RISIKOANALYSE AV AMS KNYTTET TIL INFORMASJONS-SIKKERHET OG PERSONVERN

Av *Inger Anne Tøndel, Maria B. Line, Gorm Johansen og Martin G. Jaatun, SINTEF IKT*

Sammendrag
Innføringen av AMS gjør at nettselskaper må forholde seg til risiko knyttet til bruk av IKT i større grad enn før. Bransjen er vant til å gjøre risikoanalyser, men mange opplever det likevel som utfordrende å få oversikt over risiko knyttet til informasjonssikkerhet og personvern. I DeVID-prosjektet har det blitt utviklet støttemateriale for denne typen risikoanalyser av AMS. Vi har evaluert støttematerialet ved å sammenligne risikoanalyser som har blitt utført med og uten bruk av dette. Denne rapporten presenterer resultater fra dette arbeidet.

1. INNLEDNING

Innføringen av avanserte måle- og styringssystemer (AMS) fører til et skifte i teknologi mot mer avhengighet av informasjons- og kommunikasjonsteknologi (IKT). Økt bruk av IKT-systemer gir mange muligheter, for eksempel knyttet til nye markedsmodeller og mer effektiv drift. Samtidig øker kompleksiteten i systemene, hvilket bringer med seg nye sårbarheter.

Risikoanalyser har blitt gjennomført i kraftbransjen lenge, og gjennomføres også for ulike deler av innføringen av AMS. Informasjonssikkerhets- og personvernrisiko omfattes av noen av de risikoanalysene som har blitt gjennomført.

Denne rapporten presenterer resultater fra arbeid med risikoanalyser knyttet til informasjonssikkerhet og personvern i DeVID-prosjektet, som er støttet av Norges Forskningsråd. Et av målene i dette prosjektet er å bidra til bedre metodikk i slike risikoanalyser av AMS-systemer og tilgrensende systemer.

Denne rapporten gir en kort innføring i viktige begreper knyttet til informasjonssikkerhet og personvern, samt en kort beskrivelse av den risikoanalysemetodikken som har blitt benyttet i DeVID-prosjektet. For å evaluere denne metodikken har det blitt innhentet erfaringer med risikoanalyser gjennomført av tre ulike nettselskap. Det har også blitt

gjennomført to analyser basert på metodikk-anbefalingene i DeVID-prosjektet [1]. Erfaringer fra disse analysene beskrives i rapporten og oppsummeres som konkrete råd og anbefalinger for hvordan risiko-analyser kan gjennomføres, samt hvilken type støtte som kan være nyttig i en slik analyse.

2. RISIKO KNYTTET TIL INFORMASJONSSIKKERHET OG PERSONVERN: BEGREPER OG METODIKK

I et IKT-system er informasjon en viktig verdi. Dermed snakker man ofte om informasjonssikkerhet når man omtaler sikkerhet i IKT-systemer; selv om begrepet informasjonssikkerhet rommer mer enn sikring av IKT-systemet. Når informasjonen det er snakk om er knyttet til individer, blir personvern viktig. I det følgende gir vi en introduksjon til informasjonssikkerhet og personvern, samt en oversikt over det støttematerialet som har blitt utviklet i DeVID-prosjektet for å analysere risiko.

2.1 Introduksjon til informasjonssikkerhet

Når det gjelder sikring av IKT-systemer og den informasjonen som ligger i disse systemene snakker man gjerne om sikring av:

- **Konfidensialitet;** det å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang
- **Integritet;** det å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige – innebærer at uvedkommende ikke kan endre informasjon eller systemet som behandler informasjonen
- **Tilgjengelighet;** det å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov

Når man vurderer hvilket sikkerhetsbehov ulik informasjon har, må man gjøre avveininger mellom *tilgjengelighet, integritet* og *konfidensialitet*; dette er avveininger som hver enkelt organisasjon eller virksomhet må gjøre i henhold til egne prioriteringer og vurdert akseptabel restrisiko.

I informasjonssikkerhetsarbeidet må man ta hensyn til villede ondsinnede handlinger rettet direkte mot et gitt system, i tillegg til feil og ulykker som kan forårsake sikkerhetsbrudd. På denne måten er ikke informasjonssikkerhet en ren teknisk problemstilling, men i høyeste

grad også avhengig av menneskene som opererer systemene, samt organisasjonen som systemene opereres i.

