte protokollen for styre trafikken på Internett. Den kan anses som en grunnleggende standard for datakommunikasjon.[212]

FTP er en av flere standarder for filoverføring og er i utstrakt bruk.[213]

HTTP (Hypertext transfer protocol) er den mest brukte protokollen for å overføre tekst på web. Standarden ligger på applikasjonslaget i OSI-modellen. Støtte for denne protokollen er en forutsetning for å lage nettjenester for brukere.[214]

IPv4 og IPv6 (forkortelse for Internet Protocol version 4/6) er grunnleggende protokoller for kommunikasjon på internett. Alt utstyr som skal kobles opp mot internett trenger en protokoll-adresse for å kunne nåes, enten det er en PC, en printer eller et kjøleskap.[215]

UDP er en grunnleggende protokoll for å styre trafikken i nettverk basert på IP. Den tilbyr ikke pålitelighet (ingen garanti for pakke levering) og dermed må applikasjoner som benytter protokollen akseptere litt tap.[216]

TLS [Transport Layer Security] protokollen tok over etter SSL og begge er kryptografiske protokoller for sikker kommunikasjon på internett. HTTPS er i hovedsak HTTP trafikk transportert på et TLS lag.

SSH [Secure SHell] er en kryptografisk protokoll for å styre nettverkstjenester over usikre nettverk. Et velkjent eksempel er applikasjoner for brukeres fjerntilgang til datasystemer. Filer lekket av Edward Snowden indikerer at NSA kan dekryptere SSH.[217]

---

[212] TCP (Transmission control protocol), https://www.difi.no/artikkel/2015/11/tcp-transmission-control-protocol , besøkt 05.03.2017.

[213] FTP (File transfer protocol), https://www.difi.no/artikkel/2015/11/ftp-file-transfer-protocol besøkt 05.03.2017.

[214] HTTP (Hypertext transfer protocol), Difi, https://www.difi.no/artikkel/2015/11/http-hypertext-transfer-protocol besøkt 05.03.2017.

[215] 4.1 - Nettsted og tjeneste er tilgjengelig over både IPv4 og IPv6, Difi, https://kvalitet.difi.no/artikkel/2015/11/41-nettsted-og-tjeneste-er-tilgjengelig-over-bade-ipv4-og-ipv6 besøkt 05.03.2017.

[216] UDP, Wikipedia, https://no.wikipedia.org/wiki/UDP besøkt 05.03.2017.

[217] Secure Shell, Wikipedia, https://en.wikipedia.org/wiki/Secure_Shell besøkt 05.03.2017.

TOR [Tor Onion Routing] softwaren krypterer kommunikasjon på applikasjonsnivået. Data, inkludert IP adresse krypteres flere ganger og sendes via tilfeldig valgte enheter. Målet er å hindre overvåking av nettaktiviteten. Funksjonen er basert på et frivillig nettverk av datamaskiner.

IEC 60870-5-101 er en standard for kraftsystem overvåkning, kontroll og tilhørende kommunikasjon for elektriske kraftsystemer.[218]

IEC 60870-5-104 er en forlengelse av IEC 101 protokollen med endringer i transport, nettverk, lenke og fysisk lag for å tilpasses full nettverkstilgang. Standarden bruker en åpen TCP/IP interface for tilgang til local area network og rutere med ulike løsninger som ISDN, X.25, Frame relay, etc. for oppkobling mot wide area network.[219]

IEC 61850 er en kommunikasjonsstandard for automatiske transformator systemer. Standarden kan benytte flere protokoller (manufacturing message specification, Generic object oriented substation event, Sampled measured values, og snart Web services). Disse protokollene kan kjøre over TCP/IP nettverk eller transformator local area networks.[220]

DNP 3.0 [Distributed Network Protocol] er et sett av kommunikasjonsprotokoller benyttet mellom komponenter i prosesskontrollsystemer. Benyttes hovedsakelig for kommunikasjon mellom hovedstasjon og Remote Terminal Unit eller Intelligent Electronic Devices.[221]

IEC 60870-6 er en standard for inter-kontroll senter kommunikasjon som benyttes for inter-master stasjon kommunikasjon i SCADA systemer.[222]

OPC (OLE for Process Control) er en industristandard som definerer kommunikasjonen mellom flere typer automasjonsutstyr, f. eks. mellom et HMI/SCADA-system og et PLC-system. Standarden bygger på klient-/serverkonseptet, noe som innebærer at klienten henter data fra serveren.[223]

12.3.9 Trådløs kommunikasjon

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
GSM/GPRS	GPRS er en standard for trådløs data-overføring	Dataoverføring over GSM mobiltelefon nettet	http://www.etsi.org/technologies-clusters/technologies/mobile/gprs

[218] Core IEC Standards, http://www.iec.ch/smartgrid/standards/, besøkt 05.03.2017, og IEC 60870-5-104, https://en.wikipedia.org/wiki/IEC_60870-5#IEC_60870-5-101 besøkt 05.03.2017.

