NTNU
Det skapende universitet

IT-sikkerhetsberedskapsøvelser i smartgrids

Ingrid Graffer

Master i kommunikasjonsteknologi
Innlevert: juni 2015
Hovedveileder: Karin Bernsmed, ITEM
Medveileder: Maria B. Line, ITEM

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Tittel: IT-sikkerhetsberedskapsøvelser i smartgrids

Student: Ingrid Graffer

Problemstilling:

Overgangen fra dagens strømnett til et smartere nett åpner for et mangfold av teknologiske muligheter. Nøkkelfaktorer er blant annet overvåkning og fjernstyring av anlegg og komponenter, tilrettelegging for flere type energikilder og økt bruk av fornybar energi. Avanserte måle- og styringssystemer (AMS) skal installeres i alle norske hjem før 2019, og vil gi både brukere og leverandører nye muligheter. Alt dette skaper et behov for et smartere og mer fleksibelt strømnett. Økt konnektivitet og koblinger mot Internett åpner for store sikkerhetsutfordringer, og sikkerheten må ivaretas for at smartgrids skal bli en suksess.

Å lage 100% sikre systemer er en umulig oppgave, og for å håndtere uønskede hendelser på en god måte er det avgjørende å øve. Angrepet "Dragonfly" sommeren 2014 var en vekker for bedrifter i kraftbransjen, og beredskapsøvelser med IT-sikkerhetsscenarier står nå på agendaen. Dette er en ny utfordring for en bransje som er gode på å gjennomføre øvelser med hendelser forårsaket av for eksempel vær og vind, men mangler erfaringer og kunnskap om øvelser basert på IT-hendelser. Skrivebordsøvelser er et trygt valg, og IT-sikkerhetsøvelser gjennomført den siste tiden har vært av denne typen. Å designe praktiske og funksjonelle øvelser blir ikke prioritert, og er en oppgave som kan bidra til å gjøre bransjen enda bedre forberedt på fremtidens IT-sikkerhetsutfordringer.

Nøkkelpunkter for denne oppgaven:

- Kartlegge sikkerhetstrusler og mulige angrep rettet mot smartgrids og AMS.
- Utvikle scenarier som kan brukes i en beredskapsøvelse.
- Designe en praktisk øvelse.
- Teste øvelsens funksjonalitet, få tilbakemelding fra bransjen og evaluer øvelsen.

Ansvarlig professor: Karin Bernsmed, ITEM

Veileder: Maria B. Line, ITEM

Abstract

The modernization of power management and control systems introduces smart grid technology, which lets customers and providers manage and generate power in a more efficient way. The benefits of smart grids are many, but it also entails a lot of security issues. To be able to respond to these security incidents, industrial control organizations need to perform IT security preparedness exercises. However, other than a few guidelines on table-top and functional exercises, it exists limited support material and existing exercises, a challenge that needs to be solved in order to conduct more IT security preparedness exercises.

To facilitate for organizations to strengthen their incident response capabilities, this thesis presents a board game to be used in a preparedness exercise. The board game simulates a large scale attack on the electric power grid, and introduces a number of relevant scenarios and questions that trigger discussions and knowledge exchange between different kinds of personnel participating in the game. The game dynamics and the technical content of the scenarios and questions have been evaluated. Feedback from the electric power industry indicates that this board game can be a relevant tool for preparedness exercises for IT security incidents.

Sammendrag

Overgangen fra tradisjonelt strømnett til smartgrids introduserer teknologi som gjør at både kunder og produsenter kan bruke og generere strøm på en mer effektiv måte. Fordelene ved smartgrids er mange, men det fører også med seg nye sårbarheter og trusler når det kommer til IT-sikkerhet. For at bedrifter i kraftbransjen skal være i stand til å håndtere disse hendelsene på en tilfredsstillende måte, er det viktig å gjennomføre øvelser jevnlig. Erfaring og kunnskap, i tillegg til veiledninger for øvelser som ikke er skrivebordsøvelser eller funksjonelle øvelser, eksisterer i begrenset grad, og er en stor utfordring i gjennomføringen av slike øvelser.

For å legge til rette for at kraftbransjen skal styrke sin hendelseshåndteringsevne, presenterer denne oppgaven et samarbeidsbrettspill til bruk i en beredskapsøvelse. Spillbrettet simulerer et angrep på strømnettet, og underveis introduseres deltagerne for relevante scenarier og spørsmål. Disse trigger diskusjon og læringsutveksling mellom ulike typer personell som deltar, og vil ved tilfredsstillende svar hjelpe deltagerne til å vinne spillet. Evaluering og testing av øvelsen er gjennomført, både av spillets funksjonalitet alene, og av øvelsen som helhet med scenarier. Bidragsytere fra kraftbransjen har kommet med sine tilbakemeldinger, og viser en positiv innstilling til at brettspillet kan fungere som en øvelse på IT-sikkerhetshendelser.

Forord

Denne masteroppgaven avslutter min 5-årige mastergrad i kommunikasjonsteknologi, ved Institutt for telematikk (ITEM), Fakultet for informasjonsteknologi, matematikk og elektroteknikk (IME) , ved Norges teknisk-naturvitenskapelige universitet (NTNU).

Jeg vil gjerne takke ansvarlig professor Karin Bernsmed og veileder Maria B. Line fra ITEM for verdifulle innspill underveis. Deltagere i tester og bidragsytere fra kraftbransjen, Statnett og Norges vassdrags- og energidirektorat (NVE), har også bidratt til å gjøre denne oppgaven mulig.

Til slutt vil jeg også takke min nærmeste familie, venner og kjæreste for å ha støttet meg gjennom årene på NTNU.

Trondheim, 15.juni 2015

Ingrid Graffer

Innhold

Figurer

Definisjoner og begreper

Informasjonssikkerhet Bevaring av konfidensialitet, integritet og tilgjengelighet for informasjon. I tillegg kan også autentisering, ikke-benekting, sporbarhet og personvern være involvert [8].

Informasjonssikkerhetshendelse Enkel eller en serie av uønskede eller ikke forventede sikkerhetshendelser som har en signifikant sannsynlighet for å kompromittere virksomhetens drift og true informasjonssikkerheten. På engelsk skilles det mellom *incident* og *event*. En *event* defineres som en identifisert forekomst av et system, tjeneste eller nettverkstilstand som indikerer et mulig brudd på en informasjonssikkerhetspolitikk eller kontrollsvikt, eller en tidligere ukjent situasjon som kan være sikkerhetsrelevant [8].

Håndtering av informasjonssikkerhetshendelser: En prosess bestående av deteksjon, rapportering, respons, håndtering og læring fra informasjonssikkerhetshendelser [9].

Datasikkerhet: Sikring av data, enten analog eller digital. Brukes ofte som et annet ord for informasjonssikkerhet [10].

IT-sikkerhet Informasjonsteknologi-sikkerhet omhandler sikring av IT/IKT, for eksempel hardware og software. Blir ofte feilaktig blandet med ordet informasjonssikkerhet, da mye informasjon er lagret og overført via IKT. For å beskytte denne informasjonen, må teknologien brukt til å lagre og overføre, beskyttes [10]. Dette begrepet brukes mer av profesjonelle, som en kortform av informasjonssikkerhet [11].

Cyber-sikkerhet: Defineres som ting som kan være sårbare på grunn av IKT, dette kan være informasjon og andre ting [10]. Brukes også ofte som IT-sikkerhet i SCADA-verden [11], og er i Amerika ofte brukt i betydning av de to begrepene nevnt ovenfor. [10].

Integritet Sikre at informasjonen er nøyaktig, fullstendig og gyldig [12].

Konfidensialitet Kun autoriserte personer har tilgang til informasjonen [12].

Responsteam Nasjonal Sikkerhetsmyndighet (NSM) og Norsk Senter for Informasjonssikkerhet (NorSIS) definerer et CERT[1] på følgende måte:

> Ekspertgruppe som håndterer sikkerhetshendelser. Et CERT skal forebygge alvorlige angrep mot samfunnskritisk infrastruktur og informasjon på IT-siden. De skal også varsle om alvorlige angrep, trusler og sårbarheter, og koordinere responsen i forbindelse med alvorlige sikkerhetsangrep.

NorCERT er den norske CERT-gruppen, og KraftCERT er en nyopprettet instans spesialisert på kraftbransjen.

Sikkerhet og safety Ordet sikkerhet kan ha forskjellige betydninger, og på engelsk finnes to ord som omhandler dette. *Safety* handler typisk om å hindre at et system gjør skade på omgivelsene, altså beskytte liv, helse og miljø, mens *security* handler om å beskytte systemet mot skade fra omgivelsene [11].

Tilgjengelighet Sikre at autoriserte brukere har tilgang til informasjon og tilknyttede ressurser når det behøves [12].

[1] Computer Emergency Response Team

Liste med forkortelser

AMS Avanserte måle- og styringssystemer.

DCS distribuerte kontrollsystemer.

DSB Direktorat for Samfunnssikkerhet og Beredskap.

HSEEP Homeland Security øvelse- og evalueringsprogram.

IME Fakultet for informasjonsteknologi, matematikk og elektroteknikk.

ITEM Institutt for telematikk.

NorSIS Norsk Senter for Informasjonssikkerhet.

NSM Nasjonal Sikkerhetsmyndighet.

NTNU Norges teknisk-naturvitenskapelige universitet.

NVE Norges vassdrags- og energidirektorat.

OED Olje- og Energidepartementet.

P&D Protection and Deception.

PLC programerbar, logisk kontroller.

SCADA supervisory control and data acquisition.

UiS Universitetet i Stavanger.

Kapittel 1
Introduksjon

1.1 Motivasjon

Kraftbransjen har ansvaret for håndtering av kritisk samfunnsinfrastruktur, og grunnet et stadig høyere krav om kosteffektivitet og kompleksitet i strømnettene, står bransjen ovenfor en stor utviklingsprosess de neste 10-20 årene. Overgangen fra tradisjonelle strømnett til et smart nett (*smartgrids*) åpner for mange teknologiske muligheter. Det forenkler satsning på fornybar energi, åpner for flere typer energikilder, og bedrer muligheten for overvåkning og fjernstyring. Smartgrids er fra et IT-sikkerhetsperspektiv veldig viktig og utfordrende. Tidligere har kontrollsystemene basert seg på proprietære teknologier, som nå blir erstattet med hyllevare og software/hardware med åpen kildekode. Samtidig skjer en integrasjonsprosess av tradisjonelle IKT-systemer og kontrollsystemer, noe som resulterer i en betydelig økning av sårbarheter når det kommer til IT-sikkerhet [13].

Et angrep på strømnettet i Norge kan få store konsekvenser, og enkelte går så langt som å sammenlikne med et atomangrep. Når elektrisiteten stopper, stopper fort alt annet også [14]. Etter dataangrepet mot energibransjen, Dragonfly [15], i 2014 har bransjen forstått at de er et reelt mål for angripere. I følge NSM øker mengden oppdagede alvorlige angrep norsk industri betraktelig, og er forventet å øke fremover [16].

Det er umulig å beskytte seg 100% mot uønskede hendelser. Å velge det rette nivået av sikkerhet, sett opp mot et akseptabelt nivå av risiko, er det viktigste, men også det mest utfordrende [11]. Alle organisasjoner bør ha etablerte planer for hendelseshåndtering og øvelser, men studier av kraftbransjen viser at det begrenset hvor flinke organisasjonene er på dette [17, 18]. Tilsynsmyndighetene melder om at avstanden mellom krav og etterfølgelse er for stor [19]. Dette gjelder blant annet overdreven tro på egen sikkerhet i driftskontrollsystemene, manglende risikoanalyser, beredskapsplaner og dokumentasjon, samt for dårlig kontroll på tilgangspunkter fra Internett. Seniorrådgiver Roar Sundseth i Watchcom Security Group mener det må

en kulturendring til. Overdreven satsning på teknologi gir ikke bedre sikkerhet, fokus på tykke brannmurer og antivirusprogrammer hjelper lite i den store sammenhengen [20].

> *"Når det gjelder cyber- og informasjonssikkerhet dreier 20 prosent seg om teknologi, og 80 prosent handler om det menneskelige"*
>
> - Roar Sundseth

For å være i stand til å respondere på en tilfredsstillende måte når uønskede hendelser inntreffer, er det viktig at involvert personell øver jevnlig. Det er liten tid til å studere dokumenterte prosedyrer når en hendelse oppstår, derfor er tilegnet erfaring fra øvelser essensielt for å ta korrekte avgjørelser under press. Feil avgjørelser i disse situasjonene kan føre til at hendelsen eskalerer, og får større konsekvenser enn nødvendig. Før angrepet i 2014 var det rapportert lite øvelser på IT-spesifikke hendelser i kraftbransjen [13]. Det virker derimot som bransjen nå har innsett behovet for trening på disse type hendelsene. Kraftbransjen er generelt gode på øvelser som omhandler for eksempel vær og vind [21], men har begrenset erfaring på øvelser om IT-sikkerhet. Studier avslører at skrivebordsøvelser om IT-sikkerhet er den eneste typen øvelser som i en viss grad gjennomføres [22, 23]. Disse øvelsene er nyttige av mange grunner, men mangler mulighet for en praktisk tilnærming. For å teste ut alternative type øvelser, og skape mer variasjon i øvelsene som gjennomføres, vil det i denne masteroppgaven utvikles en praktisk øvelse for kraftbransjen. Øvelsen tar utgangspunkt i samarbeidsbrettspill, og utgjør en øvelsesvariant som ikke eksisterer i dag. Videre testes og evalueres øvelsen for å utforske om denne formen for praktisk øvelse kan fungere.

1.2 Avgrensninger

Øvelsen som presenteres i denne oppgaven har et spesifikt nettselskap som målgruppe, noe som gjør det mulig å sikre en konkret og grundig tilbakemelding. For at øvelsen skal passe i andre organisasjoner enkelte endringer gjøres.

Grunnet begrensninger i tid og avhengighet av andre personers deltagelse i testing, er kun et begrenset antall tester gjennomført. Hver testrunde tok opp mot times tid, og det krever at 2-3 personer kan sette av denne tiden, noe som la en grense på mengden tester som var mulig gjennomføre.

1.3 Struktur

Videre er denne oppgaven strukturert på følgende måte:

Kapittel 2 - Metode. Beskriver metodebruken i denne masteroppgaven, gjennom bakgrunnsstudie, utvikling av scenarier og øvelse, testing og evaluering.

Kapittel 3 - Bakgrunn. Gir en introduksjon til hendelseshåndtering, IT-sikkerhetsutfordringer i kraftbransjen, beredskapsøvelser og relatert arbeid.

Kapittel 4 - Scenarier. Presenterer et utvalg eksisterende scenarier, hvordan scenarier til øvelser bør utvikles og legger frem scenarier på tre former som skal brukes som grunnlag for øvelsen.

Kapittel 5 - Øvelsen. Legger frem øvelsen og beskriver dens funksjonalitet. Øvelsen bygger på et eksisterende samarbeidsbrettspill, og er lagt til en parallell faglig del med scenarier.

Kapittel 6 - Resultater. Presenterer resultater fra testene av spillets funksjonalitet og øvelsen som helhet. Innspill fra bransjen blir også lagt frem.

Kapittel 7 - Diskusjon. Diskuterer resultater fra testingen, for å finne ut om dette er en type øvelse som kan brukes i kraftbransjen.

Kapittel 8 - Konklusjon og videre arbeid. Oppsummerer resultater og diskusjon, og presenterer en konklusjon av arbeidet basert oppgavens problemstilling.

1.4 Terminologi

Masteroppgaven er skrevet på norsk grunnet den sterke koblingen til kraftbransjen, en bransje der arbeidsspråket er norsk. Muligheter for testing og bruk ble vurdert betydelig høyere dersom språket er norsk.

Begreper som omhandler IT og sikkerhetsterminologi finnes ofte kun på engelsk, og for å unngå tvetydighet i oversettelsen av engelske faguttrykk, brukes det engelske uttrykket markert i *kursiv*.

Kapittel 2
Metode

Dette kapittelet beskriver metoden brukt i arbeidet med masteroppgaven, som videre kan deles inn i fire hovedfaser:

- **Bakgrunnsstudie:** Gjennomføre en bakgrunnsstudie om kraftbransjen, IT-sikkerhet, beredskapsøvelser og samarbeidsbrettspill.
- **Utvikling:** Basert på bakgrunnskunnskapen, designe scenarier som kan brukes som grunnlag for en øvelse. Deretter lage en tilpasset øvelse, i form av videreutvikling eller endring av eksisterende spill, med kraftbransjen som målgruppe.
- **Testing:** Gjennomføre tester, både av spillets endrede funksjonalitet og øvelsen som helhet.
- **Evaluering:** Finne ut, gjennom resultat av tester og tilbakemelding fra bransjen, om øvelsen kan fungere som en del av et beredskapsprogram.

2.1 Bakgrunnsstudie

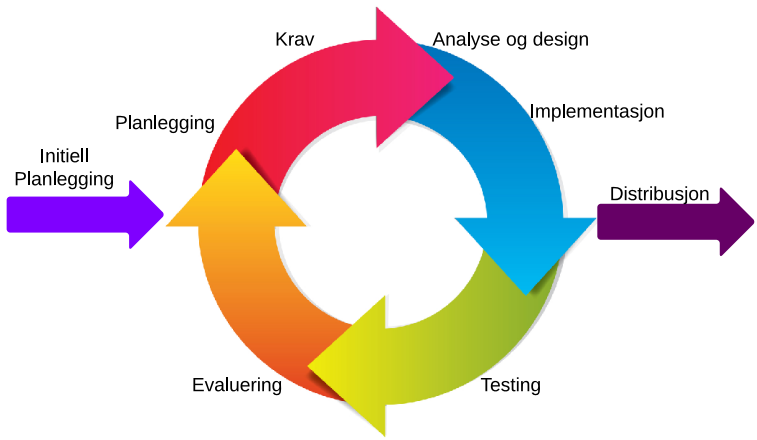
Bakgrunnsstudien gikk ut på å sette seg inn i standarder om hendelseshåndtering, samt basiskunnskap om kraftbransjen og de teknologiske utfordringene som finnes sett fra et IT-sikkerhetsperspektiv. I tillegg ble det studert veiledninger om beredskapsøvelser og undersøkt ulike typer øvelser. Som en del av bakgrunnstudien ble også relatert arbeid gjennomgått. Ut fra denne informasjonen ble det identifisert et behov for en praktisk øvelse. Under gjennomgangen av eksisterende praktiske øvelser ble blant annet spill vurdert. Samarbeidsspillet Pandemic viste seg å ha grunnfunksjonalitet som gjennom visse endringer åpnet for muligheten for å kunne fungere som en praktisk øvelse. Et viktig aspekt under valg av type øvelse, var at den var realistisk å utvikle innenfor gitt tid og omfang. Ved å bygge på et eksisterende konsept kan hovedfokuset være å teste om denne formen fungerer som øvelse, fremfor å bruke mye tid og ressurser på å bygge et spill helt fra bunnen. Dette styrker muligheten for å svare på oppgavens problemstilling på en grundig måte.

2.2 Utvikling

Øvelsen ble utviklet med bakgrunn i et eksisterende samarbeidspill. Spillet fikk visse endringer i grunnfunksjonalitet, og det ble lagt til en faglig del for å gjøre om spillet til en øvelse med læringsutbytte. Den faglige delen er et fellesbegrep for scenarier på tre ulike former. Utviklingen av øvelsen har skjedd gjennom en iterativ og inkrementell prosess.

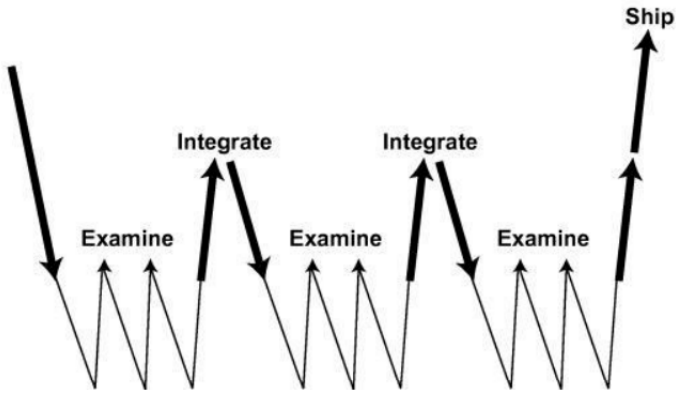
Inkrementell utvikling er en iscenesettende og planlagt strategi der ulike deler av systemet er utviklet ved forskjellige tidspunkter eller satser, og integrert ettersom de er fullført [1].

Iterativ utvikling er en bearbeidende planleggingsstrategi der tid er avsatt til å revidere og forbedre deler av systemet [1], vist i figur 2.1.



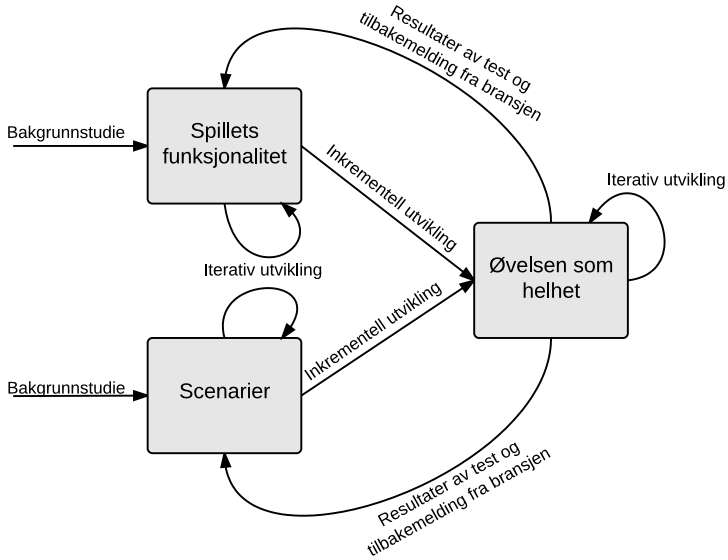
Figur 2.1: Iterativ utviklingsprosess

Cockburn anbefaler en kombinasjon av inkrementell og iterativ utvikling når et utviklingsprosjekt skal gjennomføres [1]. Hvis det bare inkrementeres risiker man en stor overraskelse på slutten av prosjektet dersom kvaliteten viser seg å være for dårlig. Alternativt kan en iterativ prosess av hele systemet medføre at ringvirkningene av endringene lett kommer ut av kontroll. Figur 2.2 viser en eksempelprosess der inkrementell og iterativ utvikling brukes i kombinasjon i løpet av tre perioder.