2.2 Introduksjon til personvern

Det finnes mange definisjoner på personvern; et tidlig forsøk kan oversettes til "retten til å få være i fred" [2]. Imidlertid er vårt samfunn nå så fundamentalt basert på kommunikasjon at ingen er i stand til å leve helt i isolasjon fra andre. Dermed må vi akseptere at det vil finnes informasjon om oss hos de vi kommuniserer med; det er da opp til personvernfremmende mekanismer og regler å sikre at informasjonen behandles slik at personvernet ivaretas så godt som mulig.

Personopplysninger skal kun samles inn for et definert formål, og skal kun brukes for det definerte formålet, og når det ikke lenger er bruk for dataene til det opprinnelige formålet, skal de slettes.

I forbindelse med smarte strømmålere betyr den økte presisjonen at mye informasjon om hvordan abonnenten(e) lever livet sitt kan leses ut fra forbruket; man ser når de står opp, når de dusjer, når de lager middag, og ikke bare når de ser på TV, men til og med kanskje hvilken type TV det er [3]. Slike opplysninger kan misbrukes av uvedkommende og bør derfor beskyttes tilfredsstillende.

2.3 Risikoanalysemetodikk benyttet i DeVID

SINTEF har utviklet en veiledning for gjennomføring av risikoanalyse av AMS og tilgrensende IT-systemer hos et nettselskap, hvor fokus for analysen er informasjonssikkerhet og personvern [1]. Veiledningen bygger på en metodikk som mange nettselskap er kjent med fra før, og som anbefales benyttet av NVE og Energi Norge [4]. Det er ikke nødvendigvis bruk for nye metoder for å gjennomføre risikoanalysene, men det er behov for å kunne håndtere nye typer risiko. SINTEFs veiledning skal være til støtte ved gjennomføring av risikoanalyser av AMS ved å bidra til at de rette spørsmålene stilles. Prosjektpartnere i DeVID har bidratt i utvikling av veiledningen.

Det er naturlig å dele en risikoanalyse inn i følgende hovedaktiviteter: *Planlegging, risiko/sårbarhetsvurdering* og *risikohåndtering* [4]. Veiledningen gir anbefalinger og inneholder sjekklister for alle disse. God planlegging er en forutsetning for å oppnå et godt resultat. Gjennomføringen er ressurskrevende og ledelse og gjennomføringsapparat må ha en omforent forståelse av hvilket system man analyserer, hvilken

fase analysen gjelder (*strategi/innkjøp, utrulling, drift*), hvordan resultatet skal dokumenteres og hva det skal brukes til.

Det kanskje viktigste bidraget i SINTEFs veiledning er knyttet til den aktiviteten der risiko vurderes. I motsetning til tradisjonelle analyser hvor fokus ofte er på fysiske komponenter, har veiledningen fokus på informasjonsverdier. Før man identifiserer trusler og uønskede hendelser, bør man identifisere hvilke informasjonsverdier som finnes i målsystemet. Det er informasjon som har verdi, ikke systemet i seg selv, og man må vite hva som skal beskyttes for å kunne bestemme passende sikkerhetsnivå og akseptabel restrisiko. Eksempler på viktige informasjonsverdier er ikke-anonymisert forbruk og tilgang til brytersignalet (brytersignalet kan benyttes til å koble ut strømmen hos forbrukeren). Det anbefales at man velger ut et begrenset antall informasjonsverdier (typisk 3) som man kartlegger detaljert med hensyn på informasjonsflyt og lagring.

Uønskede hendelser knyttes til de utvalgte informasjonsverdiene og hendelsene gis en sannsynlighet og en konsekvensvurdering. Eksisterende barrierer legges til grunn for en vurdering av sannsynlighet og konsekvens. Veiledningen gir eksempler på konsekvens- og sannsynlighetsdimensjoner, men disse må tilpasses den enkelte virksomhet. Det anbefales å vurdere gjenbruk av konsekvensdimensjoner virksomheten har benyttet i tidligere analyser.

Nye tiltak bør foreslås i forbindelse med gjennomføringen av risikoanalysen. En full vurdering av nye tiltak, hvorvidt de foreslåtte tiltak er tilstrekkelige, eller om de skal gjennomføres, gjøres ikke under risikoanalysen, men som en egen aktivitet: *Risikohåndtering*. Når man skal identifisere relevante tiltak, anbefales det blant annet å benytte *Eksempler for å oppnå kontrollmål* i *Veileder til sikkerhet i avanserte måle- og styringssystem* [5] som sjekkliste.

