Teknologiskifte i energiforsyningen

Studie om muligheter og sårbarheter

Janne Hagen, Forsvarets forskningsinstitutt

118
2015

RAPPORT

Rapport nr 118-2015
Teknologiskifte i energiforsyningen

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør: Janne Hagen, Forsvarets forskningsinstitutt

Forfattere: Forsvarets forskningsinstitutt/NVE

Trykk: NVEs hustrykkeri
Opplag: 50
Forsidefoto: NVE
ISBN 978-82-410-1170-2
ISSN 1501-2832

Sammendrag: Kraftbransjen står overfor en betydelig digitalisering i forbindelse med utrulling av AMS, bruk av skytjenester og lignende. IKT gir mulighet til mer effektiv styring og drift av kraftinfrastrukturen. Trenden kan derfor bli at IT blir en enda viktigere del av nettselskapenes tjenesteutvikling. Samtidig endres risikoen, særlig når ulike system integreres og alt koples til Internett. Denne rapporten er initiert av NVE som en del av et kontinuerlig arbeid med å revidere og oppdatere beredskapsforskriften.

Emneord: AMS, bryterfunksjonalitet, IKT-sikkerhet, skytjenester, sårbarheter, IKT-hendelseshåndtering, logging, beredskap.

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

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

Desember 2015

Teknologiskifte i energiforsyningen

Studie om muligheter og sårbarheter

Norges vassdrags- og energidirektorat
2015

Innhold

Forord

Den teknologiske utviklingen gir nettselskapene nye, store muligheter til å effektivisere drift, planlegging og vedlikehold av strømnettet. Med det vil også gi store utfordringer som vil kreve innsikt og kompetanse til å forstå kompleksiteten og risikoen den medfører.

NVE engasjerte derfor Forsvarets forskningsinstitutt (FFI) våren 2015 for å foreta en kartlegging av hvilken teknologisk utvikling vi kan forvente i energiforsyningen.

Rapporten er skrevet av Janne Hagen, FFI, og i forbindelse med sitt arbeid har hun samarbeidet og diskutert ulike problemstillinger med en gruppe bestående av:

- Seksjonsleder Arthur Gjengstø, NVE, seksjon for tilsyn og beredskap
- Seksjonsleder Heidi Kvalvåg, NVE, Elmarkedstilsynet, seksjon for sluttbrukermarkedet
- Seniorrådgiver Frank Skapalen, NVE, seksjon for tilsyn og beredskap

IKT-sikkerhet vil bli stadig viktigere i energibransjen i årene fremover, og NVE vil ha fokus på både å følge utviklingen og kontinuerlig vurdere behovet for regulering og tilsyn.

NVE gjør oppmerksom på at innholdet og anbefalingene i rapporten står for forfatterens regning.

Oslo, desember 2015

Per Sanderud
Vassdrags- og energidirektør

Ingunn Åsgard Bendiksen
Avdelingsdirektør

Sammendrag

Kraftbransjen står overfor en betydelig digitalisering i forbindelse med utrulling av strømmålere med toveiskommunikasjon (AMS). Teknologien gir mulighet til mer effektiv styring og drift av kraftinfrastrukturen, feilretting og dermed økt nettnytte. Sammen med bruk av skytjenester utvides mulighetene for forretningsutvikling for nettselskapene. Trenden kan derfor bli at IT blir en viktigere del av nettselskapenes tjenesteutvikling. Samtidig endres risikoen, særlig når ulike system integreres og alt koples til Internett.

Det er lite som tyder på at trusselen mot digitale systemer blir mindre i årene som kommer, og trusselen på Internett følger ikke landegrensene. Dette er ikke nytt, men tendensen er at avansert spionprogramvare og teknologi tas i bruk av en stadig bredere brukergruppe. Skadevare, kriminelle digitale tjenester og angrep kan kjøpes på Internett, og angrep mot norske systemer kan utføres fra hele verden så lenge det er en kopling til Internett. Antall hendelser som er avdekket og omfanget av disse, viser at trusselaktørene ofte ligger foran sikkerhetsindustrien.

Som følge av utviklingen i teknologi, forretningsmodeller og trusler, må virksomhetene i energisektoren være svært bevisste med å vurdere verdien av informasjonen de besitter og forvalter. Med dagens trusselbilde er det en klar risiko for informasjonslekkasje, og det er nødvendig å implementere sikkerhetstiltak. Men selv med god sikkerhet vil det alltid finnes en restrisiko. Logging, logganalyse og overvåkning av systemer og datatrafikk gir mulighet for å oppdage hendelser, utbedre sårbarheter og lære fra hendelsene.

Landegrenser, nasjonal sikkerhetstilstand og jurisdiksjon er et viktig tema for outsourcing og bruk av skytjenester. Jurisdiksjonsspørsmålet er satt på prøve i forbindelse med den pågående rettsaken om amerikanske myndigheters tilgang til informasjon som ligger hos Microsofts datasenter i Irland i forbindelse med en narkotikasak. Utfallet av saken kan få konsekvenser for i hvilken grad utenlandske myndigheter kan få tilgang til sensitiv data fra norske virksomheter som er lagret hos utenlandske skyleverandører.

Norske myndigheter er pådrivere bak AMS. AMS gir effektiv drift, bedre og mer effektiv innfasing av fornybare energikilder og mulighet for utvikling mot smarte nett. Det har vært diskusjoner i både USA og Europa relatert til beskyttelse av personopplysninger og til generell sikkerhet knyttet til de digitale målerne. Imidlertid er det bryterfunksjonen som peker seg ut som den viktigste strategiske sårbarheten. I Nederland har debatten rundt sikkerhet ført til at nederlandske myndigheter har sagt at det er frivillig å installere målerne. I Norge som i Norden for øvrig har vi ikke hørt de samme kritiske røstene. Finland har nylig ferdigstilt sin AMS utrulling.

I Norge er NVE en pådriver for å tenke sikkerhet i hele verdikjeden hos energiselskapene også når det gjelder innføring av nye teknologier. NVE sin «Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen» (beredskapsforskriften) regulerer i kapittel 6 beskyttelse av sensitiv informasjon og i kapittel 7 sikkerhet i prosesskontrollsystemer. Også øvrige deler av beredskapsforskriften er relevante, bl.a. krav til risiko- og sårbarhetsanalyser, beredskapsplaner, øvelser og fysisk sikkerhet mot inntrenging i anlegg. Denne rapporten er initiert av NVE som en del av et kontinuerlig arbeid med å revidere og oppdatere beredskapsforskriften.

Utviklingen går fort og IKT-sikkerhet er et stort og omfattende fagfelt. NVE bør derfor også engasjere seg i europeisk arbeid knyttet til sikkerhet i AMS, skytjenester og overvåking og logging. Dette kan være viktig både for at NVE skal utvikle egen kompetanse på området, men også for at NVE skal kunne gi bidrag til det arbeidet som foregår i EU, og som i neste omgang slår tilbake på rammene for norsk kraftforsyning. NVE bør også følge med på arbeidet kommunal- og moderniseringsdepartementet (KMD) og Nasjonal sikkerhetsmyndighet (NSM) og andre gjør med skypolitikk og sikkerhet i skyen. Samarbeid med andre tilsynsmyndigheter på IKT-området er viktig, og NVE bør også prioritere dette. Truslene er ikke spesifisert etter sektor, men rammer bredt. Det er fornuftig å lære av hverandre og løfte sikkerhetsnivået i fellesskap.

1 Innledning

1.1 Bakgrunn

Digitalisering av kraftbransjen vil øke betydelig med utrulling av AMS. I Europa og USA foregår det en storstilt utrulling av AMS. I USA skal ca. 127 millioner målere være rullet ut i 2015. Disse skal bidra til bedre forsyningssikkerhet. I EU er utrulling av AMS og implementering av smarte nett begrunnet med hensynet til miljø og fornybare kilder.[1]

AMS med bryter som kan fjernstyres av nettselskapet vil også i Norge kunne gi nettselskapene bedre styringsmuligheter til å opprettholde effektbalanse og kvalitet på levert strøm. De amerikanske erfaringene så langt peker på bedre laststyring og drift, mer effektiv fakturering og bedre håndtering av nettutfall.[2] Ringeriks-Kraft i Buskerud, som var ferdig med sin utrulling av AMS i 2013, har erfart at AMS har redusert behovet for utbygging og forsterking av trafostasjoner i forbindelse med utbygging av nye boligfelt. Dette er mulig da selskapet har tilgang på detaljerte forbruksdata innenfor sitt forsyningsområde. Forbruksdata gir svært gode prediksjonsmuligheter, som igjen gir effektiv styring av investeringskostnader.[3]

Innføring av AMS med bryterfunksjonalitet (bryte eller begrense last) kan imidlertid endre risikobildet i kraftbransjen. Internasjonalt har utrullingen av smarte målere vært omdiskutert, og bekymringene er knyttet til blant annet ikke-autorisert tilgang til målerne og styring av disse, med konsekvenser for personvern, forsyningssikkerhet og tilliten til kraftsystemet.

AMS er ikke det eneste teknologiskiftet som er underveis. Også bruk av skytjenester brer om seg, blant annet som følge av sterke økonomiske incentiver og god funksjonalitet. Men også her kan bransjen stå overfor potensielle sikkerhetsutfordringer, som blant annet å ha kontroll med hvem hos skyleverandøren som har tilgang til selskapets data.

Innføringen av AMS og økt bruk av skytjenester vil sette større krav til selskapenes evne til å ha kontroll med IKT-infrastrukturen som etableres. Overvåking og logging av trafikken i egen IKT-infrastruktur vil da være viktig for å kunne agere raskt ved en hendelse, men også å finne årsaken etter at en hendelse har oppstått.

I 2015 fikk NVE ved beredskapsseksjonen innvilget interne forskningsmidler til et prosjekt – «Analyse av potensielt kritiske IKT-sårbarheter i energiforsyningen». Målet med prosjektet har vært å identifisere, belyse og drøfte ulike strategiske sårbarhetsutfordringer og hvordan disse kan møtes møtes gjennom regulering og tiltak hos selskapene. NVE har gjennom beredskapsforskriften samt «Måle- og

---

[1] Egozcue, E., Rodríguez , D. H., Ortiz, J. A., Villar, V. F. and L. Tarrafeta., Annex I. General Concepts and Dependencies with ICT, [Deliverable – 2012-04-19], ENISA 2012., URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid

[2] *2014 Smart Grid System Report, Report to Congress, August 2014*, United States Department of Energy, Washington DC 20585.

[3] Zachariassen, E., "Dette er effekten av big data", Digi.no, 20. mars 2015, URL: http://www.digi.no/bedriftsteknologi/2015/03/20/dette-er-effekten-av-big-data.

avregningsforskriften» satt klare sikkerhets- og beredskapskrav til selskapene i energiforsyningen. Prosjektet har særlig sett på om sårbarhetene og risikoene som blir tatt opp i denne rapporten er ivaretatt i disse forskriftene.

1.2 Problemstillinger

Denne rapporten diskuterer følgende fire spørsmål:

- Hvilke sårbarheter er relatert til lagring av informasjon i skyen, og hvilken type informasjon bør ikke legges i skyen?
- Hvilke digitale sårbarheter i AMS-systemet kan potensielt sette forsyningssikkerheten i fare?
- Hva er sårbarhetene og utfordringene i forhold til logging, hendelseshåndtering og personvern?
- Hvordan håndterer de andre myndighetene lignende utfordringer og hva kan kraftbransjen lære av dem?

Spørsmålet om sårbarheter i AMS er særlig viktig når det gjelder bryterfunksjonaliteten.

Skytjenester er en IT-driftsmodell som gir store økonomiske besparelser sammenlignet med tradisjonell IT-drift. Enkelte leverandører tilbyr i dag drift av systemer for kontroll av AMS og systemer for overvåking og kontroll av anlegg i distribusjonsnett via skytjenester, og i framtiden kan en ikke se bort fra at dette nærmest blir den mest vanlige driftsformen.

Med et mer komplekst trusselbilde kan vi anta at behovet for verifikasjon og etterprøvbarhet øker. Når det gjelder overvåking og logging er det relevant å se på sårbarheter og utfordringer relatert til personvern og virksomhetssensitiv informasjon som kan kreve særlig beskyttelse.

Siste spørsmål ble belyst ved å søke etter idéer og råd om oppfølging av informasjonssikkerhet fra andre myndigheter i Norge og i utlandet.

1.3 Metode

Prosjektet har innhentet data gjennom litteratursøk og gjennom:

- Brev til bransjen med spørsmål
- Epost til et utvalg av myndigheter
- Telefonintervjuer med et par leverandører av AMS og forskere
- Møter med en stor programvareleverandør
- Møte med Braadlandprosjektet
- Workshop i NVE om AMS-sikkerhet 29. april 2015

Arbeidet er gjennomført som vist i følgende trinn, se Figur 1.1. Først beskrives trussel- og faresituasjonen. Deretter diskuteres skytjenester, så AMS- og bryterfunksjonaliteten og til slutt følger logging og hendelseshåndtering. Til slutt diskuterer vi policyen i noen utvalgte land før det i rapporten gis en anbefaling om hva NVE bør gjøre med regelverk, veiledning og samarbeid.

Figur 1.1 Arbeidsmetode

Arbeidet er gjennomført av et team i NVE bestående av:

- Seksjonsleder Arthur Gjengstø, NVE Beredskapsseksjonen
- Seksjonsleder Heidi Kvalvåg, NVE Elmarkedstilsyn
- Seniorrådgiver Frank Skapalen, NVE Beredskapsseksjonen
- Janne Hagen, NVE Beredskapsseksjonen (Forsker FFI)

Rapporten er ført i pennen av Janne Hagen.

2 Trusselbildet

I takt med digitaliseringen av samfunnet har også truslene mot både samfunnet og individet økt betydelig. Identitetstyveri, svindel, industrispionasje og etterretningsvirksomhet utføres i stor skala over Internett. Dette setter stadig større krav til myndigheters og virksomhetenes risikostyring og verdivurdering, men også hvordan enkeltpersoner vurderer risiko knyttet til sin tilstedeværelse på de ulike digitale arenaene.

For virksomheter vil risikoanalysene være viktige hjelpemidler for å belyse risikoeksponeringen ved bruk av IKT. Alle hendelser bør vurderes, også de man vanligvis ikke anser som særlig sannsynlige. Dette kapittelet gir derfor en introduksjon til bredden i trusselbildet.

2.1 Personvern

Beskyttelse av personopplysninger har vært årsaken til kritiske diskusjoner rundt innføringen av AMS i utlandet, særlig i USA og i Nederland. Målesystemet kan gi detaljerte opplysninger om hva enkeltpersoner gjør i hjemmet. Innføring av AMS innebærer at alle husstander får strømmåler som registrerer strømforbruket på timebasis og sender automatisk informasjonen om strømforbruket til nettselskapet. I tillegg kan nettselskapet kommunisere med måleren for for eksempel å oppdatere programvare i måleren eller stenge av strømtilførselen ved flytting, mislighold av betaling eller liknende. Personopplysningsloven stiller krav til hvordan nettselskapene kan bruke opplysningene, og et av kravene er å sikre informasjonen på en forsvarlig måte slik at ikke uvedkommende får adgang til den.

Datatilsynet mener løpende registrering og lagring av den enkelte husstands strømforbruk medfører en ikke ubetydelig trussel mot personvernet, og er kritisk til hvorvidt man trenger målerdata på individnivå for å kunne effektivisere driften av nettet.

Ved å analysere detaljerte data om strømforbruk kan det i fremtiden ifølge Datatilsynet være mulig å anta eller å forutsi når personene i hjemmet er på ferie eller på jobb, når de sover og er våkne.

Forbruksmønstrene kan være nyttige for å analysere vårt strømforbruk med tanke på for eksempel strømsparing. Men forbruksmønstrene kan også bli brukt til andre ting, slik som markedsføring og reklame. Politiet, skattemyndighetene, forsikringsselskaper, utleiere, arbeidsgivere og andre tredjeparter kan også være interessert i informasjon om det personlige strømforbruket.[4] Metadata brukes også i økende grad av sosiale medier og kontoer til digitale systemer for å logge bevegelser, aktivitet og kommunikasjon. Utfordringene er knyttet til digital identitet som gjør det mulig å forstå mer av personer, grupper og lokasjoner. Dermed øker sårbarheten for enda mer målrettede angrep mot personer, for eksempel mer «autentiske» spearphishing eposter.

The European Data Protection Supervisor (EDPS), advarer mot storstilt innsamling av måledata og mener denne må sikres forsvarlig. EDPS anbefaler videre at selskapene må innhente samtykke fra forbrukerne før nettselskapet bruker måledata til andre formål enn det som er nødvendig for å utføre virksomheten.[5]

NVE vedtok 8. juni 2015 regelverket som regulerer hvordan aktørene i kraftmarkedet og den nasjonale databasen for utveksling av AMS målerdata (Elhub) skal opptre når de får tilgang til AMS målerdata. Et viktig prinsipp er at det er strømkundene selv som bestemmer hvem som skal gis tilgang til egne strømdata. Statnett som har fått oppdrag å utvikle og drifte Elhub har brukt 'privacy by design' metodikk som utgangspunkt for sin kravspesifikasjon – se mer på www.elhub.no.

[4] «Automatiske målesystemer kan registrere adferd i hjemmet», Datatilsynet, 20.04.2015, URL: https://www.datatilsynet.no/Teknologi/Stromavlesing/

[5] "Smart meters: consumer profiling will track much more than energy consumption if not properly safeguard.ed, says EDPS", Press release, EDPS/10/12, Brussels, Monday 11 June 2012, URL: http://europa.eu/rapid/press-release_EDPS-12-10_en.htm?locale=en

Hvorfor er personvern relevant?

Juli 2014: Office of Personal Managemen (OPM) etterforsker innbrudd i datanettverket, innbruddet går tilbake til mars 2014.

August 2014: USIS (et selskap som tilbyr bakgrunnssjekk for U.S Department of Homeland Security ble hacket. Selskapet tilbyr 27 000 DHS ansatte kredittovervåkning selskapet AllClearID.

November 2014: En rapport fra den amerikanske riksrevisjonen (Office of Inspector general) finner store svakheter i departementets IT-sikkerhet.

Desember 2014: KeyPoint, et selskap som tok over bakgrunnssjekken for USIS opplever datainnbrudd. De hevder det er ingen bevis for at data er forsvunnet, men informerer 48439 offentlige ansatte om risikoen.

Februar 2015: Helseforsikringsgiganten Anthem avdekker datainnbrudd som har konsekvenser for 80 millioner kunder.

Mai 2015: Premera Blue Cross og Carefirst Blue Cross opplever datainnbrudd, 12,1 millioner kunder informeres om mulig tap av sensitive helseopplysninger. Selskapene tilbyr to års gratis kredittovervåkning.

Juni 2015: OPM avdekker innbrudd i sine systemer som berører 4 millioner offentlig ansatte og tilbyr 18 måneders gratis kredittovervåkning. Etterforskning av bruddet viser at bruddet også angår folk som har søkt om sikkerhetsklarering.Sporene går til kinesiske IP-adresser, men Kina nekter for dette, og viser til Snowden at USA selv er ansvarlig for storstilt datatyveri, avlytting og overvåkning.

Den viktigste lærdommen fra hendelsene over er overførbart til kraftbransjen – invester i sikkerhet. Sørg for å etterleve bestemmelsene i NVEs beredskapsforskrift. Sett egne mål og krav ut over dette.

NSM gir råd om hvordan du teknisk stopper 90% av alle angrep: Oppdater program- og maskinvare, vær rask med å installere sikkerhetsoppdateringer, ikke tildel administratorer sluttbrukerrettigheter og blokker kjøring av ikke autoriserte programmer.

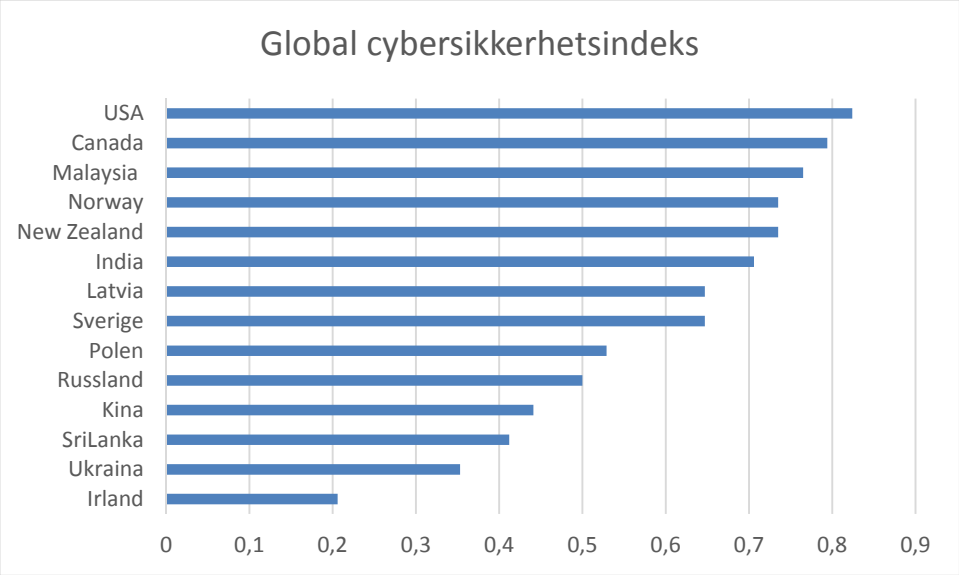
OPM-hendelsen viser hvorfor personvern er viktig.[6] [7] Personopplysninger koplet sammen med andre data som kan knyttes til samme personer kan misbrukes for vinningsformål og svindel.

[6]Catching Up on the OPM Breach, June 15, KrebsonSecurity, URL: http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

[7] Fire effektive tiltak mot dataangrep, Nasjonal sikkerhetsmyndighet, Oppdatert 2014-01-31, URL: http://nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf

2.2 Digital sikkerhetstilstand hos utvalgte land

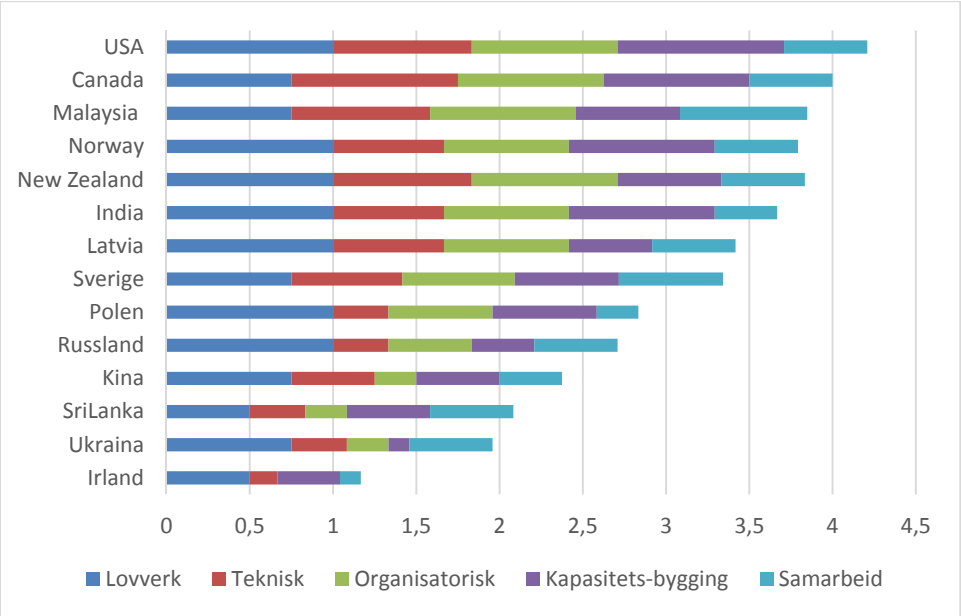
Internett og IT-support krysser fysiske landegrenser. Leverandører vedlikeholder teknisk utstyr i Norge fra andre land, og maskinvare og programvare blir levert av leverandører som har sin produksjon på andre siden av kloden. Dette er til en viss grad også situasjonen i kraftbransjen. Globaliseringen gir mange fordeler, ikke minst reduserte kostnader og tilgang til nødvendig spesialistkompetanse. Men globaliseringen gir også noen utfordringer i forhold til landrisiko. Det finnes flere indekser som gir sammenlignbar informasjon om sikkerhetsstatus på tvers av landegrenser. The Global Cybersecurity Index[8] er en slik indeks som måler modningsnivå på IKT-sikkerhet i ulike land.



Figur 2.1 Oversikt over utvalgte lands cybersikkerhetsstatus, korrupsjonsstatus og risikobilde for naturkatastrofer

Figur 2.1 viser at USA, Canada, Malaysia og Norge ligger på topp når det gjelder cybersikkerhet (IKT-sikkerhet). Ser vi nærmere på hva som ligger inne i cybersikkerhetsindeksen får vi opp bildet som vist i Figur 2.2 Cybersikkerhetsbildet i utvalgte land. Figuren viser en rangering.