Figur 2.2: Iterativ og inkrementell utvikling i kombinasjon [1]

Utviklingen av øvelsen presentert i denne masteroppgaven er gjort inkrementelt i to perioder, og iterativt i hver av disse, illustrert i figur 2.3. Med bakgrunn i et eksisterende spill ble det først gjort videreutvikling og endring for å gjøre spillet tilpasset IT-sikkerhet og kraftbransjen. Funksjonaliteten ble deretter testet, og ut fra resultatene kunne spillet justeres for å oppnå ønsket funksjonalitet.



Figur 2.3: Arbeidsprosess

Parallelt med utviklingen av spillet ble det laget scenarier med inspirasjon fra eksisterende scenarier, samt tilegnet kunnskap om bransjen og IT-sikkerhet i deres systemer. På denne måten kunne spillet og den faglige delen med scenarier tilpasses hverandre etterhvert som utviklingen foregikk.

Deretter ble den faglige delen inkludert i spillet, og øvelsen som helhet ble testet. Det ble også her gjort justeringer iterativt, med grunnlag i tilbakemeldingene fra bransjen og resultater fra tester.

I utviklingen av spillet, særlig i design av spillbrett og kort, ble det brukt skisser tidlig i designfasen. Skisser er ofte laget for å utvide design, mens en prototype er laget for å evaluere designideer. Prototyper kan variere i stor grad, og hovedfordelen er at de på et tidlig punkt kan bekrefte om et designet spillmekanikk resulterer i det ønskede spilldynamikken når det spilles [24]. Spillet som presenteres i denne masteroppgaven er en prototype som brukes til å vurdere om dette er en type øvelse som kan brukes i kraftbransjen. Dersom den skal innføres i bransjen bør det gjøres mer arbeid med design og kvalitet på de fysiske elementene som spillbrett, kort og brikker.

2.3 Testing

Hovedmålet for testingen var å finne ut om denne formen for øvelse kunne fungere som beredskapsøvelse i kraftbransjen. Som beskrevet i forrige seksjon, forgikk testene underveis i utviklingen, både av øvelsen som helhet og spesifikt på spillets funksjonalitet uten den faglige delen.

Eladhari et al. fremhever viktigheten av en nøye planlegging når det kommer til designprosessen av prototypene, deres utvikling og testingen av dem. Dette gjelder også vurderingen av hva slags data man ønsker å innhente, og hvordan behandle dem for å skaffe materialer for analyse som kan støtte utforskningen av problemstillingen i studien [24]. I forkant av hver test ble det satt opp sentrale mål for testen. Observasjoner underveis ble notert og resultatene ble diskutert med deltagerne i etterkant. Dataene dannet grunnlaget for anbefalinger, og skapte et utgangspunkt for diskusjon, vurderinger og justeringer.

Kvalitative forskningsmetoder er spesielt gode i tidlige faser av prosjektet. Her blir skisser og prototyper evaluert for å forstå både hva som er riktig design å jobbe videre med, samt hvordan designet kan forbedres for å komme opp med nye ideer [24]. Denne metoden ble vurdert til å være mest hensiktsmessig i testing av øvelsen. Ved å gjennomføre relativt få og grundige tester med et begrenset antall deltagere var det mulig å oppnå et ønsket datagrunnlag for videre diskusjon og vurdering av øvelsen.

De initielle spilltestene ble utført av utvikler selv, da det er lite hensiktsmessig å inkludere mange deltagere når man vil teste spesifikke elementer uten å ha spillets helhet som fokusområde. Funksjonelle tester og tester med ekte spillere er mer hensiktsmessig å gjennomføre senere i prosessen, hvor målet er å oppdage feil i funksjonaliteten til spillet, i tillegg til å balansere spillingen i forhold til tiltenkt spillopplevelse [24]. Testing av spillets funksjonalitet med flere deltagere ble gjort både med og uten faglig del.

2.4 Evaluering

Tilbakemelding fra bransjen er viktig for å kvalitetssikre øvelsen, særlig den faglige delen. Utvikler av denne øvelsen har IT-sikkerhet som fordypningsemne, og begrenset bakgrunn innenfor energi. Det er liten hensikt å ha som målsetning at øvelsen skal kunne brukes i kraftbransjen dersom den viser seg og ikke fungere der, derfor er slike tilbakemeldinger essensielle.

Etter at problemstillingen for masteroppgaven var satt, ble relevante bidragsytere kontaktet. Henvendelsen inneholdt en presentasjon av oppgavens hovedmål, og en forespørsel om å sette av tid til å komme med innspill rundt øvelsen på et senere tidspunkt. Cassel og Symon [25] anbefaler at dette gjøres så tidlig som mulig. Med en gang noen har bundet seg til en avtale, er det mindre sannsynlig at de senere trekker seg. Dette viste seg å være viktig, bidragsyterne er travle mennesker, men de som hadde sagt ja i første omgang holdt avtalen og ga tilbakemeldinger.

Etter at testingen av øvelsen var gjennomført, ble bidragsyterne kontaktet på nytt. De mottok en presentasjon av øvelsen med faglig del, samt spørsmål og nøkkelpunkter rundt øvelsen sett fra deres perspektiv. I ett tilfelle ble responsen diskutert og forklart i en oppfølgende telefonsamtale. Innspillene fra bransjen bidro til justeringer i den faglige delen og til øvelsen som helhet. I tillegg til tilbakemeldinger fra bransjen ble evaluering av øvelsen gjort på grunnlag av resultater fra testene. Disse to ble diskutert og vurdert opp mot hverandre for å komme frem til et svar på problemstillingen.

Kapittel 3
Bakgrunn

Dette kapittelet presenterer bakgrunnsinformasjon om emner som hendelseshåndtering, beredskapsøvelser, kraftbransjen og IT-sikkerhet, samt relatert arbeid.

Hendelseshåndtering er et begrep som brukes om hele prosessen av aktiviteter som trengs i en situasjon der sikkerhetshendelser skal håndteres. En organisasjon må være i stand til å gjennomføre hendelseshåndtering for å detektere hendelser, minimere tap og skader, begrense utnyttede svakheter og gjenopprette IT-tjenester [26]. En nødvendighet for vellykket hendelseshåndtering er å teste planer, trene på sikkerhetshendelser, og å holde øvelser for at skal personalet være drillet i fremgangsmåter dersom en sikkerhetshendelse skulle oppstå. Selv den minste test, øvelse eller trening vil styrke virksomheten i forkant av en sikkerhetshendelse [27].

De mest kjente standardene om hendelseshåndtering er utgitt av ISO/IEC[1] [9], NIST[2] [26], ENISA[3] [28], SANS [4] [29] og NorSIS [27]. Til forskjell fra de andre er ISO er basert på internasjonal enighet og dermed mest anerkjent. Alle har delt hendelseshåndterings-prosessen inn i faser. Den første fasen, om å etablere en evne til å håndtere hendelser gjennom planlegging og forberedelser, er ganske lik i alle, de andre fasene varierer i større grad. Den første fasen foregår kontinuerlig, mens de påfølgende fasene trigges av en hendelse. Disse standardene er laget generelle, de er ikke industrispesifikke eller rettet spesifikt mot kritiske infrastrukturorganisasjoner, men noen er rettet mot organisasjoner av visse størrelser. Alle standardene fremhever viktigheten av å ha etablerte planer, og ha et trenings og bevisstgjøringsprogram ovenfor ansatte.

ISO/IEC 27035 [9] omhandler håndtering av informasjonssikerhetshendelser. Det er viktig for alle organisasjoner å ha en strukturert og planlagt tilnærming for å

[1] International Organization for Standardization and the International Electrotechnical Commission

[2] National Institute of Standards and Technology

[3] European Union Agency for Network and Information Security

[4] SysAdmin, Audit, Networking, and Security Institute

oppdage, respondere, rapportere og lære fra disse type hendelser. Hendelseshåndtering blir beskrevet som en prosess delt inn i fem faser, og med bakgrunn i denne oppgavens problemstilling vil det bli fokusert på den første:

1. Planlegging og forberedelser
2. Deteksjon
3. Vurdering og rapportering
4. Respons
5. Evaluering/læring

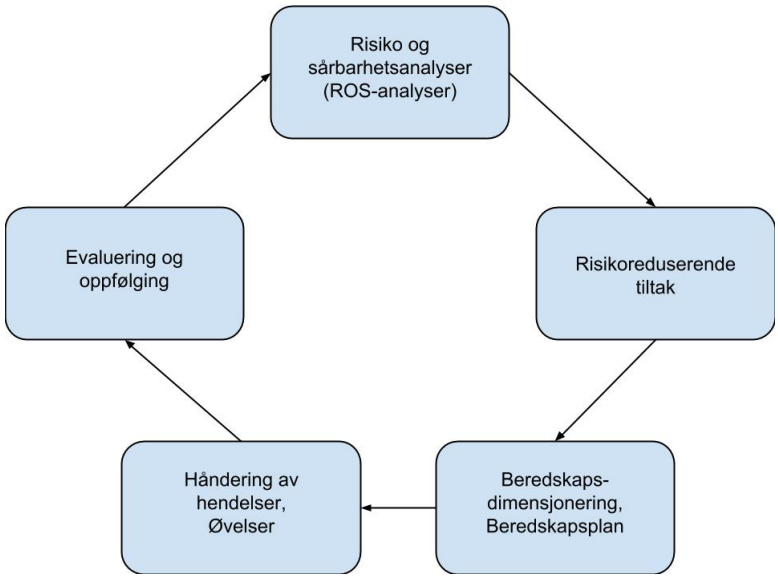
Planlegging og forberedelser er den mest omfattende fasen. Før organisasjonen formulerer en hendelseshåndteirngspolitikk bør det gjennomføres en sikkerhetsgjennomgang som vurderer dagens sårbarheter, sier noe om behovet for en hendelseshåndteringsplan og identifiserer organisasjonens fordeler. I denne delen er det viktig å sikre engasjement fra toppledelsen for å sikre forpliktelse til ressurser og vedlikehold av organisasjonens evne til å håndtere hendelser.

Det må utarbeides en detaljert hendelseshåndteringsplan som omhandler hvordan man skal respondere på en hendelse. Den skal inneholde hvordan man detekterer og rapporterer en hendelse, samt en klassifiseringsskala av ulike typer hendelser med både innvirkning og sannsynlighet.

En av hovedoppgavene i denne fasen er å utforme et trenings og bevisstgjøringsprogram, der øvelser en betydelig del. Det er viktig at alle i organisasjonen forstår hvorfor deres deltagelse i dette programmet er til stor fordel for både dem selv og organisasjonen som helhet. Denne fasen består også av etablering av et responsteam (CERT).

3.1 Beredskapsøvelser

For etablere en god evne til krisehåndtering, og være i stand til å respondere på en god måte når det skjer uventede situasjoner, bør beredskapsøvelser stå høyt på agendaen hos alle organisasjoner. Viktige samfunnsfunksjoner har krav om å gjennomføre slike øvelser med jevne mellomrom, og mest brukt er diskusjonsøvelser og øvelser der en ekte hendelse blir simulert, i ulik omfang og kompleksitet. NVE har plassert håndtering av hendelser og øvelser som en fase av et kontinuerlig beredskapsprogram, vist i figur 3.1. Tema for øvelser må være relevante og gjenspeile trussel- og risikobildet avdekket gjennom risiko-og sårbarhetsanalyser og beredskapsplanverk [2].



Figur 3.1: Beredskapsprogram [2]

Energiloven[5] gir de overordnede rammene for organiseringen av kraftforsyningen i Norge, og danner i kombinasjon med Beredskapsforskriften, grunnlaget for lover og forskrifter når det kommer til beredskap i kraftbransjen. Tilsynsansvaret ligger hos Direktorat for Samfunnssikkerhet og Beredskap (DSB) og NVE, som har opprettet et tilsynsforum, og der sistnevnte også veileder og støtter i beredskapssituasjoner. Fra og med 2013 inkluderer Beredskapsforskriften krav om å gjennomføre øvelser basert på IT-sikkerhetshendelser.

3.1.1 Øvelsesfaser

NVE deler en beredskapsøvelse inn i fire faser: Planlegging, gjennomføring, evaluering og oppfølging [2].

Planlegging: I denne fasen er målet å komme frem til en enighet om formål og overordnede mål med øvelsen. Organiseringen av resten av arbeidet må fordeles, og det må etableres en planleggingsgruppe med representanter fra forskjellige fagfelter. Scenariet som skal brukes i øvelsen bør skreddersys henhold til aktører og mål. Øvelsen skal føles relevant og realistisk, og bør utvikles på en slik måte at deltagerne oppnår mestringsfølelse samtidig som den er utfordrende. Støttedokumenter må

[5]av 29. juni 1990 nr. 50. Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.

utformes, for eksempel kan en dreiebok med strukturerte innspill være nyttig til en diskusjonsøvelse.

Gjennomføring: Å legge til rette for praktisk gjennomføring av øvelsen i et lokale kan bestå av plassering av utstyr og bruk av kart som hjelpemiddel. En innledende presentasjon fra øvingsleder bidrar til at alle deltagerne har en felles forståelse når øvelsen starter. Øvingslederen leder øvelsen og har det overordnede ansvaret underveis, men samtidig er det ønskelig at vedkommende er mest mulig passiv. Personen ansvarlig for evaluering bør gjennomføre en muntlig førsteinntrykksevaluering av øvelsen, noe som bidrar til å få øvelsen "ut av systemet".

Evaluering: Evaluering er en viktig og nødvendig del av en øvelse. Erfaringspunkter kan samles i en evalueringsrapport, der fokus er på suksessfaktorer, utfordringer og forbedringspunkter. Strukturen på dokumentet bør være: Innledning, om øvelsen, evaluering(i henhold til øvingsmål og momenter), samt oppfølging.

Oppfølgning: Oppfølging handler om å iverksette forbedringstiltak indentifisert under øvelsen. Når tiltakene er iverksatt og implementert i organisasjonen og i relevant dokumentasjon, er det nyttig med en ny øvelse. Øvingsopplegget som helhet bør også evalueres.

Det amerikanske departementet for sikkerhet[6] presenterer en veldig lik prosess når de beskriver utvikling og gjennomføring av en beredskapsøvelse, vist i figur 3.2.

Figur 3.2: Faser av en beredskapsøvelse [3]: Design/utvikling, gjennomføring, evaluering og forbedrende planlegging.

3.1.2 Type øvelser

Det eksisterer mange typer beredskapsøvelser, som ofte deles inn i to hovedkategorier: diskusjonsbaserte- og operasjonsbaserte øvelser. Beskrivelsene nedenfor er hentet fra

[6] U.S department of Homeland Security

det amerikanske øvelses- og evalueringsprogrammet [30].

Diskusjonsbaserte øvelser er en god måte å gjøre deltagerne kjent med gjeldende planverk og prosedyrer, samt utvikle nye. Felles for disse øvelsene er at de sjelden overskrider en arbeidsdag, og at handlingene ikke blir utspilt fysisk.

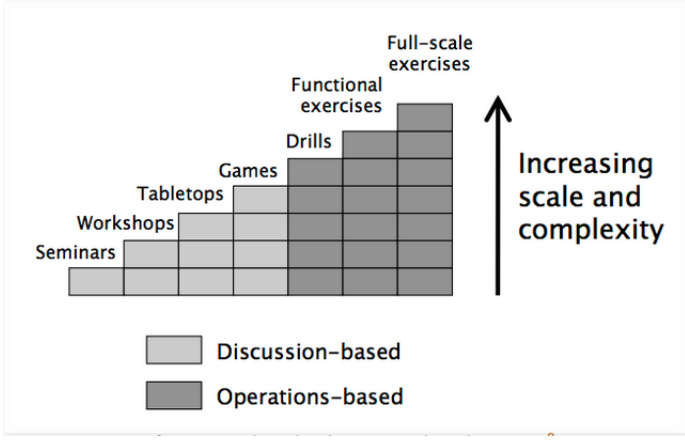
- Et **seminar** har som formål å orientere deltagerne for nye eller nåværende planverk, ressurser, strategier eller idéer.
- En **workshop** har som fokus å utvikle et nytt produkt, for eksempel å endre eksisterende planverk, mål, osv. Den skiller seg fra et seminar ved at deltagerne i større grad bidrar med innspill i prosessen.
- **Skrivebordsøvelser** hjelper deltagerne til å forstå planverk og prosedyrer. Her blir hypotetiske situasjoner tatt opp og man diskuterer ulike måter å håndtere den på. Skrivebordsøvelser kan brukes til å øke generell oppmerksomhet, validere planverk og prosedyrer, eller øve på spesifikke konsepter. Generelt er de brukt til å oppnå en felles forståelse, identifisere styrker og områder for forbedring, og/eller oppnå endringer i oppfatninger hos deltagerne.
- **Spill** er en simulering av operasjoner, og omfatter ofte grupper som konkurrerer i et miljø med regler, data og prosederer designet for å skildre en faktisk eller antatt virkelig situasjon. Beslutningstakingen kan oppleves stressende avhengig av hvordan spillet er designet, og inkluderer en stor mengde "Hva om.."-situasjoner. Konsekvensene av spillernes handlinger kan enten være forhåndsbestemte eller dynamiske. Å identifisere kritiske beslutningstakingssituasjoner er en stor del av evalueringsprosessen.

Operasjonsbaserte øvelser har ofte samme mål som diskusjonsøvelser, men skiller seg fra dem ved at gjennomføringen består av faktiske handlinger og skjer i nåtid. Dette kan for eksempel være å initiere kommunikasjon eller mobilisere personell og ressurser.

- En **drill** er en koordinert, veiledet aktivitet brukt til å validere spesifikke funksjoner eller evner, for eksempel trening på nytt utstyr eller etablering av krisesenter. Kan også brukes til å vurdere om planer utføres som designet, for å identifisere om mer trening er nødvending eller til å styrke beste praksis.
- En **funksjonell øvelse** er designet for å teste en eller flere funksjoner av krisehåndteringen gjennom en interaktiv, tidsbegrenset, simulert hendelse i et realistisk miljø. Deltagere kan for eksempel få innspill via telefon/radio/TV-sendinger og må handle deretter. Begrenser seg typisk ved at bevegelse av personell og utstyr er simulert.

– En **fullskala** øvelse er den mest komplekse og ressurskrevende typen av øvelser. Den involverer flere aktører fra ulike etater og organisasjoner, og validerer alle fasene av beredskap. Her trener man som om det skulle vært en virkelig hendelse.

Disse øvelsestypene varierer i omfang og kompleksitet, se figur.



Figur 3.3: Variasjoner av diskusjonsbaserte og operasjonsbaserte øvelser [4]

3.1.3 Eksisterende praktiske øvelser

Ulike tilnærminger ble vurdert som grunnlag for øvelsen som skal lages i denne masteroppgaven. Da øvelsen skulle være praktisk basert, og realistisk å få testet, ble det fokusert på ulike former for spill som kan inneholde læring eller som har en potensiell kobling til IT-sikkerhet, samt øvelser basert på simulering.

Fysiske spill. Det finnes en del brettspill på markedet som handler om IT-sikkerhet eller bygger på prinsipper som ligner en angrepssituasjon.

– **Control-Alt-Hack** [31] er et spill der spillerne innehar ulike IT-sikkerhetsrelaterte roller og spiller mot hverandre, og hovedoppgaven er å fullføre individuelle oppdrag. Spillet krever ingen kunnskap om IT-sikkerhet for å vinne, som er vedkommende som oppnår flest poeng på oppdragene (terningkast vs deres karakters individuelle egenskaper), men man introduseres for en del IT-sikkerhetsterminologi.

– **Pandemic** [32] Er et strategispill for hele familien, i form av et samarbeidsbrettspill der 2-4 spillere beskytter verden mot flere sykdommer som sprer seg. Målet med spillet er å utrydde disse ved å utvikle vaksiner.

- **[d0x3d!]** [33] er et brettspill om nettverkssikkerhet. Et nettverk bestående av kjente nettverkselementer representert ved spillkort settes opp. Systemet er under angrep fra utenforstående, og gruppa spiller med hverandre mot systemet for å vinne. Spillet er inspirert av "Forbidden Island", der man hindrer en øy fra å synke. [d0x3d!] er testet hos bedrifter, og det rapporteres å ha god funksjon som en "icebreaker" mellom ledere og ansatte før man diskuterer lokale IT-retningslinjer [34].
- **The Disaster game** [35] er et verktøy med formål å utvikle unike og veldig detaljerte krisesituasjonsscenarier til en diskusjonsøvelse som engasjerer og utfordrer øvelsesdeltagerne. Et hovedscenario blir trukket, og ulike variabler bestemt med terningkast (tid, dag osv.). Deretter blir variable hendelser langt til, og deltagerne må diskutere rundt scenariet.
- **Protection and Deception (P&D)** [36] er et strategisk brettspill for to personer med formål om å introdusere kunnskap om IT-sikkerhet. Begge spillere setter opp nettverk på brettet sitt, og fordeler angrep- og forsvarspakker, og prøver å bryte seg inn i hverandres nettverk.

Digitale spill om IT-sikkerhet:

- **Secure Empire** [37] er et spill der en person eier en bedrift, og må kjøpe og selge komponenter på et marked. Underveis kommer det opp problemstillinger innen IT-sikerhet som må løses for å skape en suksessfull bedrift.
- **Cybersecure: Your Medical Practice** [38] er et spill basert på drift av en suksessfull legepraksis. Underveis må man svare riktig på IT-sikkerhetsspørsmål realatert til dette.

