NVE

RAPPORT

Nr 90/2018

IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen

Elisabeth Kirkebø, Mathias Ljøsne

Rapport nr 90-2018
IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen

Utgitt av: Norges vassdrags- og energidirektorat
Redaktør: Janne Hagen
Forfattere: Elisabeth Kirkebø, Mathias Ljøsne

Trykk: NVEs hustrykkeri
Forsidefoto: Thomas Richter via Unsplash
ISBN: 978-82-410-1762-9
ISSN: 1501-2832

Sammendrag: Energiselskapene er avhengige av leverandører. Samtidig er dataangrep mot virksomheter via digitale verdikjeder en reell trussel. Denne rapporten drøfter IKT-sikkerhet i verdikjeden mellom leverandør og energiselskap. Resultatet viser at innsyn i IKT-sikkerhet knyttet til leveransene omfatter i praksis bare det første leddet ned i verdikjeden, noen ganger også underleverandøren. Den komplekse verdikjeden for produksjon og sammenstilling av maskinvare er særlig utfordrende. Rapporten oppfordrer blant annet til videre bransjesamarbeid for å utvikle felles krav.

Emneord:
Cybersikkerhet
Sikkerhetshendelser
Informasjonssikkerhet
IKT-sikkerhet
Leverandørsikkerhet
Anskaffelser
Tjenesteutsetting

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

Telefon: 22 95 95 95
Epost: nve@nve.no
Internett: www.nve.no

22.10.18

Innhold

Forord

NVE-rapport 90/2017 om Informasjonssikkerhetstilstanden i energiforsyningen viser at energisektoren har stor avhengighet til leverandører. Samme rapport viser samtidig at mange virksomheter er utsatt for uønskede IKT-hendelser, både tilfeldige og menneskeskapte. Så langt har heldigvis ikke dette medført brudd i strømforsyningen som ville slått ut i kostnader, men kan potensielt gjøre det i fremtiden. Risikoen for alvorlige hendelser øker med videre digitalisering og innovasjon. Nye digitale tjenester og produkter slippes på markedet med sårbarheter som ikke blir kjent før etter en viss tids bruk.

Det er en trend med økt bruk av skytjenester og utkontraktering, samt spesialisert tjenestekjøp på blant annet sikkerhet. Lange digitale verdikjeder er opphav til leverandøravhengighet. NVE mener det er nødvendig å se nærmere på digital beredskap i praksis, spesielt samspillet mellom ulike aktører i en stresset situasjon, der deler av den digitale infrastrukturen svikter. På den ene siden tar sektoren i bruk en rekke digitale systemer og verktøy som er til god hjelp i en mulig ekstraordinær situasjon, på den annen side kan disse systemene svikte helt eller delvis.

NVE har som ledd i et FOU-prosjekt om proaktiv digital beredskap fått Elisabeth Kirkebø og Mathias Jore Ljøsne, begge studenter ved universitetet i Oslo, Institutt for informatikk, til å undersøke IKT-sikkerhetsutfordringer i relasjonen mellom kunde og leverandør. Arbeidet ble gjennomført sommeren 2018. Vi takker virksomhetene som har bidratt med informasjon til studentene. Rapporten vil være ett av flere bidrag inn i NVEs FoU-prosjekt, der også den danske Energistyrelsen har kommet med som samarbeidspartner etter at prosjektet ble etablert.

Oslo, 17.oktober 2018

Eldri Holo

Seksjonssjef

for å hindre at sikkerhetsgradert eller sensitiv informasjon om energiforsyningen blir offentlig tilgjengelig gjennom anbudsdokumentene. [7]

Angående datalagring sier selskapene at lovverket er ganske tydelig, men at det er vanskelig å følge opp. De sier at de har stilt krav om hvor dataene skal lagres, men kan ikke kontrollere at kravene blir fulgt. I *Regulering av IKT-sikkerhet* advares det mot slike utfordringer ved bruk av skytjenester: *Data kan fort bli sendt til servere i land hvor jurisdiksjonen er annerledes enn i Norge og derfor er kryptering og kontroll av krypteringsnøklene viktige tema* [10, p. 107]. Selskapene ønsker dessuten en klarere definisjon av hvor kraftsensitiv informasjon kan lagres.