[219] Core IEC Standards, http://www.iec.ch/smartgrid/standards/, besøkt 05.03.2017, og IEC 60870-5-104, https://en.wikipedia.org/wiki/IEC_60870-5#IEC_60870-5-104 besøkt 05.03.2017.

[220] Core IEC Standards, http://www.iec.ch/smartgrid/standards/, besøkt 05.03.2017, og IEC 61850, Wikipedia, https://en.wikipedia.org/wiki/IEC_61850 besøkt 05.03.2017.

[221] DNP3, Wikipedia, https://en.wikipedia.org/wiki/DNP3 besøkt 05.03.2017.

[222] DNP3, Wikipedia, https://en.wikipedia.org/wiki/DNP3 besøkt 05.03.2017.

[223] Open Platform Communication, https://en.wikipedia.org/wiki/Open_Platform_Communications besøkt 05.03.2017.

Bluetooth	Radiooverførings-protokoll	Protokoll for å sende og motta data trådløst	https://www.inf.ethz.ch/personal/hvogt/proj/btmp3/Datasheets/Bluetooth_11_Specifications_Book.pdf
ZigBee	Kommunikasjons-protokoll	Enklere protokoll enn Bluetooth[224]	https://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/s2011/kjb79_ajm232/pmeter/ZigBee%20Specification.pdf

GSM/GPRS (Groupe Spécial Mobile / General Packet Radio Service) GPRS er en standard for trådløs dataoverføring over GSM mobiltelefon nettet. Basestasjonene i telenettet benyttes til sending og mottak av digitaliserte, komprimerte og krypterte lydfil-pakker[225]

Bluetooth er en global standard for trådløs kommunikasjon tilpasset internet of things. Åpner for bruk av meget små sensorer og høykvalitets streaming[226]. Bluetooth baserer seg på frekvenshopping. Trådløs kommunikasjon etter Blutooth standarden er derfor robust for interferens.

ZigBee er den ledende globale standarden for å implementere lav-kost, kortdistanse trådløse nettverk som støtter forlenget batteritid. ZigBee alliansen er en non-profit allianse som tilbyr en åpen standard tilpasset internet of things.

12.3.10 Kryptering

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
AES	Internasjonal krypterings standard	Kryptografisk standard av typen block cipher men med ulike blokk og nøkkellengder	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
DES	Internasjonal krypterings standard	Kryptografisk standard fra 70-tallet som ikke lenger regnes som sikker	http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
RSA	Internasjonal krypterings standard	Kryptografisk standard av typen public key	http://people.csail.mit.edu/rivest/Rsapaper.pdf
NIST FIPS 140-2	Amerkiansk standard	Security requirements for cryptographic modules	http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

AES (Advanced Encryption Standard), også kjent som Rijndael er en krypteringsmetode publisert av Amerikanske National Institute of Standards and Technology i 2001.

[224] ZigBee, Wikipedia, https://no.wikipedia.org/wiki/ZigBee besøkt 05.03.2016.

[225] GPRS, Wikipedia, https://no.wikipedia.org/wiki/GPRS besøkt 05.03.2017.

[226] What is Bluetooth?, https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth besøkt 05.03.2017.

Standarden benyttes av federale organisasjoner ved behandling av sensitiv informasjon (NB: ikke sikkerhetsgradert) som krever kryptografisk beskyttelse.

DES (Data Encryption Standard) er en eldre kryptografisk standard som ikke lenger ansees som sikker. Dette blant annet pga kort nøkkellengde.

RSA (navngitt etter de som først publiserte metoden: Rivest, Shamir og Adleman) er en asymmetrisk krypteringsalgoritme basert på public/shared key prinsippet. Muliggjør kryptert kommunikasjon uten å ha delt samme nøkkel på forhånd.

NIST FIPS 140-2 (Federal Information Processing Standards) er standard godkjent av Amerikanske myndigheter for akkreditering av krypto-moduler. Det er nå også kommet et forslag til oppdatert versjon 140-3 (men 140-2 er fortsatt den gjeldende).

12.3.11 Hashing

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
SHS	Internasjonal hashing standard	Sett av kryptografisk sikre hashing algoritmer	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
SHA-3	Internasjonal hashing standard	Permutation/sponge basert hashing teknikk	http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf
MD6	Kryptografisk hashing funksjon	Benytter hash tree struktur for parallel prosessering av hasher for lange inputs	https://groups.csail.mit.edu/cis/md6/docs/2009-04-15-md6-report.pdf

SHS [Secure Hash Standard] spesiferer algoritmer som kan benyttes for å generere message digests. Disse kan benyttes for å se om meldinger har blitt forandret siden forrige digest ble generert.