Simuleringsøvelser: Minst tre ulike instanser tilbyr trening i et simulert miljø. Det er begrenset tilgang på detaljert informasjon om konkret implementasjon, og lite forskning rundt erfaringene.

- Senter for sikkerhet i kontrollsystemer i Japan [39] har bygd opp et fysisk miljø der organisasjoner kan komme å trene på angrep mot ekte kontrollsystemer.
- ENCS[7] [40] tilbyr et avansert 3-dagers kurs for industrielle kontrollsystemer og smargrid-sikkerhet. En stor del av kurset består av en "red-team - blue-team"-øvelse, der det ene teamet beskytter et bedriftsnettverk og det andre teamet prøver å angripe det.

[7] European Network for Cyber Security

– Ved Kaspersky-instituttet i Nederland finnes en Industriell beskyttelses-simulator [41]. Deltakergrupper på 3-5 personer har ansvar for hver sitt vannanlegg, representert på et brett. De må sørge for en uforstyrret funksjon mens angrep pågår. Gruppen som vinner er den som har mest penger ved spillets slutt, og dermed har gjort de riktige valgene for å tjene mest mulig penger, og minske kostnader fra angrep.

Tabellen under oppsummerer de ulike praktiske øvelsene presentert, og sier noe om hvilke områder de dekker. Flertallet inkluderer IT-sikkerhetslæring, da det var ett av hovedkriteriene. Derimot er det ikke alltid en nødvendighet at denne kunnskapen er avgjørende for suksess eller fiasko, i enkelte spill avgjøres dette av terningkast eller tilfeldighet. Halvparten av øvelsene og spillene krever samarbeid, og kun et fåtall inneholder fysisk/digital simulering av konsekvenser av hendelser eller angrep. Kun simuleringsøvelsene dekker alle områdene, men disse øvelsene er veldig omfattende, så å lage et spillalternativ som inkluderer alle fire punktene vil være et unikt bidrag til eksisterende øvelser.

Navn	IT-sikkerhet læring	Avgjørende kunnskap	Samarbeid	Simulering av angrep
Pandemic			x	x
[d0x3d!]	x		x	
Disaster game	x	x	x	
Control, alt, hack	x			
P&D	x	x		
Digitale spill	x	x		
Simulerings-øvelser	x	x	x	x

Tabell 3.1: Sammenlikning av eksisterende praktiske øvelser

Flere organisasjoner tilbyr opplæring i nettverkssikkerhet gjennom konkurranser (”Red/blue team”,”Capture the flag”, og former av skattejakt), og en studie av disse type øvelsene viser at det er en god måte å trene på [42]. Blant hovedargumentene er å fremme kreativitet i et praktisk miljø. Samtidig påpekes det at disse øvelsene er vanskelige å lage og gjennomføre, i tillegg til at en studie av 4 av de store industrielle IT-sikkerhetskursene som tilbys i USA [43] konkluderer med at ingen av programmene dekker 100% av sikkerhetstreningen som kreves av en ansatt.

3.1.4 Samarbeidsbrettspill for læring

Det eksisterer mange samarbeidsbrettspill, og spesielt brettspill som bygger på strategitenkning har blitt populære den siste tiden [44]. Samtidig sees stadig oftere ulike spill med formål om læring, og med introduksjonen av digital læring i skolen er dette veldig aktuelt. Kunnskapsspill, i for eksempel quiz-form, fungerer ikke optimalt som en beredskapsøvelse på grunn av mangelen på samarbeid. En utfordring vil derfor være å kombinere læring og samarbeid i ett og samme spill, noe som er et lite utforsket domene. For å komme opp med et forslag på hvordan dette kan løses, må eksisterende spill og deres mekanismer studeres.

Samarbeidsspill

Tradisjonelt er alle spill basert på enten konkurranse eller samarbeid. Konkurransespill krever at spillerne utformer strategier som direkte motsetter den andre parten. I et samarbeidsspill spiller alle deltagerne sammen som en gruppe, og vinner sammen. Utfordringen i denne typen spill er å samarbeide for å maksimere "teamnytte" [45]. Felles for samarbeidsspill er at det er mange måter å tape på, men bare sammen kan man klare å vinne.

Spill som involverer samarbeid er ofte komplekse. For å analysere og forstå denne typen spill på en generell basis kan en analysering av brettspill det være godt sted å starte, da analysen av disse ofte er enklere. I studien til Zagal et al. [45] er samarbeidsbrettspillet "Lord of the Rings"analysert for å oppnå en forståelse av samarbeidsspill generelt. Basert på erfaringene fra analysen inneholder resultatene blant annet identifisering av fire mekanismer som må fungere i et vellykket samarbeidsbrettspill:

1. Et samarbeidsspill bør introdusere en spenning mellom oppfattet individuell nytte og teamnytte. Spillerne må kunne vurdere egne gode handlinger opp mot beste avgjørelse for teamet.

2. Individuelle spillere må ha lov til å ta avgjørelser og gjøre handlinger uten samtykke fra resten av teamet.

3. Spillerne må klare å spore vinninger tilbake til sine beslutninger.

4. For å oppmuntre gruppemedlemmer til å ta egoistiske beslutninger, burde et samarbeidsspill tilegne ulike evner eller ansvar på spillerne.

Ulike designutfordringer må løses for å utvikle et godt samarbeidsspill [45]. Spillet må ikke preges av at en spiller tar beslutninger for laget, da samarbeidsspill er nødt til å gi en tilstrekkelig begrunnelse for samarbeid. For at spillet skal være engasjerende må

spillerne bry seg om utfallet og at det skal ha et tilfredsstillende resultat, samtidig må erfaringene være forskjellige hver gang, og utfordringene må utvikle seg.

I en spillsituasjon kreves mange forskjellige former for tenking og beregninger underveis. Berland og Lee studerte strategispillet Pandemic for å forstå distribuert beregningstenkning [44]. Analysene ble delt inn og gjort basert på fem kjerneaspekter:

- **Betinget logikk:** Bruk av "hvis-dersom-ellers", der det tenkes og fokuseres på konsekvenser av valg.
- **Distribuert beregning:** Handlinger og beregninger basert på betraktninger, situasjoner og strategidannelse som involverer flere parter med ulike kunnskapsressurser.
- **Feilsøking:** Utforskning av problemer med bakgrunn i hva som er lov og ikke ifølge reglene.
- **Algoritmebygging:** Lage et sett instruksjoner for å planlegge handlinger for hendelser som skjer.
- **Simulering:** Å modellere eller teste algoritmer og logikk.

Hovedresultatet fra studien er en beskrivelse av og bevis for at kompleks beregningstekning kan utvikles spontant gjennom en runde brettspill. Dette kan kobles opp mot flere av de samme aspektene som oppstår i en beredskapssituasjon. Ved å bruke denne typen spill som grunnlag for en beredskapsøvelse, vil man kunne fremprovosere mange av de samme tankemønstrene som ønskes brukt i en øvelsessituasjon.

Spill for læring

De siste årene har spill for læring utviklet seg mye, og særlig digitale læringsspill. Et fellestrekk ved de fleste er at de er individuelle og ikke krever samarbeid. Wang et al. har studert hvilke egenskaper som karakteriserer et godt læringsspill. Vanskelighetsgraden burde kunne justeres etter deltagernes nivå, og tilgjengelige hjelpemidler må være lett tilgjengelig i form av bakgrunnsstoff eller hint. Spillkonseptet må inspirere spilleren til å investere tid i spillet. Ideelt bør spillerne oppleve nysgjerrighet, gjerne miste begrep om tid og sted, samt ønske å fortsette når spillet er over.

3.2 Kraftbransjen

Kraftbransjen er en kompleks bransje som innehar et viktig ansvar for samfunnskritisk infrastruktur. Elektrisitetsproduksjonen i Norge var 128 TWh i 2012, der 93% var vannkraft. Energi er en ressurs som ikke kan lagres, og må brukes når den produseres. Den totale energibalansen er en frekvens som indikerer ubalanse mellom produksjon og forbruk, og skal ligge mellom 50.1 og 49.9 hertz. I Norge har Statnett ansvar for å ivareta denne balansen, gjennom en nordisk kraftflyt [5].

Overføring av strøm

Strømnettet i Norge er delt inn i tre nivåer:

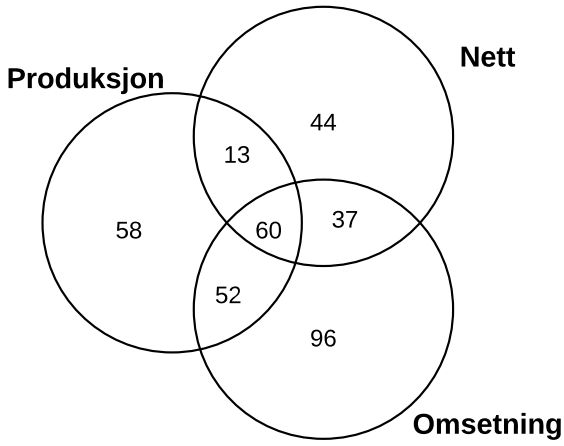
- **Sentralnettet** er et landsdekkende system med høy kapasitet, ofte referert til som hovedveiene i kraftsystemet.
- **Regionale nett** er bindeleddet mellom sentralnettet og distribusjonsnettet.
- **Distribusjonsnettet** er lokale kraftnett. Her transformeres spenningen ned til 230V for å kunne levere kraft til sluttbrukerne.

Aktører

Norsk kraftsektor er preget av et stort antall aktører innenfor forskjellige virksomhetsområder. Sektoren er organisert rundt aktivitetene produksjon, overføring og omsetning av kraft [5].

- **Produksjonsselskap** er et selskap som produserer strøm. Statkraft er største aktør i Norge, med 42% av produksjonskapasiteten.
- **Nettselskaper** driver nettvirksomhet på ett eller flere nivåer. De er sluttbrukerens kontaktpunkt til kraftnettet, og er ansvarlige for drift og vedlikehold av distribusjonsnettet i sin region, samt måling og avregning av strøm [46].
- **Omsetningsselskapenes** sentrale oppgaver er å kjøpe og videreselge kraft.

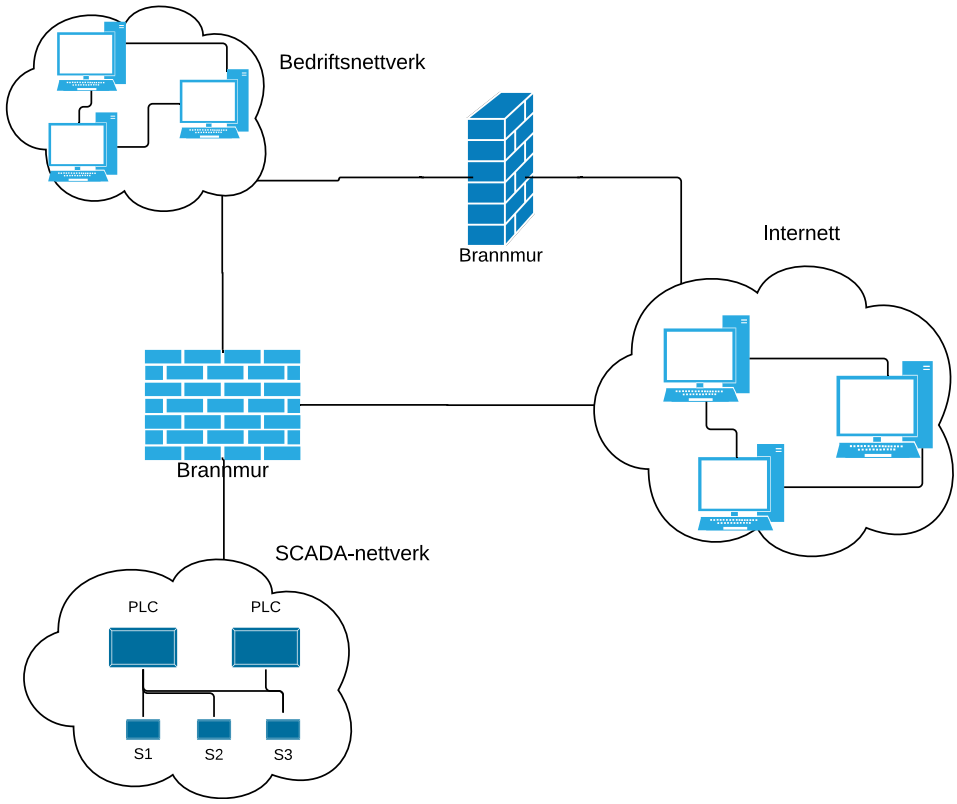
Flere av aktørene har virksomhet innenfor flere av områdene, beskrevet i figur 3.4.



Figur 3.4: Aktører i kraftbransjen, per 31.12.2012 [5]

3.2.1 Kontrollsystemer

Kontroll og styring av energi er en krevende oppgave, og kontrollsystemer (SCADA-systemer) er en vesentlig del av teknologien som bidrar til en vellykket kraftforsyning. Kontrollsystemer er adskilt fra det det vanlige bedriftsnettet og Internett. Det er komplekse nettverk som støtter kommunikasjon mellom en sentral kontrollenhet og mange eksterne enheter på en felles kommunikasjonsbuss. Kommunikasjonen skjer gjennom utveksling av kontrollmeldinger mellom master- og slaveenheter. En masterenhet er typisk en PC eller en programerbar, logisk kontroller (PLC), se figur 3.5. I mange tilfeller finnes det et eget kontrollsenter, lokalisert i en separat fysisk del av organisasjonen. Disse består av servere, skjermer og et grensesnitt for menneskelig styring [6].



Figur 3.5: Typisk SCADA-arkitektur [6]

SCADA-systemene har tradisjonelt vært avgrensende nettverk som kommuniserer over proprietære protokoller. De var ikke designet for offentlig tilgang, og mangler i mange tilfeller elementære sikkerhetsmekanismer [47]. Organisasjonenes ønske om å modernisere SCADA-systemene for å optimere kostnader og øke effektiviteten, fører til at disse i større grad blir koblet til bedriftsnettverket og internett [6]. Selv om dette skaper muligheter på mange områder, åpner det også for en ny verden av sårbarheter og mulige angrep [48].

3.2.2 Personell og kompetanse

Historisk sett har produksjonssystemer og vanlige IT-systemer hatt ulikt opphav og utvikling. Personellet som drifter og håndterer disse systemene har dermed også ulik bakgrunn og kompetanse. IT-sikkerhetskonsulentselskapet Mnemonic har jobbet tett med bransjen, og påpeker at miljøene ikke lengre skilt teknisk sett, men praktisk drift og samarbeid er hos mange fremdeles ikke samkjørt [48]. Dagens situasjon

gjør det derimot nødvendig at IT-personell og kontrollsystempersonell samarbeider. En av de største utfordringene med samarbeid, er hvordan disse to typer personell prioriterer tilgjengelighet og konfidensialitet når det kommer til IT-sikkerhet i de respektive systemene. I IT-sammenheng, hvis en datamaskin blir utsatt for et angrep, er fokuset på å frakoble den fra nettet og reinstallere. For kontrollsystemer er derimot tilgjengelighet ekstremt viktig, da nedetid er veldig kostbart både økonomisk og samfunnsmessig [49]. Kontrollsystemkomponenter må byttes av fagpersonell, og kan i verste fall ta flere måneder [50].

Oljebransjen har mange fellestrekk med kraftbransjen når det kommer til sikkerhetsutfordringer i forbindelse med kontrollsystemer og ulike typer personell. I en studie gjennomført 2009 [51] ble det avdekket mangel på tillit mellom dem, og enkelte kontrollsystempersonell gikk så langt som å benekte at systemene deres inneholdt viktige IKT-komponenter:

> ”Vi har ikke IKT” - felles oppfatning blant kontrollsystempersonell.

I en kvartalsrapport utgitt av NSM i 2013, fremhever Eirann Leverett viktigheten av fokus på hendelseshåndtering i kraftbransjen. Selv om SCADA-systemer er isolert fra internett, har flere av disse blitt angrepet av fra innsiden [50]. Virkeligheten er derimot annen, studier avdekker mangel på konsistent hendelseshåndtering i kraftbransjen, samt et stort forbedringspotensial i samarbeidet mellom de to gruppene personell [13, 17]. Allikevel klarer bransjen seg relativt bra på grunn av mye erfaring og taus kunnskap. Mange ansatte har lang erfaring og det finnes nøkkelpersoner med stor kompetanse om helheten i kraftsystemet, noe som kan bli en utfordring å opprettholde i fremtiden med et stadig mer kompleks organisasjon [52]. Det er vanskelig å opprettholde prosedyrer og planer for en hver mulig hendelse, viktigheten av kompetent personell er fremhevet av Tårnes, Hove [17] og Line et al. [49].

Det må ofte et angrep til før øvelser på et område blir prioritert, noe kraftbransjen er et godt eksempel på. Etter angrepet i 2014 har bransjen, inkludert beslutningstagere, innsett viktigheten av å gjennomføre øvelser på IT-sikkerhet. Utfordringene er derimot mange, og spesielt kompetanse i kryssdomenet mellom IT-sikkerhet og kontrollsystemer er en mangelvare, noe som må være et fokusområde for en vellykket hendelseshåndtering [22].

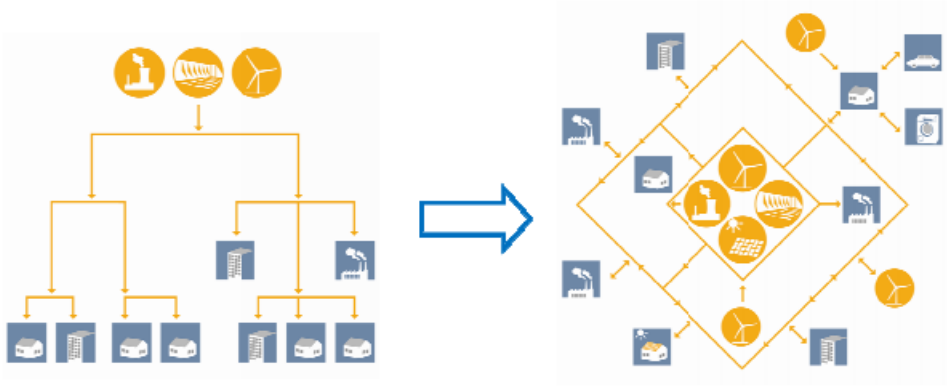
3.2.3 Fremtidens strømnett: Smartgrids og AMS

I Klimameldingen fra 2008 [53] ble det vedtatt et mål om at Norge skal være klimanøytralt innen 2030. Dersom målet om redusering av CO2-utslipp skal nåes, må det satses på fornybar energi. Dette kan være småkraftverk, bølgekraft eller vindturbinparker. Disse energikildene er ofte uregulerbare og lokalisert på steder

med dårlig nett-tilgang [7]. Dette er ikke det norske strømnettet bygget for, og nye måter å lage og bruke strøm på fører til et behov for oppdatering og innføring av nye teknologi [54]. Forbruket de siste tiårene har økt betraktelig, uten at investeringene i nettet gjenspeiler dette, noe som gjør at vi står ovenfor en situasjon med aldrende nett [55].

De siste årene har bransjen startet overgangen mot smartere nett, kalt smartgrid. Smartgrid er et begrep som omfatter mye, og Energi21 har definert det på følgende måte:

> Smartgrid er elektrisk infrastruktur basert på automatiserte løsninger, hvor en tillater toveis flyt av elektrisk energi og informasjon mellom produksjonsenheter, koblet til hvilket som helst spenningsnivå overfor forbrukerne og mellom alle andre knutepunkt i mellom [7].



Figur 3.6: Overgang fra tradisjonell overføring til smartgrid [7]

Innføringen av smartgrids fører til betydelige endringer i nettet. Kontroll og distribusjonssystemene blir integrert med kommunikasjonsnettverk, for å få nettet til å bli mer effektivt, motstandsdyktig og rimeligere å administrere og drifte [56]. Hovedforskjellene er at nå kan også små enheter, som smarthus og uregulerbare småkraftverk, være produsenter av strøm, samt at driften av nettet kan baseres på overvåkning i nåtid. Se figur 3.6 og tabellen nedenfor [7].

Tradisjonell kraftforsyning	**Smartgrid**
Sentralisert kraftproduksjon	Sentralisert kraftproduksjon og distribuert kraft produksjon (uregulerbare fornybare kilder)
Enveis transport av energi - fra produsent til forbruker	Effekt flyt i begge retninger - fra overliggende til distribusjon og omvendt
Driften baseres seg på historisk ekspertise	Driften av kraftsystemet er basert på on-line overvåking (målinger) og distribuerte algoritmer

En av de første endringene er innføringen av AMS. AMS erstatter strømmåleren i sikringsskapet, og sender automatisk avlesning til nettselskapet med en gitt tids mellomrom. Den gir mulighet for visning av prisinformasjon, momentant forbruk, automatisk styring av apparater, forbrukshistorikk og mulighet for kommunikasjon med f.eks. pc eller smarthus [54]. Dette åpner for forbrukerfleksibilitet. Sluttbrukerne vil prøve å bruke mindre strøm i dyre perioder, og på denne måten vil strømselskapene kunne redusere de store toppene i strømbruken. Ved å innføre en bryte/strupefunksjon som kontrolleres fra strømselskapet kan denne lastflyttingen gjøres ved å fjernstyre bryterne. En typisk av AMS-implementasjon vil bestå av en målernode med display hos kunde, kommunikasjonssystem mot nettselskapet og en frontend mot deres systemer.

