IT-sikkerhetsutfordringer og risikostyring for fremtidens smartgrids

Øyvind Imsland

Oppgave for graden
Master i Informatikk: informasjonssikkerhet
60 studiepoeng

Institutt for Informatikk
Det matematisk-naturvitenskapelige fakultet

UNIVERSITETET I OSLO

Våren 2022

IT-sikkerhetsutfordringer og risikostyring for fremtidens smartgrids

Øyvind Imsland

IT-sikkerhetsutfordringer og risikostyring for fremtidens smartgrids

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Innhold

Figurer

Forkortelser

AMS	Avanserte måle- og styringssystem
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
DMS	Distribution Management System
HES	Head End System
GIS	Geographic Information System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LFK	Leder for kobling
NIS	Network Information Systems
NSM	Nasjonal Sikkerhetsmyndighet
PST	Politiets sikkerhetstjeneste
NVE	Norges vassdrags- og energidirektorat
SCADA	Supervisory control and data acquisition
VPN	Virituelt privat nettverk
CISA	Cybersecurity & Infrastructure Security Agency
NIST	National Institue of Standards and Technology
IoT	Internet of Things
FFR	Fast Frequency Reserves
aFRR	Automatic Frequency Restoration Reserve
ENISA	European Union Agency for Cybersecurity
APT	Advanced Persistent Threat
CVE	Common Vulnerabilities and Exposures
HAN	Home Area Network
API	Application programming interface
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems

Del I

Innledning

0.1 Bakgrunn

Det pågår en elektrifisering i både Norge og tilkoblede strømnett i Europa. Samtidig så settes det klimamål for utfasing av kull og gass i Europa. Dette erstattes med mer variable strømproduksjon. Også i Norge får vi mer variabel strømproduksjon som sol og vindkraft. Samtidig er det også endringer i forbruk med biler som benytter elektrisk energi istedenfor bensin og diesel. Det gir nye utfordringer i nettet. Målet med oppgaven er å se på hvordan strømnettet kan se ut i fremtiden og hvilke utfordringer dette skaper med tanke på cybersikkerhet. Her er det en utvikling mot smartgrid som har både mer digitalisering, integrering og automatisert kontroll over både nett og kunder. Det åpner for nye sårbarheter og økt risiko. Oppgaven er skrevet som en del av InterSecure-prosjektet som er eid av Lnett.

0.2 Problemstilling og oppbyggning

Rapporten tar for seg en systembeskrivelse jeg har laget av hvordan et smartgrid-system kan se ut. Rapporten skal svare på to spørsmål:

- Hvordan ser trusselbildet ut i dag og fremover, og hvilken risiko gir det for smartgrids?
- Hvilke tiltak kan benyttes for å mitigere risiko i smartgrids?

Det vil være et spesielt fokus på AMS-målere i private husholdninger. Målerene har bryterfunksjonalitet som kan bety at en angriper kan koble ut strøm om de får kontroll over måler. Fysisk sikkerhet og eventuelle sårbarheter for komponenter i nettet som AMS-målere og digitale transformatorer er ikke vurdert i denne rapporten. Kostnadsestimater er heller ikke utarbeidet, i flere tilfeller vil det inkludere sensitiv informasjon om nettselskapers nåværende løsninger. Istedenfor har jeg i de tilfeller basert kostnad på antakelser. Rapporten inneholder 6 deler.

- Innledning som dekker viktigheten av smartgrid og gir en bakgrunn og restriksjoner på hvilke sikkerhetsløsninger og ikke basert på krav for at smartgrid skal kunne løse problemer nettet står ovenfor.
- En innsikt i dagens trusselbilde og mulige fremtidige utviklinger
- Beskrivelse av ulike systemer fra leverandører og Sintef og begrunnelse for systemvbeskrivelse valgt i denne oppgaven
- Vurdering av risiko for systembeskrivelsen
- Introduksjon og argumenter for bruk av zero trust metode.
- Anbefaling til tiltak og ny vurdering av risiko basert på tiltak.
- Konklusjon

0.3 Beskrivelse av AMS og DMS fra Sintef-rapport

> Distribution Management System (DMS) har som hovedoppgave å representere topologien i nettet slik at man bedre kan forstå konsekvensen av endringer i nettet. På driftssentralen er det leder for kobling (LFK) som har regien på DMS. LFK er den eneste som kan godkjenne endringer i nettet, og har ansvaret for at disse endringene reflekteres i DMS. DMS er en kartapplikasjon med nettverkstopologien lagt ut, hvilket gir et godt grunnlag for å forutse hva som skjer dersom en bryter kobles ut. Følgelig vil LFK ha god oversikt over hvilke områder som blir uten strøm dersom en bryter legges ut eller en feil oppstår på en ledning. ([19], s. 6)

> Det innhentes også informasjon fra f.eks. AMS-head-end og kundebehandlingssystemet, dog kan ingen av disse systemene endre tilstand i DMS-en eller oppdatere topologien, men vil bare komme som meldinger til LFK som i tur må vurdere om DMS skal oppdateres med relevant informasjon. I tillegg kan DMS ta inn informasjon om lokasjon på samtlige biler og montører/installatører, samt andre sensorer og typer data driftssentralen kan trenge. ([19], s. 6)

> Avanserte måle- og styringssystem (AMS) foretar målinger i den enkelte husstand. Det rapporteres om forbruk, evt. feil, som jordfeil, og det er innebygde funksjoner for å koble ut kunden ved hjelp av bryter- eller strupefunksjon. Strupefunksjon er i praksis en bryter som kobles ut når et gitt tak for effektforbruk er nådd. AMS-målere er knyttet til det sentrale Head End System (HES) gjennom lokale masternoder. Masternodene har mobiltilkobling (GPRS, 4G, 3G, 2G) til HES, mens vanlige AMS-målere tilknyttes masternoden gjennom et radiobasert maskenettverk. ([19], s. 7)