Cyberscurity Procurement Language for Energy Delivery Systems [9] er detaljert på mange områder, men ikke med hensyn til landvurderinger. Anbefalingen er begrenset til at leverandører skal oppgi hvilke land de selv og deres underleverandører holder til i. Leverandøren bør også være pliktig å melde fra hvis et nytt land blir introdusert til leverandørkjeden. Vi oppfatter det som at energiselskapene følger dette rådet halvveis. Den praksisen vi har sett er at leverandøren skal fremskaffe en oversikt over underleverandørene på forespørsel. Dette betyr imidlertid at leverandøren kan endre underleverandør før kunden finner ut av det.

I beredskapsforskriften §6-5 står det at *KBO-enheter som setter ut oppdrag til leverandører og andre med oppdrag for eller i energiforsyningen, skal påse at disse er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for sensitiv informasjon. Det skal også i avtale opplyses at beredskapsmyndigheten kan føre tilsyn med etterlevelsen av disse bestemmelsene. Tilsvarende opplysningsplikt gjelder for leverandører når disse inngår kontrakt med underleverandører* [7].

Dette betyr at energiselskaper bryter beredskapsforskriften hvis de har en avtale med leverandør om lagring av data som de ikke klarer å kontrollere.

5.4 Sertifisering

I intervjuene ble det påpekt hvor ressurskrevende prosessen før og under tjeneste-utsettingen er, og det var flere som uttrykte interesse for et nasjonalt samarbeid om anskaffelser og tjenesteutsetting. Når en virksomhet har tatt beslutningen om å sette ut en tjeneste eller kjøpe inn et produkt så er det fortsatt veldig mye arbeid som må gjøres. En del av dette arbeidet er å vurderer sikkerheten hos leverandøren. Både i organisasjonen til leverandøren, systemene deres, verdikjeden, og produktet eller tjenesten deres. Dette er en betydelig mengde arbeid og det er vanlig at selskap leier inn ekstern kompetanse for å ta seg av mindre eller større deler av dette arbeidet. Mindre selskaper kan ha problemer med å finne denne kompetansen eller har ikke råd til å ansette ekstern hjelp. Det kan ende opp med å gå ut over sikkerheten hos systemene til kunden, sikkerhetstilstanden i tjenesteforholdet, eller eventuelt påvirke det totale sikkerhetsbildet i energibransjen i Norge.

Det er vanskelig for et energiselskap å undersøke sikkerheten gjennom hele verdikjeden. Under intervjuene fortalte leverandørene stort sett at de hadde kontroll på IKT-sikkerheten ett ledd ned i leverandørkjeden, men ikke spesielt lenger. Verdikjedene kan bli veldig lange, spesielt i tilfeller med maskinvareleverandører. Det er ikke praktisk

mulig eller nødvendig å undersøke sikkerheten helt ned til selskapet som utvinner råmaterialet, og for så vidt ender ikke verdikjeden hos dem heller.

En mulig løsning er sertifisering med anerkjente rammeverk som er utbredt i industriell sammenheng, for eksempel ISO27001 som tilhører International Organization for Standardization (ISO) [19].

European Union Agency for Network and Information Security (ENISA) har gitt ut rapporten *Smart grid security certification in Europe* som handler om internasjonalt samarbeid angående sikkerhetssertifisering av nettselskaper [20]. Sertifiseringsordningen blir brukt for å gi trygghet til kundene, men også for å skape tillit mellom ledd verdikjeden. Det er mulig å opprette en lignende ordning i Norge, gjerne knyttet til EUs initiativer på området. En norsk ordning kan omfatte sikkerheten i systemene, produktene eller tjenestene som leveres til energibransjen i Norge/Europa.

EU har bestemt seg for å sette opp et EU-bredt sertifiseringsrammeverk [21] i henhold til *Cybersecurity Act*. Den gjelder for cybersikkerhet i informasjons- og kommunikasjonsteknologi, kommunikasjonsprodukter og tjenester. Sertifikater i henhold til ordningen vil være gyldig i alle EU-land, og gjøre det lettere for selskaper å inngå avtaler på tvers av landegrenser. ENISA anbefaler å fremme sertifiseringsordningen ved å tilby kommersielle fordeler [21]. Hvis det hadde blitt et samarbeid i EU om sikkerhetssertifisering av leverandører, ville sertifiseringen fått et moment, og de aktørene som hadde valgt bort sertifisering vil trolig oppleve sterkt svekkede markedsmuligheter.