3.3 Hendelseshåndtering og øvelser i kraftbransjen

3.3.1 Hendelseshåndtering

Det er gjennomført flere studier rundt hendelseshåndtering i kraftbransjen siste årene. Hove og Tårnes gjennomførte i 2013 en intervjustudie av store aktører i bransjen [17], og presenterte anbefalinger for øvelser og vellykket hendelseshåndtering. Det ble påpekt at gjennomføring av øvelser for å tilegne erfaring er viktig, da erfaringer har vist å være vell så viktig som å ha etablerte planer. Øvelsene bør gjelde både små og store hendelser, dersom små hendelser ikke er håndtert på en tilfredsstillende måte kan den eskalere til en mer alvorlig situasjon. Informasjonsspredning, kommunikasjon og fordeling av ansvar er områder med store utfordringer, og det bør fokuseres på disse. Nøkkeltemaer for øvelser kan være informasjonsklassifisering, oppdaging av hendelser og rapporteringsprosedyrer.

Akhtar [18] studerte i 2013 grad av beredskap som fase i en hendelseshåndteringsprosess i ulike organisasjoner, blant annet i kraftbransjen. Konklusjonen var at planer og prosedyrer for hendelseshåndtering er implementert til en viss grad. Det ble identifisert noen aktiviteter som liknet de beskrevet i standardene, men dette var til

en begrenset grad. Kun en av de undersøkte organisasjonene hadde en relativt høy grad av beredskap, men generelt rapporteres det om mangel på forberedelse når det kommer til den økende risikoen og mulige svakheter.

Et interessant aspekt er årsakene til mangelen på planer for hendelseshåndtering og lav beredskap rundt IT-sikkerhet. Line et al.[49] rapporterer at ingen av lederne de har intervjuet sier at de gjennomfører øvelser med IT-sikkerhetshendelser, og at noen av grunnene til mangelen på trening er:

- Vanskelig å prioritere, andre oppgaver har høyere prioritet
- Øvelser involverer en kostnad
- Det har sjeldent vært hendelser av denne typen
- Mangel på kunnskap om hvordan planlegge og gjennomføre slike øvelser

Kraftbransjen er godt forberedt på tradisjonelle trusler, som fysiske angrep, viser en studie av seks nettselskaper i Norge [21]. Det avdekkes derimot at fokuset på IT-hendelser i kontrollsystem-miljøet må økes. Ingen hadde gjennomført trening og sikkerhetsbevisstgjøring for dette personellet. Det scenariet som fryktes mest er et angrep der angripere får kontroll over strømswitcher og forårsaker strømbrudd i store områder, men ingen har gjennomført øvelser med dette scenariet. Skriftlige prosedyrer rundt respons på hendelser i kontrollsystemet eksisterer bare hos ett nettselskap.

En ting er hvordan utenforstående oppfatter fokuset på IT-sikkerhet i kraftbransjen, en annen sak er hvordan bransjen oppfatter dette selv. En masteroppgave av Røyksund [57] ser på hvordan kraftbransjen tolker risikoen for et angrep rettet mot sine egne kontrollsystemer. Samtlige respondenter oppfattet kontrollsystemene som tilstrekkelig sikre, mye på grunn av en konservativ tankegang når det kommer til å koble SCADA-systemet opp mot internett. Derimot finner NVE mange avvik hver gang de er på tilsyn, og konkluderer med at systemene ikke er sikre nok.

En masteroppgave om læringsfaktorer i øvelser initiert av NVE [58], har analysert to store beredskapsøvelser på tvers av ekom-sektoren. Generelt har bransjen en god holdning til beredskapsøvelser, som blir ansett for å være en nyttig og god metode for å bedre beredskapen. Det settes av tilstrekkelig med tid og ressurser til å planlegge og gjennomføre øvelser, selv om det alltid kan øves mer, spesielt på sjeldne hendelser. Øvelser skaper en trygghet om innholdet i beredskapsplanen, i tillegg til en bedre rolleforståelse. Det er en god måte for risikovurdering og forebygging, forbedring av beredskapsplanverk, avdekking av nødvendige organisatoriske forbedringer og forberedelse til den dagen det skjer noe ekstraordinært utover bare å finne frem

et planverk. Det er viktig å merke seg at dette gjelder generelle øvelser, ikke IT-sikkerhetsøvelser.

3.3.2 IT-sikkerhetsberedskapsøvelser

Det må en IT-sikkerhetshendelse til for at (ledelsen spesielt) skal prioritere øvelser på dette området [22]. Etter angrepet i august 2014 så man en endring i bransjen. Studier etter dette viser at IT-sikkerhetsøvelser nå står på agendaen, og blir til en viss grad gjennomført, dog mest hos de store bedriftene.

Arbeidet til Chiem og Graffer [22] fra høsten 2014 inneholder anbefalinger om hvordan IT-sikkerhetsberedskapsøvelser bør gjennomføres i kraftbransjen. De øvelsene som er gjennomført har vært skrivebordsøvelser, en type øvelser bransjen har god erfaring i å gjennomføre på andre områder. Det er derimot behov for flere øvelser, og gjerne andre typer øvelser. Noen bidragsytere poengterer at relevante scenarier er en akilleshæl, og flere relevante scenarier vil gjøre det lettere å gjennomføre flere øvelser, særlig for små og mellomstore bedrifter. Fokuset på å trene samarbeid (både mellom ulike typer personell og mellom bedriftene) bør økes og være et hovedfokusområde i fremtidige øvelser.

Line og Moe [23] har observert tre ulike nettselskaper gjennomføre samme skrivebordsøvelse med en IT-sikkerhetshendelse, der to av nettselskapene ikke hadde gjennomført en slik øvelse tidligere. Observasjonene resulterte i seks anbefalinger som organisasjonene bør ta med seg til videre arbeid [59].

- Ha kun ett mål med øvelsen – løse scenarioet på en effektiv måte.
- All nødvendig kompetanse må være tilstede i gruppa. Ha gjerne en fasilitator som kan støtte gruppa, slik at de kan lære seg å ta felles beslutninger.
- Gjennomfør øvelser ofte for å sikre at alle får deltatt. Begrens tiden som brukes på hver øvelse for å gjøre det lettere for de som er travelt opptatt å finne tid.
- For at en øvelse skal framstå som realistisk, bør det være et visst tidspress. Det må også settes av god tid til refleksjon rett etter selve øvelsen, da dette øker utbyttet vesentlig.
- Ha eksisterende dokumentasjon tilgjengelig under øvelsen, som det vil være i en ekte krisesituasjon. Bruk tid i etterkant på å gå gjennom dokumentasjonen for å finne og oppdatere eventuelle avvik. Hvis den ikke ble brukt under øvelsen, diskuter hvorfor.
- Inkluder alle typer personell som vil komme til å ha en rolle i en ekte krisesituasjon.

Å gjennomføre IT-sikkerhetsøvelser for alle ansatte, ikke bare for "hendelseshåndterere", er påpekt fra flere studier, da alle har et ansvar for informasjonssikkerhet [17].

Det finnes mange måter å gjennomføre en beredskapsøvelse på. Line og Moe fremhever at også andre typer øvelser enn skrivebordsøvelser bør gjennomføres. Dette bør gjøres ved optimalisering av nåværende øvelser og eksperimentering med nye. Trening i kreativt arbeid og koordinering under tidspress er den beste forberedelsen en kan gjøre.

3.4 Utfordringer for IT-sikkerhet og mulige angrep mot kraftbransjen

En kritisk del av en vellykket overgang fra dagens strømnett til smartgrid, vil være å skape gode løsninger for IT-sikkerhet. Påliteligheten til disse omfattende infrastruktursystemene vil påvirkes med umiddelbar virkning dersom sikkerheten ikke er tilfredsstillende. IT-sikkerhet må ikke bare håndtere bevisste angrep, for eksempel fra misfornøyde ansatte, industrispionasje og terrorister, men også tilfeldige og utilsiktede feil som skyldes brukerfeil, feil på utstyr og utenforliggende hendelser. Sikkerhetsproblemene kan tillate en angriper å trenge inn i et nettverk, få tilgang til kontrollprogramvare, og endre belastningen for å forstyrre nettet på uforutsigbare måter [60, 11]. Disse angrepene blir sett på som sjeldne, men med potensielt store konsekvenser [61], i verste fall føre til at et strømnett er ute av drift i 9-18 måneder [62]. Grunner for økte krav til sikkerhet i smartgrids er blant annet [63]

- Økt konnektivitet og flere tilkoblingspunkter i nettet, dermed større sannsynlighet for å bli angrepet utenfra. Flere koblinger kan angripes samtidig, og det vil være mulig med et stort tjenestenektangrep.
- Generelt flere å stole på: Beboere for eksempel kan ha ønske om å tukle med komponenter som påvirker nettet.
- Vil kreve økt kompetanse når det gjelder sikkerhetsledelse, og flere ressurser må inkluderes når det gjelder vedlikehold og overvåkning.
- Høyere krav til håndtering av softwaresvakheter, et stort antall komponenter må kunne oppdateres og vedlikeholdes.

Tilgjengelighet til systemer kan svekkes på grunn av et tjenestenektangrep, som ikke er ukjent i infrastrukturer basert på trådløs kommunikasjon. I en smartgrid-kontekst kan disse angrepene ha potensial til å forstyrre funksjoner som AMS, forbrukerfleksibilitet og administrering av strømbrudd [64]. Dersom denne typen

angrep gjennomføres mot en driftssentral, for eksempel grunnet høy aktivitet av virus eller ormer, kan kontakten med kommunikasjonsnettet mistes [11]. Ved inntrenging i et system med kontrollfunksjon, kan integriteten til systemene bli påvirket. Dette kan føre til at systemet viser gale verdier, enten ved at det gir alarmer som ikke har rot i virkeligheten, eller at alvorlige situasjoner ikke blir rapportert.

3.4.1 AMS.

AMS skal innføres i alle norske hjem innen 2019, og har potensiale til å skape informasjonssikerhetsproblemer av en type og størrelsesorden kraftbransjen hittil ikke har sett. Det er særlig to utfordringer som må løses. Store mengder data om strømbruk skal samles og lagres, så personvern blir et fokusområde. En bryte/strupefunksjon av strøm gjør det mulig for leverandørene å bryte strømmen til sluttbrukere med enkle kommandoer, noe som kan få katastrofale konsekvenser dersom denne kontrollen havner i feil hender. Den største frykten er at store områder får kuttet strømmen, og at det gjøres permanent fra angriperens side ved å bytte ut nøklene i kommunikasjonen [14].

Generelt kan sikkerhetskravene klassifiseres på følgende måte [65]:

- **Konfidensialitet:** Krav om at bare autoriserte personer og systemer kan få tilgang på data, og at tilsiktede eller utilsiktede avsløringer av dataene ikke forekommer. Sikre personvern både i endenode, kunde-til-kunde og leverandør-kunde.
- **Integritet:** Hindre endringer av data mottatt fra meteret og kontrollkommandoer, samt beskytte mot fysisk angrep. Det er vel så viktig å ha mekanismer for å oppdage angrep, som prøve å unngå dem.
- **Tilgjengelighet:** Hindre menneskelig tukling med metere, i form av f.eks frakopling. Dataene må være tilgjengelige når de trengs. Ved overbelastning av nettet eller i nødsituasjoner er tilgjengelighet ekstra viktig for vellykket håndtering av AMS.

Ved å analysere data fra strømmålerne, er det mulig å gjennomføre kundeprofilering med høy nøyaktighet. Dette kan blant annet være kartlegging av antall beboere, alarmsystemer og unormale hendelser, samt et bilde av husholdningens generelle bruksmønster. Hvis uvedkommende får tilgang til systemet, kan personlige detaljer som navn og adresse avsløres. Instanser som har interesse av denne informasjonen kan være forsikringsselskaper, innbruddstyver eller nasjonale autoriteter [66]. Presentasjon av informasjonen fra AMS-boksene til kundene kan gjøres på mange måter. En svakhet her kan gjøre det enkelt for andre personer enn personen som eier

et hus til å lese konfidensiell data. Dette kan være så enkelt som et dårlig designet API, mobilapplikasjon eller hjemmeside [67].

3.4.2 Sosial manipulering.

Mennesker blir ofte sett på som svakeste punkt i et system, og det hjelper lite med tilfredsstillende sikkerhetsteknologi, da sikkerheten ikke er bedre enn svakeste punkt. Mange av de nevnte angrepene vil være mulig å gjennomføre ved hjelp av blant annet sosial manipulering, som defineres på følgende måte [68]:

> Sosial manipulering er en teknikk som blir brukt for å skaffe seg tilgang ved å lure non. Det er således en type hacking, som i stedet for å utnytte sårbare sider ved programvare, bruker menneskelig kontakt og sosiale evner for å få tak i informasjon.

Et sosialt manipuleringsangrep kan involvere flere faser [69]:

1. Samling av informasjon om målet, for eksempel gjennom å studere telefonlister, fødselsdato og organisasjonskart.
2. Bygging av forhold. Ved å skape tillit til målet er det større sannsynlighet for et vellykket angrep.
3. Når tillitsforholdet er skapt, er det tid for å utnytte dette ved å få målet til å avsløre ønsket informasjon eller gjøre en ønsket handling.
4. Når oppgaven er gjennomført, er angrepet fullført.

3.4.3 Kjente angrep

Det finnes allerede flere eksempler på angrep på kontrollsystemer, noe som viser at at angriperne er kapable til å gjennomføre angrep. Trenden er stadig økende [70, 16], og de som er interessert i å stjele, vil klare det [71].

- **Stuxnet (2010):** En orm rammet det iranske atomkraftverket i Natanz, ved å utnytte fire hittil ukjente sårbarheter i kontrollsystemer. Den spredde seg blant pc-er med Windows operativsystem, og angrep *Simens Step7 software*, for å deretter reprogrammere PLC og skjule endringene. Frekvensen på sentrifugene ble justert på en måte de ikke var designet for å tale. Dette førte til at en stor mengde ble ødelagt uten at dette ble mistenkeliggjort [70].

- **Maroochy Shire-angrepet (2000).** En tidligere ansatt hacket seg inn i et vannkontrollsystem nær Brisbane og gjennomførte et angrep over flere faser. Dette resulterte i at et hotell og en elv ble oversvømt med en million liter kloakk [70].
- **Dragonfly (2014)**. Et stort spionasjeangrep mot tusen energiselskaper i Europa og Nord-Amerika. Mange metoder ble brukt, blant annet vedlegg til e-post. Målet var å kunne gjøre sabotasjeoperasjoner som i verste konsekvens kunne endt i strømbrudd. I Norge ble 50 bedrifter forsøkt angrepet, men det ble oppdaget i tide og resulterte uten store konsekvenser. [15]

Konkrete eksempler på svakheter og mulige angrep mot kraftbransjen finnes i kapittel 4.

Kapittel 4
Scenarier

Dette kapittelet inneholder en oversikt over viktige elementer for vellykket scenarieutvikling, en oversikt over eksisterende scenarier, og en presentasjon av scenariene som skal danne utgangspunktet for øvelsen.

Å utarbeide scenarier som kan brukes i en øvelse i kraftbransjen krever bred kunnskap på tvers av mange områder, i tillegg til mye erfaring. Både IT-sikkerhet, nettverk, strømnett og kontrollsystemer er sentrale kunnskapsområder. Risikovurderinger og oversikt over dagens trusselbilde er også viktig. Det er veldig sjelden en og samme person som sitter på all denne ekspertisen, så utvikling av øvelsen og scenariene er en prosess som krever tid og flere ressurser [22].

Scenariene må tilpasses både målet med øvelsen og formen [72]. Scenariene som er utarbeidet i denne øvelsen (presentert i avsnitt 4.2) er laget til å passe en spill-kontekst. Ved å lage en del av de på spørsmålsform åpner for muligheten for belønning, noe som hører hjemme i en spillsituasjon. Målet med øvelsen er å øke oppmerksomheten rundt IT-sikkerhetshendelser, så en god blanding av forskjellige mindre omfattende scenarier vil passe til konseptet.

Et av hovedpunktene for å lage en god øvelse er at den er realistisk [58, 17]. En realistisk øvelse innebærer at den bygger på realistiske scenarier som ikke inneholder logiske brister og virker troverdig [73]. I denne masteroppgaven sikres realisme i scenariene gjennom:

- Kvalitetssikring, gjennom intern testing og tilbakemelding fra bransjen.
- De tekniske detaljene om systemene eksisterer i liten grad. Det er fokus på at angrepene skjer, og potensielle konsekvenser av dette.
- Scenariene er utviklet med utgangspunkt i tidligere studier og kjente sårbarheter.

Øvelser vil aldri bli realistisk på samme måte som en reel hendelse [74]. Reelle hendelser er kanskje mer lærerike, men det kan vanskelig rettferdiggjøres å la være å øve på en krise som gjennom øvelse potensielt sett kunne vært håndtert bedre [58].

4.1 Eksisterende scenarier

Det finnes et mangfold av publiserte scenarier om angrep på kontrollsystemer, smartgrids og AMS. Disse er ofte laget for at bedrifter skal bli oppmerksomme på trusler og risiko, eller i forbindelse med veiledninger rundt øvelser. Likevel finnes det også mange upubliserte scenarier, blant annet basert på risikoanalyser internt i selskapene [22]. Disse holdes naturligvis skjult for omverdenen, da de kan avsløre identifiserbare sårbarheter og utnyttes av angripere. Det varierer også i stor grad hvor mye bedrifter benytter seg av og er oppmerksomme på disse eksisterende kildene, derfor er det hensiktsmessig å presentere et utvalg.

AMS

I forbindelse med innføringen av AMS i Norge, gjennomførte Sintef en risikovurdering på oppdrag fra NVE. Målet var å kartlegge informasjonssikkerhetsmessige sårbarheter [11]. Ulike scenarier 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) og industrispionasje. Fem scenarier er presentert, og omhandler:

- Stort antall AMS-målere ute av drift samtidig, ikke nødvendigvis på grunn av et målrettet angrep, men av grunner som lynnedslag, programvareoppdatering eller vedlikehold. Strømmen til husstandene vil ikke bli berørt, men nettselskapet vil ikke få registrert bruken.

- Kunde manipulerer måledata. Kan skje enten ved å flytte forbruket fra høylastperioder til perioder med lavere pris, redusere totalt forbruk, eller ved å justere naboens forbruk tilsvarende opp.

- Interne trusler og utro tjener. En person misbruker bryte/strupefuksjonen og kobler ut strømmen for intetanende kunder. Personen kan installere en bakdør inn i systemet, gi fra seg hemmeligholdt informasjon om drift (eller selge dette), eller samarbeide med kunde for å nedjustere forbruk og pris.

- Målrettet angrep på kraftforsyningen i et spesifikt geografisk område. For eksempel datainnbrudd på en nettstasjon, bruk av bakdører inn i lokale systemer eller samarbeid mellom angriper og utro tjener.

– Uheldige konsekvenser av tredjepartstilgang. Displayet for toveiskommunikasjon har for lav sikkerhet, og kan brukes som innfallsport for en angriper.

Nick Hunn presenterer et AMS-scenario [75]: En utro tjener hos AMS-utvikleren legger til noen kodelinjer som kobler ut måleren på et gitt tidspunkt i fremtiden. I stor skala medfører dette at strømmen går i store områder. Den deaktiverer også ekstern kobling fra leverandøren sånn at kommunikasjon og restart av måleren er umulig. For å gjøre det ekstra vanskelig kan angriperne skru dem av og på igjen tilfeldig for å ubalansere nettverket og restarten av systemet. Dette kan i ytterste konsekvens ta flere måneder å rette opp i.

Et omfattende dokument med scenarier fordelt på seks forskjellige kategorier innen smartgrids og AMS [76] ble publisert av den amerikanske organisasjonen for informasjonssikkerhet i kraftbransjen [1].

SCADA og kontrollsystemer

Det amerikanske senteret for maritime analyser [2] holdt en workshop hvor resultatet var et dokument med relevant informasjon om fremgangsmåten for lage realistiske scenarier [77]. Det inkluderte referanser til faktiske hendelser og et scenario der et kraftsystem ble angrepet. Angrepet gikk ut på at informasjon om produksjon og forbruk ble tuklet med. Samtidig ble et tjenestenekt-angrep gjennomført via e-mail, noe som hindret kommunikasjonsflyten mellom sentrale aktører. Situasjonen skapte usikkerhet i befolkningen, og strømselskapene mistet troverdighet.

NERC[3] publiserte en stor rapport med fokus på hvordan man skal forberede kraftbransjen på angrep på systemene sine [61], inkludert 5 scenarier:

– Sosial manipulering: Feilforespørsel eller informasjon til operatør, eller der noen spør om en tjeneste.

– Tjenestenekt-angrep mot SCADA-systemet gjør at det blir delvis utilgjengelig eller veldig tregt.

– Tjenestenekt-angrep mot SCADA-systemet hindrer noen applikasjoner til å oppdatere informasjon. Blir ikke oppdaget før noen ringer inn og man finner ut at informasjonen ikke stemmer overens med hva som observeres på skjermene.

– Indikere falske operasjoner fra en enheter i SCADA-systemet. Falske alarmer og usannsynlige sammenhenger.

[1] The National Electric Sector Cybersecurity Organization Resource (NESCOR)
[2] Center for Naval Analyses (CNA)
[3] North American Electric Reliability Corporation (NERC)

– Sette falske data inn i systemene som gjør at operatørene endrer handlinger, f.eks tillater overbelastning.

NVE har i sin øvingsveileder [2] et scenario som omhandler en IT-hendelse, ikke på grunn av et angrep men en fysisk ødeleggelse. Scenarioet går ut på håndtering av en hendelse der man må klare seg uten IT i en beredskapssituasjon.

SANS[4]-instituttet har laget en video med demonstrasjon på hvordan et angrep kan foregå [78]. Hackere kommer seg på innsiden av firmanettverket (ved hjelp av phishing eller e-mail), og finner tilslutt en sårbar kobling mot kontrollsystemet.

EPA[5] har utviklet to IT-sikkerhetsscenarier mot et kontrollsystem. [79]

– En ansatt på oppsigelse oppretter en forbindelse til SCADA-systemet fra hans hjemmepc, og infiltrerer det med et virus. Konsekvensen blir at systemet viser feilaktige alarmer.