SINTEFs veiledning inneholder følgende sjekklister og hjelpemidler:

- Aktivitetsliste for gjennomføring av analysen
- Konsekvensdimensjoner og konsekvensklasser
- Sannsynlighetsdimensjoner
- Kort beskrivelse av relevante standarder
- Støtte til kartlegging av informasjonsverdier
- Liste over hendelsestyper
- Hendelsestyper og uønskede hendelser relevant for AMS
- Liste over interessenter

- Typiske sårbarheter og svakheter i IKT-systemer
- Kort beskrivelse av relevante tiltak

3. ERFARINGER FRA GJENNOMFØRTE ANALYSER

For å kunne forbedre veiledningen som har blitt utviklet, har vi innhentet erfaringer med risikoanalyser både med og uten støtte fra SINTEFs veiledning. I det følgende beskriver vi metodikken som har blitt benyttet i dette arbeidet, samt de viktigste resultatene.

3.1 Metodikk

I arbeidet med å evaluere risikoanalysemetodikken benyttet i DeVID, ble det definerte følgende to forskningsspørsmål:

1. Hva er det med AMS som gjør risikoanalyser så vanskelige for nettselskapene?
2. Hvor god støtte gir veiledningen utarbeidet i DeVID-prosjektet til arbeidet med risikoanalyser av AMS?

Forskningsspørsmålene ble adressert gjennom et case-studie. Datainnsamling foregikk ved dokumentasjonsstudie, intervjuer og observasjoner. Vi studerte tre risikoanalyser av AMS som ble gjennomført av nettselskaper uten bruk av vår veiledning. Prosjektlederne i de respektive nettselskapene ble deretter intervjuet. Vi har også vært prosessleder for gjennomføring av to risikoanalyser av AMS hos to nettselskaper, hvor vår veiledning ble brukt aktivt. De fire[1] deltakende nettselskapene ble rekruttert til studien fra konsortiet til prosjektet DeVID. Resultatene fra de tre førstnevnte risikoanalysene ble analysert med tanke på hva de inkluderte sammenlignet med vår veiledning. Intervjuene ble brukt til å kartlegge nyttige erfaringer – gode og dårlige – som vi kunne inkludere i veiledningen. De to sistnevnte risikoanalysene ble brukt som en evaluering av vår veiledning, og forbedringer ble identifisert i løpet av prosessen.

3.2 Erfaringer fra analyser gjennomført av nettselskapene selv

De tre risikoanalyserapportene vi har fått tilgang på og vurdert i dette arbeidet, tar for seg innføringsprosjektet AMS. Informasjonssikkerhet er inkludert, men er bare en liten del av analysen. Til sammen dekkes

[1] For ett nettselskap fikk vi tilgang til en tidligere risikoanalyse, samt at vi var prosessleder for en risikoanalyse.

mange ulike trusler. Selv om hovedfokus virker å være på tekniske feil, dekker alle tre analysene også villede handlinger.

Identifisering av informasjonsverdier er en viktig anbefaling fra DeVID-metodikken. I risikoanalysene fra nettselskapene er det imidlertid ikke alltid åpenbart hvilke informasjonsverdier som er analysert; f.eks. "ny teknologi – mange oppstartsproblemer". De informasjonsverdiene som nevnes eksplisitt i hendelsesbeskrivelsene, er målerverdier, bryterkommandoer og oppdateringer av måleren. I tillegg nevnes fysiske verdier som måler, kommunikasjonsnettverk, mottakssystem og andre interne systemer hos nettselskapet.