0.4 Økt digitalisering og integrering i strømnettet

Innovasjon både innenfor kraftbransjen og andre bransjer, også inkluderte private hjem har i nyere tid hatt stort fokus på IoT. Også fra infrastrukturstandpunkt så er flere av nyvinninger i 5G over 4G rettet spesifikt mot bruk av IoT og operatører som Telenor som ikke bare snakker om forbedringer for forbrukere men også har stort fokus på å få bedrifter til å ta i bruk nye 5G nett. En annen faktor som gjør IoT mer relevant er nyvinninger innen maskinlæring som muliggjør modeller som kan ta imot enorme mengder data og prossesere disse raskt. Proactima har i sin rapport om IIoT beskrevet tre områder hvor bruk av IoT er driver for å løse nye problemstillinger.([40], s. 10)

- Ekstremvær som følge av klimautfordringer
- Elektrifiseringen av samfunnet (transportsektoren, båter, fly)
- Vindkraftutbygging – behov for mer fleksible nett

Det mest utbredte eksempelet er smartmålere som etter hvert blitt svært utbredt i store deler av verden. Denne type digitalisering inkluderer mye data fra sensorer som blir aggregert. Det fører og til at det blir utviklet flere løsninger som bygger på dette. Disse ulike løsningene blir igjen gjerne integrert med hverandre slik at resultat av behandling av ulike data er lett tilgjengelig for hele systemet. Eksempler på dette på leverandørsiden er Siemens Spectrum Power løsning og Hitachi ABB Power Grids sine MicroSCADA X løsninger[57] [48] En av fordelene Siemens viser til er å kombinere værmeldinger med historisk data for å kalkulere både forbruk og produksjon av energi fra fornybare kilder og så sette dataene inn i et optimaliseringsproblem for å eksempelvis minimere kostnad ved strømproduksjon. Planen for dette blir så sendt til et SCADA kontroll-system slik at en kan få automatisk optimert drift av kraftverk.

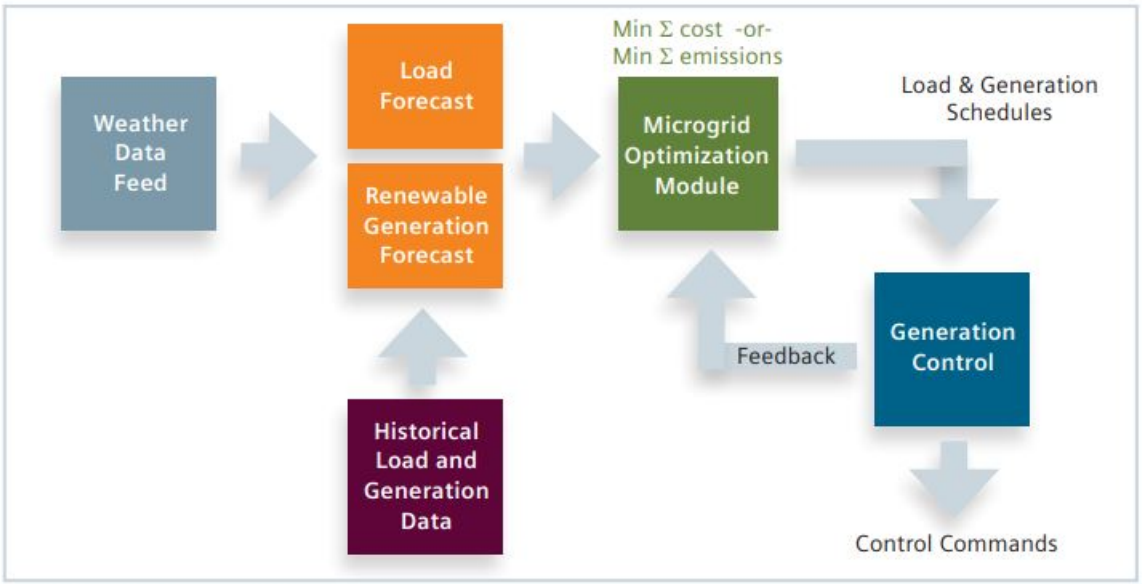


Figure 1: MGMS Operational Flow

Figur 1: Optimalisering av drift i smartgrid fra Siemens spectrum model

[55] MicroScada X er på sin side er bygget til å være veldig modulært. Det betyr i praksis at systemet er veldig åpent for nye integrasjoner av veldig mange ulike former for tjenester. Alt integreres i praksis inn i samme system.

Nettselskaper tester også ut løsninger der en bruker og behandler ny data tilgjengelig fra IIoT. Agder Energi har eksempelvis et samarbeid med Microsoft hvor Microsoft stod for prosessering av informasjon og basert på det koblet Agder Energi ut varmekabler hos storforbrukere [17] Dette er i dag en del av prosjektet NORFLEX [63] I private husholdninger kan en også oppnå lignende funksjonalitet. AMS målere har en HAN-port som tillater kunder å hente ut informasjon direkte fra sin måler og står fritt til å gi denne informasjonen til 3. part leverandører som tilbyr eksempelvis smarthus-løsninger.

Data fra AMS-måler blir da sendt til 3. part sitt datasenter, behandlet og sender kontrollsignal til strømforbrukere i husholdningen.

Det er altså en sterk økning i innsamling av mengde informasjon, og innsamling av informasjon som ikke ble samlet inn før. Informasjon blir i større grad også sentralisert og en større deling av informasjon. Her oppstår det nye problemstillinger. Det blir samlet inn mye data, men hvem har tilgang til denne dataen? Med mer integrering av ulike systemer og stadig flere leverandører involvert enn tidligere så må nye risikoer kartlegges og så blir det et spørsmål om hvordan en skal mitigere disse nye risikomomentene?

0.5 Hvilke data blir innhentet av AMS og hvem har tilgang til disse?

Data som blir innhentet: [27] Alle AMS målere i private husstander må hente inn målingsdata for strømforbruk, styrings- og jordfeilsignal. Måling av effekt begge veier er også et krav. Måleverdier lagres i måler [28]. Og prisinfo skal bli sendt til måler [29] Fra måler blir opplysninger sendt til Elhub [13] Elhub lagrer en del informasjon utover kun forbruk og genererer også data som estimert årlig forbruk.