– IT-ansvarlig i firmaet fikk ikke innvilget ønsket lønnsøkning og bestemmer seg for å reprogrammere SCADA-systemet til å skru av vannpumpene uten å utløse alarmer. Han nekter også andre brukere aksess til systemet.

De eksisterende scenariene er i stor grad varierte både når det kommer til detaljnivå, innfallsvinkler og grad av omfattelse. Alle scenariene er en god kilde til inspirasjon, men ikke alle passer rett inn i en øvelsessituasjon ubearbeidet. For å bruke scenariene som grunnlag for en øvelse må de justeres og tilpasses, blant annet for oppnå en felles struktur. Man må være kritisk og finne scenarier som er realistiske for bedriften, samt passe inn under hva som er målet med øvelsen. Kanskje vil en annen sammensetning, og oppdeling i flere faser være mer gunstig i en annen øvelsessituasjon.

4.2 Scenarier i øvelse

Scenariene i øvelsen er laget med utgangspunkt i foregående avsnitt og kjente angrep fra avsnitt 3.4.3. Det er laget tre forskjellige typer scenarier: ”Hovedscenarier”, ”Visste du at..” og ”Spørsmål”, og disse varierer både i omfang og tid. Ved å gjøre denne inndelingen kan man også belønne deltagerne når de diskuterer seg fremt til et tilfredsstillende svar, noe som kan brukes i en spillsammenheng. Intensjonen er at scenariene dekker både refleksjon over trusler, sårbarheter og konsekvenser, men også ansvarsfordeling og roller i organisasjonen.

[4]SysAdmin, Audit, Networking, and Security
[5]Environmental pro-tection agency (EPA)

Scenariene som er laget og presentert her er et begrenset utvalg, og dekker på ingen måte alle situasjoner. De er laget for å ha mulighet til teste spillet på generelt grunnlag, og vise et forslag til scenarier som kan brukes på en vellykket måte. Bedrifter som gjennomfører øvelsen presentert i denne masteroppgaven må selv tilpasse scenariene, og kan finne inspirasjon her og i de eksisterende.

4.2.1 Hovedscenarier

Hovedscenariene som presenteres i dette avsnittet er tilpasset spillet, og er derfor begrenset ved størrelsen på kortene og tidsbruk. Noen scenarier laget fra bedriftens perspektiv (der det jobbes mot angriperne), og noen er laget for at deltagerne skal prøve å sette seg inn i angripernes rolle og tanker. De varierer i omfang og detaljnivå, men er forsøkt laget så konkret som mulig. Her finnes det ofte ingen fasitsvar, men poenget er i hovedsak å få deltagerne til å reflektere rundt scenariene og bli oppmerksomme på situasjoner som kan oppstå.

Alle scenariene er laget på samme form, bestående av 1-3 faser med tilhørende spørsmål. Studien til Line og Moe [23] viser at et scenario i flere faser hjelper deltagerne til å se sammenhenger over tid, og oppdage angrep som ellers ikke ville vært oppdaget. Det er veldig sjelden at et angrep bare har en fase, og ofte oppdages de nettopp ved å se sammenhenger over tid.

Scenario 1: AMS

En sluttbruker med ønske om å spare inn noen kroner på strøm klarer med fysisk aksess å manipulere data sendt fra AMS-enheten ved å tukle med radiosignalene. Enten ved å nedjustere til et lavere forbruk eller flytter bruken til billigere perioder. Som et ledd i overgangen mot smartgrid justeres den totale strømbalansen i nåtid mot den innrapporterte strømbruken fra kundenes hus.
- *Hvordan kan dette oppdages når det skjer i såpass liten skala?*
- *Hva er eventuelle konsekvenser og hvordan kan det unngås?*

AMS-systemet gir varsel om at rapportert strømmengde fra sluttbrukere har for stort avvik i forhold til rapportert overført strøm gjennom en trafostasjon for et område. Det blir mistenkt at ryktet har gått i nabolaget, og vedkommende har delt sin kunnskap.
- *På hvilken måte forandrer dette situasjonen nå som feilmengden er betydelig stor?*
- *Hva kan bli worst-case her?*

Scenario 2: Sosial manipulering og utro tjener

En dag med ekstremvær og et ustabilt strømnett får man brudd på sentralnettet mellom Nes og Aurland. Man antar først at dette har med uværet å gjøre, men etter

gjentatte brudd på samme strekning begynner man å ane at det ligger en annen grunn bak, og mistenker at systemet kan være angrepet.
- *Nevn noen punkter som ville fått deg til å fatte mistanke. (Hvordan skiller man på årsak når det er strømbrudd?)*
- *Du er personen som først fatter mistanke, hvordan går du frem videre? Hvilke personer skal kontaktes og hvilke prosedyrer følges?*

Etter litt tid viser det seg at det var et rent sabotasjeangrep mot et backup-system, og at måten angriperne kom seg inn på var at de fant ut via firmaets hjemmeside, Linkedin og Facebook hvem som jobber der og har hvilke roller. Denne informasjonen ble deretter kryss-sjekket med informasjon om kreditt og betalingsanmerkninger for å finne et "bytte" som trengte penger. Det ble så tilbudt et visst beløp for å legge inn en bakdør inn i systemet som vedkommende ikke klarte å si nei til.
- *Hvordan kan man unngå at dette skjer?*
- *Er dette et realistisk scenario? Kunne dette skjedd hos dere (hvorfor/hvorfor ikke)?*

Scenario 3: Zero-day angrep

Du sitter på jobb på regionssentralen. Kontrollsystemet gir varsel om feil et sted i nettet, og du blir satt på saken om å undersøke hendelsen og finne en løsning. Etter nærmere undersøkelser viser feilene seg å ikke ha rot i virkeligheten.
- *Hvilke årsaker mistenker du?*
- *Hva skulle tilsi at dette er et hackerangrep?*
- *Hvilke prosedyrer følges i dette tilfellet?*

Dette er et angrep IT-ekspertene ikke har sett før (Zero-day angrep), og flere ressurser blir satt på saken. Kontroll av substasjonene avslører at firmwaren i PLCene i nøkkelsensorenheter har blitt overskrevet, noe som gjør at informasjon om produksjon og forbruk blir hentet ut og erstattet med feil data. Dette fører til at man ikke kan stole på verdiene kontrollsystemet gir.
- *Hvor langt må det gå før man må overvåke strømnettet manuelt?*

Kort tid etter rapporteres det om et massivt tjenestenekt-angrep (en mengde e-mail blokkerer informasjonsflyten mellom systemansvarlig/bedriften/ledere/ansatte), noe som gjør det mye vanskeligere å koordinere responsen.
- *Hvilke løsninger for kommunikasjonsflyt ser dere i denne situasjonen?*

Scenario 4: Personvern og AMS

Med intensjon eller feiltagelse blir en regel i brannmuroppsettet opprettet, med den konsekvensen at direkte aksess tillates fra et annet nettverk. Dette utnyttes av angripere og de klarer å komme seg inn i AMS-databasen der all informasjon om strømkundene ligger. Dette inkluderer også informasjon om strømbruk.

- Hvilke hensikter kan angriperen ha i dette tilfellet?
- Hvordan oppdager man dette?
- Hvilke tiltak kan innføres for at dette ikke skjer?

Scenario 5: Sosial manipulering

Du er en ansatt i bedriftens HR-avdeling. Tre situasjoner er gitt nedenfor.
- Hvor sannsynlig er det at noen prøver å lure deg i disse situasjonene?
- Identifiser den situasjonen du tror flest i bedriften ikke hadde mistenkt at det lå en ond tanke bak, og diskuter hva konsekvensen av denne kan bli?

- En person som presenterer seg som din nye kollega forklarer at IT-avdelingen holder på å sette opp pcen hans, og han venter bare på en mail som sier han kan hente den. Mobilen hans har dessverre gått ut på batteri, og han ber om å låne pcen din for å sjekke om denne mailen har kommet.
- En kollega kom i skade for å glemme kortet sitt på et møterom, hun spør deg om å låne ditt for å få låse seg inn og få tak i det igjen.
- Du får en telefon fra IT-support i bedriften. De forteller at pcen din trenger oppgradering av software, og for at dette ikke skal hindre ditt daglige arbeid ønsker de med adminrettigheter å gå inn å gjøre dette for deg, men de trenger info (brukernavn, passord) som du må gi dem for at dette skal være mulig.

Scenario 6: Trusler og media

NSM har fått inn et tips som etter vurdering av deres eksperter virker troverdig. En gruppe hackere hevder å ha brutt seg inn i kontrollsystemet, og truer å svartlegge en av Norges største byer. Du er sjef for bedriften.
- Hvem har hvilke ansvar her (KraftCert, NSM, bedrift, statlige myndigheter)?
- Hvilke handlinger må tas for å finne ut om dette er en faktisk trussel?
- Dere finner ingenting umiddelbart som kan motbevise et mulig angrep, hvordan håndteres denne situasjonen videre? Nevn viktige elementer i en videre plan.

Rett etter at dette er kjent for dere, har media fått nyss i saken, og dere opplever en storm av henvendelser fra både kunder og journalister.
- Hvilke tiltak må gjøres?
- Identifiser kritisk informasjon, og hvordan videreformidle denne til kundebehandlere?

4.2.2 Spørsmål med fasitsvar

Disse spørsmålene er ment for å skape små diskusjoner rundt spesifikke situasjoner eller begreper. I denne kategorien finnes en del spørsmål som har klare fasitsvar, men også en del spørsmål som ikke har et klart fasitsvar, på grunn av ulikheter i

prosedyrer og systemer. Her vil det likevel være mulig å belønne et godt begrunnet svar, da ingen svar er feil.

Spørsmål
Innen informasjonssikkerhet, hva menes med integritet og hvilken metode bruker man for å sikre dette? *Sikre at informasjonen er nøyaktig, fullstendig og gyldig. Kryptering. [12]*
Hva menes med konfidensialitet innen informasjonssikkerhet, og nevn en metode som brukes for å sikre dette? *At bare autoriserte personer har tilgang til informasjonen. Kan løses i form av passordbruk. [12]*
Innen informasjonssikkerhet, hva menes med tilgjengelighet? *Sikre at autoriserte brukere har tilgang til informasjon og tilknyttede ressurser når det behøves. [12]*
Hva skiller informasjonssikkerhet fra forsyningssikkerhet? *Forsyningssikkerhet omhandler kraftnettets evne til å kontinuerlig levere strøm til sluttkunder, mens informasjonssikkerhet går på å beskytte informasjon, og bevare dens konfidensialitet, integritet og tilgjengelighet.*
Hvilke prioriteringsforskjeller finnes mellom IT-personell og kontrollsystempersonell når det gjelder tilgjengelighet, integritet og konfidensialitet? *I prioritert rekkefølge: IT: konfidensialitet, integritet og tilgjengelighet. Kontrollsystempersonell: Tilgjengelighet, integritet og konfidensialitet*
Nevn en ytterste konsekvens av at angripere har tatt kontroll over kontrollsystemet.
Nevn en situasjon der prosedyren er å isolere driftskontrollsystemet fra øvrige nettverk.
Hvordan kan man finne ut hvor lenge noen har vært inne i systemer, og eventuelt hvilken informasjon som er sendt ut? *Beredskapsforskriften paragraf 7-4: "Virksomheten skal til enhver tid kunne kontrollere hvilken person som er eller har vært pålogget driftskontrollsystemet, også når ekstern tilkobling brukes."*
Hvordan kan man sikre at personen som ringer faktisk er den han utgir seg for? *Autentisere, f.eks stille et spørsmål bare vedkommende kan svare på.*
Du er en ansatt med onde intensjoner. Hvordan vil du gå frem for å få tak i brukernavn og passord hos personen på nabopulten?

Nevn en eller flere IT-sikkerhetsutfordringer ved en bryte/strupe-funksjon i AMS styrt fra kontrollsystemet. *Dersom en angriper får tilgang til AMS-bryterfunksjonaliteten vil vedkommende kunne stenge av strømmen for en mengde sluttbrukere eller ramme kritiske samfunnsfunksjoner.*
Nevn en situasjon der det er riktig å stenge ned kontrollsystemet.
Er det mer troverdig med en SMS med forespørsel om brukernavn/passord, enn en e-mail? Hvorfor/hvorfor ikke?

4.2.3 "Visste du at.."

Denne scenario-varianten er mindre omfattende, og består av korte innspill som ikke tar så mye tid. Disse skal leses opp av deltagerne, og fungere som en tankevekker. De er laget for å skape variasjon og dynamikk i spillet. Den faglige delen kan ikke alltid bestå av diskusjon, da dette kan ta for mye tid og fokus bort fra den praktiske delen av øvelsen.

- NSM rapporterer at i løpet av de siste tre årene er antallet alvorlige hackerangrep mot norske bedrifter mer enn doblet. [80]
- "Tilfeldig" planting av USB-minnepinner som inneholder skadelig programvare kan resultere i at noen av disse plukkes opp og brukes av ansatte i firmaer. Visste du at tidenes største angrep mot et kontrollsystem, Stuxnet, startet på denne måten?
- NSM håndterte 88 alvorlige dataangrep mot norsk næringsliv og offentlige interesser i 2014, mot 53 året før. Dette var mest digital spionasje [16].
- I 2013 registrerte NSM totalt 15 815 sikkerhetshendelser på nett. [81]
- En gruppe hackere prøvde å komme seg inn i systemet til en stor bedrift. Via Facebook fant de ut at broren til sjefen nylig døde av kreft, og at sjefen hadde engasjert seg i noen tilknyttede organisasjoner. Angriperne tok kontakt via telefon, utga seg for å være en nøkkelperson, noe som resulterte i at sjefen sa seg enig i å motta mail med informasjon om deltagelse på et arrangement. Det sjefen ikke var klar over er at angriperne har lagt ved ondsinnet kode i pdf-dokumentet, og dermed var hackerne på innsiden. [82].
- IBM-forsker Scott Lunsford brukte bare en dag på å trenge inn i systemet til et atomkraftverk, og en uke senere var han i stand til å kontrollere det [83].
- I 2014 var verdens mest brukte passord "123456", tett etterfulgt av "password". [84]

– 770 norske bedrifter har sensorer som logger databruk (enten i samarbeid med NSM eller Mnemonic). I en undersøkelse gjennomført av Næringslivets sikkerhetsråd svarer bare 4 prosent av bedriftene at de har blitt utsatt for dataangrep, når tallene fra NSM viser at tilfellet er 50 prosent. [85]

Kapittel 5
Øvelsen

Dette kapittelet presenterer øvelsen, forklarer spillets funksjonalitet og hvordan den faglige biten med scenarier fra kapittel 4 er brukt i øvelsen.

5.1 Introduksjon til spillet

Øvelsen består av et samarbeidsbrettspill der spillerne skal jobbe sammen for å tilintetgjøre angrep mot et strømnett. Spillerne flytter seg rundt på brettet og fjerner kuber (representerer angrep), samtidig som angrepet sprer seg videre i hver runde. For å sikre faglig utbytte er det lagt til en faglig del som skaper diskusjon rundt scenarier og grunnleggende IT-sikkerhetsterminologi, og som ved tilfredsstillende diskusjon og svar vil gi fordeler til bruk videre i spillet.

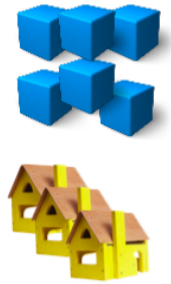
Øvelsen er laget for 3-4 spillere, der alle spillerne innehar ulike roller. Hver rolle har en spesiell egenskap, noe som må utnyttes på best mulig måte for å vinne spillet. Spillet vinnes dersom det tilintetgjøres ett angrep tre ganger, og tapes dersom en av følgende hendelser inntreffer:

- Angrepet blir for omfattende: Det er flere enn 30 kuber totalt på brettet.
- Skjer mer enn 6 sammenbrudd i strømnettet.
- Det er brukt for lang tid, bunken med spillkort går tom.

Spillet er inspirert av et eksisterende samarbeidsbrettspill, Pandemic, og bygger på den samme grunnfunksjonaliteten. Dette er beskrevet nærmere i avsnitt 5.7.

5.2 Innhold

(a) 6 Spillerbrikker og 5 markører



(b) 30 Angrepskuber og 5 forskningsstasjoner

(c) 6 Rollekort

(d) 6 Angrep!!-kort

(e) Spillbrett

(f) 38 angrepskort med by

(g) 38 spillkort med by og fase

(h) Utvalg scenario, spørsmål og "Visste du at.."-kort.

Figur 5.1: Spillets innhold

5.3 Oppsett og spillsekvens

Spillet må settes opp før start, dette kan gjøres av spillerne selv eller gjøres klart på forhånd.

1. **Sett opp brettet og gjør klar kuber.** Plasser brettet på et bord alle spillerne kan sitte rundt. Sett seks forskningsstasjoner, tre markører for tilintetgjørelse, alle kubene og oversikten av ulike handlinger lett tilgjengelig ved siden av spillbrettet. Plasser en av forskningsstasjonene på Frogner.
2. **Plasser markører.** Angrepsratemarkøren settes helt til venstre, og antall sammenbrudd settes på 0.

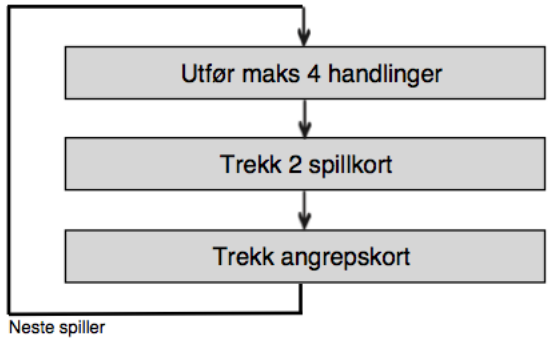
3. **Plasser angrepskuber i ni byer**, på følgende måte: Trekk tre angrepskort, legg tre kuber på hver av disse byene. De tre neste byene på angrepskortene som trekkes skal representeres ved to kuber, og de tre siste byene skal ha en kube hver. Legg de brukte kortene ved siden av resten av angrepskortene.

4. **Gi hver spiller spillkort og en rolle.** Gi alle spillerne et rollekort. Stokk bunken med spillkort, og del ut til hver spiller i henhold til tabellen under:

Antall spillere	**Spillkort**
3 spillere	3
4 spillere	2

5. **Forbered spillkortbunken.** Plasser 4-6 angrepskort, avhengig av ønsket vanskelighetsgrad, jevnt fordelt i resten av spillkortbunken. Plasser ønsket mengde scenario, spørsmål og 'visste du at..'-kort i blant spillkortene og legg bunken på spillbrettet.

6. **Start spillet.** Plasser alle spillerbrikkene på Hamang. Personen som starter er vedkommende som skiftet passord sist, og runden fortsetter videre med klokka. Hver person skal gjennomføre følgende, i gitt rekkefølge:



Figur 5.2: Spillsekvens

Spillesekvensen går helt til spillet er tapt eller vunnet.

5.4 Handlinger

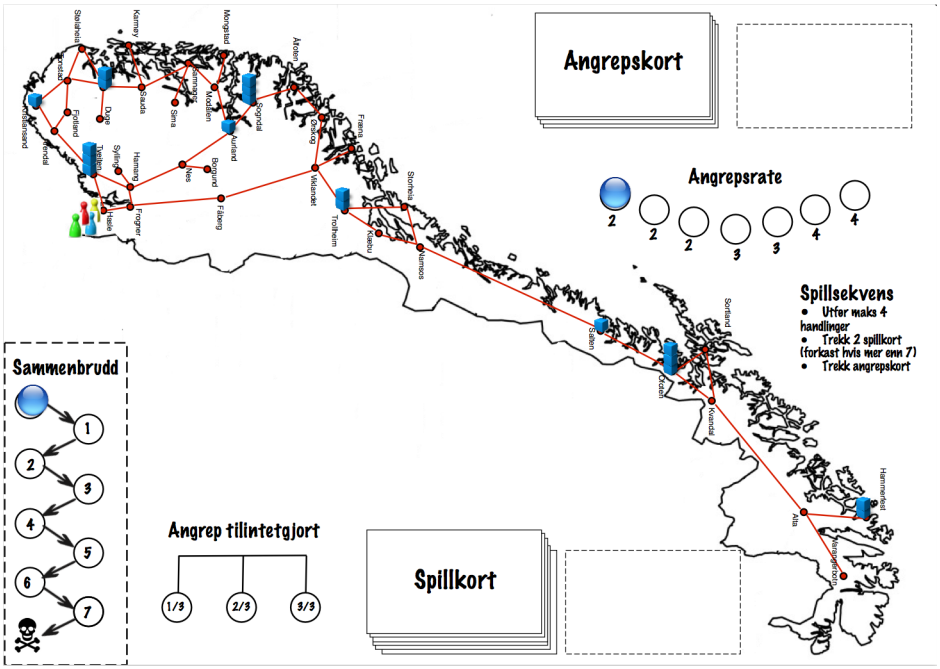
Hver spiller starter sin tur med å utføre maksimum 4 handlinger. Handlingene er beskrevet i figur 5.3, og kan utføres i valgfri kombinasjon. Samme handling kan gjennomføres flere ganger av samme spiller.

Figur 5.3: Mulige handlinger

5.5 Beskrivelse av spillet

5.5.1 Spillbrettet

I denne versjonen av øvelsen representerer spillbrettet deler av sentralnettet i Norge. For å sikre realisme i øvelsen er det viktig at brettet viser en faktisk situasjon. Ut fra slik øvelsen er presentert her vil målgruppen være den ansvarlige for det sentrale strømnettet i Norge, Statnett. Brettet kan tilpasses nettselskaper og andre målgrupper relativt enkelt ved å bytte ut eller avgrense nettet.