En annen eksisterende standard for datasikkerhetssertifisering er *Common Criteria for Information Technology Security Evaluation* [22]. I den nevnes det blant annet at den skal inkludere leverandører som har påstander om sikkerheten i sine produktene. Sertifiseringsordningen blir mest brukt i militært sammenheng, men visse kommersielle produkter, som operativsystemene Microsofts Windows 8 og Windows 10 har også brukt denne [23].

I *Regulering av IKT-sikkerhet* [10] nevner arbeidsgruppen at det fortsatt ikke finnes en nasjonal sertifiserings- eller godkjenningsordning for tilbydere av skytjenester, hvor disse kan få rangert tjenestene sine etter sikkerhetsnivå. En eventuell ordning vil blant annet kreve mellom ulike myndigheter slik at regelverk kan forenkles og harmoniseres. Det finnes allerede et par sertifiseringsordninger i EU man kan ta seg nytte av eller bruke som et grunnlag. Å lage en egen spesifikk sertifiseringsordning for energibransjen ville medført en stor arbeidsbyrde.

Med en sertifiseringsordning så vil selskaper med større trygghet kunne velge hvilke leverandører de vil bruke, uten å måtte legge så mye ressurser i prosessen eller være avhengig av omfattende ekstern kompetanse. Det vil kanskje fortsatt trenges noen for rådgivning, men ikke like mye som det trengs i nåværende situasjon. Sertifiseringsordningen kunne også blitt brukt til å støtte opp oversikten over tjenesteutsettingen gjennom livsløpet. Det hadde spesielt gagnet mindre selskaper som kanskje ikke har midlene til å besitte bestillerkompetanse.

5.5 Beredskap

Fra intervjuene fikk vi inntrykk av at selskapene generelt hadde gode beredskapsplaner. Både energiselskapene og leverandørene hadde mer eller mindre detaljerte planer for

håndtering av ulike hendelser. Energiselskapene hadde beredskapsplaner som beskrev hvordan de skulle klare seg uten leverandørene. Noen hadde noen alternative systemer på plass som kunne driftes lokalt hvis et større system var nede hos leverandøren, og noen hadde fått tilgang til personer hos leverandøren som de kunne kontakte når som helst dersom en hendelse oppstod. Leverandørene svarte at de hadde planer på plass for å støtte en kunde som opplevde en hendelse, og planer om hvem som kunne stille når.

Alle leverandørene fortalte at de hadde vært med på øvelser som kunder hadde tatt initiativ til. Flere av energiselskapene fortalte det samme, og sa at øvelsene hadde hatt variert fokus. Flere av representantene for leverandørene var positive til å delta på flere øvelser med energiselskapene. Bfe §2-7 Øvelser fastsetter at alle KBO-enheter skal gjennomføre øvelser minst én gang årlig og ha en øvelsesplan som dekker flere år. Videre, bfe §2-9 sier at det skal foregå en evaluering i selskapet blant annet etter øvelser. Mulige gevinster ved felles øvelser, der også leverandørene deltar, er bedre forståelse av partenes roller og oppgaver, avklaring av forventninger og generelt bedre kommunikasjon og samarbeid. Dette gjelder både beredskapsøvelser ved skrivebordet og mer praktisk rettede beredskapsøvelser.

5.6 Oversettelse av beredskapsforskriften

Det er uttrykt et ønske om oversetting av beredskapsforskriften til engelsk. Begrunnelsen er at internasjonale leverandører skal kunne forstå avtalene de signerer når det stilles krav til etterlevelse av beredskapsforskriften i kontrakten. Argumentene mot å gjøre dette er at slik forskriften er formulert vil mye av nyansene forsvinne ved en oversettelse. Dermed vil også betydningen endre seg. Det kunne derfor vært en bedre idé at NVE lager en engelsk veileder for hva som skal til for å oppfylle beredskapsforskriften.