Også spenningskvalitet blir målt avhengig av hvilke målere selskapene har valgt [45] [2] Kunder kan også hente ut måleverdier for strømforbruk og kostnad lokalt fra strømmålere via HAN-port. Det er svært sannsynlig at en slik løsning vil kreve kobling til Internet og disse data vil havne i en skyløsning et sted. Innenfor smarthus-løsninger så er det veldig mye integrasjon mellom ulike aktører. Sannsynligvis vil kunde ikke ha kontroll på hvem som faktisk lagrer disse dataene og hvem de blir delt med. [41] Du har ingen garanti for at et selskap faktisk følger reglene for personvern. Innen det potensielt er avdekket vil informasjon allerede være på avveie.

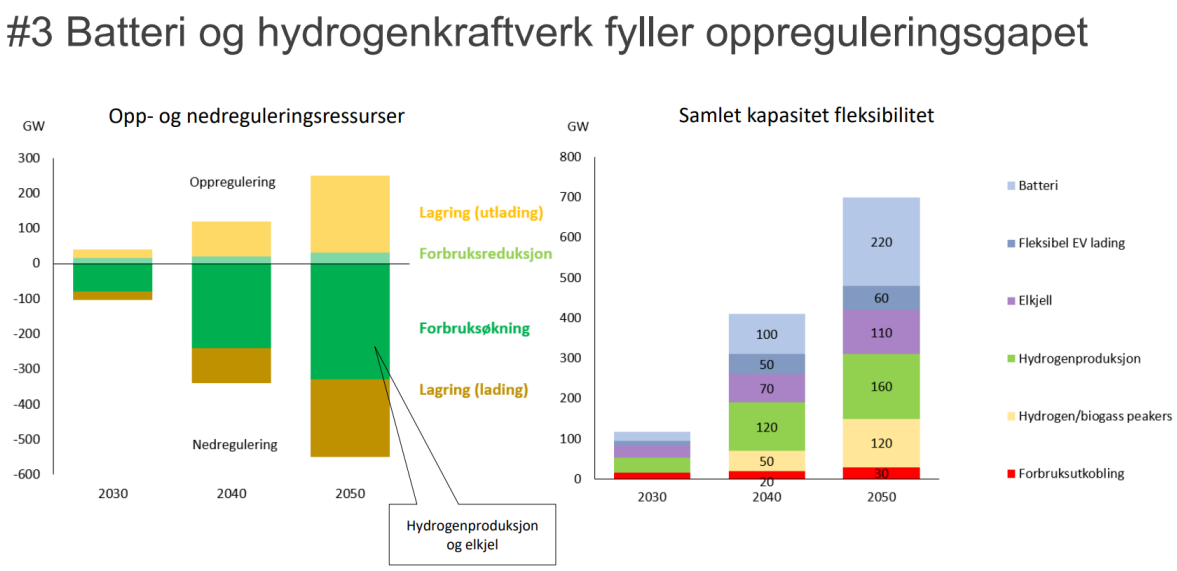
I dag finnes en slik løsning på markedet levert av Tibber som heter Tibber Pulse. Den kobles til WiFi og kommuniserer med Tibber sine serverere. Du har og mulighet for sammenkobling med en lang rekke apper for å styre diverse basert på måleverdier fra AMS måler. Dette er derimot utenfor ansvarsområdet til nettselskap da det er kundene selv som velger å overlevere sine data.

Kapittel 1

Smartgrid

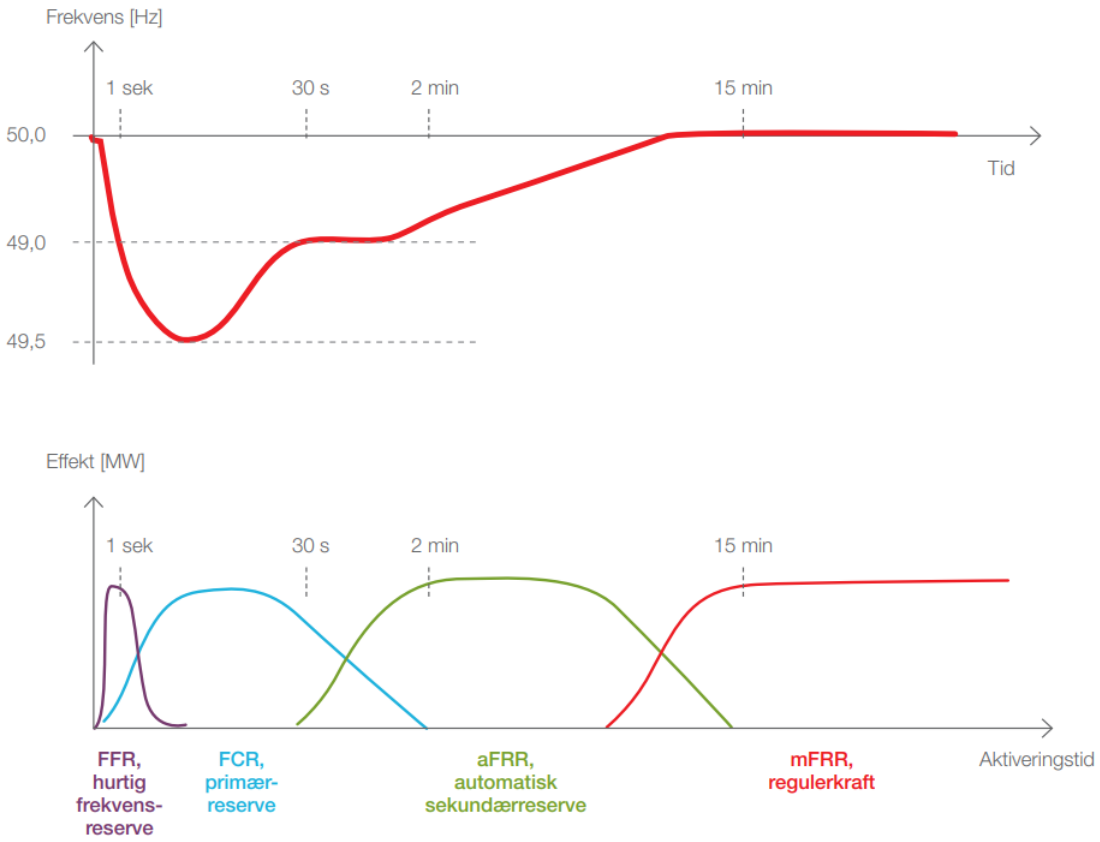
1.1 Behov for mer fleksibilitet i strømnettet