To av tre nettselskaper gjennomførte risikoanalysen med en intern prosessleder, mens det tredje leide inn konsulenter til arbeidet. Konsulentene brakte med seg en sjekkliste som opplevdes nyttig å bruke. Intervjuene indikerer at en kritisk suksessfaktor for en vellykket risikoanalyse, er å ha med seg de riktige menneskene med den riktige kompetansen for arbeidet. En intervjudeltaker uttaler: *"Området er kjempeteknologisk og vanskelig å følge. Vi trenger spesialister på datasikkerhet. Det går greit å identifisere hendelser, f.eks. at "noen hacker seg inn" eller at "data er på avveie", men det er vanskelig å finne løsninger. Dette er fordi tiltakene er veldig tekniske, og det krever kompetanse."* Eksperter som kjenner systemene, samt mulige trusler med tilhørende konsekvenser, er de som best kan bidra til et nyttig resultat. For ikke-eksperter er det svært vanskelig å gjøre realistiske vurderinger av sannsynlighet og konsekvens. Mange av de aktuelle scenariene har veldig lav sannsynlighet, men kan få enorme konsekvenser dersom de inntreffer. Det er vanskelig å vite hvor mye slike scenarier skal vektlegges i oppfølgende arbeid etter risikoanalysene.

Konsekvensdimensjonene forsyningssikkerhet, personvern, økonomi og omdømme ble vurdert i den ene analysen. For de to andre analysene er det uklart i dokumentasjonen hvilke kriterier som er lagt til grunn for vurderingen av konsekvens og sannsynlighet for hendelser.

3.3 Erfaringer fra analyser basert på metodikken i DeVID

Hos det ene nettselskapet gjennomførte vi risikoanalysen på én dag. Dette ble oppfattet som noe knapt med tid. Derfor ble den andre risikoanalysen fordelt på to dager. Det var en fordel å dele opp arbeidet i to, for å kunne gjøre ekstra innhenting og bearbeiding av informasjon i etterkant av det første arbeidsmøtet. Det er dessuten en utfordring å få de riktige menneskene til å sette av lang nok tid i løpet av en arbeids-

dag til at vi kommer gjennom alle stegene i prosessen. Det er lettere å sette av 3-4 timer to dager enn 6-7 timer en dag.

Som del av begge risikoanalysene ble det identifisert en rekke informasjonsverdier, men begge analysene gjorde ganske like prioriteringer for den videre analysen. Verdier som ble spesielt vektlagt var:

- "Måleverdi", eller "kobling måler-ID og kunde"
- "Bryterfunksjon", eller "mulighet til å påvirke bryterstyring"
- "Krypteringsnøkler", eller "krypteringsnøkler og passord"

Hendelsene som ble identifisert i analysene var av ulik art, men det var ikke så stor andel tekniske feil som i de analysene som ble beskrevet i forrige delkapittel. En større andel av hendelsene var angrep.

Veiledningen vår inneholder en rekke sjekklister for ulike faser av risikoanalysen. I analysene ble disse benyttet etter at deltakerne hadde identifisert verdier eller hendelser selv. Da virket de ikke begrensende på deltakerne og man fikk en friere kreativ prosess hvor alle bidro så godt de kunne ut ifra egen kunnskap og egne erfaringer. Bruk av sjekklister førte til at noen informasjonsverdier og noen hendelser ble lagt til de som ble identifisert av deltakerne.

Konsekvenser ble vurdert for forsyningssikkerhet i begge analysene. Økonomisk risiko og omdømmerisiko ble i tillegg vurdert i den ene analysen, og personvern i den andre.

Tilbakemeldingene fra deltakerne tyder på at de opplevde metodikken som god, men at det samtidig var noe utfordrende å holde tråden i de ulike stegene i metodikken. Ekstern prosessleder ble vurdert å være en viktig suksessfaktor. Det opplevdes utfordrende å gjøre risikoanalyse av et fremtidig system, der man ikke kjenner detaljene rundt hvordan det vil bli. Omfanget var også noe stort – begge analysene så på AMS og tilgrensende systemer.

4. LÆRINGSPUNKTER OG ANBEFALINGER

Risikoanalyser slik det anbefales utført i DeVID-prosjektet skiller seg fra det som har vært anbefalingene ellers i bransjen primært på ett punkt: Fokus på *informasjonsverdier*. I tillegg bidrar DeVID-prosjektet med sjekklister som kan benyttes undervegs i arbeidet. Basert på erfaringene fra analyser utført i bransjen er det vanskelig å si om et fokus på informasjonsverdier gir bedre analyser. Det er en for-

skjell i hvilke hendelser som blir identifisert, om man sammenligner med tidligere analyser. Det er imidlertid ikke mulig å si om resultatet nå er bedre. Tilbakemeldingene fra deltakerne tyder imidlertid på at de opplevde det som nyttig å bli bevisst verdiene i systemet.