5.7 Tilsyn

Med tilsyn menes både revidering av dokumentasjon og fysisk inspeksjon hos leverandøren. Tilsyn er egnet til å avdekke feil, mangler og sikkerhetshull som ellers ikke ville ha blitt oppdaget. Ut ifra intervjuene vi har gjort så er inntrykket at tilsyn i liten grad blir gjennomført To forskjellige leverandører svarte at de hadde opplevd at kunder hadde forespurt eller kommet på tilsyn. En av leverandørene fortalte at de bare hadde opplevd at én kunde hadde bedt om å få komme. Ingen av leverandørene var imot tilsyn hvis det ble etterspurt. Noen fortalte at det også kunne bli arrangert med underleverandørene deres, så her har energiselskapene muligheter som de burde benytte seg av. De fleste energi-selskapene hadde klausuler om tilsyn i kontraktene, men det var nesten ingen selskaper som hadde benyttet retten. Det naturlige spørsmålet å stille blir da: *Hvis det ble vurdert som viktig nok til å være et krav i kontrakten, hvorfor blir det ikke gjennomført i praksis?*

God kontroll kan starte tidlig i livsløpet, med å sjekke referanser. Dette innebærer å kontakte nåværende og tidligere kunder for å sjekke hvordan deres forhold til leverandøren har vært og hvordan leveransen har vært. Det er viktig å sjekke at leverandører leverer det de lover, at de er enkle å kommunisere med, og så videre. Det var flere av de intervjuede som svarte at de hadde kontaktet referanser før inngåelse av kontrakt.

Som et selskap nevnte under intervjuet så kan det være vanskelig å kreve tilsyn hos store leverandører, men er ofte lettere med de mindre. Å kontraktsfeste retten til å sjekke at en

stor leverandør for eksempel faktisk lagrer data innenfor EUs jurisdiksjon kan være veldig vanskelig å få til. Kunden må heller bare stole på det som blir fortalt. Det ble også nevnt at dette betyr at de ikke kan kontrollere om leverandøren følger nasjonale regler, men at akkurat det kanskje heller ikke burde være deres ansvar å følge opp. Det er nok ikke energibransjen sitt ansvar å kontrollere om leverandører følger nasjonale regler, men hvis man oppdager at de ikke gjør det, så må man melde ifra til myndighetene. Hvis en hendelse skulle oppstå og det viser seg at en leverandør har brutt en norsk lov så kan ikke kunden unnskylde seg med at *vi bare måtte stole på det vi ble fortalt* eller *det var ikke vårt ansvar å følge dette opp*. Det er viktig å få de store leverandørene til å tillate at tilsyn blir utført hos dem, men hvordan en skal få til dette i praksis, er en stor oppgave å løse.

Et av selskapene vi intervjuet fortalte at de aldri dro på tilsynsbesøk selv om det var avtalefestet at de hadde lov til det. Selskapet hadde ikke kultur eller for vane å gjøre det. Kultur er her et nøkkelord å ta tak i. Det totale sikkerhetsnivået i et selskap hadde økt hvis selskapet gjorde det til en del av sikkerhetskulturen sin å dra på tilsyn hos leverandørene. Å dra på tilsyn kan være veldig ressurskrevende, som noen av de vi har intervjuet har pekt på, men det kan også bidra til å øke sikkerhetsnivået og finne potensielle sikkerhetshull. Det er derfor viktig at dette blir et større tema og økt oppmerksomhet om dette i industrien. Vi tror at energibransjen har et godt utgangspunkt for å skape en god IKT-sikkerhetskultur basert på deres erfaring med HMS.

Som nevnt i beredskapsforskriften, skal det opplyses i avtalene med leverandører til energiforsyningen, at beredskapsmyndigheten kan føre tilsyn med etterlevelsen av bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon. Det gjelder også når leverandørene inngår kontrakter med underleverandører. Bfe §6-5 sier at *plikten til å påse innebærer at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves*. I visse tilfeller, for eksempel med store aktører i et internasjonalt marked, vil det bli vanskelig å følge bestemmelsen. Problemet med praktisk etterlevelse av legale pålegg bør finne løsning før det utvikler seg en kultur eller holdning om at det ikke er vits å prøve, fordi lovbestemmelsene ikke lar seg overholde uansett.