I forbindelse med elektrifisering i Norge og Europa så vil det ifølge Statnett sine prognoser være større behov for fleksibilitet[65]. Fleksibilitet blir her skissert opp løst på ulike måter. Elbillading er problematisk allerede i dag med tanke på effekten av forbrukstopper på stabilitet og kapasitet i nettet. Allerede neste år planlegger Statnett å gå fra 1 time til 15 timers tidsoppløsning for mFRR for å balansere frekvens i strømnettet. Her ser Statnett i fremtiden for seg mer fleksibel lading av elbiler for å oppnå stabil frekvens. Fleksibel lading av elbiler er ikke bare for å redusere forbrukstopper, men også produksjonstopper. Det er også lagt inn fleksibilitet i form av at varmtvann og varme i bygninger kan skrus av i perioder. Spesielt varmtvannsberedere kan regnes som batterier i den forstand at de holder godt på energi og er store nok til at varmtvann ikke må erstattes med en gang det blir brukt. Sammen med produksjon kan det også være med å balansere produksjonstopper.



Figur 1.1: Modell av fremtidig fleksibilitet i EU11 i Statnett sin LMA2020-2050 rapport [65]

Økt fleksibilitet regnet som nødvendig i stor grad på grunn av at vi får mer strømproduksjon som er veldig variabel i forhold til strøm fra store turbiner. Vannkraft kan tappes ned ekstra mye om det er en uke med nesten ingen vind i Norge og tilsvarende tappes ekstra lite en uke med mye vind. Forbeholdet her er at det er nok installert effekt i vannkraftverk til å ta over for all vindkraft. Det er både fysiske begrensninger på hvor raskt du kan kan øke produksjon men og økte driftskostnader ved å øke så raskt som mulig pga økt belastning[49]. Mange vanndammer er også fyllingsdammer og det vil være problematisk å raskt åpne opp og stenge igjen rørgater. Det kan også bli problemer med produksjonstopper av vind hvis det fører til at en må stenge kraftverk helt ned i korte perioder. Tyskland betaler eksempelvis Danmark for å ikke produsere vindkraft i perioder med store produksjonstopper i Danmark fordi de mangler evne til å håndtere produksjonstopper i nettet sitt.[11]. I Statnett sin markedsutviklingsplan har de skissert ulike kategorier av fleksibilitet i nettet som vil være nødvendig.



Figur 1.2: Modell som viser ulike kategorier som er nødvendig for stabilitet i nettet ([64], s. 17)

I pilotprosjekt i 2018 så kvalifiserte hverken vannkraftverk eller pumpekraftverk for kravene til å benyttes som FFR i denne modellen. ([62], s. 16-22) Teknologier som fungerte var utkobling av elbil-lading, utkobling av datasenter der datasenter gikk over til å bruke sine batterireserver og utkobling av veldig strømkrevende industri. For å takle behovet for fleksibilitet ser Statnett for seg at digitalisering og automatisering er en forutsetning. Her trekkes og behov for særlig fokus på digital sikkerhet. ([64], s. 12)

1.2 Elektrifisering gir store effekttopper også lokalt

Elbiler blir raskt en utfordring for nettet når ladere når 10 kW i husholdning og 300 kW for hurtigladestasjoner. I tilegg så blir det og hurtiglading av eksempelvis ferjer og fly. Det gir både lokale og nasjonale utfordringer. Også eksisterende produkter som en komfyr kan i dag trekke mer strøm. Standard effekt for induksjonskomfyr er nå på 5,4 kW. Her er ny ordning for nettleie på vei for å gi husholdninger intensiver til å unngå

slike effekttopper. Selv om dette fungerer bra er det likevel klart at det vil være veldig økonomisk å finne nye løsninger i nettet for å tilrettelegge for denne fleksibiliteten. Hvis en legger sammen 10 kW lading, 5 kW middag og kombinert 5 kW for varme og varmtvann en vinterdag så må det da bygges ut transformator og linjekapasitet til mer enn 20 kW effektuttak per hus. Det er veldig unødvendig når elbil kan lades saktere på et annet tidspunkt og varme kan være skrudd av i 15 min mens induksjonsplate er på fult uten at det vil merkes. Det er en utfordring nasjonalt for Statnett, men det vil og være en utfordring lokalt. Dette husholdningsforbruket kan eksempelvis flyttes i helgen til en hyttekommune som primært gjør det til en utfordring i lavspenningsnettet

Det er flere nettselskaper i Norge som har begynt med ulike løsninger som vil gi mer fleksibilitet. Eksempler på det er prosjekt som Lnett21 der Lnett har kontroll over strømforbruk hos bedriftskunde[39] [14] og prosjekt fra Elvia der de har kontroll over varmtvannsberedere hos private kunder. Elvia sitt prosjekt foregår i et område som krever ekstra mye fleksibilitet lokalt pga mye hytter og høy elbilandel. [16]

Alternativet til Elvia sin løsning er at kundene ved hjelp av løsninger fra aktører som ikke er nettselskap og selv sørger for fleksibelt forbruk og flater ut forbrukstopper. Et eksempel på det er produkter fra Tibber som kan brukes til å styre lading av elbil, varmvann og elektrisk varme. [70] Et problem her er at det er mest naturlig å styre etter prisnivå. Det kan fortsatt føre til store forbrukstopper innenfor en transformator. Her kan ny ordning for nettleie med fastledd basert på forbrukstopper spille inn. Det vil derimot ikke gi fleksibilitet, kun reduserte effekttopper. Her kan det godt tenkes at det blir ordninger hvor kunde eksempelvis får betalt får å gi enten nettselskap eller aktører som Tibber mulighet til å automatisk redusere strømforbruk i kortere perioder. Det kan også komme ordninger hvor kunder kan enten få svært billig strøm eller betalt for å lade elbil. Dette vil hjelpe på å håndtere produksjonstopper.