[8] *Global Cybersecurity Index and Wellness Profiles*, ITU, April 2015, URL: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

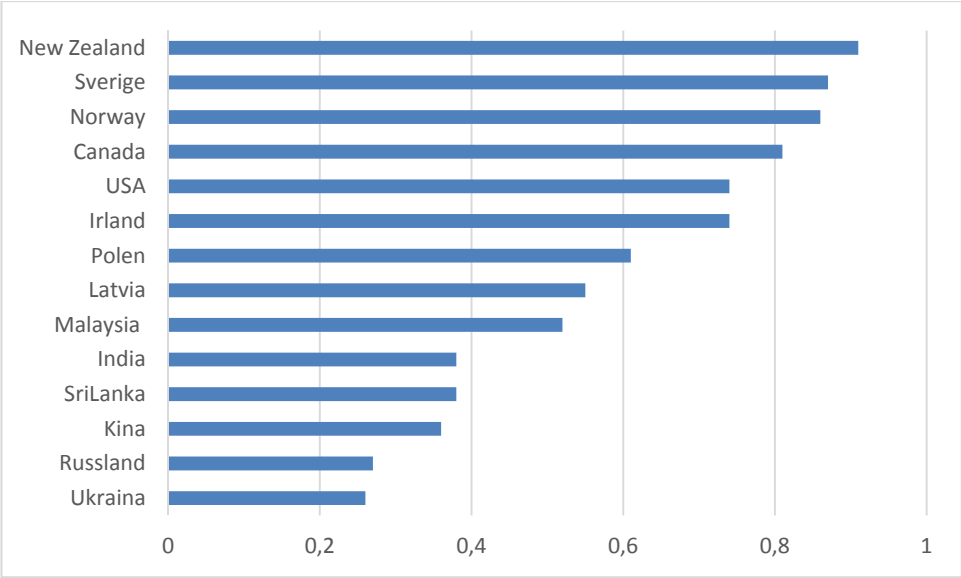


Figur 2.2 Cybersikkerhetsbildet i utvalgte land

Indikatoren «Lovverk» omfatter kriminallovgivning, regulering og compliance med lovene i landet. Indikatoren «Teknisk» omfatter i hvilken grad det er etablert CSIRT/CERT samt bruk av standarder og sertifiseringer. «Organisatorisk» omfatter policy, roadmap for cybersecurity, styring, ansvarlig myndighet og nasjonal benchmarking på området. «Kapasitetsbygging» inkluderer utvikling av standarder, kompetanse, profesjonssertifisering iht. internasjonalt sertifiseringsprogram samt sertifisering av institusjoner. Til sist omfatter «Samarbeid» samarbeid nasjonalt, sektorvis, offentlig-privat og internasjonalt. Figuren viser at USA ligger på topp, men Norge har en god plassering. Merk at Irland har ingenting på organisatorisk sammenlignet med andre land.

Sammenholdt med for eksempel korrupsjonsindeksen, som måler hvordan befolkningen oppfatter korrupsjon, får vi et bilde på sikkerhetssituasjonen i ulike land, se Figur 2.3. [9] Jo høyere verdi, jo bedre rangering og jo mindre korrupsjon i landet.

[9] *Corruption Perception Index 2014: Results*, Transparency International, URL: http://www.transparency.org/cpi2014/results#myAnchor1



Figur 2.3 Korrupsjonsindeks - befolkningens opplevelse av korrupsjon (jo høyere verdi desto mindre korrupsjon)

Korrupsjonsindeksen i Figur 2.3 viser dermed et noe annet mønster enn Cybersecurity Indexen i Figur 2.2. Så kan vi spørre hva god IKT-sikkerhet og gode systemer betyr hvis det er en oppfatning blant befolkningen i landet at korrupsjonsnivået er høyt? En åpenbar bekymring kan være myndighetenes tilgang til data som er lagret på servere i utlandet, jf. Snowden-avsløringene på hva som er mulig.[10]

2.3 Trusselaktørene tar ikke hensyn til landegrenser

2.3.1 Trusselen fra fremmede stater og myndighetenes mottiltak

I den senere tid har det blitt et økt fokus på at statlige aktører utgjør en stadig større trussel. Man har pekt på at fremmede makter i økende grad utfører industrispionasje for å tilegne seg teknologi og etterretningsvirksomhet for å innhente informasjon om kritisk infrastruktur. Og alt skjer gjennom Internett.

Får fremmede makter tilstrekkelig kunnskap om kritisk infrastruktur kan kunnskapen senere benyttes til å gjennomføre sabotasjeaksjoner. Flere stater utvikler eller ønsker å utvikle skadevare som potensielt kan brukes til å sabotere infrastruktur eller forstyrre kritiske samfunnsfunksjoner, og utviklingen minner mer og mer om et våpenkappløp[11]. Eksempelvis er amerikansk kritisk infrastruktur utsatt for målrettede angrep hver fjerde

[10] *Peace and Corruption 2015. Lowering corruption – a transformative factor for peace*, Institute for Economics and Peace, URL: http://www.visionofhumanity.org/sites/default/files/Peace%20and%20Corruption.pdf

[11] *Pentagon contractors developing lethal cyber weapons*, Nextgov.com, URL: http://www.nextgov.com/cybersecurity/2015/11/lethal-virtual-weapons-real/123417/?oref=ng-channelriver

dag. Dette gjelder både fysiske og logiske angrep, mens mindre logiske angrep skjer oftere[12].

Jakten på aktørene som utfører industrispionasje og etterretningsvirksomhet har ført til at myndigheter i flere land innfører lover som gir dem mulighet til selv å benytte skadevare eller andre teknikker for å overvåke nær sagt hvem som helst. Forslaget til fransk lov om overvåkning, som kom i kjølvannet av terroranslaget mot redaksjonen til satiremagasinet *Charlie Hebdo* i Paris, er ett eksempel på dette.[13] Lovforslaget innebærer at myndighetene har rett til å se alles epost, avlytte telefonsamtaler eller lese av tastaturet i realtid ved bruk av tilgjengelig teknologi. I Storbritannia trådte det 3. mai 2015 i kraft en lov som gir den britiske etterretningen og politiet rett til å bryte seg inn datamaskiner og mobiltelefoner uten rettslig kjennelse i forkant.[14] President Obama har også hevdet at den pågående økningen i angrep mot amerikanske virksomheter og kritisk infrastruktur representerer en nasjonal nødssituasjon. Som følge av det har han gitt klarsignal for at amerikanske myndigheter kan blokkere eller ta over ressursene til hvem som helst, i eller utenfor USA, som utfører eller er i ferd med å planlegge hackerangrep mot amerikanske interesser.[15]

2.3.2 Kommersialisering av kriminalitet på Internett

Tidligere var det kun stater som hadde kapasitet til å gjøre for eksempel etterretning og avlytting av aktivitet på Internett. De siste årene har det imidlertid vokst frem en stor kommersialisert kriminalitet på Internett, der det omsettes skadevare og tjenester for milliarder av kroner hvert år. Aktivitetene til disse aktørene er først og fremst økonomisk motivert, hvor svindel eller identitetstyveri av enkeltindivider eller virksomheter og finansinstitusjoner utgjør størsteparten av aktivitetene.

I dag kan hvem som helst kjøpe skadevare eller tjenester som gir deg mulighet til å avlytte og sabotere kommunikasjon og IT-systemer. Du trenger kun et kredittkort. RAND Corporation i USA har dokumentert det svarte markedet for skadevare og tjenesteleveranser innen digitale angrep.[16] I følge RAND er dette markedet nå modent, og trolig større enn narkotikamarkedet. I markedet for skadevare handler ulike aktører, både stater, organisasjoner og privatpersoner. Rapporten gir også innblikk i hva prisene er for ulike tjenester. Det at kapasiteter som tidligere var forbeholdt statlige aktører, nå kan kjøpes på det mer eller mindre åpne markedet, spenner ut risikoen med hensyn til hvilke aktører som kan tenkes å utgjøre en trussel.

---

[12] Santillan, M., "Once Every Four Days, The US Power Grid Is Under Attack", Apr 2, 2015, URL: http://www.tripwire.com/state-of-security/latest-security-news/once-every-four-days-the-us-power-grid-is-under-attack/

[13] Robert, A., French surveillance legislation is off to a bad start", Published 9th April 2015, Euractiv.com, URL: http://www.euractiv.com/sections/infosociety/french-surveillance-legislation-bad-start-313616

[14] Anthony, S., UK government quietly rewrites hacking laws to give GCHQ immunity, URL: http://arstechnica.com/tech-policy/2015/05/uk-government-quietly-rewrites-hacking-laws-to-grant-gchq-immunity/

[15] Schwartz, M.J., "Anti-Hacker Executive Order: 5 Concerns" , US Government Information Security, April 3, 2015, URL: http://www.govinfosecurity.com/anti-hacker-executive-order-5-concerns-a-8072,

[16] Ablon, L., Libicki, M.C., and A. A. Golay, *Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar*, RAND Nartional Security Research Division, Santa Monica CA, URL: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Det er også et faktum at legitime sikkerhetsprodukter kan ha en «dual-use» funksjon. Et eksempel på det er verktøyet Termineter, levert av SecureState. Verktøyet er egentlig laget for at selskapene kan teste sikkerheten i smarte målere og baserer seg på open source[17], men som sikkerhetsverktøy har det også en bakside hvis det brukes som ledd i et angrep.[18]

2.3.3 Et økt etterslep av sårbarheter

Den økte sikkerhetstrusselen har ført til økt satsting på tekniske sikkerhetstiltak, og som et resultat av dette har sikkerhetsindustrien vokst betydelig. Sikkerhetsproduktene har blitt svært avanserte, og har i noen grad gjort det mye vanskeligere for aktørene å komme seg inn i systemer kun ved hjelp av «tradisjonell» hacking. Derfor tyr aktørene stadig oftere til metoder for å omgå disse systemene. For eksempel kan det i mange tilfeller være enklere å bryte seg inn indirekte via menneskene som arbeider i organisasjonen ved hjelp av såkalt «sosial manipulering».[19]

Symantec™ Global Intelligence Network, har mer enn 41.5 millioner sensorer i 157 land som registrerer tusenvis av hendelser per sekund. Symantec rapporterer om økt spearphishing angrep der ansatte mottar tilsynelatende legitim epost med skadevare i form av et dokument eller en link. I dette kappløpet leder trusselaktørene foran sikkerhetsindustrien.

En av de store utfordringene enhver virksomhet har er å holde tritt med å lukke alle sårbarhetene som oppdages i de ulike systemene og protokollene. I tillegg kan enkelte leverandører bruke lang tid på å utvikle oppdateringer som lukker kjente sårbarheter. I januar 2015 ble det avdekket 494 sårbarheter; kun to sårbarheter ble lukket.[20] Denne avstanden gir også et bilde på risikoen. Når i tillegg sårbarheter i grunnleggende sikkerhetsmekanismer som SSL/TLS-protokollen blir avslørt, som skal sikre trygg pålogging på nettsider, da truer dette den grunnleggende tilliten og tryggheten til internettbaserte tjenester.[21]

---

[17] Securestate, Termineter, Nettside, URL: https://github.com/securestate/termineter nedlastet 19.03.2015

[18] Emil Protalinski, "Smart meter hacking tool released", Zero Day Net, 22. July 2012, URL: http://www.zdnet.com/article/smart-meter-hacking-tool-released/

[19] «Sosial manipulering», http://no.wikipedia.org/wiki/Sosial_manipulering, aksessert 11. juni 2015.

[20] *Symantec Intelligence Report*, January 2015.

[21] FREAK (the Factoring Attack on RSA-EXPORT Keys vulnerability or CVE-2015-0204) er en nylig oppdaget SSL/TLS. Det har tidligere vært avdekket andre sårbarheter i SSL/TLS sårbarhet som Hearthbleed og Poodle som skal sikre nettverkstrafikk, eksempelvis sikker pålogging HTTPS . Se FREAK attack: What is it? Here's what you need to know, published by Graham Cluley March 4, 2015 1:09, https://grahamcluley.com/2015/03/freak-attack-what-is-it-heres-what-you-need-to-know/ og https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204

2.4 Et norsk perspektiv på den målrettede trusselen

2.4.1 Norske sikkerhetstjenesters vurdering av trusselen

Også norsk kritisk infrastruktur er utsatt for trusler fra fremmede stater og fra kriminelle. Dette framgår av NSMs risikorapport for 2015. Den norske etterretningstjenestens åpne trusselvurdering framhever at etterretningsvirksomheten kan gi andre land innsyn i politiske, militære, kommersielle og intellektuelle forhold.[22]

Både Politiets sikkerhetstjeneste (PST) og Forsvarets etterretningstjeneste (E-tjenesten) fremhever at Russland og Kina har økt sine kapasiteter på industrispionasje og etterretning via Internett betydelig i de siste årene. I følge E-tjenesten har Russland over flere år hatt en målrettet satsing på oppbygging av kompetanse på Internettbasert etterretning. Kinesiske aktiviteter har derimot først og fremst til hensikt å understøtte landets økonomiske vekst og være et redskap for å innhente den vestlige verdens teknologiske forsprang. Av disse aktørene vurderer PST russisk etterretning til å ha det største skadepotensialet for norske interesser.[23]

E-tjenesten peker også spesielt på risikoen knyttet til skytjenester. Den store mengden informasjon som er lagret via skytjenester og mulighetene for å utnytte dem som en fleksibel og fordekt plattform for Internettbasert etterretning, gjør skytjenestene til attraktive mål. E-tjenesten fremhever at trusselen kan være i form av etterretning og bruk av utro tjenere inne i bedriftene.

2.4.2 Energisektoren også utsatt

Avansert Internettbasert etterretning kombineres og koordineres ofte med annen etterretningsvirksomhet. [24] I Norge ble det i 2014 satt søkelys på forsøk på angrep mot energibransjen da mange selskap, primært i olje- og gass-sektoren, ble forsøkt rammet av skadevare. Noen få sporadiske forsøk på å angripe kraftforsyningen ble også registrert. Blant annet ble Statnett forsøkt rammet uten at dette nødvendigvis betyr at det var et direkte målrettet angrep mot selskapet. Gjennom samarbeid og deling av informasjon mellom blant annet NorCERT og NVE, ble bransjen raskt varslet om trusselen. Totalt ble omtrent 200 selskap varslet av NVE som samtidig formidlet retningslinjer og instrukser til selskapene.

For kraftforsyningens del ba NVE selskapene om å gå igjennom logger av datatrafikken og egne nettsider.[25] Angrepsmetoden var spearphishing der angripere prøvde å komme seg inn ved å få brukere til å klikke på linker eller vedlegg i epost som synes å være legitim. Det ble imidlertid ikke registrert noen vellykkede angrep mot selskap i kraftforsyningen.

---

[22] *Etterretningstjenestens vurdering. FOKUS 2015*, URL: http://forsvaret.no/ForsvaretDocuments/FOKUS2015-endelig.pdf

[23] *Åpen trusselvurdering 2015*, PST, URL: http://www.pst.no/media/74351/PSTs_tv2015-2.pdf nedlastet 17.03.2016

[24] *Etterretningstjenestens vurdering. FOKUS 2015*, Forsvaret, URL: http://forsvaret.no/ForsvaretDocuments/FOKUS2015-endelig.pdf

[25] Jannicke Nilsen, «NVE: Dataangrep mot energiforsyningen, Ta datatrusselen på alvor», *Teknisk ukeblad*, URL: http://www.tu.no/it/2014/08/27/nve-ta-datatrusselen-pa-hoyeste-alvor,

Slike spearphishing-meldinger sendes ut i bølger: I 2014 var det registrert 841 bølger og 50 000 virus lastet ned til norske maskiner. Norge var ett av de 20 mest utsatte landene i verden for denne type angrep.[26]

2.4.3 Trusselen fra innsidere

Også ansatte og innleide konsulenter kan utgjøre en trussel. Mørketallsundersøkelsen for datakriminalitet 2006 (s 6)[27] peker nettopp på innsideren som trusselaktør. Nesten halvparten av gjerningsmennene var ansatte eller hadde oppdrag på innsiden av virksomheten ifølge undersøkelsen. Et eksempel på denne type trussel ble synlig i kraftbransjen da en utro tjener i Agder Energi ble dømt for å ha tappet Agder Energi for sensitiv informasjon. Han tok informasjonen med seg på en harddisk som inneholdt 800 dokumenter, og begynte å jobbe hos en konkurrent.[28]

En amerikansk studie viser at omtrent hver tredje utro tjener som har hatt tilknytning til en virksomhet har vært på kant med loven tidligere.[29] Bakgrunnssjekk i forbindelse med ansettelser og gjentagende personkontroll kan derfor være et viktig virkemiddel også i forbindelse med IKT-sikkerhet.

2.5 Ikke villede handlinger

2.5.1 Programvareoppdateringer og gjensidige avhengigheter

Selv om det er stor oppmerksomhet i pressen rettet mot målrettede angrep er det viktig å understreke at det ikke bare er målrettede angrep som utgjør trusler mot IKT-systemer og systemer som benyttes i kraftforsyningen. De aller fleste som jobber med IKT-drift har opplevd at systemer krasjer etter at man har installert en programvare- eller sikkerhetsoppdatering. For eksempel måtte Microsoft i desember 2014 trekke tilbake to programvareoppdateringer da de forårsaket trøbbel for enkelte prosesser som berørte mange kunder og brukere.[30] Dette viser at selv ordinære programvareoppdateringer kan få utilsiktede konsekvenser.

Naturhendelser, teknisk eller menneskelig svikt er også viktige årsaker til feilsituasjoner. Forskning viser at større antall koplinger og gjensidige avhengigheter mellom kraftnett og IKT øker risikoen for tilfeldige feil. Feil klassifiseres som kaskaderende[31] (som var årsaken til blackout i Italia i 2003), eskalerende[32] (som var årsaken til blackout i USA i

---

[26] Bakken, J.B., Christensen I. S. og M. Ånestad, «Tidenes hacker-angrep i Norge», Dagens Næringsliv, 26.08.2014, URL: http://www.dn.no/nyheter/2014/08/26/2159/IT/tidenes-hackerangrep-i-norge

[27] *Mørketallsundersøkelsen 2014*, NSR, URL: http://www.nsr-org.no/moerketall/

[28] «Dømt for å tappe kraftselskapet», NRK, publisert 11. mars 2015, URL: http://www.nrk.no/sorlandet/domt-for-a-tappe-kraftselskap-1.12254149

[29] Keeny et al, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, Carnegie Mellon Software Engineering Institute, May 2005. URL: http://www.google.no/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fwww.secretservice.gov%2Fntac%2Fits_report_050516.pdf&ei=4rwnVcjzOMelsgGBsoCYDw&usg=AFQjCNE5St461H5j-y4Iui58zlNMdKRlQQ

[30] Whitney, L. "Microsoft pulls buggy Patch Tuesday updates", cne.com, December 12, 2014, URL: http://www.cnet.com/news/microsoft-pulls-buggy-patch-tuesday-updates/

[31] Kaskaderende feil er feil som trigger en annen feil i et annet system.

[32] Eskalerende feil er uavhengige feil som styrker hverandre.

2003) og felles komponentfeil. Smarte nett øker kompleksiteten og vil i enda større grad enn tradisjonelle nett være avhengige av IKT. Man kan derfor forvente at risikoen for feil øker.

2.5.2 Klokkesynkronisering og arvede sårbarheter

Nettselskap bruker synkroniserte klokker fordelt i kraftnettet til overvåking og fordeling av belastning. Siden elektrisk energi forbrukes i det øyeblikk den blir produsert, må belastningen på nettet kontinuerlig overvåkes for å sørge for kontinuerlig balanse mellom produksjon og forbruk. Klokker benyttes også til tidsstempling av hendelser, overvåking av stabilitet og feilsøking.

Som en del av Smart Grid-utviklingen er det i Norge startet utplassering av høyoppløste fasemålingsenheter (Phasor Measurement Units - PMU) på sentrale steder i kraftnettet. PMUer benytter normalt GPS-klokker for å oppnå den påkrevede nøyaktighet på 1 mikrosekund.

Implementering av AMS og et fremtidig smart nett vil kreve nøyaktig og korrekt tid. Bruk av for eksempel GPS-klokker for nøyaktig tid medfører sårbarhet for romvær, interferens og hacking som rammer de satellittbaserte systemene som GPS-klokkene er avhengig av. Man kan da si at AMS akkumulerer eller arver sårbarheten fra satellittsystemer.[33] Arvede sårbarheter fås også fra offentlig EKOM i den grad de smarte målerne for eksempel bruker mobilnettet som kommunikasjonsmedium. Samme problemstilling om arvede sårbarheter fra EKOM er også gyldig for skytjenester som krever at data flyter i det offentlige EKOM-nettet både nasjonalt og globalt.

2.5.3 Lite sannsynlige eller utenkelige hendelser

En risikoanalyse skal vurdere alle typer uønskede hendelser. Enkelte hendelser kan man oppfatte å være svært lite sannsynlig eller nærmest utenkelig og gis derfor ikke særlig oppmerksomhet. Likevel bør man gjøre en kvalifisert vurdering av konsekvensen ved at disse typer hendelser oppstår.

Et eksempel på at en utenkelig hendelse der utilsiktede konsekvenser oppsto er hendelsen i Stockton, California i mars 2015. En lastebil kolliderte med en kraftmast, noe som førte til at toppledningen falt ned på ledningen under. Dette førte igjen til en overlastsituasjon, som i sin tur gjorde at AMS-målere fra PG&E eksploderte med ulike skadeomfang i hjemmene som ble rammet.[34]

Selv om man vanskelig kan sikre seg fullt ut mot denne type hendelser, er det viktig at man tenker gjennom slike scenarioer. En kan eventuelt gjøre en vurdering på hvilke slags konsekvensreduserende tiltak man kan gjøre dersom de likevel oppstår. På denne måten styrker man også evnen til å kunne håndtere denne type hendelser dersom de tross alt skulle oppstå.

---

[33] *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur*, Rapport, Norsk Romsenter, mars 2013. URL: http://www.romsenter.no/Aktuelt/Publikasjoner/Rapport-om-saarbarhet-ved-bruk-av-satellittnavigasjon

[34] Martinez, L. “Stockton Smart Meters Explode After Truck Causes Power Surge”, March 30, 2015, URL: http://sacramento.cbslocal.com/2015/03/30/stockton-smart-meters-explode-after-truck-causes-power-surge/

3 Avanserte strømmålere og bryterfunksjonaliteten

3.1 Kort om avanserte målesystemer (AMS)

Den Europeiske Kommisjonen definerer smarte nett som *an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added*.[35]

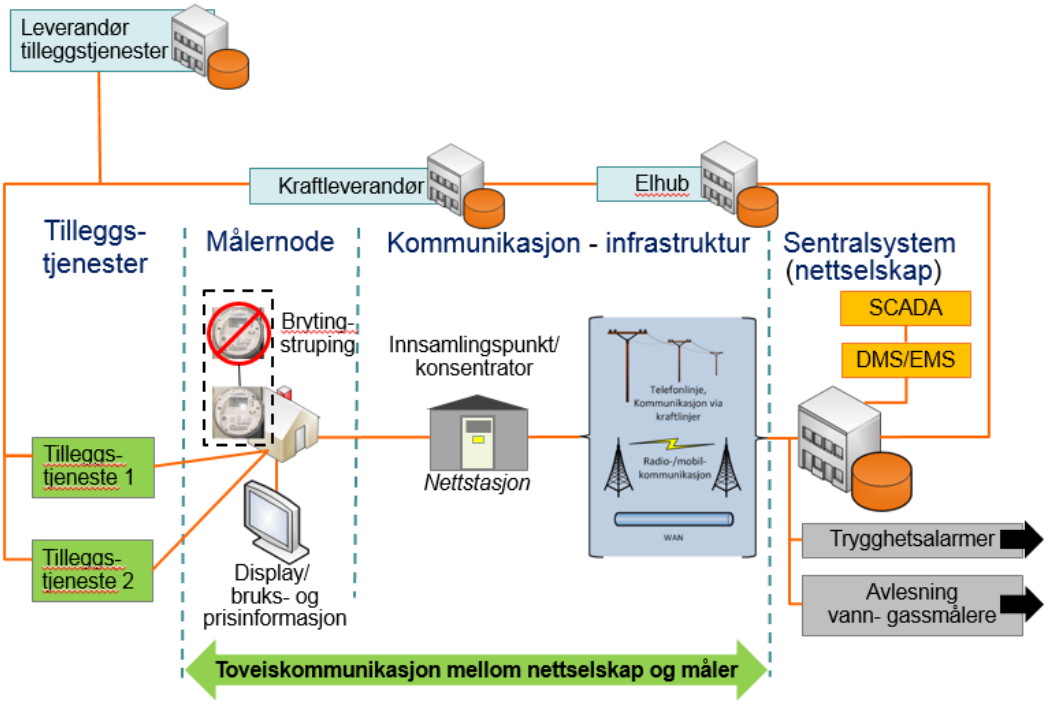
Lastprediksjon har tradisjonelt vært viktig i kraftbransjen på nasjonalt og regionalt nivå for kapasitets-, vedlikeholdsplanlegging og infrastrukturutvikling. Ettersom kraftnettet utvikler seg i retning av smarte nett, vil behovet for prediksjon av last også bli viktig i distribusjonsnettet. Behovet vil komme som følge av fremtidig integrasjon av andre energikilder, operasjon av nettkomponenter på lavere spenningsnivå, anomalideteksjon og beredskapsplanlegging. I ytterste instans er det snakk om også lastprediksjon for den enkelte husholdning.[36]

Avansert infrastruktur for måling og datautveksling består av underliggende kommunikasjonsinfrastruktur, sentralt måledatastyringssystem og mellomliggende datakonsentratorer, som fungerer som gateways mellom Elhub og målerne. Den sentrale måledatabasen består av flere deler hvorav kundedatabasen er den viktigste. Data fra de smarte målerne blir overført til styringssystemet. Både personvern og integritet skal ivaretas, og dataene skal i tillegg være tilgjengelige til tredjeparter som trenger dem til fakturering og service. Kommunikasjonsinfrastrukturen må tillate toveis kommunikasjon mellom målere og kontrollsenter for drift, styring og vedlikehold.[37]

[35] Smart Grid Security, Annex I. General Concepts and Dependencies with ICT, [Deliverable – 2012-04-19], ENISA, 2014.