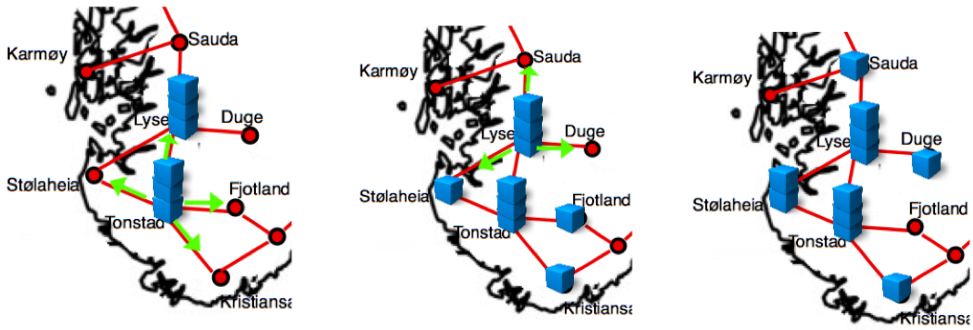


Figur 5.4: Spillbrettet, ferdig oppsatt.

Angrepsrate: Starter på helt til venstre, det vil si at det skal trekkes 2 kort i hver spillsekvens. Økes etterhvert som et "Angrep!!"-kort trekkes.

Angrep tilintetgjort: Et angrep tilintetgjøres hvis en spiller klarer å samle 5 spillkort med forskjellige nummere, og deretter levere ved en forskningsinstitusjon. For hvert angrep som tilintetgjøres fjernes hhv. 1/3, 2/3 og 3/3 av kubene på brettet. Spillerne blir enige om hvilke kuber de ønsker å fjerne.

Sammenbruddseksjon: Markøren starter på 0, og økes hver gang man får et sammenbrudd et sted i nettet. En by kan ikke ha mer enn 3 kuber, så et sammenbrudd skjer dersom en by med 3 kuber skal få en kube til. Da vil alle tilhørende byer få en kube. Figuren nedenfor viser hva som skjer når det trekkes et angrepskort med byen Tonstad, og denne byen allerede har 3 kuber. Stølaheia, Kristiansand, Fjotland og Lyse vil dermed få en kube hver. Lyse har allerede 3 kuber, dermed skjer et nytt sammenbrudd her. Angrepet sprer seg derfor til Sauda, Duge og Stølaheia. For å unngå et uendelig gjentagende sammenbrudd kan ikke sammenbruddet spre seg tilbake der det kom fra.



(a) Sammenbrudd i Tonstad

(b) Sammenbruddet fører til sammenbrudd også i Lyse

(c) Situasjonen i etterkant av sammenbrudd

Figur 5.5: Forklaring av sammenbrudd

5.5.2 Kort

Angrepskort: Viser hvilke byer angrepet sprer seg til. For hvert kort som trekkes skal tilføres en angrepskube til byen på kortet.

Spillkort: Inneholder en by og en fase i en hendelseshåndterings-prosess fra ISO 27035:

1. Planlegging og forberedelser
2. Deteksjon
3. Vurdering og rapportering
4. Respons
5. Evaluering/læring

Spillkortene har to funksjoner. Ved å se på byen på kortet kan de brukes til å gjennomføre handlinger, f.eks fly til en by langt unna. En viktig del av spillet er å tilintetgjøre angrep, og da må se på nummeret på fasen, og forsøke å samle alle de fem forskjellige fasene.

Scenario, Spørsmål og "Visste du at.."-kort: Har innhold som beskrevet i kapittel 4. Ønsket mengde av disse blandes sammen med spillkortene.

Angrep!!-kort: Beskriver hvilke handlinger som skal gjøres når det skjer et angrep:

1. Øk angrepsrate: Flytt angrepsratemarkøren et hakk mot høyre
2. Spre angrepet: Trekk et kort fra bunnen av angrepskortbunken, og sett 3 kuber på denne byen.

3. Intensiver angrepet: Stokk de brukte angrepskortene og plasser de øverst i bunken av angrepskort.

Bland 4-6 av disse Angrep!!-kortene, avhengig av ønsket vanskelighetsgrad, inn sammen med spillkortene. Plasseringen av disse kortene kan ikke være helt tilfeldig, de må plasseres med jevne mellomrom i spillkortbunken. En løsning kan være å dele spillkortbunken inn i 4-6 like bunker, og deretter plassere et Angrep!!-kort på toppen av hver bunke. Så settes bunken sammen igjen.

5.5.3 Rolle

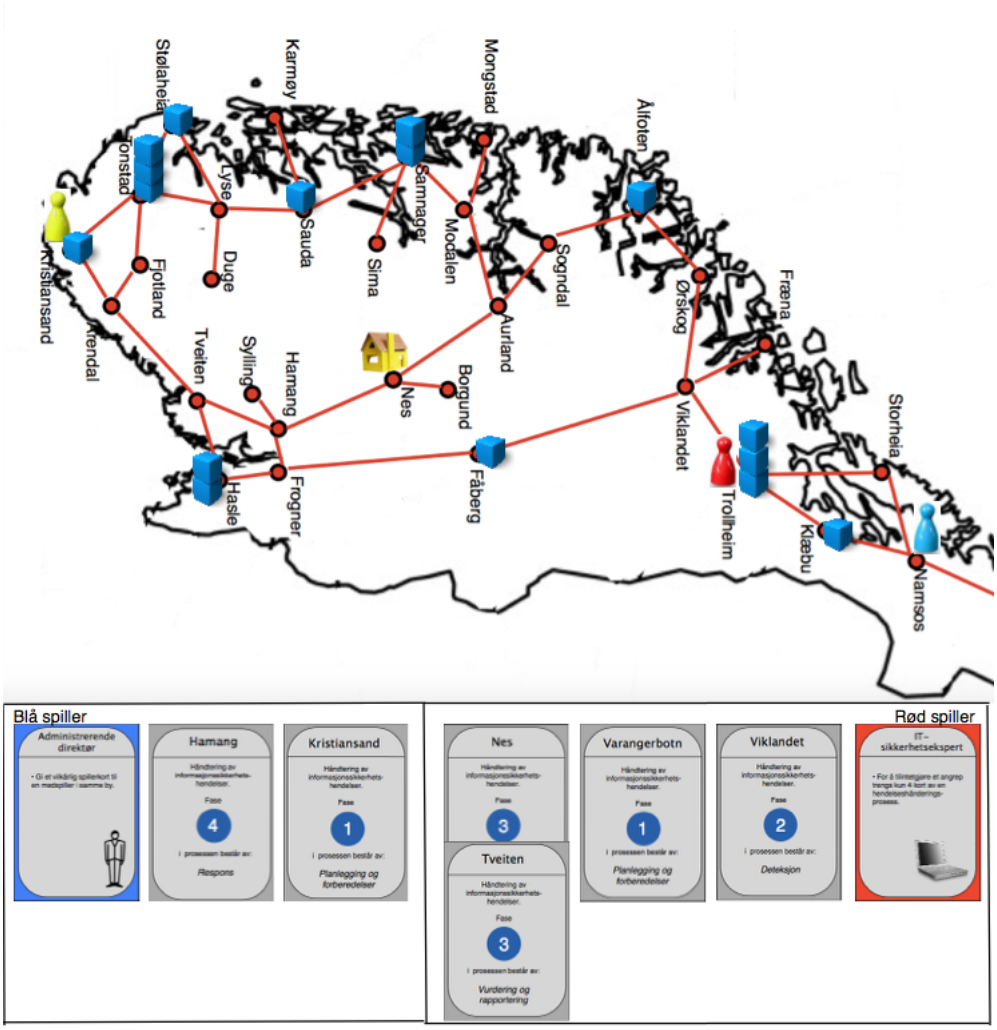
Alle deltagerne trekker eller får tildelt en rolle før spillet starter. Hver rolle har en spesiell egenskap beskrevet på kortet, og en viktig del av spillet er å samarbeide for utnytte denne på best mulig måte. Det er mulighet for å bytte ut rollene med en rolle mer tilpasset organisasjonen øvelsen skal gjennomføres i, men egenskapene bør være de samme.

Rolle	**Egenskap**
Administrerende direktør	Gi et vilkårlig spillerkort til en medspiller i samme by.
IT-sikkerhetsekspert	For å tilintetgjøre et angreps trengs kun 4 faser av en hendelseshåndterings-prosess.
Offentlig myndighet	Som en handling kan en forskningsstasjon bygges i byen du er, ved å forkaste et vilkårlig spillkort. Fly fra en by med forskningsstasjon til en annen by ved å forkaste et vilkårlig spillkort.
Nettverksoperatør	Fjern alle kuber i en by med 1 handling.
Beredskapsleder	Beveg andres spillerbrikker (med tillatelse) som det skulle vært din egen.
Kontrollsystem-ansvarlig	Kuber kan ikke plasseres i den byen du står eller tilknyttede byer.

Andre roller som kan inkluderes: Kryptoanalytiker, Nettverkssikkerhetspesialist, IT-ekspert, Nettsjef, AMS/SCADA nettverksrepratør, Driftsansvarlig, Politiet, Statsminister, Statlig myndighet (NVE / DSB).

5.6 Eksempel

Dette avsnittet viser et eksempel fra en del av en øvelse. Situasjonen på brettet er vist på figuren nedenfor, og teksten beskriver valgene til blå og rød spiller.



Figur 5.6: Eksempel på spillsituasjon

Både Trollheim og Tonstad har tre kuber hver, og situasjonen er derfor kritisk. Hvis en av disse byene får en kube til skjer et sammenbrudd. Spillernes fokus bør derfor være å få fjernet kuber fra disse byene, og samtidig samle spillkort med alle de fem fasene for å tilintetgjøre et angrep. Rød spiller innehar rollen som IT-sikkerhetsekspert (vedkommende trenger bare 4 faser av en hendelseshåndteringsprosess for å tilintetgjøre et angrep), og mangler dermed bare ett kort for å tilintetgjøre et angrep.

Det er spillerbrikke blå sin tur. Vedkommende har rolle som Administrerende Direktør, og kan derfor gi et vilkårlig kort til en spiller i samme by. Følgende fire

handlinger blir gjennomført:

1. Kjør til Klæbu.
2. Gjenoppretter systemet: fjerner en kube fra Klæbu.
3. Kjører til Trollheim. Står nå i samme by som Rød.
4. Gir et spillkort til Rød. "Hamang: Fase 4".

Deretter trekker han to spillkort. Det første er Åfoten, som han legger ned sammen med de andre spillkortene sine. Det neste kortet er fase to av et tidligere diskutert scenario. Vedkommende leser scenariet høyt for gruppen, og de diskuterer rundt spørsmålene.

Så skal angrepet spres. Angrepsraten står på to, og det skal dermed trekkes to kort. Hammerfest og Tonstad får en kube hver. Siden Tonstad allerede har 3 kuber skjer det et sammenbrudd, og alle byene tilknyttet Tonstad (Stølaheia, Kristiansant og Tonstad) får en kube hver. Markøren for sammenbrudd flyttes et hakk.

Det er nå IT-sikkerhetseksperten sin tur. På grunn av handlingene gjort i sist runde har han nå 4 faser av en hendelseshåndteringsprosses, og kan tilintetgjøre et angrep ved å levere disse hos en forskningsstasjon. Han gjør disse fire handlingene:

1. Gjenoppretter systemet: fjerner en kube fra Trollheim.
2. Gjenoppretter systemet: fjerner en kube fra Trollheim.
3. Flyr til forskningsstasjonen på Nes ved å forkaste dette spillkortet.
4. Leverer fire kort ved forskningsstasjonen og tilintetgjør et angrep. Dette er det første angrepet gruppen tilintetgjør, og de får derfor fjerne 1/3 av alle kubene fra brettet.

To spillkort trekkes. Det første er Sima og et andre er et "Angrep!-kort". Her følger deltagerne instruksjonene på kortet.

Angrepet spres ved å trekke to kort fra angrepskort-bunken. Her trekkes Frogner og Klæbu, og disse får en kube hver.

5.7 Sammenlikning med Pandemic

For å unngå å starte helt på bar bakke når det kom til den praktiske delen av øvelsen, ble det gjort en studie av eksisterende praktiske øvelser, deriblant spill. Det viste seg at brettspillet Pandemic hadde mye grunnfunksjonalitet som var ønskelig å bruke. Dette gjorde det mulig å undersøke bruken av spill i en øvelsessammenheng, uten å bruke mye av tiden på å designe et helt nytt spill.

Nedenfor presenteres sentrale elementer av spillet, og en sammenlikning av hvordan dette er løst i Pandemic og spillet som presenteres i denne øvelsen.

Element	**Pandemic**	**Videreutviklet spill**
Hovedtema	Beskytte verden mot 4 sykdommer som sprer seg	Beskytte strømnettet mot ett IT-sikkerhetsangrep som sprer seg
Spillbrett	Verdenskart	Norgeskart
Antall (byer, forbindelser)	(48,92)	(38,44)
Fiasko	En av følgende: – 8 utbrudd – Mer enn 15 av hver kubefarge er brukt – Spillkortbunken er tom	En av følgende: – 6 sammenbrudd – Mer enn 30 kuber er brukt – Spillkortbunken går tom
Suksess	Alle 4 sykdommene er kurert	Angrepet er tilintetgjort 3 ganger
Tilintetgjørelse	Samle 5 spillkort av samme farge	Samle 5 spillkort med forskjellige faser
Konsekvens av tilintetgjørelse	Angrepskortene i denne fargen gjelder ikke lenger. Alle kan bruke 1 handling på å fjerne alle kuber i en by av denne fargen.	Får fjerne hhv 1/3, 2/3 og 3/3 av alle kuber på brettet
Roller	Forsker Lege Operasjonsekspert Transportsjef Vitenskapsmann Karantenespesialist	Administrerende direktør IT-sikkerhetsekspert Offentlig myndighet Nettverksoperatør Beredskapsleder Kontrollsystemansvarlig

Pandemic er et komplisert strategispill, noe som kan være en svakhet når man skal legge til enda mer funksjonalitet i form av en faglig del. I forsøk på å gjøre denne versjonen av spillet litt enklere ble antall forskjellige angrep justert fra fire til ett, og dermed unngikk man bruk av kuber i forskjellige farger. Måten å vinne på måtte derfor gjøres om, og det ble innført et krav om å tilintetgjøre angrepet i 3 omganger, men større effekt hver gang. Dette virker realistisk i et IT-sikkerhetsangrep, det er ikke alltid man får fjernet angrepet 100% ved første forsøk.

En annen svakhet ved Pandemic den lite realistiske måten å kurere en sykdom på. Det skal utvikles en vaksine, men for å utvikle en vaksine skal det samles 5 bykort innen samme farge. Dette har ingen sammenheng med det å lage en vaksine i den virkelige verden. For å forbedre dette i øvelsen presentert her tilintetgjøres et angrep ved å samle kort med alle fasene i en hendlseshåndteringsprosess. Dette har sammenheng med en faktisk IT-sikkerhetshendelse, og at man må være forberedt i alle fasene for å håndtere hendelsen på en god måte.

En stor forskjell på Pandemic og spillet presentert her er antall byer og forbindelser. Dette er med på å påvirke totalt antall kuber tilgjengelig, samt effekten av sammenbrudd i nettet. Det er hovedsakelig antall forbindelser som er forskjellig, mange flere byer har flere forbindelser ut fra seg. Da blir det større sannsynlighet for gjentagende sammenbrudd, noe som skjer når en by som har en naboby med tre kuber får et sammenbrudd. For at det skal være en reell sjanse å tape på dette punktet, må derfor antall sammenbrudd før man taper minskes noe.

5.8 Tilpasse og gjenbruke øvelsen

For at det skal være mulig å bruke øvelsen i forskjellige organisasjoner, og fortsatt sikre realisme, må nettet på spillbrettet tilpasses den enkelte. Enten må selskapene selv bidra og gjøre endringer før øvelsen gjennomføres, ellers så må informasjon om organisasjonen deles med utenforstående som tilpasser spillet.

Noen punkter er viktig for å sikre at spillets funksjonalitet fortsatt er intakt. Kartet må tilpasses et visst antall byer og forbindelser mellom disse, og mange av byene må ha flere en to forbindelser ut fra seg. På grunn av redundans i strømnettet er det realistisk at dette er tilfelle.

En alternativ løsning er å utvikle et tenkt nett, som kan brukes av alle organisasjoner. Da slipper man biten men tilpassing, men realismen i øvelsen er noe svekket.

Spillet kan spilles flere ganger av de samme deltagerne. Dette kommer av at man bare inkluderer et utvalg av scenariekortene hver gang. Dersom det lages faglig del av størrelsesorden presentert i kapittel 4, vil spillet kunne spilles 3-4 ganger av samme

gruppe mennesker og allikevel møte på nye faglige utfordringer hver gang. Det kan også lages nye scenarier etterhvert.

Kapittel 6
Resultater

Dette kapittelet presenterer resultatene fra testene av spillet. Spillet er testet i to hovedfaser. På denne måten var det mulig og først teste spillets funksjonalitet, for å kunne justere denne, og deretter gjennomføre test av hele øvelsen med faglig del. Representanter fra bransjen har i tillegg kommet med sine innspill.

6.1 Spillets funksjonalitet

Denne delen av testingen bestod av å identifisere forbedringer og justeringer i spillets grunnfunksjonalitet. Her var ikke den faglige delen med scenarier inkludert i spillkortbunken. Målene for testen var følgende:

- Spillbrettet: Bestemme antall byer og kanter. Undersøke effekten av sammenbrudd.
- Undersøke fiaskomuligheter, det skal være mulig å tape på følgende måter med tilnærmet lik sannsynlighet:
  - Totalt antall kuber tilgjengelig
  - Antall spillkort
  - Antall sammenbrudd
- Muligheter for suksess:
  - Avhenger av vanskelighetsgrad, hvor mange Angrep!!-kort skal inkluderes?
  - Antall kuber som kan fjernes når et angrep blir tilintetgjort.
- Tidsbruk.
- Antall spillere som spiller spillet.
- Flyt i spillingen, deltagernes forståelse av spillet og spillets gang.

Etter hver spillrunde ble resultatene evaluert, justeringer gjort og eventuelle anbefalinger tatt med til videre arbeid.

6.1.1 Resultater testfase 1

Testene ble gjennomført av utvikler selv, og fokuset var på de rent funksjonelle punktene. I praksis betød dette at utvikler selv bekledde rollen som alle 3-4 spillerne for å simulere en ekte spillsituasjon.

Antall byer og kanter. Det originale spillbrettet til Pandemic har litt flere byer og dobbelt så mange forbindelser totalt. Det var derfor interessant å undersøke hvordan denne endringen påvirket spillet. Resultatet av testene viste at spillet kan ha flere byer med flere kanter ut fra seg, mye fordi effekten av sammenbrudd var mindre enn ønsket. Nå er det totalt 34 byer på kartet, men bare 40% har mer enn to kanter ut fra seg. Ved å legge til 4 byer på strategiske plasser er denne andelen økt til 45%, og det firedobler antall byer med fire kanter ut fra seg. Det hadde vært ønskelig å endre spillbrettet slik at denne prosentandelen ble enda høyere, men det lot seg ikke gjøre da nettet ble feil i forhold til virkeligheten.

Suksess. For å tilintetgjøre angrepet mot strømnettet og dermed vinne spillet, er det viktig at vanskelighetsgraden er satt til et overkommelig nivå. I denne fasen av testingen har det vært inkludert mellom tre og seks angrepskort. Resultatet viser at det er mulig å vinne med opp til 4 angrepskort. Det må tas til betraktning at testene ble gjort av en person som kjenner spillet godt, og at dette muligens vil være annerledes for deltagere som spiller spillet for første gang.

Fiasko. I hver test ble det gjort vurderinger rundt måten spillet tapes på. For å sikre variasjon bør spillet kunne tapes på alle de tre punktene med omtrent sammen sannsynlighet.

- Spillet tapes flest ganger av at spillkortbunken går tom. Det kommer til å endre seg når den faglige delen blir inkludert, noe som gjør spillkortbunken blir større. Det blir også lagt til 5 byer.
- På grunn av avviket i antall byer og forbindelser blir sjansene for gjentagende sammenbrudd betydelig mindre. Antall sammenbrudd har svært sjelden nådd 8, så ved å nedjustere denne vil det være mulig å tape ved å få for mange sammenbrudd i nettet.
- Gjentagende testing viser at antall kuber bør begrenses til ca 30, da er det en vesentlig sjanse for å tape på dette punktet.

Tid. For å få utbytte av spillet bør det være vanskelig å tape spillet fort, men samtidig mulig å vinne innen en rimelig tid. Oppsett av spillet tar omtrent 5 minutter. Tidsbruken har variert mellom 20 og 35 minutter. Her er det viktig å huske at samme person har stått bak alle rollene, så mye av tid til diskusjonen spillerne i mellom, kommer ikke frem denne testen.

Antall spillere. På grunn av begrensninger i kapasitet når en person utfører spillingen, ble det for det meste testet for tre spillere, og et par ganger for fire. Begge deler fungerer som ønsket så lenge man tar hensyn til antall spillere når det deles ut spillkort.

6.1.2 Anbefalinger etter funksjonell test, fase 1

Antall byer justeres opp for å øke effekten av sammenbrudd. Spillkortbunken blir da litt større, dermed tapes det ikke like ofte på dette punktet. Maksimalt tillatte sammenbrudd blir justert fra 8 til 6 for å øke mengden spill som tapes på denne måten.

6.1.3 Resultater testfase 2

Testen ble gjennomført av 3 personer inkludert utvikler. Spillet var helt nytt for de andre deltagerne i testen. Her ble det fokusert på de tre nederste punktene i listen for testmål.

Introduksjon. Dette er et avansert og omfattende spill, og det kan ikke forventes at deltagerne har spilt liknende spill før. Testene viste at det er viktig med en planlagt og grundig introduksjon. Deltagerne ga tilbakemelding på at eksempler var en god måte å beskrive elementer av spillet. Samtidig, hvis beskrivelsene ble for detaljerte førte det til at deltagerne mistet tråden i innføringen. Det viste seg å være en stor fordel at en av deltagerne hadde spilt spillet før, da tok denne personen ansvar i begynnelsen av spillet og sørget for at alle forstod.