1.3 Nytteverdi og besparelser ved smartgrid gir økt budsjett til sikkerhet

Behov for fleksibilitet er viktig i forhold til risikovurdering og tiltak når det kommer til sikkerhet. Rent praktisk må kostnaden av IT-sikkerhet være rimelig i forhold til reduksjon i risiko. Hvis kostnader ved sikring av et mer digitalt og integrert nett overstiger besparelsene vil det være bedre å ikke digitalisere. Hvis nettet ikke blir utviklet til et mer fleksibelt smartgrid så må kapasitet økes i forhold til et scenario hvor smartgrid benyttes. Dette er for å kunne håndtere høyere forbruks-og produksjonstopper i nettet. Det vil og være behov for mer strømproduksjon som kan raskt settes inn ved behov og der peker Statnett på hydrogen. Hvis all fleksibilitet kommer fra hydrogen så må det selvfølgelig bygges flere hydrogenkraftverk samt at vi må produsere mer energi siden

det er et eneritap når elektrisk strøm blir lagret som hydrogen og så brent for å lage strøm igjen. Hydrogenproduksjon kan også bli viktig for å håndtere produksjonstopper i det tilfellet. Hydrogen løser derimot ikke problemstilling med frekvensrespons som er klart på 2 sekund. For å kunne reagere på endringer i nettet som skjer raskt er det også behov for sensorer som kan hente denne informasjonen. Statnett peker på høy kvalitet og mye data som viktig for å kunne stabilisere frekvens og opprettholde god kvalitet på spenning i nettet.([64], s. 12) Digitalisering og automasjon i nettet blir da en forutsetning for elektrifisering og fremtidig grønn energiproduksjon. Det betyr at tilstrekkelige sikkerhetstiltak må på plass, selv om de er omfattende.

Del II

Trusselbilde

Kapittel 2

Trusselbildet i dag og potensielt nye trussler

2.1 Sikkerhetsrapporter viser lav grad av rapportering og stor økning i angrep

Bakgrunn for risikoanalyse må ses i lys av rapporter om trusselbildet eksempelvis Mørketallsundersøkelsen[59] som gir et innblikk i hendelser i Norge. Undersøkelsen viser så rapporteres kun 2% av hendelser til norCERT og 4% til CERT knyttet til den aktuelle bransjen. Det vil derfor ikke gi et skikkelig bilde av trusselsituasjonen å kun se på angrep som er offentligjort. Derfor er undersøkelser basert på anonyme data viktig for å få en innsikt i det reelle trusselbildet og vil bli lagt til grunn istedenfor angrep som har kommet frem i media.

Mnemonic er et sikkerhetsseslskap som overvåker trafikk hos kunder og publiserer årlige rapporter for trusselbildet og endringer. De har stort datagrunnlag for utvikling siden de har mange kunder i Norge som de analyserer trafikk for. Det som presenteres som størst økning er økning i rekogniseringsaktivitet som økte med 83% i 2020 og opp 5x siden 2018.([43], s. 28-29) Med korona har de også sett en dobbling i tilfeller som gjelder misbruk av autorisasjon hvor angripere har klart å autorisere seg som noen de ikke er og oppnådd tilganger de ikke skulle hatt. En økning i angrep mot autorisasjon i seg selv er ikke like relevant for system for kritisk infrastruktur hvor kun lokal tilgang er tillatt. Det viser derimot at angripere er veldig opportunistiske og kan endre fokus raskt. Med en plutselig pandemi og mange ansatte som må jobbe hjemmefra så utnytter angripere dette til å komme i forkant av tiltak for å redusere risiko ved bruk av hjemmekontor. Her kan det lett tenkes at plutselige endringer skjer i type eller omfang angrep som skjer spesifikt rettet mot strømnett. Interessen for angrep kan og øke gradvis i takt med elektrifisering av samfunnet. Angrep mot nettselskap kan bli som et supply-chain angrep mot samfunnet ellers.
newline