[36] Tideman, A., Høverstad, B., A., Langseth, H. og P. Öztürk, "Effects of scale on load prediction algoritms", *22nd Internasjonal Conference on Electricity Distribution*, Stockholm, 10-13 June 2013, Paper 1205, URL: http://www.idi.ntnu.no/~helgel/papers/TidemannHoverstadLangsethOzturkCIRED13.pdf

[37] Se Egozcue et al, 2012a



Figur 3.1 Eksempel på en forenklet AMS-infrastruktur etter at Elhub er satt i drift. Tilkobling av signaler for trygghetsalarmer og avlesning av vann- og gassmålere kan i prinsippet være mulig innenfor en AMS-løsing.

3.2 Noen erfaringer fra AMS-utrullingen i USA og Europa

USA ligger foran Europa i utrullingen av AMS-målere. I 2011 hadde United States Government Accountability Office (GAO) en revisjon av moderniseringen av den amerikanske energi-infrastrukturen. GAO fant at selskapene fokuserte på å oppnå samsvar med regelverkets krav og en helhetlig sikkerhet. Derfor fant de mangel på sikkerhetsmekanismer i smarte nett. Det manglet en sterk sikkerhetsarkitektur og muligheter for logging og etterforskning, noe som var nødvendig for å analysere og oppdage angrep. Uten denne muligheten ville ikke selskapene kunne hindre angrep.[38]

I Europa er lovgivning på plass for utrulling og regulering av AMS, inklusive tidsfrister og tekniske spesifikasjoner. Kun fire land (Belgia, Bulgaria, Ungarn, Latvia og Litauen) har ikke lovgivning på plass.[39] JRC har laget en rapport om status og erfaring vedrørende utrullingen av smarte målere i Europa. Fra 2002 til 2014 har det blitt lansert totalt 459 AMS-prosjekter. Rapporten[40] peker på flere fordeler ved utrullingen av AMS, både for

[38] *Electricity grid Modernization. Progresss Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*., United States Government Accountability Office, GAO-11-117, January 2011.

[39] Se http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2014:356:FIN

[40] Covrig, C.F., Ardelean, M, Vasiljevska, J., Mengolini, A., Fulli (DG JRC) and E Amoiralis (External), *Smart Grid Project Outlook 2014*, JRC Science and Policy Report, URL: http://ses.jrc.ec.europa.eu/smart-grids-observatory

selskaper og for husholdningskundene, men det er også utfordringer for skalerbarhet og IKT-sikkerhet.[41]

Noen av utfordringene kan illustreres med erfaringer fra UK og Nederland. Utrullingen av AMS-målere er UKs største IT-prosjekt noen sinne, men det har vært kraftig kritikk mot prosjektet. Kritikken retter seg mot myndighetenes pålegg å rulle ut smarte målere, som i løpet av noen år vil bestå av gammeldags teknologi.[42]

Nederland har valgt en annen strategi basert på frivillighet. I Nederland kan kundene velge om de vil installere smarte målere eller ikke, og hvis de vil installere smarte målere kan de velge om kommunikasjonen med selskapet skal være aktivert eller deaktivert.[43] Bakgrunnen for dette er en stor diskusjon om målernes invasjon av private hjem, personvern og grunnleggende menneskerettigheter. Hyppig innhenting av forbruksdata gir mulighet for profilering av husholdningenes energibruk og levemønster. Det opprinnelige forslaget var obligatorisk installasjon med sanksjoner (bøter og fengsel) for dem som ikke ville installere målere.

Problematisk lovgivning på området, mangel på begrunnelse for hvorfor slik invasjon av privatlivet var nødvendig, og økt risiko gjorde at det ble vanskelig å se nytten av disse målerne. Saken ble først kritisert av det nederlandske datatilsynet og deretter av forbrukerorganisasjonene. I argumentasjonen ble det hevdet at måling på 4 timers basis avdekker når en person er hjemme eller ikke. Timesintervall avdekker brukerprofiler av elektrisk utstyr i hjemmet.[44]

I Sverige og Finland har de rullet ut lignende målere som de norske. Svenskene har laget en handlingsplan for perioden 2015-2030. Den sier at smarte nett vil gi mange positive fordeler, men også økt risiko. I følge rapporten er IT er den viktigste forutsetningen for smarte nett, men overgangen representerer mye høyere grad av automatisering og styring, og et mye større antall transaksjoner. Dette innebærer i sin tur økt risiko for målrettede angrep mot IT, risiko for mangel på riktig kompetanse, risiko for avvik i automatisk styring, risiko for at manglende standarder forvansker kommunikasjon, og til sist risiko for uklare ansvarsforhold. Rapporten peker på at kommunikasjonssystemene vil bli fylt med store mengder informasjon om kunders adferd og energibruk, og for å beskytte kundene må et stort og systematisk informasjonssikkerhetsarbeid gjennomføres. En

---

[41] Covrig, C.F., Ardelean, M, Vasiljevska, J., Mengolini, A., Fulli (DG JRC) and E Amoiralis (External), *Smart Grid Project Outlook 2014*, JRC Science and Policy Report, URL: http://ses.jrc.ec.europa.eu/smart-grids-observatory Side 64

[42] Lewis, D. and J. Kerr, *Not too clever: Will Smart Meters be the next Government IT disaster?*, IoD Policy Report.

[43] Weaver, K. T. ,"Dutch case study: "smart" meter privacy invasions are unjustifiable in a democratic society", Take Back your Power, Investigating the Smart Grid, 6 November 2014, URL: http://www.takebackyourpower.net/news/2014/11/06/smart-meter-privacy-invasions-are-unjustifiable-in-a-democratic-society/

[44] Cuijpers, C. M. K. C., & Koops, E. J.." Smart metering and privacy in Europe: Lessons from the Dutch case." In S. Gutwirth, R. E. Leenes, P. de Hert, & Y. Poullet (Eds.), *European data protection: Coming of age.* Unknown Publisher. 2012: 269-293.

mulighet er å bygge inn funksjoner i tjenestene som blir utviklet, såkalt «privacy by design» eller innebygd integritet.[45]

I Finland er det Landis+Gyr som er markedsleder på smarte målere med total markedsmakt hos finske husholdninger (98%).[46] Det er ikke funnet evalueringsrapporter av den finske utrullingen utover sammenstillingsrapporter fra EU. Det er etter det NVE kjenner til så langt ikke avdekket misbruk av bryterfunksjonaliteten i AMS-målerne som finnes i Sverige og Finland.

3.3 Sårbarheter i AMS

3.3.1 Risiko som gir høyest konsekvens

SINTEF utførte i 2012 en overordnet risikovurdering av AMS for NVE.[47] Vurderingen omfattet hovedsakelig AMS basisfunksjoner.

I rapporten er det beskrevet en generell AMS infrastruktur med de avgrensningene som er gjort for dette arbeidet. Deretter er det gjort en vurdering ut ifra et informasjonssikkerhetsperspektiv, hvor konfidensialitet, integritet og tilgjengelighet er de viktigste aspektene. Ulike scenarioer og hendelser er presentert og diskutert, og de hendelsene som er vurdert til å ha høyest risiko, har ett eller flere av følgende elementer i seg:

- Uønsket utkobling hos mange kunder
- Programvarefeil
- Sentralsystemet feiler eller brukes i angrepet
- Utro tjener; egen ansatt misbruker kunnskap og/eller legitime tilganger

I tillegg er et scenario med mange målere ute av drift samtidig vurdert til å være kritisk, uten at årsaken trenger å være et målrettet angrep. Dette er fordi konsekvensene vil medføre store kostnader for reparasjon og/eller utskiftning av teknisk utstyr. Ondsinnet programvare vil kunne være årsaken, eller et verktøy i flere av hendelsene, særlig ved angrep som kjøres langveisfra (fjerntilkobling).

3.3.2 Latente tekniske feil og svakheter

Bryterne består av hardvare, fastvare og programvare, samt mindre applikasjoner på toppen av måleren. Software vil måtte bli oppdatert oftere enn selve måleren. Slik oppdatering gjør leverandøren, som kan være et internasjonalt selskap. En vil aldri kunne garantere 100 % sikkerhet i komponenter som består av maskinvare, fastvare og programvare. Det er altfor mange tusen kodelinjer å sjekke, dessuten sjekkes ikke kompilatoren som oversetter den programkoden til maskinlesbar kode, dvs. 0 og 1. Det vil alltid medfølge en viss risiko for at det ligger latente feil eller bakdører i slike komponenter.[48]

---

[45] *Planera för effekt. Slutbetenkande från Samordningsrådet för smarta elnät*, SOU 2014:84, s 283.

[46] "Landis+Gyr rolls out smart meters to 98 percent of Finland homes", 02.06.2014, Electric lights power, URL: http://www.elp.com/articles/2014/02/landis-gyr-rolls-out-smart-meters-to-98-percent-of-finland-homes.html

[47] Line M. B., Johansen G., Sæle H., «Risikovurdering av AMS», SINTEF 2012.

[48] Foredrag av Olav Lysne på KBO-møte hos NVE 19.03.2015.

3.3.3 Veier inn i målerne

Det er allerede vist at smarte målere kan hackes, at radioantenner kan avlyttes, at signaler kan stoppes eller måleren fysisk modifiseres når den ikke er godt fysisk beskyttet. Dette synet er støttet av internasjonale sikkerhetseksperter som advarer mot sårbarheter og fare for misbruk i AMS.[49] Gitt at man ikke har gode sikkerhetsløsninger, er målerne sårbare for kriminelle handlinger. Både innsidere og personer med moderate datakunnskaper vil sannsynligvis kunne kompromittere målerne med lavkostnadsverktøy og programvare som er tilgjengelig på Internett. Trusselen er forventet å øke med utrullingen av målerne, og det er allerede eksempler i USA på at selskap har tapt store økonomiske beløp på misbruk og kompromittering.[50][51]

Det er to måter å bryte seg inn i målerne på: Gjennom kommunikasjonsnettet som ofte overfører data via et SIM-kort eller gjennom å bryte seg fysisk inn i måleren og ødelegge hardvare og fastvare. I følge BBC har energiselskap i UK vært lite villige til å bruke bredbånd som hver husholdning har fordi de da kan bli ansvarliggjort nettopp av hensyn til trusselen fra hacking.

Det at målerne må være så billige som mulig for at man skal ha råd til å rulle dem ut er også en sikkerhetsutfordring. Den største bekymringen er derimot om noen bryter seg inn og fjernstyrer systemet.[52] Da er det naturlig å tenke på kryptering som et tiltak, men det er flere utfordringer relatert til kryptering: ENISA peker på sårbare kommunikasjonsprotokoller som er designet uten innebygd sikkerhet i form av kryptering fra begynnelsen av.

3.3.4 Økt endepunktsårbarhet?

Endepunktsårbarhet en annen utfordring. Med utrulling av AMS vil antall endepunkt øke formidabelt. Vazquez Vidal og Garcia Illera testet i 2014 avanserte målere, og alle lagret den samme AES-128 symmetriske krypteringsnøkkelen i en mikrochip i boksen, i lesbar form. Ergo var det mulig få tak i nøkkelen.[53] ENISA sin store bekymring er at angrep der en før måtte utnytte mange sårbarheter for å komme forbi flere nivåer av barrierer nå kan gjøres gjennom et enkelt angrep mot AMS-endepunkter. ENISA sier følgende: *Regulations should focus on pointing – by means of promoting best practices or policy actions – the way ahead so as to guide vendors and utility companies in considering security from a holistic point of view.*[54] Endepunkter er ikke bare selve målerne. Ponemon Institute peker på økningen i risiko i endepunkter som mobile enheter, bruk av

---

[49] Hamill, J., "UK smart meters arrive in 2020. Hackers have ALREADY found a flaw", The Register, 30 Oct 2014, URL: http://www.theregister.co.uk/2014/10/30/smart_meter_hackable_for_free_electricity_say_security_reseracher s/

[50] Krebs, B., "Smart meter hacks likely to pread: FBI", Theage.com, April 10, 2012, URL: http://www.theage.com.au/it-pro/security-it/smart-meter-hacks-likely-to-spread-fbi-20120410-1wm84.html,

[51] I 2009 etterforsket FBI et vidtrekkende strømtyveri som var relatert til utrullingen av smarte målere.

[52] Kleinman, Z, "Smart meters need to be harder to hack, experts say", BBC News, 25 May 2013, URL: http://www.bbc.com/news/technology-22608085

[53] Higgins, K.J., "Smart Meter Hack Shuts Off The Lights", InformationWeek, 10.01.2014, URL: http://www.darkreading.com/perimeter/smart-meter-hack-shuts-off-the-lights/d/d-id/1316242,

[54] Egozcue et al, 2012b, s 11

hjemmekontor og kommersielle skyapplikasjoner. Hele 80% av de 702 amerikanske IT-praktikerne fra ulike bransjer hadde sett regelmessig skadevare i sine nett. Kunnskapsløse ansatte var største risikofaktor. Ponemons forskning trekker fram tre strategier for å håndtere risikoen i endepunktene: Oppdage og håndtere hendelsene, trussel-etterretning og til sist bruke sluttpunktet som en sikkerhetssensor.[55] Det er et spørsmål om lignende strategier også kan vurderes i AMS.

3.3.5 Interessemotsetninger rundt sårbarheter i AMS

Struping eller bryting av effekten i AMS-måleren er pålagt i *Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester* (MAF), og gjelder alle kunder unntatt trafomålte anlegg. Det tilsvarer vel 50% av det totale strømforbruket i Norge. Nettselskapene er dermed pålagt å kjøpe utstyr som har bryter og mulighet for struping

Målerne og infrastrukturen er sårbare for rettede menneskeskapte trusler, sikkerhetsrutinebrudd, utstyrsfeil, likegyldighet og naturhendelser. [56] Anderson og Fuloria[57] peker på seks sikkerhetsbekymringer og interessekonflikter i forbindelse med utrulling av AMS:

- Industrien frykter svindel som kan gi tap.
- Personvernaktivister er bekymret for detaljmålingenes konsekvenser for personvernet.
- Bryterfunksjonen kan lede til en strategisk sårbarhet der en aktør med kapasitet kan stenge av strømmen via nettet i stedet for å bombe og sabotere anlegg.
- Det er interessekonflikter mellom myndigheter som vil kutte energibruk mens selskapene vil ønske å maksimere salg, og konkurransemyndighetene vil være bekymret for innlåsing til en leverandør.
- Det er en fare for over-regulering på den ene siden, men samtidig mangler det felles standard for kommunikasjon og arkitektur slik at systemene kan kommunisere og samvirke.

Enkle søk på Google og Youtube viser flere artikler som omhandler sårbarheter i smarte målere. Bekymringen er knyttet til personvern (konfidensialitet) og til integritet (i forhold til fakturering og prosesskontroll for kraftsystemet som helhet).

3.4 Bryte- og strupefunksjonen i AMS

3.4.1 Strategiske sårbarheter

En av problemstillingene som debatten har reist, er at målerne ikke eies av huseierne, men av nettselskapet. Dermed kan huseierne selv ikke gjøre noe selv med sikkerheten, men er prisgitt at nettselskapet sikrer målerne. Kombinasjonen av kommandoer, som vil få målerne til å stoppe strømforsyningen, av applikasjoner og programvareoppdateringer som kjører i målerne, og av krypteringsnøkler som brukes for å autentisere disse

[55] *2015 State of the Endpoint Report: User-Centric Risk*, Ponemon Institute Research Report January 2015.

[56] Se Egozcue et al, 2012b

[57] Anderson, R and S., Fuloria, “Smart meter security: a survey”, *Cambride University*, URL: www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf

kommandoene, skaper nye strategiske sårbarheter og utfordringer. Vi vil framheve noen forhold:

Det første er toveiskommunikasjonen og hvordan denne er sikret. Noen lar kommunikasjonen gå via offentlig ekomnett, andre via nettselskapets egen kommunikasjonsinfrastruktur.

Det andre er hvordan disse målerne er koplet opp mot driftskontrollsystemene. Dersom en skal kunne fullt ut utnytte styringsmulighetene denne infrastrukturen av smarte målere gir, er det vanskelig å se for seg at det kan oppnås uten kopling til driftskontrollsystemet på en aller annen måte. Dersom det er frakoplet, vil dataene bare være en tilleggsinformasjon som man kan ta hensyn til manuelt, men da må operatøren ha to skjermer. Spørsmålet er om operatøren klarer å håndtere informasjonen til enhver tid når alarmer og feilsituasjoner fort kan oppstå hele tiden.

Det tredje er hvor kritiske installasjonene er som får påmontert AMS-måler. AMS-målere skal installeres i utgangspunktet på alle målepunkt unntatt trafomålte. Spørsmålet er om viktige tekniske systemer som for eksempel basestasjoner i telenettet, vifteanlegg og pumper i tuneller, fyrlykter langs kysten etc. kommer inn under denne gruppen, og om det kan ligge noen utilsiktede samfunnsmessige konsekvenser her. Anleggene kan være sårbare for datainnbrudd.

På pluss-siden vil nettselskapet få bedre mulighet til å detektere strømbrudd med AMS.

Til sist har Anderson og Fuloria[58]en god diskusjon på sikkerhet i AMS og bryterfunksjonaliteten i sær. De hevder at bryterfunksjonaliteten og nedkopling av flere brukere vil kunne bære et politisk budskap i enkelte land, så vel som være en inntektskontrollsak, bidra til topplast utjevning og til siste også representere et spørsmål om nasjonal sikkerhet.

3.4.2 Tilgang til og bruk av bryter- /strupefunksjonaliteten

Ulike forhold vedrørende tilgang til bryter-/strupefunksjonaliteten bør vurderes ut fra hvilke konsekvenser feil bruk av bryter-/strupefunksjon kan ha for kraftsystemet.

Viktige forhold knyttet til bryter-/strupefunksjon er bl.a.:[59]

- Hvordan skal bryter-/strupefunksjonalitet implementeres og hvem skal ha tilgang til hva? F.eks. kan en person på kundeservice få tilgang kun til bryting/struping av en eller flere kunder, mens en person fra driftssentralen kan få tilgang til bryting/struping til flere kunder i et større område.
- Fra hvilke(t) system sendes styresignaler fra? (f.eks. driftssentral eller kontor hos kundeservice?)
- Når skal bryter-/strupefunksjonen benyttes? (i en beredskapssituasjon eller kun normal drift?)
- Hvilken stilling skal bryter gå til dersom AMS svikter? I de fleste tilfeller vil fornuftig oppførsel være at bryter vedvarer å være i samme stilling som før AMS sviktet.

[58] Anderson og Fuloria (2010).

[59] Hentet fra Line, M.B., Johansen, G., Sæle H.; «Risikovurdering av AMS», 2012.

- Hvilken konsekvens vil det ha for kraftsystemet hvis ikke bryter-/strupefunksjon fungerer? (ikke kobler ut/senker grense for effektuttak, eller ikke kobler inn/øker grense for effektuttak?)
- Hvilken konsekvens vil det ha for kraftsystemet hvis eksterne får tilgang til bryter-/strupefunksjonaliteten i AMS?
- Vurdere om deler av forbruket til en kunde skal fritas fra bryter-/strupefunksjonalitet? Det innebærer bl.a. å vurdere motstridende forhold som å begrense hvor mye som kan kobles ut hos en kunde, og dermed begrense konsekvensen ved at en fremmedaktør klarer å koble ut forbruk hos flere kunder, samtidig som at bryter-/strupefunksjonen ikke skal kunne overstyres av en kunde i en rasjoneringssituasjon.

I tillegg har flere nettselskap allerede outsourcet måledatainnsamlingen og har etablert avtaler om at leverandører står for drift og vedlikehold av AMS-løsningen. Dette øker risikoen for at nettselskapene – som tross alt har ansvaret – ikke fører tilstrekkelig kontroll med at avtalene og sikkerhetskravene etterleves av leverandørene.

3.5 Bransjens og leverandørenes risikobevissthet knyttet til AMS

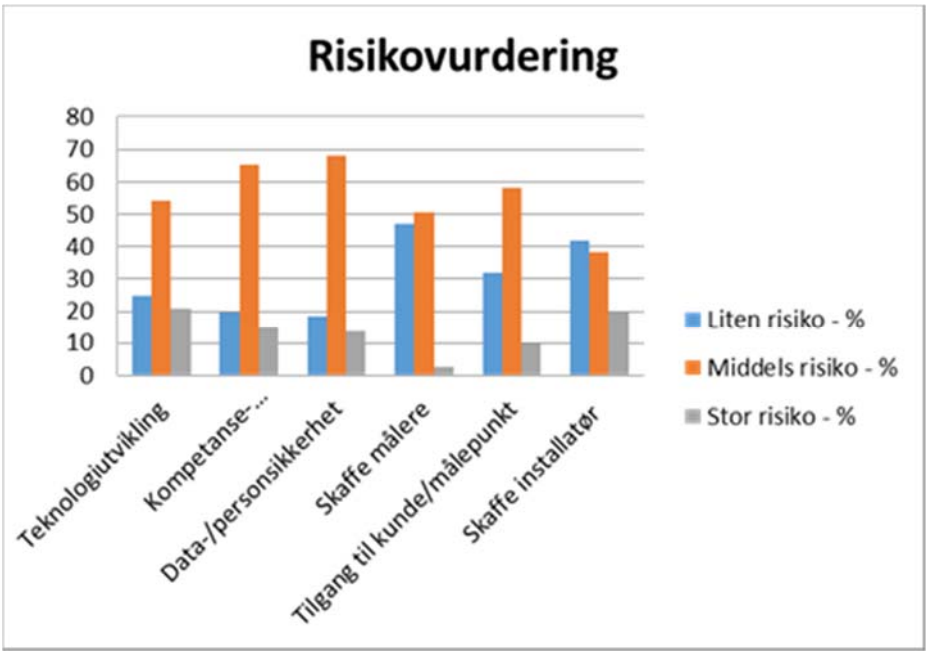
Som et ledd i oppfølgingen av AMS-utrullingen har NVE gjennomført en spørreundersøkelse der selskapene blant annet ble bedt om å gi en vurdering av om ulike risikofaktorer medfører liten, middels eller stor risiko i forhold til AMS-løsningen i deres selskap. I tillegg inviterte NVE til en workshop 29. april 2015 der formålet var å utdype selskapenes oppfatning av risiko knyttet til utrullingen og drift av AMS-løsningene.

3.5.1 Spørreundersøkelse om risikobevissthet i forbindelse med valgt AMS-løsning

3.5.1.1 Risikooppfatning i forhold til egen løsning

I spørreundersøkelsen ble selskapene blant annet bedt om å gi en vurdering av om ulike risikofaktorer medfører liten, middels eller stor risiko i forhold til den valgte AMS-løsningen i deres nettselskapene.

Resultatet er vist i Figur 3.2. De fleste selskapene vurderer risikoen knyttet til om systemet er sikkert nok både mot misbruk av data og uønsket tilgang til styrefunksjoner, hacking mv., som middels. Sett i forhold til et bekymringsfullt sårbarhetsbilde, men fortsatt få reelle hendelser, viser dette at bransjen er oppmerksom på utfordringene.