5.8 Lange livsløp og stadig nye teknologitrender

Energibransjens behov for produkter med lang levetid byr på utfordringer. Produktlevetid på 15 år er mye når man sammenligner med mobilapplikasjoner som har levetid på et par år. Å gå til anskaffelse av slike produkter krever nøye vurdering og planlegging. Teknologitrendene endrer seg stadig, og det er ikke godt å si hva som dukker opp rundt neste sving. Som en av leverandørene beskrev: *Å vurdere nye trender er en vanskelig oppgave. Hvilke teknologier skal man hive seg med på, og hvilke burde man droppe?*

Ut i fra intervjuene kan det virke som leverandørene er pådrivere for bruk ny teknologi, mens energiselskapene er mer tilbakeholdne. Leverandørene har et ønske om at energiselskapene skal bli mer frempå og bli med på ny teknologi. Det er kanskje ikke så rart at energiselskapene er mer skeptiske enn leverandørene, siden det er de som står med ansvaret hvis et prosjekt går galt.

Trenden med stadig mer utsetting er i endring. De kan være verdt å merke seg begrepet *insourcing*, for det kommer vi sannsynligvis til å høre mer om fremover. [14] viser en nedgang i andelen selskaper som sier at de vil sette ut flere tjenester. Det er dessuten en

økning på 2% i andelen selskaper som sier at de vil ta IKT-tjenester tilbake igjen det neste året. Bildet er likevel ikke entydig, siden undersøkelsen også sier at bruken av skytjenester kommer til å øke.

Leverandørene oppfordrer energiselskapene til å bli flinkere til å digitalisere arbeidsprosesser og tenke nytt. Basert på Riksrevisjonens rapport [13], kan det se ut til at leverandørene har et poeng. Statlige virksomheter er for dårlige til å utnytte innovasjonspotensialet ved IKT-anskaffelser, og statlige selskaper vet for lite om hvordan de kan bruke digitalisering til å effektivisere arbeidsprosesser. Rapporten anbefaler å kommunisere til leverandørene hvilke behov man har, i stedet for å bestille bestemte løsninger. Dette gir leverandørene mulighet til å bidra med idéer som kan gi mer effektive løsninger [13].

6 Anbefalinger

Basert på det vi har funnet ut gjennom intervjuene og litteraturstudier vil vi komme med fem anbefalinger:

1. Det bør arbeides videre med et bransjesamarbeid for å utarbeide felles krav til bruk i tjenesteutsetting av IKT og bestilling av nye IKT-systemer. Ved at bransjen går sammen vil det sannsynligvis bli lettere å få gjennomslagskraft i forhandlinger med de største leverandørene. Vi ser at et felles europeisk krav om personvern har ført til at leverandører over hele verden har måttet tilpasse seg. Hvem som kan lede et slikt bransjesamarbeid er ikke klart, men vi tror at KraftCERT kunne vært en god kandidat, fordi KraftCERT har relevant kompetanse og et allerede etablert samarbeid med energiselskaper.

2. IKT-sikkerhetstilstanden hos de små energiselskapene bør undersøkes nærmere. I følge Mørketallsundersøkelsen fra 2016 kan det se ut som de små selskapene mangler tilstrekkelig sikkerhetsnivå for å beskytte seg mot virus og andre uønskede IKT-hendelser. Med en energibransje som stadig blir mer digital vil det være viktig at også de minste selskapene er godt nok rustet til å håndtere digitale sårbarheter.

3. Energiselskapene bør benytte seg av en kontraktsfestet rett til å komme på tilsyn hos sine leverandører. Dette kan bidra til å oppdage sikkerhetsfeil og mangler. Tilsynsbesøk er en god måte for selskapene å kontrollere at de får det produktet de betaler for. I følge beredskapsforskriften er energiselskapene dessuten forpliktet til å påse at leverandørene oppfyller de samme sikkerhetskravene som de selv er pålagt.

4. Energiselskapene bør gjennomføre øvelser sammen med sine leverandører. Både større øvelser og muntlige gjennomganger av beredskapsrutiner kan være nyttige. Begge parter kan lære av dette.

5. NVE bør komme med en engelsk veileder til hvordan man kan oppfylle kravene i beredskapsforskriften. En slik oversettelse vil gjøre det enklere for energi-selskaper å forhandle med internasjonale leverandører. Slik det er i dag ligger ansvaret for oversettingen på leverandøren, og man kan ikke regne med at jobben alltid blir gjort godt nok. Spesielt ved mindre leveranser vil man dra nytte av dette, siden det er ressurskrevende å oversette og tolke lovtekster selv.

7 Intervjuguide

7.1 Intervju av energiselskap

Hva er en god leverandør for dere?