Tid. Inkludert introduksjon har totalt tid variert mellom 30 og 50 minutter, oppsettet ble gjort på forhånd.

Flyt i spillet. Byene som er representert på brettet er mindre kjente for folk flest, noe som viste seg å bli en liten utfordring. Bare en person får lest bynavnene riktig vei når man sitter rundt brettet, og dette gjør at det fort brukes litt ekstra tid. Løsningen kan være at en person som er kjent med kartet får ansvar for å plassere alle kuber. Angrepskortene inneholdt på dette tidspunktet bare navnet på byen, men vil nå i tillegg inkludere et norgeskart med markør.

Suksess og fiasko. Etter justeringene fra forrige testfase, virker det nå som om kravene for suksess og fiasko fungerer som de skal. Denne spillrunden ble tapt fordi angrepet ble for omfattende, antall kuber oversteg 30.

6.1.4 Anbefalinger etter funksjonell test, fase 2

Bruk 10 minutter i begynnelsen til å forklare spillets mål og funksjonalitet. Vis gjerne med eksempler fra spillsituasjoner for å beskrive spillet på en måte som er enkel for deltagerne å forstå. Prøv å ha med en deltager som er kjent med spillet.

6.2 Spillet med faglig innhold

Målet med testen var å gjennomføre og vurdere øvelsen som helhet. Testgruppen bestod av universitetsstudenter med fordypning i informasjonssikkerhet.

Konkrete mål for testen:

- Finne en gunstig fordeling og mengde scenariekort i spillkortbunken.
- Identifisere uklarheter i scenariekortene.
- Tidsbruk.
- Flyt i spillet.

Scenariekort i spillkortbunken. I testen var det inkludert følgende scenariekort: 2 hovedscenarier, 3 spørsmål og 3 "visste du at.."-kort. Spillkortbunken bestod dermed av 38 spillkort med byer, 8 scenariekort og 4 angrep!!-kort. Dette viste seg å være en grei fordeling, og hadde ingen stor påvirkning på spillets grunnleggende funksjonalitet.

Suksess og fiasko. En viktig ting å være oppmerksom på er at etter inkluderingen av den faglige delen har spillkortbunken blitt betydelig større. Dette må tas hensyn til når det velges hvor mange angrep!!-kort som skal inkluderes, da disse dukker opp med større mellomrom nå. I dette tilfellet var ble det valgt å bruke fire, noe som resulterte i at spillet ble vunnet relativt raskt.

Scenariekortene. Testen avslørte noen uklarheter, og ordlyden i enkelte spørsmål viste behov for justering. Generelt fungerer de som tenkt. Testgruppen kunne svare på noen av spørsmålene, men hadde ikke så mye å bidra med i diskusjon av scenariene. Det ble lagt til tid for å kompensere for dette, 5 minutter per fase av hovedscenariene.

Tid. Testen ble gjennomført med 4 angrepskort i spillkortbunken, noe som gjorde at spillet ble vunnet på 35 minutter, som er relativt raskt. Basert på hvor mye av spillkortbunken som var brukt, vil antatt tid før denne er tom være ca 60 minutter. Med introduksjon og oppsett vil øvelsen ta maksimalt 1 time og 30 minutter.

Flyt i spillet. Et av hovedmålene med testen var å undersøke hvordan den faglige delen påvirket flyten i spillet. Den faglige delen fungerer som et parallelt løp til spillingen, da scenariene ikke har noen direkte sammenheng med hva som skjer på brettet. På grunn av bakgrunnen til deltagerne i testen var det ikke mulig å få testet dette fullstendig. Scenariene i faser blir avgjørende da disse minst kobling til spillet, særlig hvis det viser seg at den delen gjør øvelsen mer kaotisk. Testen viser imidlertid at fasene i scenariene må komme med minst mulig mellomrom, på denne måten ligger diskusjonen friskt i minnet hos deltagerne.

Deltagerne i testen sa i ettertid at spillet virket komplisert når det ble introdusert, men viste seg å være enklere å forstå etter de innledende rundene. Deltagerne erfarte en bratt læringskurve, så ved gjentagende spilling bør antall angrepskort øke slik at spillet blir utfordrende nok.

Suksess avhenger av at deltagerne forstår viktigheten av å tilintetgjøre angrep, så dette er viktig å tydelig påpeke i introduksjonen av spillet.

6.2.1 Anbefalinger etter test av øvelsen som helhet

En spillkortbunke bør inneholde 2 scenarier, 2-3 spørsmål og 3 "visste du atkort for at spillet skal fungere på ønsket måte, samtidig som man får ønsket utbytte av faglig del. Angrep!!-kortene bør trekkes med samme frekvens som tidligere, noe som resulter i at mengden kort bør økes med ett siden spillkortbunken blir større. Det må undersøkes om fem minutter er for lite for diskusjon.

6.3 Tilbakemelding fra bransjen

En representant for Statnett ble presentert for øvelsen etter at testene var gjennomført. Vedkommende har et beredskapsansvar i organisasjonen, og bidratt med innspill rundt den faglige delen og øvelsen som helhet. Representanten har ikke vært borti brettspilløvelse før, men deltatt på en øvelse som inneholdt organisering av fysiske elementer på et kart i forbindelse med en beredskapssituasjon. To bidragsytere fra NVE har også gitt tilbakemelding.

6.3.1 Faglig del

Bidragsyterene påpekte at det generelt var et godt valg av viktige og riktige scenarier, og spørsmålene til scenariene var gode og relevante. Scenariene er presentert i avsnitt

4.2.1. Nedenfor er innspillene presentert.

Scenario 1: Når det gjelder sårbarheter rundt hacking av AMS, påpeker bidragsyter fra Statnett at dette enten vil gjelde hacking av målere for å gjøre bevisst sabotasje (og dermed ramme nettselskaper), eller hovedserveren som mest sannsynlig vil ligge hos Statnett. Scenariet bør justeres til å ha en av disse som målgruppe. Stanett vil forøvrig styre balansen i nettet etter frekvensen, og ikke på grunnlag av data fra AMS. Hvis sabotasje gjøres i så stor skala at det påvirker strømbalansen vil Statnett regulere denne manuelt. Det påpekes også at radiosignalene mest sannsynlig vil være kryptert, så manipulasjon av data må gjøres fra innsiden av selve måleren.

Organisasjonene er redd for at hacking av AMS-målerne blir en konkurranse blant datanerdene på "gutterommet", noe som kan resultere i strømbrudd for et større område. Andre relevante scenarier er å bevisst sabotere viktige samfunnsinstitusjoner, som politi eller sykehus. Kartlegging av forbruksmønster for å planlegge innbrudd eller stjeling av industrihemmeligheter hos en konkurrerende bedrift kan også være aktuelt.

Scenario 2: Et høyst relevant scenario, men fordi personer i sentrale posisjoner blir sikkerhetsklarert med jevne mellomrom, påpeker bidragsyter fra Statnett at det er relativt liten sannsynlighet for å finne en person som oppfyller kravene i scenariet. Det vil være mulig å nå en større målgruppe hvis det istedenfor brukes trusler mot ansattes familie og venner. NVE påpeker at det bør spesifiseres om det menes brudd på strøm eller kommunikasjon.

Scenario 3: Noen ord og uttrykk kan med fordel byttes ut, blant annet ordet "substasjon", som ikke brukes i bransjen. Setningen med informasjon om produksjon og forbruk blir mer presis ved å si informasjon om styring og kobling, da arbeidsoppgavene i større grad omhandler det.

Delen med tjenestenektangrep vil lite trolig være et problem, da kraftforsyningen bruker egne uavhengige samband.

Scenario 4 og 5: Dette er veldig relevante scenarier som fungerer godt slik de er presentert.

Scenario 6: Mange av deltagerne vil ha vanskelig med å sette seg inn i en situasjon der de er sjef i bedriften, og scenariet vil fungere uten denne opplysningen. Den siste fasen er rettet mot kommunikasjonsavdelingen, og målgruppen her avviker dermed fra resten av scenariet.

6.3.2 Øvelsen som helhet

Brettspill er en engasjerende form for øvelse, samt at det er nyttig å jobbe på andre måter enn man er vant med. Morsom og uformell måte å lære på. Tidsbesparende både i gjennomføring og planlegging.

"Jeg ser for meg IKT-gutta i full sving med dette og i ivrig diskusjon"

- Bidragsyter NVE

Både Statnett og NVE mener denne øvelsen kan bidra til å øke samarbeidsevnen og kunnskapsdeling mellom IT-personell og kontrollsystempersonell. Alle diskusjonsforumer på tvers av fagområdet er nyttige, og det er alltid behov for å øve mer sammen på tvers. Representanten fra Statnett var generelt positiv til øvelsen, og viste interesse for å prøve den ut i organisasjonen. (NVE) Tror det, men vanskelig å si med sikkerhet da jeg ikke har sett spillet i aksjon.

Statnett

For at deltakerne ikke skal bruke for mye tid til å sette seg inn i spillet, er det viktig å lage spillereglene så enkle som mulig. Spesielt ledere har vanligvis en veldig tett kalender, og de setter pris på øvelser som er tidseffektive og rett på sak. Den største ulempen i dette tilfellet vil være at brettspillets regler tar tid bort fra faglige diskusjoner.

Bidragsyter ser for seg at målgruppen i organisasjonen vil være IKT personell, personell på kontrollanlegg, IKT-beredskapsledelse, og beredskapsledelse i driften. Rollene i spillet bør kunne velges etter hvem som deltar. Dersom beredskapsleder er med på øvelsen, bør beredskapsleder få lov til å spille beredskapsleder også under spillet.

Nivået på det faglige innholdet og spørsmålene virker riktig, noe som gjør at store deler av organisasjonen vil kunne bidra i diskusjonene. Derimot vil 4-5 minutter være litt kort tid på diskusjon av scenarier. Det er diskusjonene som er viktige, og ikke selve spillingen, så bidragsyter ville lagt til mere tid her.

Organisasjonen må endre litt på scenario 1, da dette ikke er en relevant problemstilling for dem. Ellers kan den faglige delen av øvelsen brukes som den er. Under intern testing har det vist seg å være en utfordring at deltagerne ikke kjenner til byene på kartet, men det vil ikke være et problem hos Statnett, da disse stedsnavnene er veldig kjente for de ansatte.

NVE

Bidragsyter fra NVE synes spillet virker litt komplisert, det kan bli en utfordring å sette seg inn i alle detaljene rent spillteknisk. Samtidig er dette vanskelig å si noe om uten å ha observert spillet i aksjon, men dersom det viser seg å fungere på testgruppen, kan det være en tidseffektiv og morsom måte å øve på. Spesifikke utfordringer kan være mulige logiske brister i scenariene, samt vanskeligheter med å forstå spillreglene eller se en rød tråd i øvelsen.

Målgruppen kan, i tillegg til Statnett, være andre store nettselskap. Spesifikt IT-personell, kontrollsystempersonell og kanskje også beredskapspersonell/ledere.

Bidragsyteren mener man vil få et visst utbytte av diskusjonen selv om det bare er beregnet 5 minutter per fase i scenariene. For at øvelsen skal tilpasses andre nettselskaper kreves kun mindre endringer i den faglige delen, og vedkommende mener det er overkommelig for selskapene å utføre dette.

6.3.3 Anbefalinger etter tilbakemeldinger fra bransjen

Scenariene justeres i henhold til tilbakemeldingene. Rollene vil kunne velges eller trekkes, etter som hvem som er tilstede. Diskusjonen vil i første omgang begrenses til 5 minutter for å ikke miste flyten i øvelsen mellom spill og diskusjon.

Kapittel 7
Diskusjon

I det følgende kapittelet diskuteres øvelsen som helhet, med tilbakemeldinger fra bransjen og erfaringer fra tester.

7.1 Tester og evaluering

Målgruppe og testgruppe. I den funksjonelle testen av spillet har det liten betydning at testgruppen ikke er den samme som målgruppen i organisasjonene. Den faglige delen med scenariene er tilpasset IKT og kontrollsystem-personell, og når denne delen inkluderes i testen av øvelsen som helhet, har forskjellen på kompetansen til målgruppen og testgruppen betydning. Selv om testgruppen har IT-sikkerhetsbakgrunn, var de ikke i stand til å sette seg inn og diskutere rundt hovedscenariene. Det var kun spørsmålene som gikk spesifikt på sikkerhet, og "visste du at.." det mulig å få tilbakemelding på, og her var resultatet tilfredsstillende. Mangelen på observasjon av hvordan diskusjonen av hovedscenariene påvirket flyten i spillet, viser en svakhet ved testingen. Dette kan være et kritisk punkt, da bruken av hovedscenarier potensielt kan vise seg å ha avgjørende innvirkning på øvelsen som helhet. Grunnen er at spilldelen og diskusjon rundt hovedscenariene ikke har noen direkte sammenheng, og kan dermed resultere i at hele øvelsen virker kaotisk eller mangle en rød tråd, som påpekt av NVE. Statnett nevner ikke dette i sin tilbakemelding, og en forklaring kan være at problemet først kommer til syne etter å ha testet øvelsen i bransjen.

Tilbakemelding fra bransjen. Innspillene på øvelsen kom fra et spesifikt nettselskap og et direktorat med beredskaps- og tilsynsansvar. På denne måten var det mulig å få tilbakemeldinger fra forskjellige vinkler, noe som styrker kvaliteten på øvelsen. NVE ser bransjen fra et overordnet perspektiv, og kan si hvilke type selskaper og personell som er målgruppe for øvelsen, og Statnett kan komme med spesifikke endringer de måtte ha gjort før øvelsen eventuelt kan gjennomføres. Tilsvarende for den faglige delen, der Statnett kan forslå justeringer for deres organisasjon og

systemer spesielt, mens NVE kan si noe om den faglige delen er relevant for bransjen som helhet.

Bransjen har kommet med verdifull tilbakemelding på den faglige delen med scenarier, noe som har resultert i justeringer grunnet logiske brister og mangel på kompetanse om hvordan systemene til organisasjonene fungerer. Det er viktig å unngå disse tingene, da øvelsen mister troverdighet og realisme [58]. Uten denne tilbakemeldingen ville resultatene av denne masteroppgaven mangle pålitelighet, da det ikke fantes noe kobling mot den faktiske målgruppen. De reviderte scenariene er presentert i vedlegg A.

7.2 Resultater fra testing

Flyt i øvelsen. Det er viktig å opprettholde flyten mellom den faglige delen og spillet, så det ikke oppleves som to forskjellige prosesser som aldri tar slutt. Ved å presse deltagerne på tid, øker ofte effektiviteten, noe som kan sammenlignes med virkelig situasjon der en hendelse skal håndteres under tidspress. Diskusjon er viktig del av øvelsen, men hvis fokuset tas for mye bort fra spillet kan helheten i øvelsen påvirkes. Dersom det brukes 10-15 minutter diskusjon av et scenario, vil det virke unaturlig å vende tilbake til spillet, og det kan være vanskelig å huske hvordan situasjonen på brettet var. Dette ville samtidig begrenset utvalget av scenariene som kan inkluderes i hver øvelse, eventuelt gjøre øvelsen langtekkelig. En løsning kan være å bruke scenariene i spillet til å identifisere situasjoner som krever mer oppmerksomhet. På den måten kan man gå tilbake og diskutere etter at spillingen er over, og ta de med videre i en senere prosess. Dermed blir hensikten med scenariene i hovedsak å gjøre deltagerne oppmerksom på ulike situasjoner som kan skje, slik at det er større sannsynlighet for å identifisere og se sammenhengen i situasjoner når de oppstår i daglig drift. Dette var en av hovedargumentene til en av de deltagende organisasjonene for å gjennomføre flere slike øvelser, nevnt i studien av en diskusjonsøvelse om IT-sikkerhethendelser i kraftbransjen [59].

Øvelsens kompleksitet En av hovedutfordringene med denne øvelsen er at den bygger på et relativt komplekst strategispill. Tilbakemeldingene fra bransjen viser også at de største bekymringene ligger rundt om øvelsen har nok utbytte i forholdt til tid og ressurser det krever for å lære deltagerne hvordan spillet fungerer. Resultatene fra testene viser at det tar litt tid før man er inne i hvordan ting fungerer, men at spillet har en bratt læringskurve. Dette blir et enda mindre problem hvis en av deltagerne har spilt spillet før og kan veilede de andre spillerne i starten. Det må påpekes at veiledningen bare bør skje i begynnelsen, for dersom en person har all styringen på spillet blir ikke øvelsen optimal [45]. Argumentet med at introduksjon tar for lang tid, gjelder derimot bare den første gangen deltagerne gjennomfører

spillet. Øvelsen er laget på en måte at den kan gjenbrukes med ulikt læringsutbytte, noe som løser store delen av denne utfordringen.

Øvelsen blir fort kompleks når den skal inneholde konkrete og relevante scenarier, der resultatet av diskusjonen har betydning for øvelsens suksess eller fiasko. Samtidig skal det inkluderes elementer som kjennetegner en ekte situasjon, gjerne med simulering av et angrep, og hvor deltagerne i tillegg innehar roller samarbeider mot et felles mål. Ut fra tabell 3.1 på side 18 er det kun simuleringsøvelsene som oppfyller alle disse kravene, en type øvelse som var utenfor omfanget av tid og ressurser for denne oppgaven. Måten problemstillingen ble løst på, ved å ta utgangspunkt i et samarbeidsspill, og deretter legge til elementer som frembringer læring og diskusjon er unikt og ikke brukt som grunnlag for en beredskapsøvelse før. Det nærmeste som eksisterer er bedriftssimulatoren hos Kasprsky-instituttet, der brettet simulerer et lite kontrollsystem. Gruppen som taper minst penger på hackerangrepene, vinner spillet. Dette viser at brettspill som konsept kan funke i en øvelsessammenheng, og det var derfor veldig interessant å utforske hvor tilfredstillende resultatet av testingen av øvelsen laget i denne oppgaven ble.

7.3 Faglig del

Hvert scenario kan potensielt gjøres mer ut av med tanke på diskusjon, flere faser og grundigere spørsmål. Men for å tilpasse scenariene til spillet, begrenses de av både tid og plass på spillkortene. Det er et poeng at scenariene gjenspeiler arbeidsflyten i hendelseshåndtering i en virkelig situasjon. Selv om f.eks ISO/IEC 27035 presenterer prosessen som rett frem, er det ofte en iterativ prosess mellom fase 2-4. En oppdager først et symptom på en hendelse, begynner å nøste litt, rapporterer, prøver å rydde opp, og så dukker det opp nye alarmer som kanskje henger sammen med den forrige. Scenariene er derfor forsøkt laget slik at det ikke øves på noe som er fullstendig i tråd med standarden når det ikke gjenspeiler virkeligheten 100%.

Spørsmålene krever et kunnskapsnivå som gjør at mange i organisasjonen bidra i en diskusjon, noe som ble påpekt som en viktig del av designe et spill med læringshensikt [86]. En annen ting var muligheten for å justere vanskelighetsgraden i spillet, og det kan gjøres ved å justere den faglige delen eller gjøre spillet lettere (færre ”angrep!!-kort”). På en annen side, selv om kanskje ikke alle bestandig kan svare på alt, er noe av hensikten med øvelsen at man skal lære av hverandre. Ved å øke samarbeidsevnen, kan terskelen for diskusjon være lavere, og flere vil bidra med innspill.

7.4 Brettspill som øvelse

Et av målene med utvikling av denne øvelsen var å presentere et alternativ til de tradisjonelle skrivebordsøvelsene. En spilløvelse kjennetegnes ved at den er engasjerende

og spennende, samt at det er lettere å se konsekvenser av avgjørelser [30]. Dette er også noe av bidragsyterne trekker frem som den største fordelen ved øvelsen, det er nyttig å jobbe på en annen måte enn man er vant med.

Ved å gjennomføre noen øvelser som skiller seg fra de tradisjonelle øvelsene, skaper man større variasjon i et beredskapsprogram. Øvelsen som presenteres er en type øvelse som passer til store deler av organisasjonen, dermed kan et bredt spekter av delakere inkluderes. Viktigheten av trening for alle ansatte, ikke bare hendelseshåndterere, er påpekt fra flere [17]. Øvelsen har en lavere terskel for deltagelse, og kan sees på som mindre formell enn de tradisjonelle beredskapsøvelsene. Målet består like fullt av å skape samarbeidsevner som å få læringsutbytte og bli oppmerksom på ulike sårbarheter og trusler. Hver enkelt ansatt kan være en betydelig ressurs både til å avverge og oppdage hendelser dersom de har et visst nivå av forståelse for informasjonssikkerhet [17], og øvelsen som presenteres her kan bidra til at flere i organisasjonene tilegner seg kunnskap om IT-sikkerhet.

Tilbakemeldingene fra bransjen påpeker at øvelsen vil bidra til å styrke samarbeidsevnene mellom tradisjonell IT- og kontrollsystempersonell, noe flere studier fremhever som en av de største utfordringene bransjen står ovenfor for å utvikle evnen til å håndtere IT-sikkerhetshendelser [22]. Statnett mener at diskusjonsforumer på tvers av fagområder er nyttige, det er alltid behov for å øve mer sammen på tvers, noe denne øvelsen vil bidra til. Det engelske begrepet *Communities of practice* omhandler nettopp dette, og i organisasjoner hvor kunnskap basert på erfaring er en hovedkomponent i vellykket drift, er fokus på dette essensielt for å lykkes også i fremtiden [87].