Figur 3.2 Resultat fra NVEs survey om AMS[60]

3.5.2 Leverandørenes sikkerhetsbevissthet

Flere nettselskap har pekt på at det er stor variasjon i leverandørenes sikkerhetsløsninger. Inntrykket er at i tidlig anskaffelsesfase hadde ikke alle leverandørene et bevisst forhold til IKT-sikkerhet. For å få spesifisert tilstrekkelig sikkerhet i løsningene, hadde flere nettselskaper benyttet NVE sin veileder og annet veiledningsmateriale på nett. Enkelte hadde også engasjert eksterne konsulenter for å få assistanse i forbindelse med sikkerhetsproblematikken og for å få stilt sikkerhetskrav til leverandørenes løsninger. Som følge av blant annet leverandørenes modenhet på enkelte områder, var noen krav, som for eksempel PKI og kryptering, hos samtlige som deltok på NVE-workshopen et «bør»-krav og ikke et «må-krav». Alle hadde derimot stilt krav om at sikkerhetsløsningen på sikt bør kunne tilpasses til et endret trusselbilde. [61]

Samtaler med leverandører som deltok i anbudsprosessen har bekreftet virksomhetenes oppfatning. Leverandørene uttalte at de ikke hadde tenkt så mye på sikkerhetsløsninger i starten av prosessene. De mente de norske kravene var sære sammenlignet med internasjonale krav. En av de store leverandørene som deltok i anbudsprosessen i Norge, sa for eksempel at de ikke møtte tilsvarende krav til sikkerhet i målerne i andre markeder som de opererte i, globalt.

---

[60] Teknologiutvikling: Hvordan vurderer nettselskapene risikoen for å sitte igjen med gammeldags/innelåst teknologi som resultat? Kompetanse/ressursbegrensninger: I hvilken grad vurderer nettselskapet at tilgangen på eget personell og faglig kompetanse vil begrense eller påvirke AMS-utrullingen? IKT-/datasikkerhet: Er det en risiko knyttet til om systemet blir sikkert nok både i forhold til misbruk av data og uønsket tilgang til styrefunksjoner, hacking etc.?
Anskaffe målere tidsnok: Er det noen risiko knyttet til at leveringstiden på målere er så lang at det påvirker tidsplanen? Tilgang til målepunkt: Hvordan vurderer nettselskapene risikoen for at manglende tilgang til målepunkt gjør det vanskelig å nå tidsfristen om utrulling innen 2016?

[61] Basert på svarbrev og diskusjon på workshopen hos NVE 29. april.

3.5.3 Risikoanalyse som læring

Kompetanse om informasjonssikkerhet og personvern knyttet til AMS-løsninger er mangelfull selv om det stadig blir bedre. En av de største utfordringer internt er å få tilstrekkelig god bevissthet hos ansatte. I følge enkelte nettselskap og AMS-sammenslutninger har det å gjennomføre en ROS-analyse en læringseffekt i seg selv. En erfaring er at risikoanalysene bidrar til å få et overordnet blikk, men de spesifikke problemstillingene for IKT-sikkerhet får man ikke like godt fram via analysene. Mange har fokus på å gjennomføre risikoanalyse, men det er vel så viktig å bruke den også som grunnlag for å lage en beredskapsplan[62].

3.5.4 Bransjens oppfatning av risiko ved egen drift av AMS-løsningen

I workshopen NVE arrangerte 29. april 2015 ble deltakerne presentert for to ulike driftsmodeller for AMS-løsningen. I den ene modellen drifter selskapet alle systemer selv, og i den andre var driften av AMS-løsningen satt ut til en ekstern driftsleverandør. Diskusjonen om hvilke digitale sårbarheter som følger med disse to ulike driftsmodellene i workshopen oppsummeres under.

3.5.4.1 Uautorisert tilgang

Dersom noen klarer å gjennomføre et tjenestenektangrep i et nabolag, vil dette frata muligheten til å sende og motta informasjon og dermed styre bryterne i AMS-målerne. Ved uautorisert tilgang til målenoden kan man potensielt styre bryteren i nabohuset. Tilsvarende vil uautorisert tilgang til sentralsystemet i AMS-løsningen (DMS) kunne gjøre det mulig å manipulere brytere i AMS-målerne. Samme konsekvens kan oppnås dersom driftskontrollsystem og DMS koples sammen. Dessuten vil en slik sammenkobling kunne gi muligheter for manipulering av data.

Utro tjener i eget selskap eller hos leverandøren er også en trussel. Dersom noen får uautorisert tilgang kan vedkommende tappe systemet for informasjon og i verste fall overta styringen av hele systemet. Det trengs i dette tilfellet bare en markedsaktør som misbruker data, og det kan få omdømmekonsekvenser for selskapet. Dersom fremmede stater har interesse av å sette ut kraftforsyningen i Norge, er det et verre scenario.

3.5.4.2 Arvet sårbarhet fra offentlig kommunikasjon

AMS-systemet som helhet avhenger av kommunikasjon. Her bruker nettselskapene ulike løsninger, men kommersielle ekomtjenester benyttes i svært stor grad. En problemstilling som ble tatt opp var redundans i kommersielle ekomtjenester. Det ble pekt på at det er mulig å bygge redundans til et visst punkt, men når man kommer til leverandører av kommersielle ekomtjenester, har disse gjerne et eller annet single-point-of-failure. Et mulig tiltak er to helt uavhengige leverandører. Problemet er at i Norge er det mange leverandører som henger på Telenors kjernenett.

3.5.4.3 Endringshåndtering og konfigurasjonsstyring

AMS-systemet er komplekst, og det er mange grensesnitt som selskapet må ha kontroll med. Systemet kjennetegnes av at det er mange gjensidige avhengigheter mellom ulike komponenter. Det er avhengigheter til eksterne systemer som elektroniske

[62] Basert på svarbrev og diskusjon på workshopen hos NVE 29. april.

kommunikasjonssystemer, satellittbaserte tjenester og strømforsyning til hele AMS-løsningen.

Et annet grensesnitt er den fysiske tilgangen til for eksempel måleren og hvordan måleren fysisk er beskyttet. Måleren er nettselskapets eiendel og det er selskapets ansvar å beskytte den. Disse grensesnittene mellom ulike komponenter må beskyttes, og da må en legge til grunn et helhetsperspektiv på sikkerheten, der tilgangskontroll og trafikkontroll er to elementer. Det er derfor viktig å sikre fysiske grensesnitt siden selskapet «går inn i huset til folk» med AMS.

Det er ulike implementasjonsmodeller for bryterstyring. Infrastrukturen er bygd opp med mange lag med sikkerhet, men så lenge det er en logisk kopling så kan det være en mulig vei inn.

Endringshåndtering i driftskontrollsystemet er ett av kravene i Beredskapsforskriften. Det er ingen slike krav for AMS-løsningen, men det vil likevel være krevende å holde oversikt over og få verifisert at alle målerne er oppdatert og riktig konfigurert. Noen leverandører sender konfigurasjonsdata til nettselskapene som selv gjennomfører oppdateringen dersom nettselskapet drifter AMS-løsningen selv. Det er gjerne stor tillit til leverandøren og at oppdateringene fungerer som de skal, og en tilfeldig feil vil da kunne få utilsiktede konsekvenser et annet sted i verdikjeden. Et tiltak er et godt dokumentasjonssystem for konfigurasjonsendringer og systemarkitektur. Det er også viktig at programvaren fra leverandøren er signert av leverandøren. Det vil bidra til å redusere risikoen for infeksjon med skadevare.

3.5.4.4 Overvåking, logging og hendelseshåndtering

Systemkompleksiteten gjør at det blir viktig å kunne oppdage unormal og utilsiktet trafikk. Nettselskapene eier AMS-kanalen og har ansvaret for sikkerheten der. Leverandører har hevdet at trafikk fra målere er lett å gjenkjenne – det danner seg et mønster. Ved å overvåke og logge datatrafikk og være i stand til å analysere loggene, kan en skille ut uvesentlige feil mot det en bør agere på.

For å oppdage om måleren er fysisk manipulert kan en for eksempel se på adferden til sensorene. Det er ikke sikkert at en hendelse betyr noe alene, men dersom en kan se den i sammenheng med andre hendelser, så kan det gi et annet bilde.

Selskapene har investert mye i AMS-løsningene. Dersom selskapene ser inntektsmuligheter, så vil det kunne komme nye tjenester. Det er videre ytret et ønske om at NVE gjør det tydelig hvilke andre bruksmuligheter AMS åpner for. Så langt har NVE standardisert at det ut mot kundene av nettselskapene kun skal være et lesegrensesnitt.

3.5.4.5 Utpressing og svindel

I workshopen hos NVE var selskapene bevisste på at utpressing og svindel har forekommet i utlandet og kan også treffe kraftbransjen i Norge. Slike scenarier må en derfor ta høyde for ved å tenke igjennom på forhånd hvordan en skal håndtere denne type situasjon dersom den oppstår.

3.5.4.6 Trusler mot bryterfunksjonen i AMS

Det var enighet blant selskapene på workshopen om at en enda mer alvorlig situasjon kan oppstå dersom noen uautoriserte overtar styringen av AMS-bryterne og setter i gang

masseutkopling. Bryterfunksjonen har både en fordel og en risiko, men trusselen om innbrudd i systemene må settes inn i et større perspektiv og vurderes opp mot andre trusler. Uansett må selskapene ha beredskapsplaner for hvordan et stort uønsket utfall skal håndteres, og likeså planer for tilbakerulling av programvare dersom systemet er infisert med skadevare. Et tiltak er å øve. Teknisk sikkerhet hjelper lite hvis det ikke øves. Poenget er å trene folk til å se sammenhenger og samarbeide.

3.5.4.7 Kompetanse og ledelsesfokus

Flere deltakere på workshopen pekte på kompetanseutfordringen. Det er krevende å være en god bestiller. Når systemet kommer i drift kan det være en utfordring å være profesjonell nok. Særlig små selskaper kan komme til å slite med dette. I enkelte selskap er ansvaret gitt til kun én person, som da må dekke et svært bredt fagområde. Fagområdet kan strekker seg fra prosesstyring til IKT-sikkerhet. Å drifte kommunikasjonsinfrastruktur er et nytt fagområde for en del nettselskap. En workshop-deltaker pekte på at kraftbransjen er preget av «dette fikser vi»-holdning, men det er ikke like riktig når det kommer til sikkerhet. Et tiltak er å bygge opp egenkompetanse på området.

I enkelte selskap er det en utfordring å nå fram med forståelse for sikkerhetsproblemstillinger hos ledelsen. Tiltak som bøter på dette kan være at NVE bidrar med klarere retningslinjer og mer målrettede tilsyn på området.

3.5.5 Kraftbransjens oppfatning av sårbarheter relatert til at AMS-løsningen driftes av en ekstern driftsleverandør

I følge Sæle, Sagosen, og Bjørndalen (2014) drifter 70% av nettselskapene sin egen AMS-løsning, men dette bildet kan endres i framtida. Under gis en sammenstilling av sårbarheter som bransjen selv har pekt på i relasjon til outsourcing.

3.5.5.1 Forhold knyttet til leverandørens leveranser

Når en ikke drifter selv, er det vanskelig å bygge opp tilstrekkelig med kritisk kompetanse i eget selskap. Som regel er årsaken til at selskaper velger å benytte en ekstern driftsleverandør at de mangler kompetanse selv, mens de eksterne kravene og kompleksiteten bare fortsetter å øke.

Når selskaper velger å benytte en ekstern driftsleverandør er risikoen stor for at man gjør seg avhengig av leverandøren. Store leverandører med bredde i tjenestetilbudet har ikke nødvendigvis kunnskap om nettselskapets samlede system som AMS-systemet blir en del av. Utfordringen er spesielt synlig for utenlandske leverandører.

Å være liten kunde hos en stor leverandør har innvirkning på maktforholdet mellom de to, og også på hvilken prioritet den lille kunden får sammenlignet med større kunder. Denne problemstillingene er relevant spesielt for hendelser som må håndteres raskt.

Innlåsingseffekt er en annen sårbarhet, det vil si at selskapet låser seg så mye til én leverandør at det kan være vanskelig å bytte dersom det er ønskelig. Her bør selskapet i kontrakten sikre seg mulighet for overflytting til annen leverandør.

Det som regulerer forholdet mellom nettselskap og leverandør av driftstjenester er avtalen. Det er viktig at det er lagt ned grundig arbeid for å redusere mest mulig

potensielle sårbarheter og for å klargjøre leverandørens plikt for driftsstabilitet og tjenesteleveranser. Feil i komplekse systemer et sted kan få utilsiktede konsekvenser et annet sted. På dette området ble det pekt på at det kan oppstå en mulig drakamp om hvem som har ansvar for hva.

Revisjonsmuligheter og kontroll med at krav blir etterlevd er en annen mulig sårbarhet. Selv om nettselskapet benytter en ekstern driftsleverandør, er nettselskapet fortsatt ansvarlig overfor norske myndigheter. Revisjon og kontroll av leverandør vil være særlig utfordrende når en bruker skytjenester, se også pkt 4.3.2.

På workshopen kom det forslag om at mulige tiltak bør komme fra myndigheten i Norge eller i EU, som setter krav til driftsleverandører. Et eksempel er at norske myndigheter og virksomhetene i fellesskap kan bidra til å sette felles krav til skyleverandører og IT-driftsleverandører. Et nettselskap i Norge har liten innflytelse på en større driftsleverandør, og små bøter og sanksjoner fra en liten kunde har begrenset betydning for store leverandører.

3.5.5.2 Ressurser og systemer i eget selskap

På workshopen ble det pekt på at det er viktig at nettselskapet har egne rutiner og prosedyrer på plass for å følge opp leverandøren og for å kunne håndtere oppgraderinger og systemendringer, samt hendelser når disse oppstår. Mulig tiltak er å lage en beredskapsplan og å øve denne sammen med leverandøren og eventuelt andre samarbeidspartnere. Et annet forslag er at KraftCERT inviterer leverandørene med i samarbeidet.

Selv om selskapene benytter en ekstern driftsleverandør, må selskapet likevel ha kompetanse på nettdrift og på hele verdikjeden. Bestillerkompetansen er viktig. Utfordringen er at en risikerer å utarme den lokale kompetansen når en setter ut IT-driften. Derfor er det å forstå hele verdikjeden svært viktig, og ikke bare se på AMS-sikkerhet isolert sett.

3.6 Potensielle sårbarheter men fortsatt umoden trussel?

Som påpekt i kapittelet om trusler, så klarer ikke sikkerhetsindustrien å lukke alle sårbarhetene raskt nok etter hvert som de oppdages. Det bygges opp over tid en mengde ikke-lukkede sårbarheter. En ting er tekniske null-dags sårbarheter i dag, noe annet er hvilke sårbarheter som vil kunne avdekkes i framtiden når forskere og sikkerhetsindustrien verden over har studert og plukket fra hverandre både fysisk og logisk slike målere. I følge Mørketallsundersøkelsen for datakriminalitet (2014) skjer de fleste angrep i Norge mot gamle og ikke oppdaterte systemer, og bare 0,1 % er nulldags-sårbarheter. Spørsmålet er da om bransjen har en vedlikeholds- og sikkerhetsplan for den infrastrukturen som nå bygges ut, og om de har gjort gode nok risikoanalyser.

Det er stor bevissthet i fag- og forskningsmiljøer på potensielle sårbarheter i AMS-målere. Innbrudd er demonstrert i praksis. I den virkelige verden er det foreløpig vanskelig å vise til mange angrep og kompromitteringer. USA ligger langt foran Europa i utrulling av AMS. Det er her de fleste oppslag på misbruk også har sin opprinnelse, men en forespørsel til ICS-CERT i USA viser at de så langt har registrert få hendelser. De skriver i en epost til NVE at de har ingen rapporter på direkte angrep mot selve målerne,

men de kjenner til at målerne har sårbarheter som kan utnyttes. Videre skriver ICS-CERT at de kjenner til en hendelse der en tidligere ansatt rekonfigurerte en basestasjon til å ha svak autentisering. En annen aktør utnyttet dette, og det ble på den måten en kilde skadevaretrafikk mot andre enheter. Tiltak som retter denne sårbarheten er lett å implementere.[63] Kontakt med store produsenter av smarte målere bekrefter dette bildet av fravær av reelle hendelser.[64] Av dette kan vi trekke en konklusjon på at akkurat når det gjelder trusselen mot AMS-infrastruktur, så er denne ennå i en tidlig utviklingsfase, men framtidig systemintegrasjon og flere endepunkter vil kunne øke risikoen.

3.7 Bruk og utfordringer ved kryptering

En av de beskyttelsesmekanisme som gir størst trygghet mot kompromittering av måledata er om kommunikasjonen mellom måler og AMS-løsningen til selskapene er kryptert. Men dette krever kompetanse i å håndtere krypteringsfunksjonalitet og krypteringsnøkler.

Thales og Ponemon Institute's survey av 4714 individ på tvers av industrisektorer i 10 land (2015) dokumenterer virksomhetenes utfordring med å holde kontroll på alle krypteringsnøklene og sertifikatene. Kontroll med nøkler og sertifikater er spesielt vanskelig fordi ingen har eierskap og systemene er fragmenterte[65].

Mnemonic peker på at kryptert datatrafikk gir beskyttelse for personvern, men det hindrer innsyn også for sikkerhetsprogramvare. Det som skjer på trusselsiden er at også trusselaktørene er i ferd med å gå over til kryptert trafikk for å distribuere skadevare. I følge mnemonic endrer dette spillereglene fordi det blir vanskeligere å skille mellom tillatt trafikk og uautorisert trafikk. Flere sikkerhetsselskaper er nå derfor i ferd med å tilby produkter som foretar en dekryptering av trafikken før den går ut av selskapet. Det er nødvendig for å inspisere hva slags data som går ut. Blir det oppdaget mistenkelig trafikk, så blir denne analysert av et eget system. Men det gir igjen utfordringer for personvernet, for eksempel ved innsyn i meldinger og epost.[66]

3.8 Regulering av sikkerhet i AMS-løsningen

I MAF er selskapene pålagt å sørge for at AMS-løsningene sikres mot misbruk av data og uønsket tilgang til styrefunksjoner. Beredskapsforskriften regulerer sikkerhetskrav til den delen av AMS løsningen som eventuelt måtte benytte samme infrastruktur som selskapets driftskontrollsystem.

Alle forholdene som er belyst blant annet i workshopen, tilsier at gode risikovurderinger og kompetanse på tekniske løsninger vil være avgjørende for å forebygge hendelser i AMS-løsningen. Spesielt viktig vil det være å belyse forhold som kan sette forsyningssikkerheten til forsyningsområdet eller til enkeltkunder i fare hvis det skjer utilsiktede eller tilsiktede feil på løsningene som styrer bryter-/styrefunksjonaliteten.

---

[63] Svar på epost fra ICS CERT, 29.04.2015.

[64] Telefonsamtale med Aidon og Landis+Gyr.

[65] *2015 Global Encryption & Key Management Trends Study*, Ponemon Institute Research Report, April 2015.

[66] Fra Frank Skapalen, epost 06.05.2015 Kryptert trafikk - gir det beskyttelse eller er det en hemsko?, basert på Mnemonic frokost seminar samme dag.

Bransjens usikkerhet på hva slags sikkerhetskrav som myndighetene forventer skal implementeres i henhold til kravene i forskriftene, tilsier at det er et behov for å konkretisere sikkerhetskravene i forskrifts form. Særlig gjelder det i forhold til konkret sikring av løsningen for bryterfunksjonaliteten i AMS-løsningen og sammenkoblinger mellom bryterfunksjonaliteten i AMS og driftskontrollsystem. Det vil ikke være unaturlig at behovet for tettere samhandling mellom disse systemene er nødvendig for å oppnå full effekt av ønsket om bedre nettnytte og forsyningssikkerhet. Det vil da bli en utfordring å formulere krav som både gir tilstrekkelig sikkerhet men samtidig åpner for samhandling mellom ulike system.

I tillegg vil det også være fornuftig å vurdere krav til kryptering av kommunikasjonen mellom AMS-måler og AMS-løsningen samt konkretisere krav til å ha evne til å oppdag oppdage og håndtere hendelser og bruke sluttpunktet som en sikkerhetssensor.

4 Skytjenester

Mørketallsundersøkelsen 2014 hos Næringslivets sikkerhetsråd NSR viser en trend mot økt IKT-tjenesteutsettelse i næringslivet. Trenden inkluderer bruk av skytjenester.

Skytjenester er i bunn og grunn fjernlagring og prosessering av data over Internett hos en ekstern leverandør. Dataprosessering, datalagring og tilgang til programvare skjer fra servere som står i eksterne serverparker tilknyttet internett.

Historien til skyen (cloud) kan spores tilbake til 60-tallet og til den tid da forskere koplet sammen datamaskiner for første gang for å øke prosessorkapasiteten og dele på ressursene.

Skytjenester innebærer i de fleste tilfeller store fordeler. De viktigste er at virksomheten får skalerbare tjenester når det gjelder båndbredde, lagringskapasitet og prosessorkraft. I tillegg gir skytjenestene tilgang til tjenestene hvor brukeren enn befinner seg. Kostnadsmessig gir bruk av skytjenester store fordeler ved at virksomheten slipper å investere i store maskinparker og vedlikeholde disse. Skytjenestene er oppdaterte og har de siste sikkerhetsfunksjonene. Det sørger skyleverandøren for.

Nå som fiber er rullet ut over store deler av verden er det etablert skyløsninger med stordriftsfordeler i store datahaller. Google, Amazon og Microsoft har vært viktige foregangsvirksomheter for industrialisering av datahaller. På norsk territorium er Evry og Jotta Cloud de største leverandørene som leverer skytjenester i dag, men stadig flere leverandører er i ferd med å etablere seg i Norge.

Mange hevder at det kan bli vanskelig å stå på utsiden av denne utviklingen uten å havne i en situasjon der en blir hengende etter. Imidlertid er det enkelte risikofaktorer man må ta i betraktning før man benytter skytjenester til virksomhetskritiske prosesser. De viktigste risikofaktorene vil bli diskutert i dette kapittelet.

4.1 Nettsky-politikk i Europa og i Norge

I Norge og i EU er digitalisering en uttalt politikk. EU sin politikk er uttrykt i Digital Agenda[67], og Norge sin politikk beskrevet i dokumentet *Digital Agenda for Norge*[68]. Ambisjonen i EU er «*a digital single market*», der blant annet fri mulighet til virksomhetsetablering er lett, der sikkerhetskrav og personvern især er harmonisert, og der alle kan nyte godt av samme digitale innhold og tjenester uavhengig av hvilket land en er i. Europa trenger dette markedet fordi nesten 60% av nettbaserte tjenester i dag tilbys av amerikanske selskaper. Skytjenester er en del av den digitale agendaen.[69] Skytjenester gir store økonomiske besparelser og bedre skalering av IT-tjenester når det tas i bruk. ENISA har utgitt flere veiledere for bruk av skytjenester,[70] og i UK har man etablert et marked for offentlige etater og skytjenesteleverandører; UK GovCloud.[71]

I Norge har Kommunal og Moderniseringsdepartementet (KMD) ansvaret for digitaliseringsstrategien, og departementet har for tiden en nasjonal strategi for bruk av skytjenester.[72] Strategiarbeidet er forankret i Digital agenda for Norge. KMD har igangsatt et arbeid for å utarbeide en nasjonal strategi knyttet til offentliges bruk av skytjenester. I første omgang ble en arbeidsgruppe nedsatt for å kartlegge hvilke lover og forskrifter som hindret bruk av skytjenester. I arbeidet med kartleggingen har det kommet fram at avklaringer knyttet til bruk av skytjenester i hovedsak er knyttet til regulering av hvor data lagres og prosesseres, spesielt med tanke på om dette skjer innenfor/utenfor Norges grenser.

I følge arbeidsgruppen er de viktigste juridiske hindrene å finne i arkivloven og bokføringsloven med forskrifter[73].

NSM har startet opp et arbeid på sikkerhet i skytjenester og skal gjøre en dybdestudie av sikkerhet i sky og i virtualisering. NSM skal blant annet se på kryptering og beskyttelse av brukernes data. NSM har dialog med KMD.