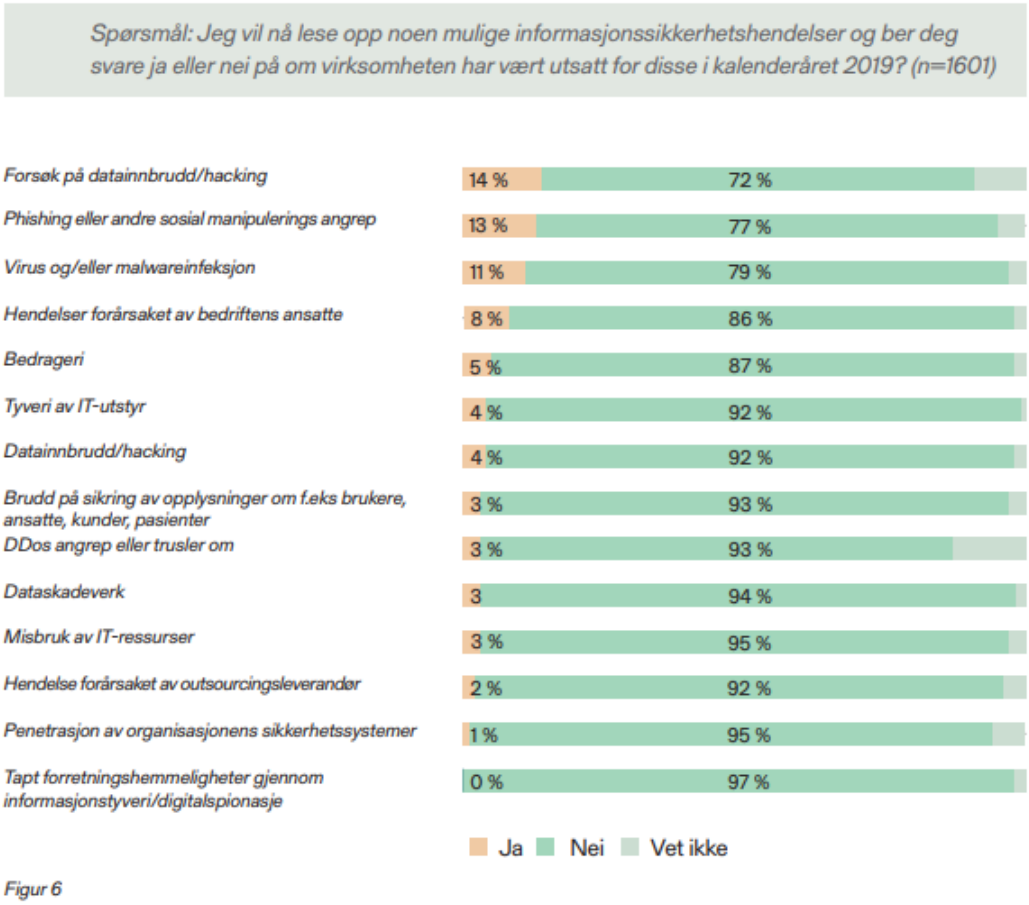
Et annet viktig moment her er økning i rekognisering. Det vises spesielt til svært stor aktivitet som følger av avsløringer av svakheter. Rekognisering er første steg for et angrep og det viser at det er veldig stor aktivitet for å lete etter mål uansett bransje. Det gir stor sannsynlighet for å bli rammet av tilfeldig angrep hvis zero-day svakheter ikke blir utbedret. Mørketallsundersøkelsen viser at feilkonfigurering er en vanlig feil. Risikoen for å bli tilfeldig angrepet vil øke når du har flere som konstant leter etter slike feil i bedriftens systemer.

I europeisk energisektor er nå halvparten av IT-sikkerhetshendelser som følge av direkte kriminell handling. Menneskelig feil er rapportert til 25% [44]. Her ser vi altså et litt annerledes bildet enn det generelle fra Mørketallsundersøkelsen hvor energi-sektor i større grad blir aktivt angrepet eller alternativt har bedre rutiner for å motvirke eller redusere konsekvens av menneskelig feil. ENISA har i sin rapport for 2020/2021 rangert trussler mot tilgjengelig som nummer 6, og supply-chain som nummer 9 i sin top 9 liste over trussler. Disse er spesielt relevante for energisektor siden tilgjengelighet er det viktigste i nettet.

Supply-chain angrep er også relevant siden det kan gi angriper en lett vei inn i systemer selv om nettselskapet har god sikkerhet. Det er en type angrep som er vanskeligere å mitigere siden det gjelder sikkerhet hos leverandør og er delvis utenfor kontrollen til et nettselskap. Hvis nettselskapet har god sikkerhet vil en angriper lete etter letteste vei inn som gjerne gjør nettselskp med høyere lovkrav til sikkerhet en selskaper generelt spesielt utsatt for slike type angrep. Underleverandører er ikke underlagt de samme lovkravene og nettselskapet er ansvarlig for sikkerhet.

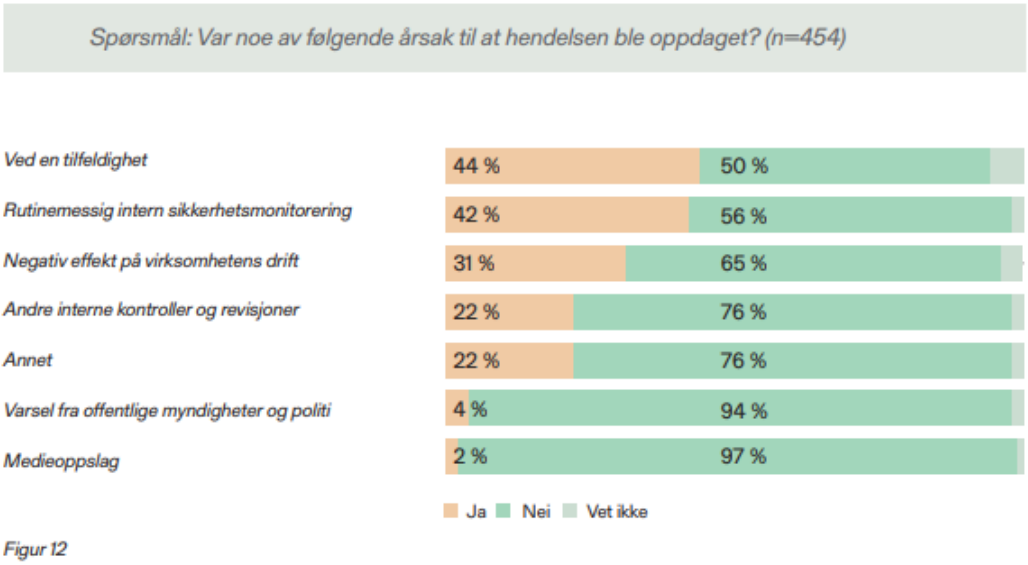
2.2 Manglende kompetanse og manglende sikkerhetsmonitorering hos norske virksomheter

I Mørketallsundersøkelsen svarer hele 72% at de ikke har vært utsatt for et forsøk på datainnbrudd/hacking. 14% sier ja og 14% svarer at de ikke vet. ([59], s. 18)