Kompetanse er helt klart det som peker seg frem som den største utfordringen for å få til gode risikoanalyser, og intervjuene med prosessledere viser at en del opplever kompetanseutfordringer knyttet til informasjonssikkerhet og personvern. Sjekklistene kan benyttes for å bøte på dette, spesielt når det gjelder å identifisere hendelser og tiltak. Imidlertid virker den største utfordringen å være å forstå sannsynlighet og konsekvens for hendelser. Dette kan ikke løses av sjekklister alene. Prioritering av informasjonsverdier kan bidra inn i vurderingen av konsekvens. Hovedproblemet virker imidlertid å være mangel på erfaringsdata – noe som er naturlig da AMS ikke har vært i drift lenge nok til å få relevante data på dette. Det øker kravene til kompetanse – man må forstå de tekniske mulighetene og begrensningene, samt trusselbildet.

Basert på erfaringene vi har gjort oss, har vi følgende anbefalinger for risikoanalyser som omhandler informasjonssikkerhet og personvern:

- Inkluder de riktige menneskene med den riktige kompetansen.
- Sett av to halve dager framfor en hel, for å få tid til innhenting og bearbeiding av informasjon mellom arbeidsmøtene
- Benytt sjekklister eller andre, tidligere utførte, risikoanalyser for å komplettere diskusjonen i analysegruppa.
- Bruk tid på å diskutere sannsynlighet og konsekvens. Ta tak i eventuelle uenigheter. Der man har uenighet i gruppa, vil man ofte ende opp med grundigere vurderinger.
- Man kan gjerne leie inn ekstern fasilitator eller annen kompetanse som mangler. Det er imidlertid viktig at virksomheten selv er aktive i arbeidet. Det å delta i risikoanalyser gir en økt bevissthet om sikkerhet. Prosessen i seg selv kan ofte være vel så viktig som sluttrapporten.
- Tekniske feil og angrep er viktige å vurdere, men informasjonssikkerhet og personvern er ikke primært et teknisk anliggende. Mennesker og prosesser i organisasjonen er også viktige, og disse aspektene bør tas inn i analysen.
- Vær klar på hva analysen dekker. Fokuser gjerne på mindre deler av systemet om gangen. Slik blir arbeidet mer overkommelig, og man får mulighet til å gå mer i dybden. Samtidig er det nyttig også å gjøre overordnede analyser for å få det store bil-

det, og øke forståelse for hvordan sikkerhet ett sted påvirker sikkerhet andre steder i systemet.

5. KONKLUSJON

Denne rapporten har gitt en oversikt over arbeidet som har blitt gjort i DeVID-prosjektet med risikoanalyser av AMS med spesielt fokus på informasjonssikkerhet og personvern. Basert på våre erfaringer er det behov for støtte til å gjennomføre slike risikoanalyser. Mye av det som trengs av støtte er ikke nødvendigvis spesifikt for enkeltorganisasjoner eller enkeltsystemer, og kan derfor gis i form av en veiledning. Samtidig vil det alltid være behov for å vurdere alle aspektene i lys av hvert enkelt selskaps infrastruktur, systemer, løsninger, og ikke minst akseptabelt risikonivå. En veiledning vil derfor aldri kunne framstå som noe mer enn en veiledning. Hvert selskap er nødt til å gjøre sine egne vurderinger. Erfaringene fra risikoanalysene vi har studert og gjennomført i regi av DeVID, vil benyttes til å oppdatere veiledningen vi har laget i prosjektet.

6. REFERANSER

[1] Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer, SINTEF, ISBN 978-82-14-05320-3

[2] Jaatun, M.G., Tøndel, I. A., Bernsmed, K., Nyre, Å.A. (2012). *Privacy Enhancing Technologies for Information Control*, kapittel 1 i *Privacy Protection Measures and Technologies in Business Organizations – Aspects and Standards*, Information Science Reference, ISBN 978-1-61350-501-4

[3] Lisovich, M.A., Mulligan, D.K., Wicker, S.B. (2010) *Inferring Personal Information from Demand-Response Systems,* IEEE Security & Privacy, vol. 8, no. 1, pp. 11-20, January/February

[4] Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen. Proactima, NVE, 2010. ISSN 1501-0678

[5] *Veileder til sikkerhet i AMS,* NVE, 2012