4.2 Ulike modeller for skytjenester

4.2.1 Driftsmodeller

Skytjenesteleverandørene deler i utgangspunktet driftsmodellene inn i tre;

- *Infrastructure as a Service* (IaaS): Her tilbyr en tredjepart maskinvare, programvare, servere, lagring og andre komponenter. IaaS-miljøer inkluderer

[67] «Digital Agenda for Europe», URL: https://ec.europa.eu/digital-agenda/en/our-goals/pillar-vii-ict-enabled-benefits-eu-society

[68] «Digital Agenda for Norge», URL: https://www.regjeringen.no/nb/dokumenter/meld-st-23-20122013/id718084/?docId=STM201220130023000DDDEPIS&ch=1&q=

[69] European Cloud computing strategy, URL: https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

[70] «Cloud computing», ENISA, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

[71] «Digital marketplace», Gov.uk, URL: https://www.gov.uk/how-to-use-cloudstore

[72] Samtale med KMD telefon 7. april 2015

[73] https://www.regjeringen.no/no/aktuelt/vil-legge-til-rette-for-bruk-av-skytenester/id2425281/

automatisering av administrative oppgaver, dynamisk skalering, desktop virtualisering og policy-bestemte tjenester. Kjøperen betaler for bruk.

- *Platform as a Service* (PaaS) er en modell der leverandøren leverer maskinvare og programvare, vanligvis slikt som trengs for å utvikle applikasjoner. Denne tjenesten brukes typisk på enkelte nøkkelområder, som for eksempel programvareutvikling.
- *Software as a Service* (SaaS) er en modell for programvaredistribusjon der programvare blir gjort tilgjengelig for en kunde gjennom en internettforbindelse. Fordelene er lettere administrasjon av programvare, automatiske oppdateringer, alle brukere har samme programvare og lettere samarbeid og global rekkevidde. Noen leverandører har en betalingsmodell med en flat månedlig avgift.

I tillegg er noen skyleverandører i ferd med å tilby ulike hybridløsninger der særlig virksomhetskritisk informasjon forblir lagret lokalt hos virksomheten, men der prosessering skjer gjennom tjenester hos skyleverandøren.

4.3 Risiko og sårbarhet ved bruk av skytjenester

Risiko og sårbarhet knyttet til skytjenester var bare for noen få år siden ikke et tema. Ettersom store deler av verden har eller er i ferd med å koble seg på Internett med fiberforbindelser, og stadig flere virksomheter flytter virksomhetskritiske IKT-prosesser i skyen, har risiko og sårbarhet blitt et stadig mer aktuelt tema.

I tillegg fikk tilliten til datalagring i skyen en knekk når Snowden avslørte at den amerikanske etterretningsorganisasjonen NSA gikk direkte på leverandørene for å få ut informasjon om enkeltpersoner i jakten på potensielle terrorister. Dette har medført at det er mange bekymringer knyttet til sikkerhet i skyen.[74]

4.3.1 Risiko knyttet til ulike driftsmodeller

Generelt innebærer bruk av skytjenester de samme risikoene som tradisjonell tjenesteutsetting av IT-drift. På oppdrag fra NVE så Deloitte på sikkerhetsutfordringer knyttet til bruk av skytjenester for selskap i energiforsyningen, og knyttet risikoene opp mot bestemmelsene i Beredskapsforskriften (Borgund, 2014). I følge rapporten kan risiko og sårbarhet være knyttet til leverandører, i kommunikasjonskanaler eller i egen arkitektur. Skytjenester i forbindelse med bruk av bærbare eller private enheter kan igjen føre til nye utfordringer. Brukere av skytjenesten må derfor ha god kontroll på lovverk og virksomhetskrav. De må sørge for at kontrakter med leverandører reflekterer dette, samt forsikre seg om at kravene i kontrakter blir etterlevd.

Sikkerheten i skytjenestene avhenger av hvilken tjeneste som brukes:

IaaS: Kjøperen betaler for bruk, men det er viktig å sjekke at en ikke over-faktureres for tjenester en ikke bruker. Fordi tjenesteleverandøren eier infrastrukturen kan det bli

---

[74] Venters, W. and E. A Whitley, "A critical review of cloud computing: researching desires and realities", *Journal of Information Technology* (2012) 27, 179–197. doi:10.1057/jit.2012.17; published online 14 August 2012, URL: http://www.palgrave-journals.com/jit/journal/v27/n3/full/jit201217a.html,

vanskelig å overvåke egne data og egen dataprosessering. Amazon Web Services (AWS), Windows Azure, Google Compute Engine, Rackspace Open Cloud, og IBM SmartCloud Enterprise er eksempler på IaaS. Energiforsyningen vurderer i særlig grad bruk av Azure for å prosessere data. Windows Azure ligger i front når det gjelder transparens i skytjenester. Kunder skal kunne bygge løsninger for å kunne se logger, monitorere, analysere og sjekke compliance. I Customer Lockbox for Office 365 skal kunden kunne nekte eller godkjenne om en ingeniør fra Microsoft skal kunne logge seg inn i deres Office 365-tjeneste i tilfeller det er behov for support. I de neste månedene blir det lansert innholdskryptering av epost i tillegg til Bitlocker krypteringen som er i dag. Neste år skal kundene kunne kreve at lagret data er kryptert.[75] De andre leverandørene vil høyst sannsynligvis raskt kunne tilby tilsvarende sikkerhetstjenester.

- *PaaS*: Risikofaktorer knyttet til denne tjenesten er blant annet nedetid og innlåsing til leverandør.
- *SaaS*: Risikofaktorer for denne modellen kan være innlåsing til én leverandør, nedetid og slutt på support på det aktuelle programmeringsspråket. Vattenfall har for eksempel valgt Tieto som skyleverandør i Finland. Tietos Saas tjenester inkluderer kundeadministrasjon, salg, digitale online tjenester og fakturering. Selskapet tilbyr også drift av AMS infrastrukturen som inkluderer både kommunikasjon, høyhastighets datavalidering og lagring, automatisering av prosesser og operasjoner i felt.[76]

En annen potensiell risiko ved bruk av skytjenester kan være tidsforsinkelser på signaler ved lange strekk, som kanskje vil passere flere land, med mange knutepunkt og noder mellom bruker og datasentre, og mellom datasentre. Flere Smart Grid-prosjekter legger til grunn prosessering av data i nær sagt sanntid for å kunne gi et umiddelbart bilde over situasjonen til operatørene på driftssentralen.

Norske ekomtilbydere vurderer å tilby en ny tjeneste der kunder av skyleverandører skal kunne kople seg direkte mot dataserveren via dedikerte fiberlinjer.

Dersom en virksomhet er avhengig av sanntids- eller nær sanntidsinformasjon for å kunne operere sikkert, bør man vurdere denne type risiko.

En annen risiko som kan oppstå er dersom man i stor utstrekning benytter ende-til-ende kryptering av data mellom kunde og skyleverandør. Enkelte skybrukere har opplevd begrensninger i båndbredden, og dette kan bli en framtidig utfordring med tingenes internett – der alt koples på nett og kommuniserer med hverandre.[77]

Mørketallsundersøkelsen for datakriminalitet 2014[78] viser at mens norske virksomheter har høy grad av tillit til skyleverandørene og leverandørens evne til å beskytte data, står det svakere til når det gjelder sikkerhetsbevissthet. Kun 2 av 5 av virksomheter i offentlig

---

[75] Seals,T. "#RSAC: Microsoft Azure Focuses on Transparency and Control", published 22. April 2015, URLhttp://www.infosecurity-magazine.com/news/rsac-microsoft-focuses-on/

[76] Vattenfall selects Tieto to deliver new Industry Cloud solutions in Finland, URL: http://www.tieto.com/news/vattenfall-selects-tieto-to-deliver-new-industry-cloud-solutions-in-finland nedlastet 21.04.2015

[77] Basert på samtale med Microsoft.

[78] *Mørketallsundersøkelsen 2014*, URL: http://www.nsr-org.no/moerketall/

sektor har avsatt interne ressurser til å følge opp leverandøren, i motsetning til halvparten i privat sektor. 3 av 4 av virksomhetene stoler på at skyleverandørene har rutiner for logging av uautorisert tilgang, samt tilfredsstillende sletting av data om dette er aktuelt. Over halvparten vet ikke om avtalen regulerer tilsynsrett for offentlige myndigheter. Hos mindre virksomheter er andelen 2 av 3.

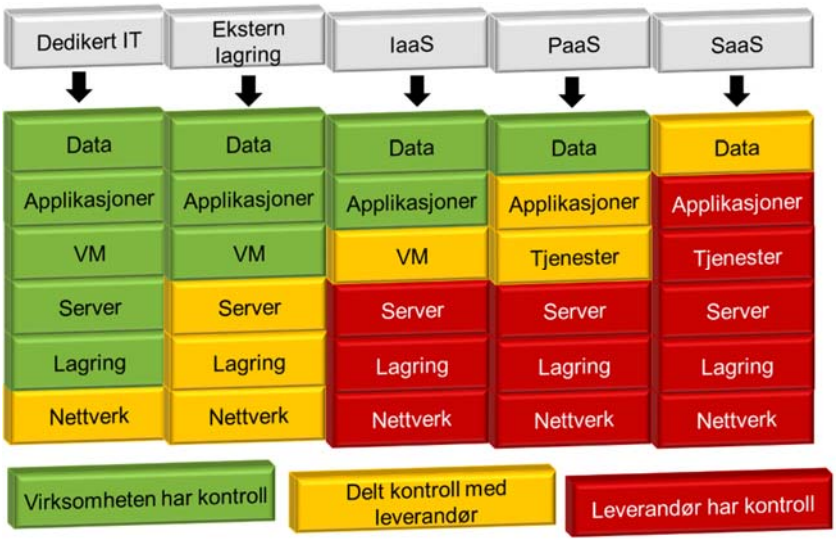
Tallene indikerer at det er behov for større oppmerksomhet hos både private og offentlige virksomheter rundt kontroll og oppfølging av leverandørene av skytjenester.

4.3.2 Hva slags kontroll har du egentlig?

Siden bevisstheten rundt sikkerhet og beskyttelse av data har økt blant skyleverandørenes kunder, har leverandørene økonomiske interesser av å legge stor vekt på sikkerhet og tilgjengelighet. I mange tilfeller vil de store skyleverandører være bedre skodd enn små selskaper når det gjelder sikkerhet og tilgjengelighet. Men å være stor gir i seg selv ingen garanti for sikkerhet.

Når en har besluttet å benytte skytjenester og er i ferd med å flytte data over i skyen, er det viktig å huske at man i praksis overlater til leverandøren å sørge for at dataene er sikret i henhold til avtalen med leverandøren. Det vil alltid være en liten risiko for at ukjente kan få tilgang til data. Man vil aldri ha full kontroll med data så lenge de ligger hos en skyleverandør, eller en annen leverandør som tilbyr fjernlagring av data.

Et samlet bilde av hvilken kontroll selskaper har ved ulike driftsformer er illustrert i Figur 4.1. I skyløsninger som Software as a Service (SaaS) er brukeren helt avhengig av skyleverandøren. I Infrastructure as a Service (IaaS) har brukeren mer kontroll over de ulike tjenestedagene, der brukeren kan lage og tilby virtuelle maskiner.



Figur 4.1 Kontroll delt mellom virksomhet og leverandør i ulike driftsmodeller[79]

For å kunne dokumentere god sikkerhet og kontroll, sørger de store leverandørene for å sertifisere seg i henhold til standarder og normer for sikkerhet og beskyttelse av personopplysninger. Microsoft er ett eksempel, og selskapet er blant annet sertifisert i

[79] Se: URL: http://srmsblog.burtongroup.com/2009/06/cloud-computing-who-is-in-control.html

henhold til den nye standarden ISO 27018 om forvaltning av personlig identifiserbare data i skyen.[80] Datasentrene til Microsoft har flere nivåer av sikkerhet, både fysisk, logisk og når det gjelder personell. Data er kryptert og spredt utover mange disker, og anomalibaserte algoritmer sørger for at det blir reagert mot unormal trafikk.

4.3.3 Sanksjonsmuligheter, leverandørkontroll og risiko for innlåsing

Norske myndigheter har ingen formell jurisdiksjon over leverandører utenfor norsk territorium som gis tilgang til sensitiv informasjon om energiforsyningen. Bryter leverandørene norske lover og forskrifter vil det være vanskelig å forfølge disse rettslig. Derfor er det som regel kun de kommersielle kontraktene som regulerer eventuelle sanksjonsmuligheter dersom klausulene i avtalene eller taushetserklæring brytes.

Mange skyleverandører sertifiserer sine tjenester etter internasjonale standarder og normer for sikkerhet og beskyttelse av personopplysninger. Det er likevel viktig å huske at sertifisering eller etterlevelse av normer ikke erstatter nasjonalt lovverk. Dersom en leverandør av skytjenester er lokalisert i land med en svakere lovgivning enn for eksempel den norske, har selskapene ingen garanti for at myndighetene i landet for eksempel kan kreve sensitiv informasjon om norsk kraftforsyning utlevert.

Dette kan gjør det svært utfordrende for selskapene å ha kontroll med hvem hos leverandøren som har tilgang til visse typer informasjon. Det samme gjelder for selskapene i energiforsyningen å føre stedlig kontroll med leverandørene. De største leverandørene vil høyst sannsynlig ikke tillate at enhver kunde kommer på tilsyn for å kontrollere at avtaler blir etterlevd. Leverandørene inngår i stedet avtaler med ett eller flere revisjonsfirma som med jevne mellomrom utfører revisjon av skyleverandørens sikkerhet. Rapportene kan kundene som regel få innsyn i. Men også her er det viktig å huske at skyleverandørene blir revidert etter standarder, ikke etter nasjonale lovverk.

Alle sikkerhetstiltak og etterlevelse av standarder og normer til tross, det er eksempel på at angripere har vært i stand til å kompromittere en virtuelle maskiner og bruke disse for å komme forbi sikkerhetsmekanismene i skytjenester. På samme fysiske harddisk kan også fiendtlige virtuelle maskiner sameksistere. Useriøse skyleverandører kan tilby virtuelle maskiner som genererer ekstra trafikk som igjen kunden må betale for. En annen utfordring er konfigurasjonsstyring og sporing av dataflyten mellom ulike skyløsninger og egne driftsløsninger. [81]

Hvor vidt skyleverandørene gjør sitt ytterste for å sørge for god nok sikkerhet avhenger blant annet av hvor sterk konkurransen er på dette området og hvor lett det er å skifte leverandør. I en artikkel i teknisk Ukeblad (2014) rettes det kritikk mot måten

---

[80] Plummer, Q., "Microsoft Adopts ISO/IEC 27018 For Personal Data, Privacy Protection In Public Cloud", Tech Times, February 18, URL: http://www.techtimes.com/articles/33342/20150218/microsoft-adopts-iso-iec-27018-for-personal-data-privacy-protection-in-public-cloud.htm

[81] Zage, D., Franklin, D. and V. Uries, "What does the future holds for cloud computing? In: Cross talk", Sept Oct 2013, *The Journal of Defence Sortware Engineering*, ***25***. No. 5. http://www.crosstalkonline.org/storage/flipbooks/2013/201309/index.html

skytjenester markedsføres på. Blant annet nevnes det at bytte av leverandør er bortimot umulig da alle data og all logikk ligger hos leverandøren.[82]

4.3.4 Hvilke land er akseptable at leverandøren kommer fra?

Det er svært få norske lover og forskrifter som har satt begrensninger til hvilke land det er tillatt eller ikke tillatt å overføre informasjon som kan være sensitiv, enten for kritisk infrastruktur eller personopplysninger. Unntaket er for virksomheter som er underlagt Sikkerhetsloven eller informasjon som er omfattet av for eksempel arkivloven. Norske energiforsyningsanlegg er ikke underlagt Sikkerhetsloven med tilhørende forskrifter.

I *Lov om behandling av personopplysninger (personopplysningsloven)* § 29 tillates overføring av personopplysninger til stater som har gjennomført direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Dette betyr i praksis land som er medlem i EU eller land som er en del av EØS-samarbeidet.

Norge har et sikkerhetspolitisk samarbeid med flere land gjennom NATO-samarbeidet, og innenfor dette samarbeidet utveksles det også gradert informasjon som har høyere sensitivitet enn informasjon som kan benyttes for å skade energiforsyningen.

Man kan derfor anta at land innen EU/EØS og land som er med i NATO-samarbeidet har et lovverk der det er muligheter for å forfølge virksomheter rettslig dersom disse bryter avtaler eller taushetserklæringer knyttet til beskyttelse av sensitiv informasjon om kraftforsyningen eller personopplysninger.

Utover disse samarbeidsorganene har selskapene i energiforsyningen liten eller ingen mulighet til å kontrollere i hvilken grad lovgivning eller andre myndighetspålegg samsvarer med det som kan forventes for å sikre at leverandører ivaretar kravene som stilles til beskyttelse av sensitiv informasjon om den norske energiforsyningen.

4.3.5 Konsentrasjonsrisiko

Store leverandører som Microsoft, Apple, Google, Amazon m.fl. har et fåtall enorme datasentre lokalisert over hele verden.[83] Microsoft har to datasentre i Europa, mens Google har fire. Det lave antallet datasentre gir en konsentrasjonsrisiko globalt, men på en annen side er det vanskelig å se for seg verdensomspennende trusler som skal kunne slå ut alle sentrene.

Konsentrasjonsrisikoen ved at mange i bransjen kan ende opp med samme leverandør ble illustrert ved driftsforstyrrelsen hos Tieto i november 2011. 50 av kundene i privat og offentlig sektor i Sverige opplevde alvorlige driftsforstyrrelser på grunn av hardvarefeil hos leverandøren. Selv om leverandøren hadde systemet i drift etter to døgn var flere av leverandørens kunder uten IT i ukesvis. Hendelsen er en tankevekker for

[82] Zachariassen, E., «Skyleverandør slakter egen bransje: – Kutt ut nettskyen», *Teknisk ukeblad*, 22. september 2014, http://www.tu.no/it/2014/09/18/skyleverandor-slakter-egen-bransje--kutt-ut-nettskyen

[83] Se for eksempel http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm og http://www.google.com/about/datacenters/inside/locations/index.html

konsentrasjonsrisiko på leverandørmarkedet, som kan føre til at mange kan bli rammet av samme feil.[84]

4.4 Personvern og skytjenester

Beskyttelse av personopplysninger har vært ansett som en utfordring knyttet til bruk av skyløsninger. Hovedutfordringene er relatert til beskyttelse av data og samsvar med krav, interoperabilitet og portabilitet, identitet- og tilgangsstyring, revisjon, hvor lett tjenestene er å ta i bruk, tilgjengelighet og risiko.

Det mangler fortsatt en løsning både i forhold til avtale med leverandøren når det gjelder tekniske mekanismer som kryptering,[85] og når det gjelder beskyttelse av personopplysninger i skytjenester. Ifølge Datatilsynet[86] kan ikke personopplysninger uten videre overføres til land utenfor EØS eller Safe Harbor[87]-området, og selv om de aller fleste norske virksomheter håndterer personopplysninger i større eller mindre grad, er bevisstheten på dette området svært lav. Mørketallsundersøkelsen i 2014 viser at 1 av 5 virksomheter ikke vet om virksomhetens data blir overført til andre land ved sikkerhetskopiering. 1 av 5 virksomheter vet heller ikke hvor virksomhetens data fysisk blir lagret.

I oktober 2015 ble imidlertid Safe Harbor-avtalen mellom EU og USA kjent ugyldig av EU-domstolen. Bakgrunnen for kjennelsen var at domstolen ikke fant at avtalen i stor nok grad tok hensynet til privatpersoners rett til innsyn og kontroll med data som omhandlet dem og som ble sendt mellom virksomheter mellom EU og USA.

Rettsaken mellom Microsoft og den amerikanske staten om å gi tilgang til data i Microsoft sin server i Irland i forbindelse med en narkotikasak, har pekt på viktige prinsipper for beskyttelse av data i datasentre utenfor USA. Saken er interessant: Dersom den amerikanske staten vinner, vil også andre nasjoner kunne påberope seg samme rett til å hente ut data som er plassert på et tredjelands territorium. De tyske myndighetene har allerede uttalt at dersom den amerikanske staten vinner, vil de ikke benytte seg av amerikanske skyleverandører.[88]

Cloud Security Alliance utførte i 2013 en online spørreundersøkelse der de mottok 456 svar, hvorav 234 fra USA. Resultatet viste at hele 47% mente det er for lite transparens i hvordan landets myndigheter får tak i informasjon med formål å etterforske terror og

---

[84] *Refleksjoner kring samhällets skydd och beredskap vid alvarliga ut-incidenter. En studie av konsekvensarne i samhället efter driftsstörningen hos Tieto i november 2011*, MSB, URL: https://www.msb.se/RibData/Filer/pdf/26170.pdf

[85] Se Liveri and Dekker, 2015

[86] «Overføring av personopplysninger til utlandet», Datatilsynet», 25.11.2011, URL: https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/

[87] «Safe Harbor – prinsipper om overføring av opplysninger til USA», Datatilsynet, 30.11.2014 URL: https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/Safe-Harbor-prinsippene/

[88] Rushe, D., "Privacy is not dead: Microsoft lawyer prepares to take on US government", the Guardian, 14th December 2014, URL: http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government,

kriminalitet. Like ens mente 56 % av respondentene utenfor USA at de i mindre grad ville bruke amerikanske leverandører.

Sannheten er likevel at mange benytter applikasjoner (apper) – gjerne på sin smart-telefon - som lagrer data i skyen. Med *Bring Your Own Device* (BYOD)-trenden er risikoen stor for at sensitive data blir lastet opp i skyen og delt via apper med både autoriserte og uautoriserte brukere.[89]

Det er likevel ikke nødvendigvis slik at en skytjenste er mer sårbar for logiske innbrudd enn for de som har alt i eget hus. Bare 4% har rapportert at de har erfart datainnbrudd i appene det siste året.[90]

Norsis har to veiledere som omhandler sikkerhet i skytjenester. Den ene er Veiledning for outsourcing av IT[91] og den andre er Veiledning i hendelseshåndtering som også omtaler skytjenester (s 10).[92] For de mange små og mellomstore selskapene i kraftbransjen kan det være nyttig å se på Norsis sine veiledere som er spesielt tilpasset små og mellomstore virksomheter, samt ENISA sin veiledning for sikkerhet i skytjenester for små og mellomstore virksomheter.[93]

4.5 Regulering av bruk av skytjenester

Det er ingen konkrete forbud mot å benytte skytjenester i NVEs beredskapsforskrift. Imidlertid er det strenge krav i kapittel 6 i forskriften om å sikre informasjon som er sensitive om energiforsyningen, det vil si informasjon som kan benyttes til å skade anlegg eller system i energiforsyningen.

Kravene til beskyttelse av sensitiv informasjon innebærer at virksomheten som eier og forvalter informasjonen til enhver tid skal ha full kontroll med hvor informasjonen er, hvem som har tilgang til den og hva informasjonen brukes til. I tillegg skal virksomheten som eier informasjonen, gjennom kontrakten med leverandøren sikre at både virksomheten og beredskapsmyndigheten (NVE) kan føre tilsyn med den eksterne virksomheten som får tilgang til sensitiv informasjon

I §§ 6-3, 6-4 og 6-8 begrenser bestemmelsene mulighetene til å legge informasjon i skyen. Her stilles det krav til beskyttelse, avskjerming, tilgangskontroll, sikkerhetskopier og sikker avhending av informasjon som det er vanskelig å få spesialtilpasset fra globale skyleverandører som har standardkontrakter på disse forholdene. NVEs veileder gir noen eksempler. [94]

---

[89] Evans, D., ”What is BYOD and why is it important?”, Computing, August 23 2013, URL: http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important--1175088,

[90] Se Luciano and Yeoh, 2014

[91] *Veiledning for outsourcing av IT, spesielt rettet mot små og mellomstore bedrifter*, september 2010. Utgitt av Norsis og NSR, tilgjengelig: https://norsis.no/2012/07/veiledning-for-it-outsourcing/

[92] *Veiledning i hendelseshåndtering*, https://norsis.no/2012/07/hendleseshandtering/

[93] Dekker, M.A.C. and D. Liveri, *Cloud Security Guide for SMEs, Cloud computing security risks and opportunities for SMEs*, ENISA, April 2015. ENISA.

[94] *Veileder til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen*, 1, 2013, NVE.

Beskyttelseskravene gjør det derfor utfordrende for selskap i energiforsyningen å benytte utenlandske skytjenester for å lagre eller prosessere informasjon som er sensitiv.

Dagens regelverk peker på spesifikk type informasjon som må beskyttes og krav til beskyttelse, men gjennom integrasjon av systemer og utvikling av nye tjenester kan det produseres nye typer data som aggregert kan gi svært detaljert informasjon om energiforsyningen og personer. I tillegg kan bruk av skyteknologi for økt nettnytte gi stor avhengighet av skytjenester.

Denne utviklingen kan komme gradvis over tid og ikke være lett synlig. Det er dermed behov for klare krav til hvilke data som kan legges til skyen og hva som kan integreres med skytjenester.

Dagens beredskapsforskrift tar i noen grad ikke høyde for denne utviklingen, og det vil sannsynligvis ikke være samfunnsøkonomisk forsvarlig å forby bruk av skytjenester som benytter kraftsensitiv informasjon som en del av datagrunnlaget for å øke nettnytte og forsyningssikkerhet.