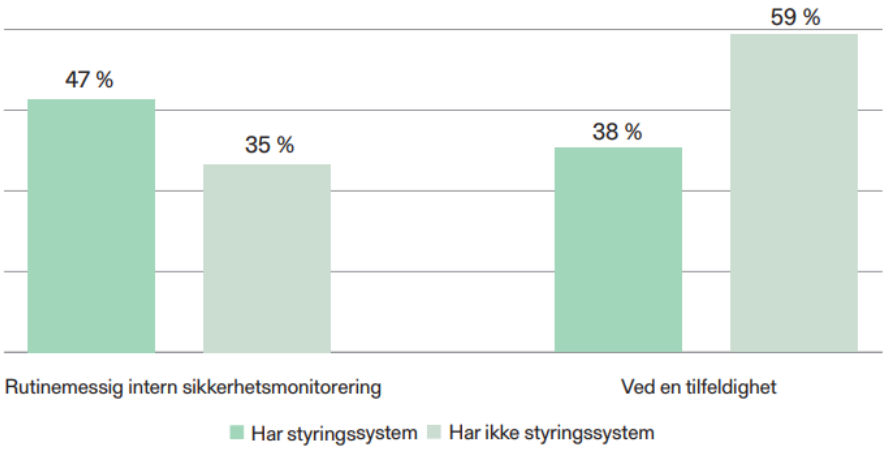
Figur 2.1: Sikkerhetshendelser virksomhet har blitt utsatt for fra Mørketallsundersøkelsen 2020

Dette er ikke et spørsmål en eneste virksomhet bør svare nei. Det er også beskrevet i kapittel 8.3 som er kommentar fra Visma ([59], s. 62). Visma sine tall indikerer angrep hver eneste dag der de skriver flere er så sofistikerte at de bør rapporteres. Selv om Visma sine data indikerer at virksomheter blir angrepet hver dag svarer altså 72% av de spurte at de ikke har hatt noen slike forsøk i løpet av hele 2019. Visma peker i sin kommentar på at siden de fleste angrep mislykkes og det ikke finnes noen krav fra ledelse til å overvåke eller rapportere, så ignoreres det. Manglende krav og da gjerne manglende ressurser for overvåkning kan være grunnen til at 14% her svarer at de ikke vet. De som svarer nei derimot viser at det mangler en forståelse for de trusslene som eksisterer og at disse angrepene forekommer daglig. Det er også viktig å se denne figuren i sammenheng med hva virksomhetene oppgir som grunnen til at de oppdager en hendelse.



Figur 2.2: Årsaker til at hendelse ble oppdaget fra Mørketallsundersøkelsen 2020 ([59], s. 25)

Dette spørsmålet gjelder virksomheter som har svart ja i en kategori i figuren over og har hatt en hendelse som har skjedd og de har oppdaget. Selv om 42% har oppdaget hendelse ved rutinemessig intern sikkerhetmonitorering viser tallene at mye oppdages ved tilfeldighet (42%) eller ved at en merker negativ effekt (31%). Det beste ville vært om alle hendelser ble oppdaget av sikkerhetmonitorering, men dette er vanskelig å få til. Spesielt for mer avanserte angrep som bruker nye teknikker. Det er likevel en høy andel som blir oppdaget ved en tilfeldighet her. Det tyder på at sikkerhetsmonitorering er manglende. Figur 13 fra undersøkelsen som viser forskjellen på om virksomhet har rammeverk for informasjonssikkerhet eller ikke viser at det kan iverksettes tiltak for å øke andel hendelser som blir oppdaget ved monitorering og minske andelen som blir oppdaget ved en tilfeldighet.