I en tidligere studie av IT-sikkerhetsberedskapsøvelser i kraftbransjen ble det undersøkt holdningen til andre typer øvelser enn skrivebordsøvelser. Tilbakemeldingene gikk ut på at gjeldende øvelser fungerte på en grei måte, og var ønskelig å prioritere en videreutvikling av disse fremfor bruk av ressurser på utvikling av andre typer øvelser. Hovedargumentet lå i at risikoen var for stor når liknende arbeid ikke eksisterte, men absolutt en spennende tanke om et positivt bidrag [22]. Et interessant aspekt er å se om resultatet av denne masteroppgaven har endret holdingen, er bransjen villige til å prøve en spilløvelse nå som de får en presentert. Statnett var veldig positive, og NVE synes det var vanskelig å si uten å ha sett øvelsen i aksjon, men mente den hadde et godt potensiale.

Fordi erfaringen på øvelser som omhandler IT-sikkerhetshendelser er begrenset, anbefaler forskere at hovedfokuset er på å gjennomføre disse type øvelsene, det er ikke så viktig hvordan øvelsene gjennomføres [88]. Øvelsen som presenteres er et godt eksempel på en øvelse som ikke er optimal på alle punkter, men allikevel kan bidra til at flere øvelser gjennomføres.

Tilpassing og gjenbruk. Øvelsen kan tilpasses ulike selskaper, og eventuelt andre bransjer. NVE mener det ikke krever store justeringer på den faglige delen for at den kan brukes i andre store nettselskaper i kraftbransjen, noe de mener selskapene er villige til å gjøre. Øvelsen kan også fungere i andre bransjer med fysisk spredning av kontroll og drift, som for eksempel oljebransjen. For at spillet skal kunne spilles gjentatte gange, og stadig trekke nye scenarier, må denne mengden økes. Ved å se på øvelsen slik den er presentert i denne oppgaven, kan inspirasjon finnes i form av type scenarier, struktur og innhold.

7.5 Oppsummering

Øvelsen som presenteres i denne masteroppgaven er et verktøy som kan hjelpe nettselskaper i kraftbransjen til å øke oppmerksomheten rundt IT-sikkerhet i smartgrids. De andre hovedbidragene er som følgende:

- En engasjerende og annerledes lavterskeløvelse som presenterer et nytt alternativ til IT-sikkerhetsrelaterte øvelser.
- Øvelsen fremmer diskusjon på tvers av ulike fagområder og personell.
- Presentasjon av relevante IT-sikkerhetsscenarier, tilpasset bransjen, noe som gjør netteskapene bedre forberedt på eventuelle hendelser. Dette muliggjør også identifisering av svakheter i eksisterende planer og prosedyrer.

For at øvelsen skal fungere på en tilfredsstillende måte bør følgende punkter være oppfylt:

- Spillbrettet må tilpasses selskapet, og den faglige delen bør gjennomgås og eventuelt justeres.
- En av deltagerne bør være kjent med spillets funksjonalitet, og dermed være i stand til å veilede de andre i begynnelsen.
- Øvelsen bør være et supplement til eksisterende type øvelser, for å sørge for variasjon i en organisasjons beredskapsprogram.

Kapittel 8

Konklusjon og videre arbeid

Innføring av smartgrids i kraftbransjen fører til en betydelig økning av trusler og sårbarheter når det gjelder IT-sikkerhet. En stor mengde ressurser brukes på teknologiske sikkerhetsmekanismer som brannmurer og deteksjon av innbrudd i systemer, men dersom menneskene fremstår som det svakeste punktet på grunn av manglende trening, er mye bortkastet. For å være i stand til å respondere på hendelsene som oppstår, er det avgjørende å ha et variert øvelsesprogram. Øvelser som omhandler IT-hendelser står nå på agendaen i kraftbransjen, men mangel på erfaring og kunnskap om disse øvelsene er en utfordring.

Utforming av relevante scenarier har vært en begrensende faktor for utvikling av IT-sikkerhetsøvelser. For å skape et grunnlag for en øvelse, ble nåværende og fremtidige IT-sikkerhetsutfordringer i kraftbransjen studert, i tillegg til eksisterende scenarier. På dette grunnlaget var det mulig å designe relevante scenarier på et format som passet den foreslåtte øvelsen. Scenarier på tre ulike former er presentert i denne oppgaven.

For å lage et alternativ til de eksisterende diskusjonsøvelsene, ble ulike praktiske tilnærminger studert. Dette inkluderte fysiske og digitale spill, samt øvelser basert på simulering. En type spilløvelse basert på et fysisk brettspill har potensiale til å dekke mange av hovedelementene i en praktisk beredskapsøvelse, men viste seg å være et veldig lite utforsket område, noe som skapte interesse for videre utforskning. Samarbeidsspillet Pandemic har en grunnfunksjonalitet som gjorde det mulig å bruke som et utgangspunkt. Spillet ble videreutviklet og justert til å bygge på et IT-sikkerhetsangrep, og det ble lagt til en faglig del som sørget for diskusjon rundt relevante scenarier. Øvelsen ble testet internt, først spesifikt på spillets nåværende funksjonalitet. Endringer og justeringer skapte en iterativ utviklingsprosess, noe som la et grunnlag for å teste øvelsen som helhet med den faglige delen bestående av scenarier. Bransjen, representert ved Statnett og NVE, har bidratt med tilbakemeldinger på øvelsen, noe som styrker kvaliteten og resultatenes troverdighet.

Øvelsen som presenteres i denne masteroppgaven er en prototype laget for testing. Det gjenstår litt utvikling, i form av design, kvantitativ intern testing og testing i bransjen, før spillet kan benyttes i en øvelse. Noen utfordringer ved øvelsen er identifisert, men resultatene så langt er en indikasjon på at den vil fungere under visse betingelser. Tilbakemeldingen fra bransjen er positive, og åpner for mulighet til utprøving, noe som vil være et naturlig videre steg i prosessen. Da kan øvelsen observeres i bruk av den rette målgruppen, og justeres ytterligere for å bli så optimal som mulig.

En alternativ tilnærming i videre arbeid kan være å ta utgangspunkt i scenariene presentert her og utvikle en annen type øvelse, gjerne digitalt. Et eksempel kan være implementasjon av et kontrollsystem, med hendelser basert på disse scenariene. Eventuelt kan det legges til rette for en konkurranse deltagere imellom, da engasjement og motivasjon er to avgjørende faktorer for gjennomføring av en god beredskapsøvelse.

Kilder

[1] D. A. Cockburn, "Using both incremental and iterative development," 2008.

[2] "Øvelser - en veiledning i planlegging og gjennomføring av øvelser i NVE." URL: http://webby.nve.no/publikasjoner/rapport/2013/rapport2013_53.pdf, besøkt 05.10.2014.

[3] "The homeland security exercise and evaluation program: The exercise process." URL: https://www.llis.dhs.gov/hseep, besøkt 04.11.2014.

[4] B. A. Jackson and S. McKay, "Preparedness exercises 2.0: Alternative approaches to exercise design that could make them more useful for evaluating – and strengthening –preparedness," 2011.

[5] "Fakta: Energi- og vannressurser i norge," 2015. Olje- og Energidepartementet.

[6] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," 2006.

[7] "Innsatsgruppe energisystemer - delrapport 1: Transmisjon." URL: http://smartgrids.no/wp-content/uploads/sites/4/2012/11/EnergisystemerTransmisjon.pdf, Besøkt 09.05.2015.

[8] "ISO/IEC 27000:2014," *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, 2014. International Organization for Standardization.

[9] "ISO/IEC 27035:2011," *Information Technology - Security Techniques - Information Security Incident Management*, 2011. International Organization for Standardization.

[10] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security 38 (2013), s.97-102*, 2013.

[11] M. B. Line, G. Johansen, and H. Sæle, "Risikovurdering av AMS - kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS," 2012.

[12] "NS 7799:2003 norsk standard for informasjonssikkerhet – norsk oversettelse av ISO/IEC 27001:2005: Information security management systems," 2003.

[13] M. Line, "A case study: Preparing for the smart grids - identifying current practice for information security incident management in the power industry," *Seventh International Conference on IT Security Incident Management and IT Forencis*, 2013.

[14] R. Anderson and F. Shailendra, "Who controls the off switch?," 2010.

[15] "Dragonfly: Western energy companies under sabotage threat." URL: http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, Symantec, Besøkt 18.04.2015.

[16] "Risiko 2015," 2015. URL: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf, Nasjonal Sikkerhetsmyndighet (NSM), Besøkt 28.05.2015.

[17] C. Hove and M. Tårnes, "Information security incident management - an empirical study of current practice," Master's thesis, NTNU, 2013.

[18] S. Akhtar, "Information security incident management - a case study about preparedness and readiness," Master's thesis, NTNU, 2014.

[19] F. Skapalen, "Veileder bfk, kap 6 – informasjonssikkerhet med fokus på klasse 2 og 3-anlegg." URL: http://www.nve.no/Global/Sikkerhet%20og%20tilsyn/Kraftforsyningsberedskap/Konferanser/IKT-sikkerhet_BfK%20seminar.pdf?epslanguage=no, Besøkt 22.05.2015.

[20] R. Sundseth, "Uansett hva vi gjør i dag er det ikke godt nok!." URL: http://paranoia.watchcom.no/?v=4915a, Besøkt 22.05.2015.

[21] M. B. Line, A. Zand, G. Stringhini, and R. A. Kemmerer, "Targeted attacks against industrial control systems: Is the power industry prepared?," *Proceedings of the 2nd Workshop on Smart Energy Grid Security, SEGS@CCS 2014, Scottsdale, AZ, USA, November 7, 2014*, pp. 13–22.

[22] H. Chiem and I. Graffer, "Computer preparedness exercises," *Instititt for Telematikk, NTNU*, 2014.

[23] M. B. Line and N. B. Moe, "Understanding collaborative challenges in it security preparedness exercises," 2015.

[24] M. P. Eladhari and E. M. Ollila, "Design for research results: Experimental prototyping and play testing," 2012.

[25] C. Cassell and G. Symon, "Essential guide to qualitative methods in organizatoral research," 2004.

[26] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," 2008. National Institute of Standards and Technology.

[27] "Veiledning i hendelseshåndtering. håndtering av sikkerhetshendelser for små og mellomstore bedrifter," 2010. NorSIS.

[28] "Good practice for incident management," 2010. European Union Agency for Network and Information Security.

[29] P. Kral, "The incident handler's handbook," 2011. SANS Institute.

[30] "Homeland security exercise and evaluation program (HSEEP)," 2013. Homeland Secuirty.

[31] T. Denning, A. Lerner, A. Shostack, and T. Kohno, "Control-alt-hack: The design and evaluation of a card game for computer security awareness and education," 2013.

[32] "Pandemic board game," 2008. Z-Man Games.

[33] M. Gondree and Z. N. Peterson, "Valuing security by getting [d0x3d!], experiences with a network security board game," 2013.

[34] T. Denning and Z. N. Peterson, "Security through play," 2013.

[35] "The disaster game: about." URL: www.disastergame.com/about, Besøkt 10.04.2015.

[36] S. Zahir, J. Pak, J. Singh, J. Pawlick, and Q. Zhu

[37] "Secure empire." URL: https://www.usenix.org/conference/3gse14/summit-program/presentation/olano, Besøkt 10.04.2015.

[38] "Cybersecure: Your medical practice." URL: http://www.healthit.gov/sites/default/files/cybersecure/cybersecure.html, Besøkt 10.04.2015.

[39] "Control system security center." URL: http://www.css-center.or.jp/pdf/about_cssc_en.pdf, Besøkt 10.04.2015.

[40] "Advanced cyber security course." ENCS URL: https://www.encs.eu/training/advanced-cyber-security-course, Besøkt 28.05.2015.

[41] "Critical infrastructure protection & industrial security, kaspersky industrial protection simulation." ENCS URL: http://www.kaspersky.com/industrial-security-cip, Besøkt 28.05.2015.

[42] G. Vigna, "Red team/blue team, capture the flag, and treasure hunt: Teaching network security through live exercises," 2003.

[43] T. Yardley, "A gap analysis of cyber security training in the smart grid," 2014.

[44] M. Berland and C. R. Lee, "Collaborative strategic board games as a site for distributed computational thinking," 2011.

[45] J. P. Zagal, J. Rick, and I. Hsi, "Collaborative games: Lessons learned from board games," *Simulation & Gaming, Vol. 37 No. 1*, pp. 24–40, 2006.

[46] P. A. Strøm, "Vurdering av informasjonssikkerheten ved innføring av AMS innen kraftdistribusjon," Master's thesis, NTNU, 2012.

[47] Y. Wang, "sscada: Securing SCADA infrastructure communications," 2012.

[48] J. T. Sørensen, "Hvor starter vi?!." URL: http://www.mnemonic.no/no/Faglig/Fagartikler/Scada-og-prosessnett/, Besøkt 09.05.2015.

[49] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Information security incident management: Planning for failure," 2014. (NTNU).

[50] "Nasjonal sikkerhetsmyndighet (NSM): Kvartalsrapport, k2/k3," 2013.

[51] M. Line, I. A. Tøndel, E. Albrechtsen, M. G. Jaatun, and O. H. Longva, "A framework for incident response management in the petroleum industry," *Intl. Journal of Critical Infrastructure Protection 2*, pp. 26–37, 2009.

[52] P. G. Almklov, S. Antonsen, J. Fenstad, E. Jacobsen, A. Nybø, and G. Kjølle, "Fra forvaltning til forretning: Restrukturering av norske nettselskaper og konsekvenser for samfunnssikkerhet," 2008.

[53] Stortinget, "Avtale om klimameldingen," 2008. URL: https://www.regjeringen.no/contentassets/fbe5a5829a5d468fab6e4eec0a39512d/avtale_klimameldingen_2008_01_17.pdf, Besøkt 09.05.2015.

[54] "Om smartgrid." Det norske smartgridsenteret, URL: http://smartgrids.no/senteret/about-smartgrid/, Besøkt 09.05.2015.

[55] S. Solberg, "Smart grid og dynamiske analyser," Master's thesis, NTNU, 2012.

[56] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," 2010.

[57] M. Røyksund, "Informasjonssikkerhet i kraftforsyningen," Master's thesis, Universitetet i Stavanger (UiS), 2011.

[58] S. Gåsland, "Gjør øvelse mester? om læringsfaktorer i beredskapsøvelser initiert av NVE," Master's thesis, Universitetet i Oslo, 2014.

[59] M. B. Line and N. B. Moe, "Utfordringer ved it-beredskapsøvelser." URL: http://infosec.sintef.no/informasjonssikkerhet/2015/03/utfordringer-ved-it-beredskapsovelser/, Besøkt 22.05.2015.

[60] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," 2011.

[61] "Cyber attack task force," 2012. North American Electric Reliability Corporation.

[62] J. Weiss and D. Savenije, "Why cyberattakcs could knock out the u.s. power grid for 9-18 months." URL: http://www.utilitydive.com/news/why-cyberattacks-could-knock-out-the-us-power-grid-for-9-18-months/170480/, Besøkt 22.05.2015.

[63] M. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in smart grids," 2011.

[64] A. AlMajali, A. Viswanathan, and C. Neuman, "Analyzing resiliency of the smart grid communication architectures under cyber attack," 2012.

[65] R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure and its application in smart grids," 2014.

[66] F. Cleveland, "Cyber security issues for advanced metering infrastructure," 2008.

[67] R. Link, "Smart meter attack scenarios," URL: http://blog.trendmicro.com/trendlabs-security-intelligence/smart-meter-attack-scenarios/, Besøkt 16.04.2015.

[68] "Sosial manipulering." URL: http://www.nettvett.no/personvern/sosial-manipulering, Besøkt 22.05.2015.

[69] M. Allen, "Social engineering," 2006. SANS institute.

[70] B. Miller and D. Rowe, "A survey of SCADA and critical infrastructure incidents," 2012.

[71] S. McLaughlin, E. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," 2009.

[72] F. Skapalen and B. Jonassen, "NVE: Veileder til sikkerhet i avanserte måle- og styringssystem," 2012.

[73] D. J. Dausey, J. W. Buehler, and N. Lurie, "Designing and conducting tabletop exercises to assess public health preparedness for manmade and naturally occurring biological threats," 2007.

[74] A. L. Fimreite, P. Lango, P. Lægreid, and L. H. Rykkja, "Øvelser som krise-forebygging," *Organisering, samfunnssikkerhet og krisehåndtering*, 2011. Oslo: Universitetsforlaget.

[75] N. Hunn, "When smart meters get hacked," URL: http://www.nickhunn.com/when-smart-meters-get-hacked/, Besøkt 16.04.2015.

[76] "Electric sector failure scenarios and impact analyses," 2013. North American Electric Reliability Corporation.

[77] M. Keogh and C. Cody, "Cybersecurity for state regulators with sample questions for regulators to ask utilities," 2012.

[78] "Fictional cyber attack," SANS Institute.

[79] "Emergency response tabletop exercises," US Environmental Protection Agency.

[80] "Sterk økning i hackerangrep mot norske bedrifter," URL: http://www.aftenposten.no/nyheter/iriks/Sterk-okning-i-hackerangrep-mot-norske-bedrifter-7506439.html, Aftenposten, Besøkt 16.04.2015.

[81] "Sikkerhetstilstanden 2014," 2014. URL: https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2014.pdf, Nasjonal Sikkerhetsmyndighet (NSM), Besøkt 29.05.2015.

[82] C. Hadnagy, "Social engineering: 3 examples of human hacking," 2011. URL: http://www.csoonline.com/article/2126983/social-engineering/social-engineering--3-examples-of-human-hacking.html, Besøkt 18.02.2015.

[83] Forbes, "America's hackable blackbone," URL: http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html, Besøkt 16.04.2015.

[84] SplashData, ""123456"maintains the top spot on splashdata's annual "worst passwordslist," URL: http://splashdata.com/press/worst-passwords-of-2014.htm, Besøkt 16.04.2015.

[85] "26.000 hackerangrep mot norske bedrifter i 2013," URL: http://www.adressa.no/nyheter/innenriks/article10156739.ece, NTB Adressa, Besøkt 16.04.2015.

[86] A. I. Wang, T. Øfsdahl, and O. K. Mørch-Storstein, "Collaborative learning through games - characteristics, model, and taxonomy," 2009.

[87] E. Wenger and W. Snyder, "Communities of practice: the organizational frontier," *Harvard Business Review*.

[88] "El-nettselskaper øver ikke på it-angrep." URL: http://gemini.no/2015/03/el-nettselskaper-over-ikke-pa-it-angrep/, Besøkt 22.05.2015.

Vedlegg

A Reviderte scenarier

Scenario 1: AMS

En sluttbruker med ønske om å spare inn noen kroner på strøm klarer å manipulere data i AMS-enheten ved å fysisk aksessere selve måleren, og deretter nedjustere forbruket sånn at måleren viser mye mindre strømbruk.
- *Hvordan kan dette oppdages når det skjer i såpass liten skala?*
- *Hva er eventuelle konsekvenser og hvordan kan det unngåes?*

AMS-systemet gir varsel om at rapportert strømmengde fra sluttbrukere har for stort avvik i forhold til rapportert overført strøm gjennom en trafostasjon for et område. Det blir mistenkt at ryktet har gått i nabolaget, og vedkommende har delt sin kunnskap.
- *På hvilken måte forandrer dette situasjonen nå som feilmengden er betydelig stor?*
- *Hva kan bli worst-case her?*

Scenario 2: Sosial manipulering og utro tjener

En dag med ekstremvær og et ustabilt strømnett får man brudd på sentralnettet mellom Nes og Aurland, noe som medfører strømbrudd i et område. Man antar først at dette har med uværet å gjøre, men etter gjentatte brudd på samme strekning begynner man å ane at det ligger en annen grunn bak, og mistenker at systemet kan være angrepet.
- *Nevn noen punkter som ville fått deg til å fatte mistanke. (Hvordan skiller man på årsak når det er strømbrudd?)*
- *Du er personen som først fatter mistanke, hvordan går du frem videre? Hvilke personer skal kontaktes og hvilke prosedyrer følges?*

Etter litt tid viser det seg at det var et rent sabotasjeangrep mot et backup-system, og at måten angriperne kom seg inn på var at de fant ut via firmaets hjemmeside, linkedin og facebook hvem som jobber der og har hvilke roller. Deretter ble det utpekt en ansatt som potensielt kunne bidra til angrepet, og vedkommende mottok flere

personlige trusler mot familien som kunne endt med alvorlige konsekvenser dersom han ikke la inn en bakdør i systemet.
- *Hvordan kan man unngå at dette skjer?*
- *Er dette et realistisk scenario? Kunne dette skjedd hos dere (hvorfor/hvorfor ikke)?*

Scenario 3: Zero-day angrep

Du sitter på jobb på regionssentralen. Kontrollsystemet gir varsel om feil et sted i nettet, og du blir satt på saken om å undersøke hendelsen og finne en løsning. Etter nærmere undersøkelser viser feilene seg å ikke ha rot i virkeligheten.
- *Hvikle årsaker mistenker du?*
- *Hva skulle tilsi at dette er et hackerangrep?*
- *Hvilke prosedyrer følges i dette tilfellet?*

Dette er et angrep IT-ekspertene ikke har sett før (Zero-day angrep), og flere ressurser blir satt på saken. Kontroll av systemet avslører at *firmwaren* i PLCene i nøkkelsensorenheter har blitt overskrevet, noe som gjør at informasjon om styring og kobling blir hentet ut og erstattet med feil data. Dette fører til at man ikke kan stole på verdiene kontrollsystemet gir.
- *Hvor langt må det gå før strømnettet må overvåkes manuelt?*

Scenario 6: Trusler og media

NSM har fått inn et tips som etter vurdering av deres eksperter virker troverdig. En gruppe hackere hevder å ha brutt seg inn i kontrollsystemet, og truer å svartlegge en av Norges støreste byer.
- *Hvem har hvilke ansvar her (KraftCert, NSM, bedrift, statlige myndigheter)?*
- *Hvilken handlinger må tas for å finne ut om dette er en faktisk trussel?*

Dere finner ingenting umiddelbart som kan motbevise et mulig angrep.
- *Hvordan håndteres denne situasjonen videre?*
- *Nevn viktige elementer i en videre plan.*