Sikkerhetsteknologien har kommet såpass langt at det ikke vil være teknologisk vanskelig for eksempel å kreve at data som skal benyttes i skytjenester og som er sensitiv, skal være kryptert til enhver tid, for eksempel i henhold til standarder gitt av NSM.

Som følge av utviklingen på området, er det viktig at beredskapsforskriften revideres slik at den tar høyde for den teknologiske utviklingen som vil komme, og legger til rette for sikker utvikling av tjenester som skal gi bedre nettnytte og forsyningssikkerhet.

Det bør også så langt det er mulig også gis retningslinjer for fra hvilke land man kan akseptere at leverandøren lagrer og prosesserer informasjon for selskap i energiforsyningen.

5 Mot Smart-Grid funksjonalitet

5.1 Forskjellene mellom sikkerhet i driftskontrollsystem og tradisjonell IT-sikkerhet

Energiforsyningen har i en årrekke benyttet IKT-baserte industrielle kontrollsystem (kalt (driftskontrollsystem) for å fjernstyre anleggene i energiforsyningen. Et driftskontrollsystem består av driftssentraler, datautstyr, nettverkskomponenter, infrastruktur for samband og signalføring mellom driftssentral og anleggene, programvare, og øvrige anlegg og komponenter som ivaretar driftskontrollfunksjoner.

Allerede nå er enkelte selskap i ferd med å vurdere å prøve ut bruk av ny teknologi som skytjenester og Smart-Grid teknologi i tilknytning til industrielle prosesskontrollsystem. Leverandørene av slike system peker på fordelene denne teknologien har for å bidra til å prosessere data billigere og mer effektivt, spesielt i kontrollsystem som styrer og overvåker strømnett på et lavere distribusjonsnivå.

Det er imidlertid flere utfordringer relatert til dette konseptet. Mange av dagens system består av maskiner som fortsatt inneholder gamle Windows operativsystemer og som ikke er direkte kompatible med nyere versjoner. Det betyr at man er nødt til å investere betydelig i nye system eller utvikle systemkoblinger som gjør det mulig at både eldre og

nye system kan snakke sammen. Dette kan medføre nye sårbarheter og høyere risiko for feil.

På en annen side utfører virksomhetene i kraftforsyningen store beregninger som kjøres på egne servere i dag, og som kan være egnet for å legge opp i skyen. Men da må man ta hensyn til sikkerhetsutfordringene som følger med. Det omfatter for eksempel behov for å overvåke privilegerte administratorbrukere hos skyleverandøren, behov for å vurdere samsvar med lovverk og jurisdiksjon i forhold til serverlokalisering. Et annet moment en må vurdere er behovet for å sikre datasegregering siden en kjører sine egne data på samme server som andre ukjente brukere. Til sist må en også vurdere hvordan gjenoppretting ved feil kan foretas, hvordan en skal få støtte ved etterforskning og ikke minst den kommersielle levedyktigheten til leverandøren på lang sikt[95].

Det er flere motsetninger mellom sikkerhet i driftskontrollsystem og tradisjonell IT-sikkerhet. Mens tradisjonell IKT-sikkerhet handler om å beskytte IKT-systemene mot uautorisert tilgang eller angrep, snakker man gjerne om sikkerhet i prosesskontrollsystemene som tiltak for å hindre at uautorisert tilgang eller angrep ikke kompromitterer driftskontrollsystemenes *tilgjengelighet* og *integritet*. Dette innebærer at beskyttelsestiltakene ikke må gå på bekostning av systemenes tilgjengelighet og at man må kunne stole på at systemene til enhver tid gir riktig informasjon. En annen, men vesentlig forskjell mellom sikkerhet i tradisjonell IKT og sikkerhet i driftskontrollsystem er at dersom driftskontrollsystem blir utsatt for uautorisert bruk, kan det medføre skade på utstyr, anlegg eller miljø og i ytterste tilfelle personskader eller dødsfall.

De prinsipielle forskjellene er oppsummert i Tabell 5.1. Her blir utfordringene enda tydeligere dersom prosesskontrollsystemer flyttes til skyen og underlegges alminnelige IT-sikkerhetskrav.

[95] *Protecting Industrial Control Systems Annex I: Desktop Research Result*s, ENISA, [Deliverable – 2011-12-09], URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/annex-i,

Tabell 5.1Sammenligning mellom sikkerhet i driftskontrollsystem og tradisjonell IT-sikkerhet[96]

Sikkerhetsutfordring	Driftskontrollsystem	Sikkerhet i tradisjonell IKT
Tilgjengelighet	Svært høy	Lav til moderat
Integritet		
Konfidensialitet	Lav	Høy
Autentisering	Høy	Moderat
Oppdatering av programvare	Sakte eller kanskje umulig	Hyppig
Anti-virus	Uvanlig	Vanlig
Teknologisk levetid	15-20 år	3-5 år
Tidskritikalitet	Kritisk	Forsinkelser kan tolereres
Kommunikasjons-protokoller	IEC 61850, IEC 60870-5/6, DNP3, Modbus etc.	TCP/IP, UDP
Kommunikasjons-ressurser	Veldig begrenset	Ubegrenset
Cyber-etterforskning	Begrenset om den finnes	Tilgjengelig
Sikkerhetsbevissthet	Tradisjonelt dårlig	God
Konsekvenser av sikkerhets-kompromittering	Økonomiske konsekvenser, utstyr blir ødelagt og personlig sikkerhet, mulig trussel mot kritisk infrastruktur.	Økonomiske konsekvenser

Ulikhetene mellom driftskontrollsystem og tradisjonell IKT gir store utfordringer dersom man ønsker å lage et helhetlig sikkerhetsregime og en felles sikkerhetsarkitektur for alle typer system hos nettselskapene. Et eksempel er bruk av anti-virus programvare som i noen tilfeller kan komme i skade for å stoppe eller forsinke lovlig og nødvendig trafikk (falske positive) i driftskontrollsystem. Et annet eksempel er oppdateringer av programvare som ofte kan gjøres uproblematisk på enkeltstående maskiner, men som må testes grundig ut når det er snakk om å oppdatere system i et industrielt kontrollsystem. Mange av driftskontrollsystemene i kraftforsyningen består av en svært kompleks infrastruktur og som kan være følsom for endringer som påvirker funksjonaliteten.

[96] Y. Yang, K. McLaughtlin, T. Litttler, S. Sezer, Eul Gyu Im, Z.Q. Yao, B. Pranggono and H..F.Wang, "Man-in-the-Middle Attack Test-Bed Investigating Cyber-Security Vulnerabilities in Smart Grid SCADA Systems", International Conference on Sustainable Power Genereation and Supply (SUPERGEN 2012), s 1-8, 10.1049/cp.2012.1831.

Internasjonalt utarbeides det også nye standarder for kontrollanlegg (IEC 61850) som innebærer synkroniseringskrav på mikrosekundnivå. Det anses derfor som sannsynlig at strengere tidssynkroniseringskrav på sikt kan bli relevant også i Norge.[97] Dette kan igjen få konsekvenser for sårbarheten i systemet som helhet.

5.2 AMS og skytjenestenes betydning for sikkerhet i moderne driftskontrollsystem

I dag er det varierende i hvilken grad nettselskapene har overvåking av nettets tilstand på lavere spenningsnivåer. Dette gjør at driftssentralen har liten oversikt over spennings- og avbruddssituasjonen hos vanlige forbrukere. Det har derfor vært ønskelig for nettselskaper å ta i bruk «*Distribution Management Systems*[98]» (DMS), som benytter seg av måledata fra AMS for å overvåke lavere spenningsnivåer i nettet. Noen få selskap benytter seg av enklere versjoner av disse systemene for å få bedre oversikt over distribusjonsnettet, men fremdeles er de fleste selskapene avhengig av at kundene melder fra ved strømbrudd eller ved unormale spenningsverdier.

Frem mot 2019 vil nettselskapene være opptatt med innføringen av AMS og få etablert en stabil drift av AMS-løsningene. Etter 2019 er det forventet at selskapene vil vurdere hvilken annen nytte de kan få utover automatisk måling og avregning. Eksempler er det såkalte Braadland-prosjektet samt prosjekter som Demo Steinkjer, Demo Hvaler og andre utviklingsprosjekt er eksempler på at flere selskap allerede nå planlegger for hva de ønsker å gjøre etter at AMS er innført.

Braadlandprosjektet er et samarbeidsprosjekt mellom EB Nett, Fredrikstad Energi, Sogn og Fjordane Energi, Ringeriks-Kraft og eSmart Systems. Prosjektet ønsker å utvikle en overvåkningsløsning med sømløst samvirke mellom skytjenester, Big Data og sanntidsanalyseteknologi, mobile løsninger, og effektiv bruk av sosiale medier for å øke for effektiviseringen av nettdriften.[99]

Ifølge SINTEF Energi[100] kan DMS ha funksjoner som dekker visualisering av nettets aktuelle driftstilstand, verktøy for analyse og tiltaksplanlegging og for vedlikeholds- og nettplanlegging, samt oversikt over systemet. I tillegg kommer funksjoner for avbruddshåndtering, kart, kundeinformasjon og løsninger for distribuering av informasjon. I tillegg kan det legges opp til at systemet selv kan vurdere tilstanden på nettet og foreta egne valg og tiltak ved for eksempel feil i nettet. Dette krever at driftskontrollsystemene og de systemene som overvåker og styrer på distribusjonsnivå vil få økt systemintelligens.

---

[97] *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur* Oslo, Rapport, Norsk Romsenter, mars 2013.

[98] Et DMS er en samling av programmer og en arkitektur som er utviklet for å overvåke og kontrollere hele distribusjonsnett helt inn til kundens måler effektivt og pålitelig. Det fungerer som et beslutningsstøttesystem for å bistå operatørene i driftssentralen og driftspersonell i felt med overvåking og kontroll av strømnettet. Moderne DMS har også innebygget logikk som innenfor gitte rammer kan foreta egne vurderinger og valg knyttet til for eksempel omkoblinger ved strømbrudd.

[99] «EB velger Smart», 2 februar 2015, URL: https://www.eb.no/eb-velger-esmart-fremtiden/

[100] Se Sæle, Sagosen, & Bjørndalen, 2014

Ved å ta i bruk smartmålere og flere målepunkter i nettet vil det bli mulig å effektivisere lokalisering av feil sted på lavere spenningsnivåer. Målerne kan også registrere forbigående forstyrrelser som jordfeil. Det kan også være aktuelt å integrere feltverktøy mot DMS slik at montører i felt kan motta arbeidsordre og tegninger, oppdatere sanntidsbildet av nettet, og slik frigjøre operatørens tid. Om DMS knyttes opp mot kundehåndtering, kan programmet assistere utsending og innhenting av informasjon gjennom telefonsvarer, SMS eller epost.

Dette vil gi forsyningssikkerhetsmessige gevinster, men samtidig by på store IKT-sikkerhetsmessige utfordringer. DMS og effektiviseringsmuligheter

Dersom det blir innført automatisk omlegging av kraftflyt er denne bryterfunksjonaliteten nødvendig. En mulighet er at driftssentralene i første omgang tester ut programmets forslag til omlegging, og etterhvert kobler DMS mot fjernstyring og lar dette skje automatisk dersom programmet fungerer tilfredsstillende. Også arbeidsprosessene kan effektiviseres. Samon Voima Verkkos har etablert sømløs og automatisk arbeidsprosess fra alarmen går til feilen er reparert. I tillegg til Aidons målere og ABBs DMS-system skal de integrere Tietos GridWise-system med real-time geografisk informasjon og Tietos elektroniske kartapplikasjon (PGField) for mobile enheter. Så snart integrasjonen er klar, vil systemet prosessere alarmer automatisk som inkluderer informasjon om bruddlokasjon og feilrettingsbeskrivelser, og meldingen vil bli levert direkte til operatørene i felt.[101]

5.3 Sikkerhet i DMS

Med økt systemintelligens og ny teknologi, samt bruk av skytjenester for prosessering av data, forventes det at selskapene i nær fremtid vil få svært gode prediksjoner på hva som kan forventes av belastning og slitasje på kort og lang sikt. Det er også en risiko for den økte kompleksiteten medfører at man ikke er i stand til å forstå systemet fullt ut[102].

Sikkerhet har lenge vært et tema i forbindelse med moderne driftssentraler. I en undersøkelse blant seks leverandører støttet fire av DMS-systemene kobling av fjernstyrte brytere. Denne funksjonaliteten vil sette større krav til sikkerhet rundt systemet og dermed øke kostnadene. Det er likevel omdiskutert hvorvidt der er aktuelt å koble DMS sammen med kontrollsystemene for høyspentnett grunnet kostnader og krav til sikkerhet.

I tillegg vil sensitive informasjonsverdier og funksjoner som må beskyttes, er målerverdier, målerverdier koblet mot kunde ID, bryterfunksjon i kundens installasjon, samt passord og krypteringsnøkler[103]. ENISAs studie på beskyttelse av prosesskontrollsystemer har presentert en oversikt over sårbarheter:[104]

---

[101] "Kortere responstid", Aidon, URL: http://www.aidon.com/no/savon-voima/

[102] Wäfler J. and P. E. Heegaard, "Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability, Advances in Communication Networking", Lecture Notes in *Computer Science* Volume 8115, 2013, pp 185-196
http://www.item.ntnu.no/_media/projects/smartgrid/futurecontrolcenter/doc_interdependency_meta_model-camera_ready_eunice.pdf,

[103] Tøndel, Line, Johansen, & Jaatun, 2014

[104]« Industrial Control Systems/SCADA", ENISA, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems

- Forsinke, blokkere eller endre informasjonsflyt og produksjonsprosessen hos en produsent
- Forfalske informasjon om tilbud og etterspørsel, og manipulere markedet
- Fysisk eller logisk angrep mot single-point-of-failure smart grid komponenter
- Teknologirelatert raseri (informasjonskampanje på twitter)
- Organiserte kriminelle som manipulerer smartgridmålere hos sluttbrukere eller på konsentratorpunkter
- AMS er inngangspunkt til kritiske prosesskontrollsystemer for hackere og kriminelle
- Misbruk av personopplysninger som brukes for å skade omdømmet til selskaper

Forskning viser at det er for lite overvåkning på innsiden av driftskontrollsystemene. Det er mange lag og barrierer inn, men kommer man først på innsiden kan en inntrenger operere uten å bli oppdaget. Forfatternes inntrykk er at selskapene stoler mye på leverandøren og stiller for lite krav. Det er også i tråd med Mørketallsundersøkelsen 2014. Sett opp mot markedet for kjøp av sårbarheter og skadevare, og der det også er sårbarheter for driftskontrollsystemer til salgs,[105] er dette grunn til bekymring.

5.4 Forbrukerfleksibilitet

I Japan, der prisene varierer mye over døgnet, har prisvariasjonene skapt et marked for batteri for hjemmebruk. Forbrukerne kjøper strøm og lader batteriene når strømmen er som billigst, som regel på natten, og benytter batteristrøm om dagen når strømmen har høy pris. Overskuddsstrøm selger forbrukeren tilbake. Strømmen mates tilbake i nettet. Mange kunder forsøker å tjene penger på dette.

Problemstillingen her er at systemet kan tilpasse seg denne betingelsen på sikt, men en kan ikke kreve at forbrukerne skal levere pålitelig energi tilbake i nettet. Da må deres batterier bli laget i henhold til standarder for batterier brukt i datasentre, noe som vil bli svært kostbart. Dermed vil den økonomiske fordelen bli redusert. Dersom bruk av batterier får tilstrekkelig utbredelse, kan det føre til økt avhengighet av private batterier i ordinær drift, og med det økt sårbarhet. Nettselskapene vil i prinsippet ikke har kontroll med batteriene, da disse plasseres på innsiden av målerne. Et spørsmål er hvordan nettselskapene skal håndtere slike situasjoner hvis det blir en realitet i Norge.

5.5 Fra kraft- og nettselskap til IT-selskap?

Om selskapene i energiforsyningen bygger ut full Smart-Grid funksjonalitet i kraftsystemet i framtiden, vil selskapene i større grad kunne bli IT-selskaper som analyserer data og leverer informasjon og tjenester til forbrukernes smarttelefoner og nettbrett. Målerne blir en god anledning til å legge grunnlaget for velferdsteknologi og

[105] Revuln er et selskap registrert på Malta som selger sårbarheter til industrielle kontrollsystem som for eksempel SCADA, fra deres nettside: We provide information and technology for our private undisclosed 0-day security vulnerabilities affecting a wide range of products: both vastly used software like web browsers and office applications for desktop and mobile, and specific products like SCADA/HMI.: http://revuln.com/#services
De hyrer for tiden (juni 2015) både "forskere" og salgsfolk.

trygghetspakker for eldre, selv om det også finnes andre og løsninger.[106] I dette perspektivet vil personvern bli en viktig sak, og da kan det være nyttig å se på den konflikten som nå har utviklet seg mellom Facebook og EU om Europeisk lov.[107] [108]

Dersom selskap i energiforsyningen blir ansvarliggjort for brudd på personvernlovgivningen, kan dette representere en klar økonomisk risiko for selskapene i framtidige systemer. Dette er en reell risiko: En kunde av strømleverandøren Hafslund oppdaget ved en tilfeldighet at selskapets mobil-app «Hafslund Strøm Privat» lagret brukerens tekstmeldinger. Hafslunds hadde ingen rutiner for å teste appens funksjonalitet, men levde i den tro at utvikleren bygget løsningen på en teknisk forsvarlig måte.[109]

Det forventes at det etableres kreative tjenester på AMS-infrastrukturen i framtiden som vi ikke har mulighet til å forestille oss i dag. En studentkonkurranse ved NTNU om tjenesteutvikling illustrerer dette. Her ble det utviklet både tjenester for å optimalisere energibruken og for å bruke energidata til å lage en dating profil basert på døgnrytme.[110]

Norsk Teknologi har utviklet en veileder med kort oversikt over de kommersielle mulighetene og utfordringene som kan oppstå i forbindelse med utrulling av AMS, drift og vedlikehold, samt nye tjenester. [111]

5.6 Regulering av DMS- og Smart-Grid funksjonalitet

Hvorvidt selskapene i energiforsyningen vil investere i Smart-Grid funksjonalitet avhenger av hva selskapene kan forvente å få igjen for investeringene, i hvilken grad kundene etterspør tjenestene som er mulig gjennom Smart-Grid-funksjonalitet. Hvilke sikkerhetskrav som pålegges vil også ha stor betydning for i hvilken grad selskapene vil implementere av funksjoner og integrasjon i neste generasjons kontrollsentre.[112] Legger man til rette for utviklingen, kan dette medføre at driftskontrollsystemene og DMS-løsningene i kraftforsyningen blir enda viktigere for overvåkning, planlegging, respons og

---

[106] Amundsen, G., «Fem ting du bør vite om smarte strømmålere», Aftenposten, 19 februar 2015, URL: http://www.aftenposten.no/digital/Fem-ting-du-bor-vite-om-smarte-strommalere--489651_1.snd,

[107] "ICRI/CIR and iMinds-SMIT advise Belgian Privacy Commission in Facebook investigation", URL: http://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation,

[108] Van Alsenoy, B. Verdoodt, V., Heyman, R., Ausloos. J. and E. Wauters, *From social media service to advertising network, A critical analysis of Facebook's Revised Policies and Terms*, Draft 31. March 2015, v 1.2 the Interdisciplinary Centre for Law and ICT/Centre for Intellectual Property Rights (ICRI/CIR) of KU Leuven, URL: http://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-1.pdf,

[109] Zachariassen, E., «Hafslund-app med skjult lagring av private tekstmeldinger», Digi.no, publisert 04.05.2015, URL: http://e24.no/digital/hafslund-app-med-skjult-lagring-av-tekstmeldinger/23446266

[110] «50 000 kroner i premier til powerhack vinnerne». Demo Steinkjær, ikke datert, URL: https://www.demosteinkjer.no/content/170/50.000-kroner-i-premier-til-PowerHack-vinnerene

[111] *Avanserte Måle- og Styringssystemer – AMS, Kommersielle muligheter og utfordringer,* Veileder utgitt av Norsk Teknologi, URL: http://norskteknologi.no/Bibliotek/Nyhetsarkiv/2011/Avanserte-Male--og-Styringssystemer---AMS/

[112] Se Sand, 2012.

dokumentasjon enn det er i dag. Dette skyldes integrasjon av systemer og realtidsdata som vil kunne gi mer funksjonalitet og også mulighet for å øke forsyningssikkerheten.

Sett i lys av hva man mener utviklingen vil innebære av bruk av IKT-teknologi, programvare- og tjenesteutvikling vil de ikke være unaturlig å anta at IKT i nær fremtid vil være en vel så stor del av et nettselskaps virksomhet som selve drift og vedlikehold av strømnettet.

Dette vil utfordre myndighetenes evne til å fastsette rammevilkår som både fremmer utvikling, men også sikrer at selskapene har nødvendig kompetanse og evne til å ivareta sikkerheten til både system og infrastruktur og beskyttelse av personopplysninger.

6 Overvåking, logging og hendelseshåndtering

Det er ikke mulig å sikre seg fullstendig mot feil og tilsiktede hendelser. Kompleksiteten i store integrerte systemer gjør at sannsynligheten for feil og hendelser øker, som for eksempel at en oppgradering utløser en feil som ikke var forutsatt på forhånd. Samtidig ser man også at sårbarhetene og aktørenes evne til å finne sårbarheter og sikkerhetshull øker. Logging, logganalyse og hendelseshåndtering blir derfor stadig viktigere

Dette er også påpekt av Mørketallsundersøkelsen for datakriminalitet 2014 (s 25-26): Det er viktig å ha logger fra nettverksutstyr, webservere, brannmurer og påloggingstjenester sammen med gode rutiner rundt logging kan avdekke kvalitetsproblemer og om utstyr er i ferd med å gå i stykker. Det er også ifølge undersøkelsen viktig å ha loggmateriale tilstrekkelig tilbake i tid slik at etterforskning og effektiv feilretting blir mulig. Logger kan bidra til at svikt eller innbrudd i AMS-målere eller andre komponenter blir oppdaget.

Uten logger, verktøy og kunnskap til å kunne analysere disse kan man fort stå på bar bakke og være blind. I Mørketallsundersøkelsen 2014 svarte 15 % av de virksomhetene som svarte at de ikke logget.

Torres (2015) påpeker at det er fullt mulig for en aktør å være inne i et nettverk ubemerket. Imidlertid er deteksjon mulig med riktig teknologi, prosess og ekspertise, men i hvilken grad man investerer i verktøy og ressurser er avhengig av organisasjonsmessige forhold og hvor mye risiko selskapet er villig til å ta.

Ved å samle inn relevante data og sette disse sammen, kan for eksempel tegn på en angripers forflytning i skjul av legitim bruker bli oppdaget. En automatisert prosess for håndtering av hendelser i systemet kan deles inn i kontinuerlig datainnhenting, aggregering og trussel-analyse, og til sist en strømlinjeformet levende responskapasitet.

For selskapene i kraftforsyningen innebærer dette at virksomheten, for å overvåke og logge alt som har betydning for informasjonssikkerheten, til enhver tid må ha fullstendig sporbarhet på hendelser. Man må da innhente logger på nettverks-, system- og applikasjonsnivå fra alle komponenter som inngår i driftskontrollsystemet. De fleste datasystemer har automatiske loggfunksjoner, men det er også muligheter å kjøpe egne

dataloggere for måling og logging av temperatur, luftfuktighet, CO2, strøm (4-20 mA), spenning, puls/frekvens, trykk/nivå med mer.[113]

6.1 Logger og personvernhensyn

Selskapene bør ha overvåking og logging på nettverk og system som ikke er en del av driftskontrollsystemet for å forhindre at uvedkommende får tilgang til andre typer virksomhetskritisk informasjon. Dette kan dessuten innebære å overvåke og logge e-post-trafikk og endring i brukerrettigheter for å forhindre at skadevare kommer inn i virksomhetens nettverk via e-post.

Det er også reist spørsmål om beskyttelse av lagrede data. Data kan være sensitive i aggregert form. Store mengder informasjon om sluttbrukere blir lagret, og dette vil kunne si noe om profilen til sluttbruker. Da er det igjen et spørsmål om personvern. Men dersom det er driftshensyn å ta, dataene er beskyttet og det er rutiner for å hente dem ut, så er personvern vanligvis ikke noe problem.[114] Overvåking, logging og lagring av logger krever imidlertid at virksomhetene har et bevisst forhold til hvilke regler som gjelder for beskyttelse av personopplysninger.