Oversikt over leverandørkjeden:

- Har dere oversikt over hvor mange underleverandører leverandørene deres har?
- Har deres leverandører rapporteringsplikt for endringer hos dem?
    - Hvis ja: Hvilke typer endringer?
    - Får dere beskjed ved eierskifte hos leverandøren?
    - Hva hvis leverandøren endrer underleverandør?
- Har dere kontroll på ikt-sikkerheten helt ned i verdikjeden?

Risikovurdering av tjenesteutsettingen:

- Har det vært klare kriterier for risikoaksept?
- Hva med bestillerkompetansen til de som har vurdert?
    - Har de hatt nok IKT-kompetanse?

Vurdering av leverandøren:

- Har dere oversikt over leverandørens sikkerhetsrutiner?
    - Eksempel: Ansettelsesrutiner, tilgangskontroll, teknologier, rapporteringsrutiner.
- Har man kontaktet referanser for å undersøke leverandørene før kontraktsinngåelse?
- Tar dere med landvurderinger?
- Hva gjør dere dersom leverandøren ikke vil/kan holde det sikkerhetsnivået som dere trenger?
    - Har det noen gang skjedd at dere har avbrutt kontraktsinngåelse pga. dette?
    - Har dere alltid et reelt alternativ til å signere kontrakten? Andre leverandører? Gjøre arbeidet selv? Forhandle frem en bedre løsning?

Revidering av sikkerheten i tjenesteutsettingen underveis i livsløpet (etter kontrakten er inngått):

- Hvor ofte tar dere en ny vurdering på sikkerheten av tjenesteutsettingen?

    - Hvem er det som gjør det?
    - Hvordan?
    - Hva er motivasjonen for å gjøre det?
- Reviderer dere grunnlaget for selve tjenesteutsettingen?

Revidering av sikkerheten i leverandørforholdet:

- Hvordan validere at hardware/software/firmware har blitt levert som avtalt uten å ha blitt moderert under frakt/montering?
- Etter levering/implementering: Har det vært avvik fra leveransekravene? I såfall: Hvilke tiltak gjøres?
- Drar dere på tilsyn hos leverandøren? Har dere lov til å komme på tilsyn? Hvor ofte?
- Har dere noen gang avdekket nye sårbarheter i en slik revidering?
    - Hvilke tiltak ble iverksatt?
- Hva om risikobildet har endret seg, for eksempel at risikoen har gått opp:
    - Har dere mulighet til å gå ut av kontrakten?
    - Har man mulighet til å endre på krav underveis i henhold til kontrakten?
    - Har dere noen gang sagt opp en leverandør pga. endret risiko?

Beredskap:

- Er leverandøren inkludert i beredskapsplanen?
    - Eksempel:
        - Står det for eksempel i kontrakten hvor kort varsel leverandøren må kunne stille på?
        - Er det kontraktsfestet at leverandøren skal være tilgjengelig hele tiden?
        - Hva skal man gjøre hvis nøkkelpersoner hos leverandøren er på ferie?
- Er leverandørene inkludert i beredskapsøvelser?
- Dekker beredskapsplanen sikkerhetsoppdateringer i software, hardware, firmware?

Internasjonalt/lover?

Avslutting av tjenester:

- Har dere rutiner for:

- Sletting av data?
- Fjerne tilgang?

7.2 Intervju av leverandører

Hva kjennetegner en god kunde for dere?

Hva kjennetegner en god leverandør for dere?

Oversikt over leverandørkjeden:

- Har dere oversikt over hvor mange underleverandører leverandørene deres har?
- Har deres leverandører rapporteringsplikt for endringer hos dem?
  - Hvis ja: Hvilke typer endringer?
  - Får dere beskjed ved eierskifte hos leverandøren?
  - Hva hvis leverandøren endrer underleverandør?
- Hvor langt ned i verdikjeden opplever dere at dere har kontroll?

Vurdering av leverandøren:

- Har dere oversikt over leverandørens sikkerhetsrutiner?
  - Eksempel: Ansettelsesrutiner, tilgangskontroll, teknologier, rapporteringsrutiner.
- Har man kontaktet referanser for å undersøke leverandørene før kontraktsinngåelse?
- Tar dere med landvurderinger?
- Hva gjør dere dersom leverandøren ikke vil/kan holde det sikkerhetsnivået som dere trenger?
  - Har det noen gang skjedd at dere har avbrutt kontraktsinngåelse pga. dette?
  - Har dere alltid et reelt alternativ til å signere kontrakten? Andre leverandører? Gjøre arbeidet selv? Forhandle frem en bedre løsning?