SHA [Secure Hash Algorithm] er nummer fire i SHA familien (SHA-0, SHA-1, SHA-2, SHA-3). SHA-3 er første hashing algoritme NIST har utarbeidet ved hjelp av offentlig konkurranse.

MD6 (Message-Digest Algorithm er en kryptografisk hashing funksjon som ble levert inn som et av alternativene i den åpne SHA-3 konkurransen. Funskjonen benytter hash tree struktur for parallel prosessering av hasher for lange inputs

12.3.12 HAN port AMS (Referanser anbefales av NVE i dag)

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
MBUS	Europeisk standard	Standard for fjern-avlesing av gass eller elektrisitetsmålere	EN 13757-2
RJ-45	Internasjonal standard	Standard for endestykker på nettverkskabler	ISO/IEC 8877

MBUS (Meter-Bus) er en Europeisk standard for fjernavlesing av gass eller elektrisitetsmålere. Det er en kosteffektiv løsning designet for kommunikasjon over to ledninger. Det finnes også en radio-variant av MBUS kalt Wireless MBUS[227].

RJ-45 (RJ = Registered Jack) er en standard for endestykker på nettverkskabler. RJ-45 pluggene har åtte kontaktpunkter.

12.3.13 Kartlegging av sårbarheter

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
OWASP Top Ten Project	Internasjonal veiledning	Oppsummering av de mest kritiske web applikasjon sårbarhetene	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
SANS Top 20 Critical security controls	Internasjonal veiledning	Prioritert liste for å redusere de vanligste cyber sikkerhet risikoene	https://www.sans.org/critical-security-controls/
NSM 10 viktige tiltak mot dataangrep	Norsk veiledning	Beskriver 10 effektive tekniske tiltak for å beskytte IT systemer	https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf

OWASP Top Ten Project er et bevisstgjøringsverktøy for web applikasjon sikkerhet. Prosjektet gir ut fra et vidt perspektiv oversikt over de mest kritiske web applikasjon sikkerhets sårbarhetene.

SANS Top-20 Security Risks gir et prioritert sett med sikkerhetstiltak fro å redusere de vanligste og mest alvorlige cyber sikkerhet risikoene.

NSM 10 viktige tiltak mot dataangrep beskriver effektive tekniske tiltak som systemeiere i offentlig sektor bør benytte for å beskytte sine ugraderte systemer mot internett-relaterte dataangrep.

12.3.14 Krav om internkontroll i det norske regelverket

Referanse	Type/målgruppe	Beskrivelse av innhold	Publisert
Beredskaps-forskriften	Kraft bransjen	Forebyggende sikkerhet og beredskap for å redusere konsekvenser ved ekstra-ordinære situasjoner i energiforsyningen	https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157?q=beredskapsforskriften
Personopplysnings-loven	Alle virksomheter og organisasjoner som behandler person-opplysninger	Krav om internkontroll for informasjonssikkerhet	https://lovdata.no/dokument/NL/lov/2000-04-14-31?q=personopplysningsloven

[227] Meter-BUS, wikipedia, https://en.wikipedia.org/wiki/Meter-Bus besøkt 05.03.2017.

eForvaltnings-forskriften	Offentlige virksomheter	Krav om internkontroll for informasjonssikkerhet	https://lovdata.no/dokument/SF/forskrift/2004-06-25-988?q=eforvaltningsforskriften
Internkontroll-forskriften	Alle virksomheter	Systematisk helse-, miljø- og sikkerhetsarbeid	https://lovdata.no/dokument/SF/forskrift/1996-12-06-1127?q=hms
Forskrift om risikostyring og internkontroll	Finans relaterte institusjoner og virksomheter	Utdyping av ledelsens ansvar innen finans	https://lovdata.no/dokument/SF/forskrift/2008-09-22-1080
Brann- og eksplosjonsvern-loven	Behandlere av brannfarlige varer samt væsker og gasser under trykk	Krav om internkontroll for helse-, miljø- og sikkerhetsarbeid	https://lovdata.no/dokument/NL/lov/2002-06-14-20?q=brann

Internkontroll i virksomheten bør etableres som et sett av integrerte systemer hvor alle områdene samles, og ikke som flere parallelle systemer. Dette for å utnytte fordelene av felles tilgangspunkt med alt på ett sted, samt at layout, struktur og metode gjenkjennes på tvers av områder. Det gjør det lett å finne frem og motvirker at det utføres dobbeltarbeid i virksomheten.