6.2 Krav til logging i andre sektorer

6.2.1 Regler fastsatt av Datatilsynet

Virksomheten må som hovedregel ha et frivillig, uttrykkelig og informert samtykke fra de ansatte dersom overvåking og logging skal brukes til andre formål enn administrasjon og informasjonssikkerhet. Logging er i utgangspunktet en behandling av personopplysninger som er meldepliktig etter personopplysingsloven. Loggingen er likevel fritatt fra meldeplikten dersom opplysningene bare skal brukes til administrasjon av datasystemet eller oppdagelse og oppklaring av brudd på sikkerheten. Dersom loggene indikerer straffbare forhold, skal politiet alltid kontaktes.[115]

6.2.2 NSM

Store nasjonale forskjeller i sikkerhetspraksis i EU har fremtvunget et arbeid med felles sikkerhetsregulering på tvers av sektorene.

Virksomheter underlagt Sikkerhetsloven er pliktige til å rapportere hendelser. I følge NSM er det til tross for dette mangelfull rapportering. Noe av grunnen er gammelt lovverk der dette knyttes til noe en fysisk sett har mistet. Det pågår nå et arbeid med å revidere Sikkerhetsloven. Det er vel så viktig å se på nesten-hendelsen eller forsøk på innbrudd/scanning etc. Det sier noe om hvor trenden går.

NSM har utarbeidet en veileder som gir noen råd om logging på lukkede systemer.[116] I følge veilederen skal følgende hendelser alltid logges: Start og stopp av systemet, inn– og

---

[113] «Dataloggere for temperatur og andre behov», Eskeland Electronics, URL: http://www.detektor.no/subdet192.htm?gclid=CPO9uv7x_8UCFebDcgodgysAXw

[114] Fra møte med KraftCERT

[115] «Overvåking og logging av arbeidstakernes nettbruk», Datatilsynet, 01.08.2013, URL: http://www.datatilsynet.no/Sektor/Arbeidsliv/Overvaking-logging-nettbruk/

[116] *Nasjonal Sikkerhetsmyndighet, Veiledning i grunnleggende sikkerhetsarkitektur og*

utlogging av brukere, endring av systemobjekter ifm. normal drift (dvs. ikke ifm. installasjon og oppgradering), all mislykket tilgang, endringer i systemets sikkerhetspolitikk, endringer i brukerdatabasen og sikkerhetskopiering.

Systemet skal kunne logge data, dvs. innholdet som importeres og eksporteres. Systemet skal stoppe normal drift hvis logging stopper, f.eks. ved fulle loggfiler. Systemadministratoren skal varsles i rimelig tid før loggfiler blir fulle. Loggdata skal lagres på andre partisjoner enn brukerdata, operativt system og nettverksapplikasjoner. Systemet skal ha et verktøy for å konsolidere/revidere loggdata. Brukere skal regelmessig informeres om viktige sikkerhetsrelevante hendelser som har involvert deres brukerkonti. Blant annet skal det informeres om tidligere innlogginger mht. sted (terminal), tidspunkt, status og eventuelt varighet. Følgende loggdata skal sikkerhetskopieres til off-line media og lagres i minimum fem år: Originale server-loggdata, uavkortet og i originalformat. Konsoliderte loggdata på sentrale loggservere og originale loggfiler på arbeidsstasjoner kan overskrives sirkulært og behøver ikke lagres.

6.2.3 Norsis

Norsis sier følgende om logging i forbindelse med trådløse nettverk. Logging av trafikk på nettverket er kritisk for å finne flaskehalser, oppdage feilsituasjoner eller oppdage ulovlig bruk av linjene. Aktiver et fornuftig nivå av logging på alle aksesspunkt, og etabler rutiner for å gjennomgå loggene med jevne mellomrom. Husk også å ta sikkerhetskopi av loggene. Den enkleste metoden er å logge MAC-adresser for å kunne dokumentere når mobile enheter har vært pålogget. Denne funksjonen finnes innebygd i de fleste trådløse aksesspunkt. Systemet kan skaleres opp slik at man kan finne ut hvilke brukere som var pålogget og hva de brukte nettverket til.[117]

6.2.4 Nasjonal kommunikasjonsmyndighet (NKOM)

NKOM har ingen konkrete formkrav til logging, men sikkerhetskravene i ekomloven forutsetter i praksis at tilbyderne gjør tilstrekkelig logging for å kunne avdekke sikkerhetsbrudd i egne nettverk. Forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften) kapittel 2 gir informasjon om hva som er lagringspliktige data i forbindelse med telefoni og internett-trafikk. Til nå har det ikke vært noe krav om videresending av logger for analyse hos NKOM, men det kan ikke utelukkes at dette ikke kan skje i fremtiden. NKOM har derimot strenge krav til rapportering om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til elektroniske kommunikasjonstjenester. Dersom IKT-hendelser kan redusere eller har redusert tilgjengeligheten til ekomtjenester skal disse varsles til NKOM i henhold til eksisterende retningslinjer.

6.3 Regulering og veiledning

Alle selskap i energiforsyningen som har et driftskontrollsystem i klasse 2 eller 3, har i henhold til beredskapsforskriften krav på seg til å 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. Selskapene

---

-*funksjonalitet for FELLESNIVÅ operasjonsmåte*, NSM, 12.12.2006, URL: https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/

[117] «Trådløst nettverk», Norsis, URL: https://norsis.no/2013/12/tradlost-nettverk/

har også plikt til å rapportere omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemet og AMS.

Kravet gjelder spesifikt for driftskontrollsystemet, men for å få en effektiv beskyttelse, anbefales det at også trafikk utenfor driftskontrollsystemet overvåkes og logges. Dette sees i sammenheng med at sensitiv informasjon om kraftforsyningen også lagres og prosesseres utenfor driftskontrollsystemet. Anbefalingen om overvåking utenfor driftskontrollsystemet må sees i sammenheng med kravet om å hindre uautorisert tilgang til sensitiv informasjon.

NVE fikk utarbeidet en spesialveileder av mnemonic med forslag til hvordan man effektivt kan implementere overvåking og logging i driftskontrollsystemet.

I kravspesifikasjonen til AMS utgitt av SINTEF er det konkretiserte krav til logging av sikkerhetsrelaterte operasjoner (lesing, skriving, endring) og administrative forhold (versjon etc.) om komponenter i AMS-innsamlingssystemet. Også NVEs veileder til sikkerhet i AMS har et punkt om logging og overvåking for å sikre kontroll med tilganger og avdekke uautoriserte tilganger i systemet.

I tilknytning til dette ligger det en latent utfordring for bransjen i å møte nye sikkerhetstjenester innenfor dette området som krever tilgang til systemer og logger for å utføre dataanalyse for sikkerhetsformål. Slike systemer, selv om de har sikkerhet som hovedmål, kan introdusere andre sårbarheter, eksempelvis overføring av data til tredjeland.

Det bør arbeides videre med å utvikle regelverket på dette området siden loggdata er viktig for å oppdage hendelser og for å sikre bevis i etterkant, i tilfelle det skulle oppstå hendelser som virksomheten vil politianmelde.

En annen viktig faktor som tilsier at det er viktig å utvikle regelverket som omhandler logging og hendelseshåndtering er forventningen om at kompleksiteten til systemene som selskapene i energiforsyningen forventes å implementere vil øke betydelig i årene som kommer. Overvåking og evnen til å kunne håndtere hendelser vil da bli stadig viktigere for selskapene.

7 Strategier for beskyttelse av kritisk infrastruktur

7.1 IKT-sikkerhetsstrategier i utvalgte land for beskyttelse av kritisk infrastruktur

Strategier for IKT-sikkerhet legger rammene for sikkerhetsarbeid nasjonalt. Mange land har slike strategier. Vi trekker fram noen få her.

Den nederlandske cyber-sikkerhetsstrategien vektlegger en bevegelse over mot samarbeid med private selskaper, fokus på nettverk og strategiske allianser, og å bygge kapasiteter globalt for å håndtere utfordringene nasjonalt. Strategien vektlegger sivilt-militært samarbeid og sier klart at Nederland skal utvikle offensive kapasiteter, dvs. kunne angripe

tilbake. Sektorielle tilsyn skal styrkes ved å inkludere cybersikkerhet uten at dette gir overlapp.[118]

Japan er ved siden av Finland og Norge de land i verden som har renest nett.[119] Den japanske strategien har et mer defensivt fokus enn den nederlandske strategien. Den tegner et godt overordnet bilde av trusselen innledningsvis. Sett opp mot beskyttelse av kritisk infrastruktur vektlegger den tiltak som risikoanalyse, informasjonsdeling og årlige øvelser på å håndtere store cyberangrep der en gjerne kan basere seg på cases fra andre land. Interessant nok nevner den også sertifisering av SCADA-systemer og et regime for slik sertifisering som et tiltak.[120] Strategiene for Japan og Nederland illustrerer hvor stor forskjell det kan være på tilnærminger til cybersikkerhet i ulike land. Finland og Sverige er andre interessante caser. Disse landene har begge rullet ut smarte målere.

Den finske cyber security strategien peker på ansvarsprinsippet. Den vektlegger, i motsetning til de andre vi har nevnt, psykisk motstandsdyktighet (hos befolkningen) på linje med beskyttelse av kritisk infrastruktur og forsvarsevne. Et cybersikkerhetssenter skal bli bygget opp under den finske kommunikasjonsmyndigheten.[121] Senteret skal bidra til god situasjonsforståelse. Et eget styre (Board) for myndighetene (Government Information Security Management Board) skal koordinere arbeidet med sikkerhetsstrategi og retningslinjer. Strategien vektlegger ellers å involvere både næringsliv og frivillige organisasjoner.[122]Den svenske strategien for informasjonssikkerhet retter seg mot staten og har seks mål: Å styrke tilsyn og styring, styrke statens evne til å stille krav i anskaffelser, bidra til at myndighetene skal kommunisere sikkert, at samtlige myndigheter rapporterer IT-sikkerhetshendelser, å bidra til å forebygge IT-relatert kriminalitet og til sist at Sverige skal være en sterk samarbeidspartner internasjonalt.[123]

Store nasjonale ulikheter i cybersikkerhetsinitiativ og tiltak samt en erkjennelse av at sikkerhetsutfordringene er globale i sin natur, er grunnen til at EU Kommisjonen satte i gang arbeidet med et direktiv for nettverks- og informasjonssikkerhet; NIS-Direktivet. Kommisjonen gjennomførte også survey om behovet for NIS, og fikk 160 svar på denne. I energisektoren var det stor oppslutning om NIS (89%). NIS-tiltak som myndigheter tar i bruk skal være konsistente for å minimere konsekvensene av hendelser. Kravet er videre satt til et minimumskrav som er nødvendig for å opprettholde nødvendig beredskap. NIS vektlegger internasjonalt samarbeid om forebyggende sikkerhetsarbeid og hendelseshåndtering. Tiltakene som hvert selskap skal implementere, skal være basert på

---

[118] *National Cyber Security Strategy 2. From awareness to capability*, 2013, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

[119] Kilde: Microsoft.

[120] *Cyber Security Strategy. Towards a world leading, resilient, vigorous cyberspace*, 2013, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world,

[121] Se https://www.viestintavirasto.fi/en/

[122] *Finland's cyber security strategy, Government Reolution*, 24.01.2013, URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[123] *Informations- och cybersäkerhet i Sverige Strategi och åtgärder för säker information i staten*, SOU: 2015:23.

risikoanalyse. De skal være proporsjonale ift. risiko i selskapene. Det skal lages en nasjonal NIS-strategi og en samarbeidsplan. NIS skal revideres regelmessig av Kommisjonen.

7.2 Myndighetssamarbeid i Norge

Digitale trusler er sektorovergripende. Derfor kan det, som NIS-direktivet påpeker, være gunstig med samarbeid mellom tilsynsmyndighetene. Myndighetene kan samarbeide om forebyggende IKT-sikkerhet, hendelseshåndtering, kompetanseheving på IKT-hendelser, og om IKT-tilsyn.

NVE har hatt kontakt med noen norske tilsynsmyndigheter i andre sektorer. Det er stor variasjon i hvor mye ressurser tilsynsmyndighetene har for å føre tilsyn med IKT-sikkerhet. De mest åpenbare samarbeidspartnerne er NKOM, Datatilsynet, Petroleumstilsynet, NSM og Finanstilsynet, men andre som har ansvar for kritisk infrastruktur er også aktuelle samarbeidspartnere. NVE har tatt et initiativ her til å etablere en møteplass for tilsynsmyndigheter med ansvar for kritisk infrastruktur. Første møte ble holdt i NVE 24. februar 2015.

Et synspunkt som er forfektet av andre myndigheter er at de nye avanserte strømmålerne med all sannsynlighet vil være attraktive mål ettersom de er med i en stor gruppe enheter, som noen kan ønske å kontrollere. Sårbarheten til utstyret vil være avhengig av hvor enkel tilgang det er til grensesnittet på hver boks (ettersom de er distribuerte), og hvor godt kommunikasjonen mot strømleverandøren er sikret (gjennom autentisering og kryptering).

I følge NSM plukkes trusseltrender opp ved å studere hvordan trusselaktører utnytter tilsvarende utstyr, hvem som angriper, hvilken metodikk som brukes, motivasjon og konsekvens. Dette krever en operativ kapasitet som deltar i et nasjonalt/internasjonalt fagnettverk av sikkerhetseksperter, som har tilgang til mer informasjon enn den man finner i åpne kilder. I hovedsak vil NorCERT være "fasilitator" i de sektorovergripende aktivitetene, mens KraftCERT vil kunne få en viktig rolle i kraftbransjen. Det er samtidig helt avgjørende med rask og presis deling av informasjon fra NorCERT til NVE og andre myndigheter. Det er sektormyndighetene som har autoritet til å fatte vedtak og gi instrukser for å forebygge og håndtere sikkerhetstruende hendelser i sin sektor.

Utfordringen er at kommunikasjonsinfrastruktur ligger på tvers i bunn, og tjenesteleverandører innen mange segmenter tilbyr sine tjenester på tvers av sektorene. Sektormyndigheten må ha kunnskap om egen bransje, men også oversikt over verdikjeden som gjerne strekker seg over flere sektorer. Derfor blir IKT-sikkerhet sektorovergripende. Samarbeid på tvers av myndigheter og med bransjen kan bidra til å gi et helhetsbilde med hensyn til trusler og beskyttelse.

Størrelsen på fagområdet IKT-sikkerhet er utfordrende. I samtaler med andre myndigheter, har ideen om for eksempel å låne spesialistkompetanse fra andre myndigheter i tilsynsarbeidet blitt fremmet. Tilsynene må samtidig være forankret i god innsikt i sektorenes ulike forutsetninger og hvordan IKT-systemene fungerer som en integrert del av virksomhetenes forskjellige produksjonssystemer.

NKOM har mange grenseflater mot kraftbransjen hvor ingen- eller få andre sektorer er involvert. Disse grenseflatene er selvklare områder for samarbeid. NKOM ser også nytten av tverrsektorielt samarbeid for gjensidig tidlig varsling av trusler. Det vil være en fordel å dele informasjon og bli oppdatert uten å kunne være tilstede på alle arenaene. Dette krever automatiske varslingssystemer.

8 Konklusjoner og anbefalinger

Denne rapporten har tatt opp fire spørsmål som vi oppsummerer i dette kapittelet. Til hvert spørsmål har vi foreslått tiltak eller pekt på områder som det bør arbeides videre med.

8.1 Hvilke sårbarheter er relatert til lagring av informasjon i skyen, og hvilken type informasjon bør ikke legges til skyen?

Store globale skyleverandører har store ressurser og er profesjonelle i sitt sikkerhetsarbeid. Microsoft og Dropbox er skyleverandører som begge er sertifisert iht. ISO 27018. [124] [125] De tilfredsstiller kriterier vedrørende lagring og bruk av personopplysninger, kundenes kontroll med hvordan deres data blir brukt og hvor data befinner seg, krav om at leverandør skal kommunisere hendelser til kunden ved datainnbrudd, og til sist at leverandøren skal ha en uavhengig årlig revisjon utført av en nøytral revisor.

På den andre siden gir kjøper av skytjenester fra seg kontroll og innsynsmulighet. Et sikkerhetsspørsmål er knyttet til i hvilket land data lagres i og hvilket lovverk som gjelder i det landet der data er lagret. Også korrupsjon er viktig å undersøke. Dernest kommer et spørsmål om konsentrasjonsrisiko. Selv store leverandører har en risiko for at også deres systemer har sårbarheter. Feil må utbedres etterhvert som de blir oppdaget og mange kan rammes av den samme feilen. Så er det spørsmålet om gjenoppretting, og hvilken prioritet en liten kunde kan få dersom flere rammes av samme feil, jf. Tieto-hendelsen i 2011.

Hovedbegrunnelsen for å ta i bruk skytjenester er driftsmodellen. Driftsmodellen gir store økonomiske besparelser sammenlignet med å drifte selv. Man betaler kun for prosessorkraft eller/og mengde lagret informasjon. Denne driftsmodellen kan passe for noen anvendelser. Dagens driftsmønster i prosesskontrollsystemer og motsetninger i sikkerhetsbehov mellom tradisjonell IT og prosesskontrollsystemer gjør at skytjenester her er lite hensiktsmessig. Derimot kan skytjenester være anvendelige på andre områder. Dersom en tar i bruk skytjenester og integrerer disse tjenesten mot egne systemer, kan det innføre sårbarheter.

---

[124] Trent, R., WindowsITPro, “Microsoft First to Achieve ISO/IEC 27018 Privacy Standard for Azure”, URL: http://windowsitpro.com/azure/microsoft-first-achieve-isoiec-27018-privacy-standard-azure

[125] Stevenson, A., Dropbox for Business gets ISO 27018 cloud security classification, v3.co.uk, 18 May 2015, URL: http://www.v3.co.uk/v3-uk/news/2409027/dropbox-for-business-gets-iso-27018-cloud-security-classification

Det finnes ulike modeller for skytjenester. De ulike modellene gir ulik grad av kontroll over infrastruktur og systemer. For det enkelte nettselskap, som ønsker å ta i bruk skytjenester, er det tilpasningsmuligheter gjennom de ulike modellene og gjennom hybride løsninger. NVEs veileder peker på behovet for å gjøre risikoanalyse i forkant av systemendringer.

8.1.1 Reguleringsutfordringer relatert til skytjenester

KMD og NSM arbeider med en skypolitikk og en sikkerhetsanalyse for skytjenester. Dette arbeidet kan legge føringer for hvilke anbefalinger NVE bør gi til bransjen om bruk av skytjenester.

Systemintegrasjon på tvers av virksomheter og land utfordrer tradisjonell sikkerhetstankegang og grensesetting. For tiden anbefaler vi å se til NVEs veileder, Datatilsynets, NorSIS' og ENISAs veiledere for skytjenester (Cloud) som gir råd om sikker bruk av skytjenester. På møte i regi av NSM og Norsis 15. juni 2015[126] ble det sagt fra NSM at virksomheter må gjøre en verdivurdering av informasjonen virksomheten besitter, og identifisere den aller mest kritiske informasjonen. Så må en vurdere om denne skal inn i systemer som er koplet til Internett. I følge NSM er skytjenester noe som vil bli tatt mer og mer i bruk, og sannsynligvis ligger allerede mye sensitiv informasjon lagret i skyen.

8.1.2 Anbefalinger

NVEs Beredskapsforskrift setter klare føringer for skytjenester på at selskapene må ha kontroll med hvem som har tilgang til informasjonen og implementere sikkerhet deretter. Beredskapsforskriften beskriver hva som minimum er å regne som kraftsensitiv informasjon som skal sikres mot uvedkommende.

Etter vår oppfatning betyr kravene i forskriften at det er begrensninger til bruk av skytjenester. Eksempel på dette er Braadlandprosjektet som baserer seg på skytjenester fra Microsoft Azure. Her er følgende punkt i forskriften relevant;

§ 6-2 c) Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre anlegg.

I Braadlandprosjektet vil selskapene bruke skytjenester for å få en tilnærmet sanntids risikoanalyse av lavspent distribusjonsnett. Det kan oppnås ved at selskapene i forbindelse med AMS-utrullingen også forsyner enkelte nettstasjoner med logikk og brytermulighet. Selskapet vil da få presentert et «sanntids» enlinjeskjema basert på dataprosessering i skyen.

8.2 Hvilke digitale sårbarheter i AMS-systemet kan potensielt sette forsyningssikkerheten i fare?

I Norge har folk høy tillit til myndighetene, og er åpne for å ta i bruk ny teknologi. Kritiske debatter, som den vi har sett i Nederland, UK eller USA har ikke oppstått her. Dersom det oppstår alvorlige hendelser kan dette bildet endre seg.

[126] Foredrag av NSM, Roar Thon.

Det er selskapene som er ansvarlige for effektiv drift og sikkerhet i AMS-løsningen. AMS-systemet er et komplekst system. Systemintegrasjon og mange tusen endepunkter gir digitale sårbarheter som kan utnyttes. Trusselbildet er enda prematurt på dette området og eksisterer mest på forskningsstadiet. Ettersom denne teknologien tas i bruk i hele Norge og Europa, vil dette bildet kunne det endre seg. AMS har en fordel og en ulempe: Forsyningssikkerheten blir på den ene siden styrket fordi AMS gir bedre situasjonsbilde og styringsmuligheter for det enkelte nettselskap. AMS gir i tillegg mulighet for å utvikle nye tjenester slik som for eksempel Lyse og Braadlandprosjektet gjør. På en annen side øker kompleksiteten og antall endepunkter i infrastrukturen, og mer personopplysninger blir registrert elektronisk. Det finnes flere sårbarheter som potensielt kan utnyttes eller medføre utilsiktede hendelser. Sårbarhetene eksisterer både på teknisk nivå og på organisatorisk nivå. Sårbarhetsbildet avhenger videre av arkitektur og driftsmodell.

En potensiell nasjonal sårbarhet, som går på tvers i bransjen, er konsentrasjonsrisikoen. Denne er påfallende i Finland med en dominerende leverandør av smarte målere. Her kan en programvareoppdatering som feiler få utilsiktede konsekvenser for alle husholdningskundene dersom den rulles ut samtidig. Dersom bransjen i Norge gjennom anbudsrundene ender opp med et fåtall store leverandører, kan et stort antall målere falle ut som følge av en programvarefeil. Dersom slike felles digitale sårbarheter utnyttes i en konfliktsituasjon av en motpart til for eksempel å kople ut et stort antall målere, kan det gi et sterkt politisk budskap.

8.2.1 Reguleringsutfordringer knyttet til AMS

Kompleksiteten i AMS-infrastrukturen, der også tilleggstjenester inngår, gjør at utilsiktede hendelser kan oppstå med kjeder av konsekvenser. Slike hendelser er det i utgangspunktet vanskelig å forutse. En kan derfor ikke se bort ifra at det kan oppstå situasjoner der en får uønsket masseutkopling av målere. Mulige reguleringsutfordringer og behov for sikkerhet er knyttet til følgende:

- Beredskapsforskriften gir omfattende krav for informasjonssikkerhet og prosesskontroll (kapittel 6 og 7). Det er viktig å understreke at Beredskapsforskriften gir minstekrav. Trusselbildet og teknologien er i stadig endring, og det krever en aktiv holdning til sikkerhet og risiko. Ansvaret for sikkerhet ligger på ledernivå i selskapene. Sikkerhetsarbeidet bør integreres i virksomhetsstyringen (årshjulet) og i virksomhetskulturen. Det vil alltid være en restrisiko.
- NVE har i Måle-og avregningsforskriften stilt krav til nettselskapene om sikkerhet i AMS og om å gjøre risikoanalyser. Nettselskapene er dermed ansvarlig for å levere løsninger til kundene med riktig sikkerhetsnivå. Nettselskapene kan velge å bruke kommersielle ekomtjenester som delleveranser til i sin løsning eller utvikle egne løsninger. I henhold til JRCs rapport, har mange av målerne som rulles ut i Europa og i Norge, benyttet GPRS som kommunikasjonsprotokoll. Denne er sårbar for avlytting, jf. basestasjonsaken som rullet opp i Norge høsten 2014. En løsning er kryptering, men det gir uansett ikke 100% beskyttelse, og trådløs kommunikasjon vil likevel være sårbar for interferens og jamming.
- Systemintegrasjon og leverandøravhengighet er en annen sårbarhet. Med store anskaffelser og samarbeidsprosjekt er risikoen i seg selv knyttet til konsentrasjon, mangel på kontroll, fare for innlåsing til en leverandør og svak kundemakt

spesielt opp mot store leverandører. I beredskapssituasjoner kan små norske sammenslutninger eller enkeltselskaper risikere å bli nedprioritert. Det er ikke innenfor NVEs mandat å regulere konkurransen på leverandørmarkedet, men dette er forhold som bransjen bør være klar over.

8.2.2 Anbefalinger

Beredskapsforskriften bør revideres med hensyn til AMS og bryterfunksjonalitetens potensielle kritikalitet. Det kan også vurderes om Måle- og avregningsforskriften bør revideres.