Revidering av sikkerheten:

- Blir dere sikkerhets-revidert av tjenestemottaker?
  - Hvor ofte? Hvem? Hvordan?
  - Kommer tjenestemottaker på tilsyn?
- Reviderer dere sikkerheten hos deres leverandører? Hvor ofte? Hvordan?
- Har dere rutiner om å informere kunder om sårbarheter?

Energiselskaper som kunder:

- Hvordan er kravene til kontraktene i energibransjen sammenlignet med andre bransjer?
- Er den tekniske bestillerkompetansen hos kundene god nok?
  - Etter deres mening: Har de god nok sikkerhetskompetanse?
- Hva er de største utfordringene deres med tanke på krav fra kundene?

- Hvordan opplever dere det som leverandør å måtte levere i samsvar med nasjonale lover og reguleringer?

Beredskap:

- Har dere en beredskapsplan?
    - Altså: I tilfelle kunden opplever hendelser som krever at dere stiller på kort varsel?
    - Hva om nøkkelpersoner hos dere er på ferie mens kunden har behov for dere?
    - Dekker beredskapsplanen sikkerhetsoppdateringer i software, hardware, firmware?
    - Er leverandøren inkludert i beredskapsplanen?
        - Står det for eksempel i kontrakten hvor kort varsel leverandøren må kunne stille på?
        - Er det kontraktsfestet at leverandøren skal være tilgjengelig hele tiden?
        - Hva skal man gjøre hvis nøkkelpersoner hos leverandøren er på ferie?
- Kommer det klart frem av kontrakten hva som er deres rolle i en beredskaps-situasjon?
    - Får dere for eksempel betalt for å være tilgjengelig for kunden døgnet rundt?
- Er dere avhengig av deres leverandør for å kunne gjøre jobben deres under en hendelse?
    - Hvordan har dere sikret dere mot dette?
- Har dere gjennomført beredskapsøvelser?

Internasjonalt/lover?

Avslutting av tjenester:

- Har dere rutiner for:
    - Sletting av data?
    - Fjerne tilgang?

8 Referanser

[1] Norsk rikskringkasting, «Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata,» 3 mai 2017. [Internett]. Tilgjengelig fra: https://www.nrk.no/norge/helse-sor-ost_-innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443. [Funnet 16 juli 2018].

[2] Digi.no, «Ledelsen har nektet for at utenlandske IT-arbeidere kan lese pasientjournaler. Sannheten er en helt annen,» 3 mai 2017. [Internett]. Tilgjengelig fra: https://www.digi.no/artikler/ledelsen-har-hele-tiden-hevdet-av-utenlandske-it-arbeidere-ikke-far-tilgang-til-sensitiv-informasjon-sannheten-er-en-helt-annen/382401. [Funnet 16 juli 2018].

[3] Norsk rikskringkasting, «Tastefeilen som stoppet Statoil,» 3 mai 2017. [Internett]. Tilgjengelig fra: https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013. [Funnet 16 juli 2018].

[4] Dagens Næringsliv, «Statoil unngår kritikk etter IT-glipp,» 3 februar 2017. [Internett]. Tilgjengelig fra: https://www.dn.no/nyheter/2017/02/03/0518/Olje/statoil-unngar-kritikk-etter-it-glipp. [Funnet 16 juli 2018].

[5] Norsk rikskringkasting, «Driftet Nødnettet ulovlig fra India,» 7 februar 2017. [Internett]. Tilgjengelig fra: https://www.nrk.no/norge/driftet-nodnettet-ulovlig-fra-india-1.13358591. [Funnet 16 juli 2018].

[6] Digi.no, «Broadnet forpliktet seg til å drifte Nødnettet fra Norge, men driftet det ulovlig fra India,» 7 februar 2017. [Internett]. Tilgjengelig fra: https://www.digi.no/artikler/broadnet-forpliktet-seg-til-a-drifte-nodnettet-fra-norge-men-indiske-it-arbeidere-hadde-tilgang-til-a-stenge-ned-alt/376193. [Funnet 16 juli 2018].