13 Metode for vurdering av tiltak

13.1 Krav til utredninger av tiltak

Utredningsinstruksen[228] gir klare føringer for hvordan tiltak skal vurderes i statlig sektor. Instruksen har som formål å legge et godt grunnlag for beslutninger om statlige tiltak, herunder også regelendringer[229]. Minimumskravene til utredning er å besvare følgende spørsmål:

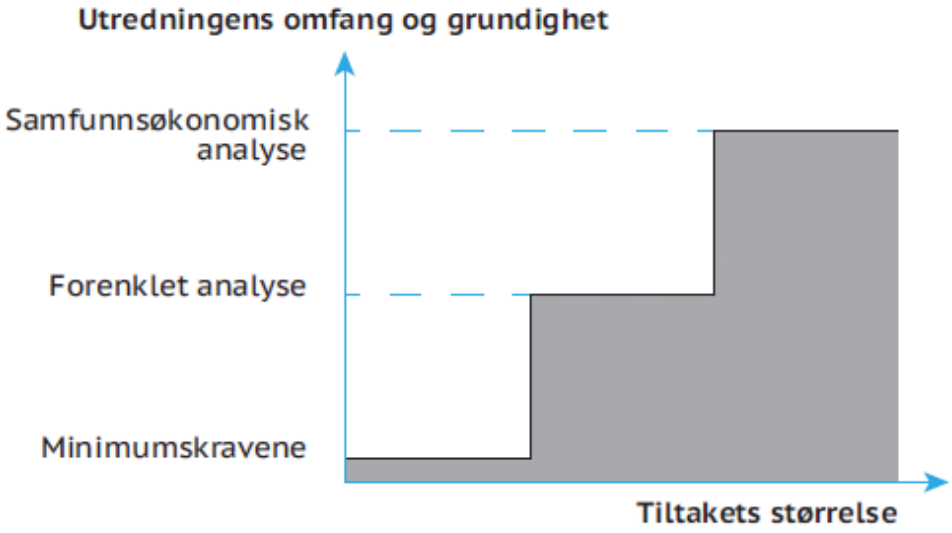
- Hva er problemet, og hva vil vi oppnå?
- Hvilke tiltak er relevante?
- Hvilke prinsipielle spørsmål reiser tiltakene?
- Hva er de positive og negative virkningene av tiltakene, hvor varige er de, og hvem blir berørt?
- Hvilket tiltak anbefales, og hvorfor?
- Hva er forutsetningene for en vellykket gjennomføring?

Utredningen skal være så omfattende og grundig som nødvendig. Vurderingen av dette skal baseres på om tiltaket reiser viktige prinsipielle spørsmål, hvor vesentlige virkningene av tiltaket forventes å bli og tiden som står til rådighet. Figur 13.1 viser en illustrasjon av omfanget og grundigheten av utredningene sett i sammenheng med

[228] Instruks om utredning av statlige tiltak (utredningsinstruksen). Fastsatt ved kongelig resolusjon 19. februar 2016.

[229] Ny utredningsinstruks, 19.02.2016, https://www.regjeringen.no/no/aktuelt/ny-utredningsinstruks/id2476510/ nedlastet 06.03.2017.

tiltakets størrelse. Videre sier instruksen at når det utredes tiltak som man forventer gir vesentlig nytte- eller kostnadsvirkinger skal det gjennomføres en analyse i samsvar med gjeldende rundskriv for samfunnsøkonomiske analyser[230].



Figur 13.1 Illustrasjon av hvordan utredningens omfang og grundighet er avhengig av tiltakets størrelse[231]

Avhengig av hvilke tiltak som foreslås i prosjektet er det aktuelt å gjøre ulike typer analyse.

Rapporten i sin helhet besvarer spørsmålene som utredningsinstruksen krever blir stilt, der innledende kapitler gir en oversikt over dagens situasjon og relevante problemstillinger før rapporten går videre inn på prinsipielle spørsmål og vurdering av de ulike tiltakene. De ulike tiltakene er sammenlignet med dagens situasjon i en svært begrenset kost-nytte vurdering. Forenklingen er begrunnet i at det ikke eksisterer datagrunnlag som gir mulighet for å gjøre større utredninger for å kvantifisere kostnader og nytteverdier. Der det er angitt kostnader er dette estimat forbundet med stor usikkerhet. Kostnadsestimat er skaffet ved å ta kontakt med selskaper og leverandører for å få et estimat for omfanget av relevante kostnader. Som følge av stor usikkerhet i reelle kostnader er kostnader ikke skalert opp for hele sektoren.

---

[230] Gjeldende rundskriv er Rundskriv R-109/14 «Prinsipper og krav ved utarbeidelse av samfunnsøkonomiske analyser mv. https://www.regjeringen.no/globalassets/upload/fin/vedlegg/okstyring/rundskriv/faste/r_109_2014.pdf , nedlastet 06.02.2017.

[231] *Veileder til utredningsinstruksen. Instruks om utredning av statlige tiltak*, Direktoratet for økonomistyring, mars 2016, https://dfo.no/documents/foa/publikasjoner/veiledere/veileder-til-utredningsinstruksen-v1.pdf, nedlastet 06.03.2017.

Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no