NVE bør vurdere klare krav til overvåking og logging av aktiviteten i AMS-løsningen. Da må selskapet og kunden ha mulighet til systemovervåkning. Dersom Beredskapsforskriften endres, må NVE også utarbeide ny veileder.

Det er uansett behov for å oppdatere veilederen på punktet sikkerhet i AMS.

NVE bør videre invitere til bransjedialog omkring sikker bruk av bryterfunksjonaliteten, der frihet til å bruke denne funksjonaliteten diskuteres opp mot risiko for misbruk.

Utviklingen fra smarte målere til smarte nett vil kreve økt tilsyn og veiledning fra NVE.

Bransjens sikkerhetskompetanse må videreutvikles. Dette kan for eksempel oppnås gjennom allerede eksisterende forum som Forum for Sikkerhet i Kraftforsyningen (FSK), som også kan diskutere AMS og andre problemstillinger i kjølvannet av ny teknologi. Et partssamarbeid mellom NVE, KraftCERT og bransjeorganisasjonene om kurs og seminarer er en annen mulighet. AMS og smarte nett bør også fortsatt adresseres i beredskapsfora i regi av NVE. Sikkerheten blir ikke bedre enn det svakeste leddet. NVE bør også videreføre samarbeide med andre myndigheter på dette området, og bygge videre på initiativet NVE har tatt til møteplass og myndighetssamarbeid innenfor kritisk infrastruktur.

8.3 Hva er sårbarhetene og utfordringene i forhold til overvåking, logging og personvern?

Logging av datatrafikk og logganalyse vil få økt betydning framover fordi ingen kan garantere 100% sikkerhet. I en del tilfeller må en anta at systemene er kompromitterte. Det er et etterslep på lapping av nulldagssårbarheter. Dette gir mulighet for angrep samtidig som mange virksomheter har en sammensetning av gamle og nye IT-løsninger. I tillegg finnes det et etablert globalt marked for salg av skadevare og sårbarheter.

Logging og logganalyse kan bidra til å oppdage hendelser, bidra til mer effektiv hendelseshåndtering, etterforskning og læring. Men logging og lagring av data reiser også spørsmål om personvern når dataene er personopplysninger. Den nederlandske konflikten rundt AMS illustrerer personvernutfordringene ved hyppige målinger. I den norske utrullingen av AMS har Datatilsynet vært tett med i prosessen. Det er viktig å fortsatt involvere Datatilsynet når større systemendringer blir gjennomført.

8.3.1 Reguleringsutfordringer relatert til logging og hendelseshåndtering

Logging og logganalyse er lite utnyttet i Norge, jf. Mørketallsundersøkelsen 2014. Norske virksomheter har lav modenhet på dette området. Kraftbransjen som helhet er heller ikke så langt framme når det gjelder logging og rapportering av hendelser.

KraftCERT kan være en paraply og et bindeledd til lokale hendelseshåndteringsteam eller sikkerhetsperson i selskapene. Hendelsene må håndteres ute i selskapene, og KraftCERT er normalt ikke on-site. KraftCERT skal gi støtte i hendelseshåndteringen med sin kompetanse, støttefunksjon og tiltak, og også koordinere når hendelsen rammer flere virksomheter.

KraftCERT skal også samarbeide med andre CERTer, både nasjonale og utenlandske, og inngå avtaler med disse om tidlig varsling. Fokus skal være på sårbarheter og trusler som er relevante for sektoren. KraftCERT skal rapportere til NVE om trender og viktige utviklingstrekk. Selskapene har et selvstendig ansvar og plikt til å rapportere hendelser til NVE slik lovverket krever.[127]

8.3.2 Anbefalinger

Etter hvert som KraftCERT får etablert seg, kan de bli en drivkraft på dette området. KraftCERT har i gang et prosjekt på overvåking og logging. NVE bør vurdere å samarbeide med bransjen, bransjeforeningene og KraftCERT med å få på plass en best mulig praksis for overvåking og logging. Siden utviklingen på IKT-siden går såpass raskt som den gjør, bør dette være et kontinuerlig arbeid.

8.4 Hvordan håndterer andre myndigheter lignende utfordringer og hva kan Norge lære av dem?

Det er mange initiativer på gang for å kartlegge risiko ved bruk av skytjenester. NVE bør se til arbeidet til KMD og NSM.

NVE bør se nærmere på de erfaringene man har gjort seg i andre land når det gjelder reguleringsarbeid knyttet til AMS. NVE bør engasjere seg mer i europeisk arbeid knyttet til sikkerhet i AMS, skytjenester, overvåking og logging. Dette kan være viktig, både for å utvikle NVE sin egen kompetanse på området og for at NVE skal kunne gi bidrag til det arbeidet som foregår i EU. I neste omgang treffer EUs direktiver og forordninger norsk kraftforsyning.

Systemintegrasjon og mulighetene for dataanalyse gjør at NVE bør se personvernutfordringer sammen med andre sikkerhetsutfordringer som kan ha betydning for forsyningssikkerheten. ENISA har gjort mye godt arbeid, og på ENISAs nettsider finner en både cyberstrategier, informasjon om smartgrid og sikkerhet i cloud. ENISA har pekt på at det trengs et regulatorisk rammeverk som inkluderer både personvern og cybersikkerhet. Rammeverket bør etablere sikkerhetsmål allerede ved utrulling, kreve obligatoriske risikoanalyser, sertifisering av produkter og organisasjoner, etablere

[127] Raaum, M., «KraftCERT – en sektorressurser», Foredrag på NVE Beredskapskonferanse 2014, URL: http://www.nve.no/Global/Seminar%20og%20foredrag/Beredskapskonferanse%202014/Dag2/KraftCERT_Margrete%20Raaum.pdf

regulatorisk press (bøter), offentliggjøre tilsynsresultater, samt kreve hendelsesrapportering[128].

9 Videre arbeid

9.1.1 Forskriftsrevisjon

Denne rapporten har diskutert trusler, digital sårbarhet og regulering i tilknytning til skytjenester, AMS, logging og systemovervåkning. Arbeidet viser at Beredskapsforskriften og Måle- og avregningsforskriften bør utvides/utdypes/suppleres med hensyn til skytjenester, AMS, logging og hendelseshåndtering. Nye trender vil kunne komme i framtiden. På sikt kan for eksempel bruk av droner bli en realitet, og denne teknologien kan gi et ytterligere press på muligheten til å holde informasjon som er synlig i terrenget skjermet. Det er viktig at beredskapsforskriften og måle- og avregningsforskriften så langt som råd blir anvendelig selv om det oppstår teknologiskifter.

9.1.2 Andre forskningsprosjekter

Demo Steinkjer tilbyr mot betaling studenter og forskere et simuleringsmiljø for AMS og data relatert til strømforbruket (tidsserier), strømproduksjon og hendelser i strømnettet. Dataene kan lastes ned fra Demo Steinkjers nettside eller man kan knytte seg til databanken. NVE kan vurdere å bruke denne infrastrukturen til å simulere bryterfunksjonen og masseutkopling, men pga. tidsbegrensninger er dette en oppgave som kanskje heller kunne egnet seg å sette bort til en masterstudent eller en doktorgradsstudent. Dette kan være en aktuell problemstilling å ta tak i særlig med tanke på studier av bryterfunksjonaliteten.

NVE bør oppfordre bransjen til å bruke nettselskapenes FoU-ordning som innebærer mulighet for utvide inntektsrammen.[129]

[128] Leszczyna, R., *ENISA Recommendations on Smart Grid Security*, URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-workshop/enisa-recommendations-on-smart-grid-security,

[129] Se URL: http://www.nve.no/no/Kraftmarked/Regulering-av-nettselskapene/Finansiering-av-FOU/

10 Referanser

Ablon, L., Libicki, M.C., and A. A. Golay, Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar, RAND Nartional Security Research Division, Santa Monica CA, URL: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Amundsen, G., «Fem ting du bør vite om smarte strømmålere», Aftenposten, 19 februar 2015, URL: http://www.aftenposten.no/digital/Fem-ting-du-bor-vite-om-smarte-strommalere--489651_1.snd,

Andersen, R. and S. Fuloria, "Who Controls the off Switch?" First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, 96 – 101, DOI: 10.1109/SMARTGRID.2010.5622026

Anthony, S., UK government quietly rewrites hacking laws to give GCHQ immunity, URL: http://arstechnica.com/tech-policy/2015/05/uk-government-quietly-rewrites-hacking-laws-to-grant-gchq-immunity/

«Automatiske målesystemer kan registrere adferd i hjemmet», Datatilsynet, 20.04.2015, URL: https://www.datatilsynet.no/Teknologi/Stromavlesing/

Avanserte Måle- og Styringssystemer – AMS, Kommersielle muligheter og utfordringer, Veileder utgitt av Norsk Teknologi, URL: http://norskteknologi.no/Bibliotek/Nyhetsarkiv/2011/Avanserte-Male--og-Styringssystemer---AMS/

Bakken, J.B., Christensen I. S. og M. Ånestad, «Tidenes hacker-angrep i Norge», Dagens Næringsliv, 26.08.2014, URL: http://www.dn.no/nyheter/2014/08/26/2159/IT/tidenes-hackerangrep-i-norge

Borgund, L, Skytjenester i energiforsyningen, En forstudie, Deloitte, 12.april 2014.

Catching Up on the OPM Breach, June 15, KrebsonSecurity, URL: http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

«Cloud computing», ENISA, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

Corruption Perception Index 2014: Results, Transparency International, URL: http://www.transparency.org/cpi2014/results#myAnchor1

Covrig, C.F., Ardelean, M, Vasiljevska, J., Mengolini, A., Fulli (DG JRC) and E Amoiralis (External), Smart Grid Project Outlook 2014, JRC Science and Policy Report, URL: http://ses.jrc.ec.europa.eu/smart-grids-observatory

Cuijpers, C. M. K. C., & Koops, E. J.." Smart metering and privacy in Europe: Lessons from the Dutch

case." In S. Gutwirth, R. E. Leenes, P. de Hert, & Y. Poullet (Eds.), European data protection: Coming of age. Unknown Publisher. 2012: 269-293.

Cyber Security Strategy. Towards a world leading, resilient, vigorous cyberspace, 2013, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

«Dataloggere for temperatur og andre behov», Eskeland Electronics, URL: http://www.detektor.no/subdet192.htm?gclid=CPO9uv7x_8UCFebDcgodgysAXw

Dekker, M.A.C. and D. Liveri, Cloud Security Guide for SMEs, Cloud computing security risks and opportunities for SMEs, ENISA, April 2015. ENISA.

«Digital Agenda for Europe», URL: https://ec.europa.eu/digital-agenda/en/our-goals/pillar-vii-ict-enabled-benefits-eu-society

«Digital Agenda for Norge», URL: https://www.regjeringen.no/nb/dokumenter/meld-st-23-20122013/id718084/?docId=STM201220130023000DDDEPIS&ch=1&q=

Global Cybersecurity Index and Wellness Profiles, ITU, April 2015, URL: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

CSA Survey Results, Government Access to Information, Cloud Security Alliance, July 2013, URL: https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf

«Digital marketplace», Gov.uk, URL: https://www.gov.uk/how-to-use-cloudstore

Dimitra Liveri and Dr. M.A.C. Dekker, Security Framework for Governmental Clouds, All steps from design to deployment, ENISA, Secure infrastructures and services Unit, February 2015.

Dutch Energy Savings Monitor for the Smart Meter, Rijkdienst voor Ondernemend Nederland, March 2014, Final. s10.

«EB velger Smart», 2 februar 2015, URL: https://www.eb.no/eb-velger-esmart-fremtiden/

Electricity grid Modernization. Progresss Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed., United States Government Accountability Office, GAO-11-117, January 2011.

Egozcue (a), E., Rodríguez , D. H., Ortiz, J. A., Villar, V. F. and L. Tarrafeta., Annex I. General Concepts and Dependencies with ICT, [Deliverable – 2012-04-19], ENISA 2012., URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid

Egozcue (b), E., Rodríguez , D. H., Ortiz, J. A., Villar, V. F. and L. Tarrafeta., Annex II. Security aspects of the smart grid, ENISA, 2012.

European Cloud Computing Strategy, European Commission, URL: https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

Etterretningstjenestens vurdering. FOKUS 2015, Forsvaret, URL: http://forsvaret.no/ForsvaretDocuments/FOKUS2015-endelig.pdf

Evans, D., ”What is BYOD and why is it important?”, Computing, August 23 2013, URL: http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important--1175088,

Finland’s cyber security strategy, Government Reolution, 24.01.2013, URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

Fire effektive tiltak mot dataangrep, Nasjonal sikkerhetsmyndighet, Oppdatert 2014-01-31, URL: http://nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften), FOR-2012-12-07-1157, URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157/KAPITTEL_7#KAPITTEL_7

Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology, February 12, 2014.

«God sikkerhet grunnleggende for vellykket AMS-utrulling», NVE, 10.02.2012, URL: http://www.nve.no//no/Nyhetsarkiv-/Nyheter/God-sikkerhet-grunnleggende-for-vellykket-AMS-utrulling/

Grindal, Kristin M. E., Brukergrensesnitt og visualisering i fremtidens driftssentral for smarte nett, NTNU, Fordypningsprosjekt Desember 2014.

Graabak, Ingeborg, og Søle, Hanne, Kravspesifikasjon for utbygging av Avanserte Måle- og styringssystemer (AMS) (toveiskommunikasjon), Teknisk rapport, SINTEF 16/9-2011.

Hamill, J., “UK smart meters arrive in 2020. Hackers have ALREADY found a flaw”, The Register, 30 Oct 2014, URL: http://www.theregister.co.uk/2014/10/30/smart_meter_hackable_for_free_electricity_say_security_reserachers/

Higgins, K.J., “Smart Meter Hack Shuts Off The Lights”, InformationWeek, 10.01.2014, URL: http://www.darkreading.com/perimeter/smart-meter-hack-shuts-off-the-lights/d/d-id/1316242,

« Industrial Control Systems/SCADA”, ENISA, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO/IEC 27018:2014(en).

Informations- och cybersäkerhet i Sverige Strategi och åtgärder för säker information i staten, SOU: 2015:23.

Keeny et al, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, Carnegie Mellon Software Engineering Institute, May 2005. URL: http://www.google.no/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fwww.secretservice.gov%2Fntac%2Fits_report_050516.pdf&ei=4rwnVcjzOMelsgGBsoCYDw&usg=AFQjCNE5St461H5j-y4Iui58zlNMdKRlQQ

Kleinman, Z, "Smart meters need to be harder to hack, experts say", BBC News, 25 May 2013, URL: http://www.bbc.com/news/technology-22608085

"Kortere responstid", Aidon, URL: http://www.aidon.com/no/savon-voima/

Krebs, B., "Smart meter hacks likely to pread: FBI", Theage.com, April 10, 2012, URL: http://www.theage.com.au/it-pro/security-it/smart-meter-hacks-likely-to-spread-fbi-20120410-1wm84.html,

Leszczyna, R., ENISA Recommendations on Smart Grid Security, URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-workshop/enisa-recommendations-on-smart-grid-security,

Luciano (J.R.) S. and J. Yeoh, Cloud Usage: Risks and Opportunities Report, Cloud Security Alliance, September 2014.

Lewis, D. and J. Kerr, Not too clever: Will Smart Meters be the next Government IT disaster?, IoD Policy Report.

Martinez, L. "Stockton Smart Meters Explode After Truck Causes Power Surge", March 30, 2015, URL: http://sacramento.cbslocal.com/2015/03/30/stockton-smart-meters-explode-after-truck-causes-power-surge/

Mørketallsundersøkelsen 2014, NSR, URL: http://www.nsr-org.no/moerketall/

Nasjonal Sikkerhetsmyndighet, Veiledning i grunnleggende sikkerhetsarkitektur og

-funksjonalitet for FELLESNIVÅ operasjonsmåte, NSM, 12.12.2006, URL: https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/

National Cyber Security Strategy 2. From awareness to capability, 2013, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

«Overføring av personopplysninger til utlandet», Datatilsynet, 25.11.2011, URL: https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/

«Overvåking og logging av arbeidstakernes nettbruk», Datatilsynet, 01.08.2013, URL: http://www.datatilsynet.no/Sektor/Arbeidsliv/Overvaking-logging-nettbruk/

Peace and Corruption 2015. Lowering corruption – a transformative factor for peace, Institute for Economics and Peace, URL: http://www.visionofhumanity.org/sites/default/files/Peace%20and%20Corruption.pdf

Planera för effekt. Slutbetenkande från Samordningsrådet för smarta elnät, SOU 2014:84, s 283.

Plummer, Q., "Microsoft Adopts ISO/IEC 27018 For Personal Data, Privacy Protection In Public Cloud", Tech Times, February 18, URL: http://www.techtimes.com/articles/33342/20150218/microsoft-adopts-iso-iec-27018-for-personal-data-privacy-protection-in-public-cloud.htm

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security accrues the Union, European Commission, Brussels 7.2.2013 COM 2013 48 Final.

Protecting Industrial Control Systems Annex I: Desktop Research Results, ENISA, [Deliverable – 2011-12-09], URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/annex-i,

Raaum, M., «KraftCERT – en sektorressurser», Foredrag på NVE Beredskapskonferanse 2014, URL: http://www.nve.no/Global/Seminar%20og%20foredrag/Beredskapskonferanse%202014/Dag2/KraftCERT_Margrete%20Raaum.pdf

Refleksjoner kring samhällets skydd och beredskap vid alvarliga ut-incidenter. En studie av konsekvensarne i samhället efter driftsstörningen hos Tieto i november 2011, MSB, URL: https://www.msb.se/RibData/Filer/pdf/26170.pdf

Risiko 2015, NSM, URL: http://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/NSM_Risiko_2015-web.pdf

Robert, A., French surveillance legislation is off to a bad start", Published 9th April 2015, Euractiv.com, URL: http://www.euractiv.com/sections/infosociety/french-surveillance-legislation-bad-start-313616

Rushe, D., "Privacy is not dead: Microsoft lawyer prepares to take on US government", the Guardian, 14th December 2014, URL: http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government,

Symantec Intelligence Report, January 2015.

Skapalen, F. og Jonassen, B., Veileder til sikkerhet i avanserte måle- og styringssystem, NVE, 2012.

Sand, K., Next Generation Control Centres – State of art and future scenarios, Teknisk rapport, 11-06-2012, NTNU, 2012.

Schwartz, M.J., “Anti-Hacker Executive Order: 5 Concerns” , US Government Information Security, April 3, 2015, URL: http://www.govinfosecurity.com/anti-hacker-executive-order-5-concerns-a-8072,

Santillan, M., “Once Every Four Days, The US Power Grid Is Under Attack”, Apr 2, 2015, URL: http://www.tripwire.com/state-of-security/latest-security-news/once-every-four-days-the-us-power-grid-is-under-attack/

Seals,T. “#RSAC: Microsoft Azure Focuses on Transparency and Control”, published 22. April 2015, URLhttp://www.infosecurity-magazine.com/news/rsac-microsoft-focuses-on/

“Smart meters: consumer profiling will track much more than energy consumption if not properly safeguarded, says EDPS”, Press release, EDPS/10/12, Brussels, Monday 11 June 2012, URL: http://europa.eu/rapid/press-release_EDPS-12-10_en.htm?locale=en

Stevenson, A., Dropbox for Business gets ISO 27018 cloud security classification, v3.co.uk, 18 May 2015, URL: http://www.v3.co.uk/v3-uk/news/2409027/dropbox-for-business-gets-iso-27018-cloud-security-classification

Sæle, H., Sagosen, Ø., & Bjørndalen, J. Norsk Driftsentralkultur. Trondheim: SINTEF Energi AS, 2014.

Tideman, A., Høverstad, B., A., Langseth, H. og P. Öztürk, “Effects of scale on load prediction algoritms”, 22nd Internasjonal Conference on Electricity Distribution, Stockholm, 10-13 June 2013, Paper 1205, URL: http://www.idi.ntnu.no/~helgel/papers/TidemannHoverstadLangsethOzturkCIRED13.pdf

Torres, A., Automation in the Incident Response Process: Creating an Effective Long-Term Plan, SANS Whitepaper, February 2015.

Trent, R., WindowsITPro, “Microsoft First to Achieve ISO/IEC 27018 Privacy Standard for Azure”, URL: http://windowsitpro.com/azure/microsoft-first-achieve-isoiec-27018-privacy-standard-azure

«Trådløst nettverk», Norsis, URL: https://norsis.no/2013/12/tradlost-nettverk/

Tøndel, I. A., Line, M., Johansen, G., & Jaatun. Risikoanalyse av AMS knyttet til informasjonssikkerhet og personvern. Trondheim: SINTEF IKT, 2014.

Van Alsenoy, B. Verdoodt, V., Heyman, R., Ausloos. J. and E. Wauters, From social media service to advertising network, A critical analysis of Facebook’s Revised Policies and Terms, Draft 31. March 2015, v 1.2 the Interdisciplinary Centre for Law and ICT/Centre for Intellectual Property Rights (ICRI/CIR) of KU Leuven, URL: http://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-1.pdf

Veileder til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen, 1, 2013, NVE.

Veiledning for outsourcing av IT, spesielt rettet mot små og mellomstore bedrifter, september 2010. Utgitt av Norsis og NSR, tilgjengelig: https://norsis.no/2012/07/veiledning-for-it-outsourcing/

Veiledning i hendelseshåndtering, https://norsis.no/2012/07/hendleseshandtering/

Venters, W. and E. A Whitley, "A critical review of cloud computing: researching desires and realities", Journal of Information Technology (2012) 27, 179–197. doi:10.1057/jit.2012.17; published online 14 August 2012, URL:

http://www.palgrave-journals.com/jit/journal/v27/n3/full/jit201217a.html,

Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur, Rapport, Norsk Romsenter, mars 2013. URL: http://www.romsenter.no/Aktuelt/Publikasjoner/Rapport-om-saarbarhet-ved-bruk-av-satellittnavigasjon

Wäfler J. and P. E. Heegaard, "Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability, Advances in Communication Networking", Lecture Notes in Computer Science Volume 8115, 2013, pp 185-196 http://www.item.ntnu.no/_media/projects/smartgrid/futurecontrolcenter/doc_interdependency_meta_model-camera_ready_eunice.pdf

Weaver, K. T. ,"Dutch case study: "smart" meter privacy invasions are unjustifiable in a democratic society", Take Back your Power, Investigating the Smart Grid, 6 November 2014, URL: http://www.takebackyourpower.net/news/2014/11/06/smart-meter-privacy-invasions-are-unjustifiable-in-a-democratic-society/

Whitney, L. "Microsoft pulls buggy Patch Tuesday updates", cne.com, December 12, 2014, URL: http://www.cnet.com/news/microsoft-pulls-buggy-patch-tuesday-updates/

Y. Yang, K. McLaughtlin, T. Litttler, S. Sezer, Eul Gyu Im, Z.Q. Yao, B. Pranggono and H..F.Wang, "Man-in-the-Middle Attack Test-Bed Investigating Cyber-Security Vulnerabilities in Smart Grid SCADA Systems", International Conference on Sustainable Power Genereation and Supply (SUPERGEN 2012), s 1-8, 10.1049/cp.2012.1831.

Zachariassen, E., "Dette er effekten av big data", Digi.no, 20. mars 2015, URL: http://www.digi.no/bedriftsteknologi/2015/03/20/dette-er-effekten-av-big-data.

Zachariassen, E., «Skyleverandør slakter egen bransje: – Kutt ut nettskyen», Teknisk ukeblad, 22. september 2014, http://www.tu.no/it/2014/09/18/skyleverandor-slakter-egen-bransje--kutt-ut-nettskyen

Zachariassen, E., «Hafslund-app med skjult lagring av private tekstmeldinger», Digi.no, publisert 04.05.2015, URL: http://e24.no/digital/hafslund-app-med-skjult-lagring-av-tekstmeldinger/23446266

Zage, D., Franklin, D. and V. Uries, "What does the future holds for cloud computing? In: Cross talk", Sept Oct 2013, The Journal of Defence Sortware Engineering, 25. No. 5. http://www.crosstalkonline.org/storage/flipbooks/2013/201309/index.html

2014 Smart Grid System Report, Report to Congress, August 2014, United States Department of Energy, Washington DC 20585.

2015 State of the Endpoint Report: User-Centric Risk, Ponemon Institute Reserach Report January 2015.

2015 Global Encryption & Key Management Trends Study, Ponemon Institute Research Report, April 2015.

«Safe Harbor – prinsipper om overføring av opplysninger til USA», Datatilsynet, 30.11.2014 URL: https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/Safe-Harbor-prinsippene/

«50 000 kroner i premier til powerhack vinnerne». Demo Steinkjær, ikke datert, URL: https://www.demosteinkjer.no/content/170/50.000-kroner-i-premier-til-PowerHack-vinnerene

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no