[7] Olje- og energidepartementet, «Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften),» 7 desember 2012. [Internett]. Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157. [Funnet 6 juli 2018].

[8] Nasjonal sikkerhetsmyndighet, «Sikkerhetsfaglige anbefalinger ved tjenesteutsetting,» 2018. [Internett]. Tilgjengelig fra: https://nsm.stat.no/aktuelt/temarapport-tjenesteutsetting/. [Funnet 6 juni 2018].

[9] Energy Sector Control Systems Working Group, «Cybersecurity Procurement Lanaguage for Energy Delivery Systems,» 2014. [Internett]. Tilgjengelig fra: https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf. [Funnet 14 juli 2018].

[10] Norges vassdrags- og energidirektorat, «Regulering av IKT-sikkerhet: En helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert enerigsektor,» 31 mars 2017. [Internett]. Tilgjengelig fra: https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/ikt-sikkerhet-regelverket-ma-folge-teknologiutviklingen/. [Funnet 2018 juni 2018].

[11] Forsvarsdepartementet, «Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven),» 20 mars 1998. [Internett]. Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/1998-03-20-10. [Funnet 3 august 2018].

[12] Norges vassdrags- og energidirektorat, «Informasjonssikkerhetstilstanden i energiforsyningen,» 2017. [Internett]. Tilgjengelig fra: http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf. [Funnet 4 juni 2018].

[13] Riksrevisjonen, «Riksrevisjonens undersøkelse av digitalisering i statlige virksomheter,» 2018. [Internett]. Tilgjengelig fra: https://www.riksrevisjonen.no/rapporter/Documents/2017-2018/Digitalisering.pdf. [Funnet 2 august 2018].

[14] Whitelane Research and PA Consulting Group, «2018 Nordic IT Outsourcing Study results,» 2018. [Internett]. Tilgjengelig fra: https://whitelane.com/2018/04/2018-nordic-it-outsourcing-results-published/. [Funnet 3 august 2018].

[15] Nasjonal sikkerhetsmyndighet, «NSMs grunnprinsipper for IKT-sikkerhet,» 2018. [Internett]. Tilgjengelig fra: https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf. [Funnet 17 juli 2018].

[16] L. Strand, «Hvor i all verdens land og rike? Hva må vurderes før du kan tenke på å tjenesteutsette IKT?,» 10 juli 2018. [Internett]. Tilgjengelig fra: https://nsm.stat.no/blogg/tjenesteutsetting-landvurdering/. [Funnet 28 juli 2018].

[17] Norges vassdrags- og energidirektorat, «Avbruddsstatistikk 2017 Nøkkeltall nettselskap,» 2017. [Internett]. Tilgjengelig fra: https://www.nve.no/Media/6910/indikator-selskap.xlsx. [Funnet 6 august 2018].

[18] Næringslivets Sikkerhetsråd, «Mørketallsundersøkelsen 2016,» 2016. [Internett]. Tilgjengelig fra: https://www.nsr-org.no/getfile.php/Bilder/M%c3%b8rketallsunders%c3%b8kelsen/morketallsundersokelsen_2016.pdf. [Funnet 6 august 2018].

[19] International Organization for Standardization, «ISO/IEC 27000 family - Information security management systems,» [Internett]. Tilgjengelig fra: https://www.iso.org/isoiec-27001-information-security.html. [Funnet 3 august 2018].

[20] European Union Agency for Network and Information Security, «Smart grid security certification in Europe,» 2014. [Internett]. Tilgjengelig fra: https://www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe/at_download/fullReport. [Funnet 3 august 2018].

[21] European Union, «EU to create a common cybersecurity certification framework and beef up its agency – Council agrees its position,» 6 juni 2018. [Internett]. Tilgjengelig fra: http://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/. [Funnet 8 august 2018].

[22] CESeCore, «Common Criteria,» [Internett]. Tilgjengelig fra: https://www.cesecore.eu/?q=node/13. [Funnet 8 august 2018].

[23] Common Criteria, «Certified Products,» [Internett]. Tilgjengelig fra: https://www.commoncriteriaportal.org/products/. [Funnet 13 august 2018].

NVE

Norges vassdrags- og energidirektorat

MIDDELTHUNSGATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (+47) 22 95 95 95

www.nve.no