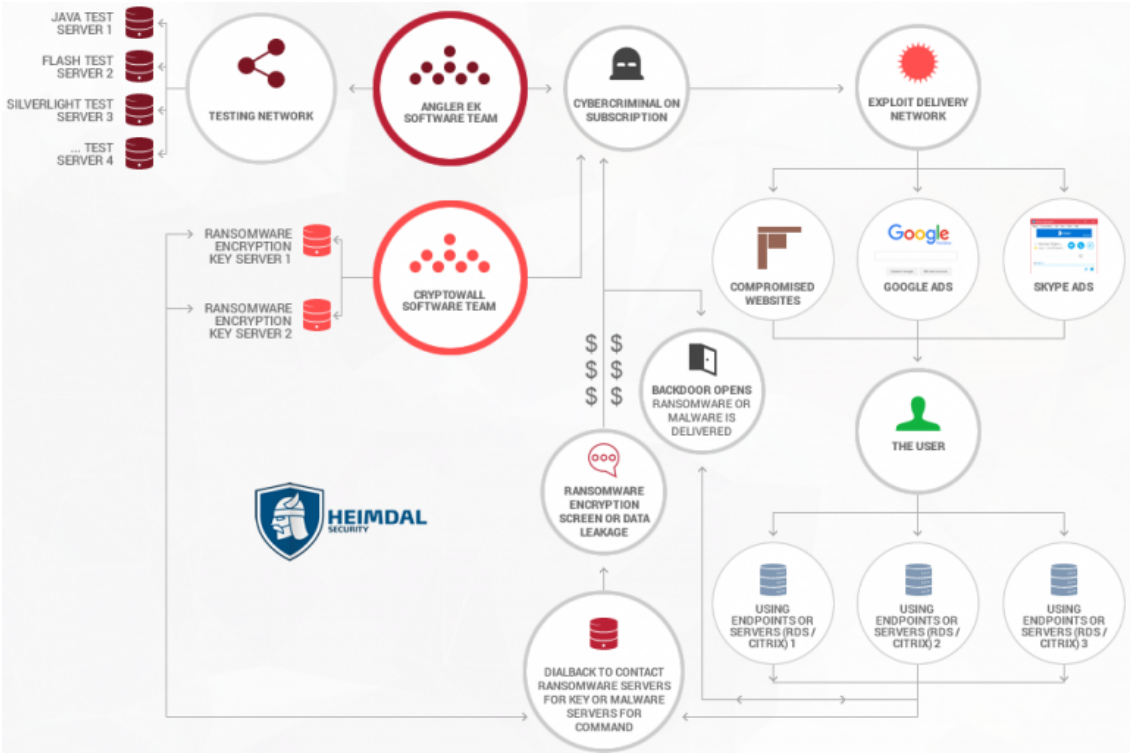


Figur 13

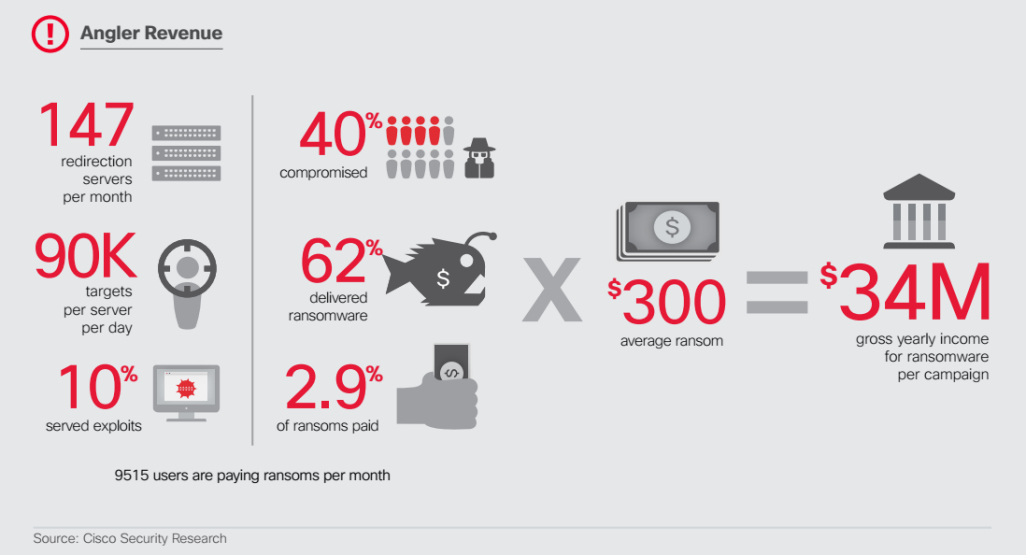
Figur 2.3: Bedre sikkerhetsmonitorering hos virksomheter med styringssystem ([59], s. 25)

2.3 Nyere utvikling innen cyberkriminalitet

Det har lenge eksistert exploit-kits tilgjengelig på det mørke nett hvor hvem som helst kan kjøpe dette. De sjekker etter kjente svakheter og kan utnytte disse. Et eksempel på et slikt kit er Angler:



Figur 2.4: Skjema fra Heimdal som beskriver hvordan et angrep med Angler foregår [77]



Figur 2.5: Figur fra en Cisco rapport i 2016 som viser hvor mye penger en angriper kan forvente å tjene[77]

Som figurene viser så er det antatt per 2016 at et slik exploit-kit kan gi mye inntekter. En stor del av årsaken er jo antall mål som blir truffet. Kun 2.9% har betalt og gjennomsnittlig betaling er på kun $300[77]. En stor del av grunnen til at gjennomsnittet er så lavt er at denne typen er angrep er kjent og ikke vanskelige å beskytte seg mot. Samtidig så er sannsynligheten for å bli truffet av et slik angrep så høy at det blir veldig økonomisk for eier av systemer som forvalter data av en viss verdi å iverksette tilstrekkelige tiltak for å ikke bli rammet av slike angrep. Det å holde seg oppdatert om slike exploit-kits som massedistribuetes er fortsatt viktig, men det er også kommet en nye trussler innenfor dette feltet i nyere tid.

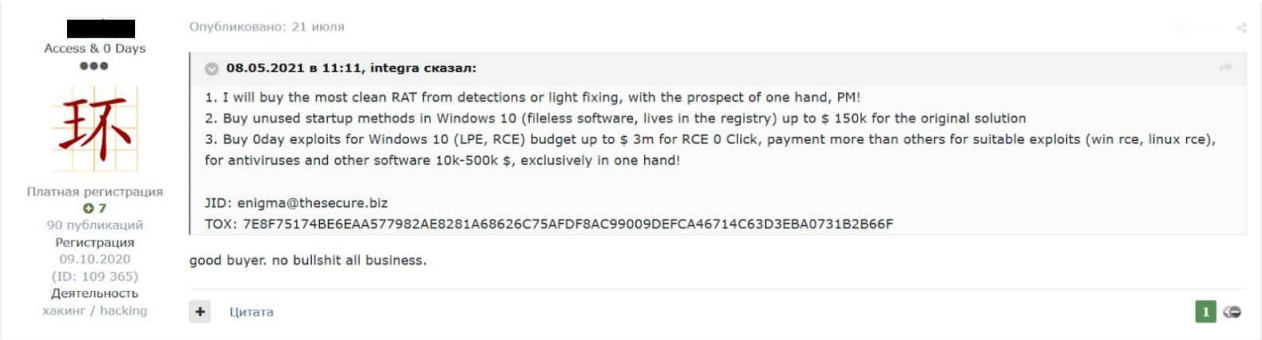
Digitalshadows har gjort undersøkelse der de hovedsaklig har hentet informasjon fra marked og forum for cyberkriminalitet. De beskriver zero-day utnyttelser som toppen av pyramiden for cyberkriminelle som ønsker å angripe et datasystem.[68] Det som er problematisk er at de observerer at grupper som driver med ransomware for økonomisk gevinst har klart å tjene inn nok penger til at de også er interessert i å kjøpe slike svakheter. Prisen er så høy at det tidligere ikke var noe slike grupper hadde råd til. En stor del av grunnen til at nettopp statlige aktører, som Russland, anses som en stor trussel mot infrastruktur er at de har ressurser til å enten kjøpe eller oppdage zero-day svakheter selv. En utvikling der kriminelle grupper som forsøker å tjene mest mulig penger i større grad har tilgang til zero day svakheter kan gi en endring i konsekvens av angrep.

2.4 Zero day utnyttelser kan i større grad bli automatisert og solgt

Angrepet på Stortinget i 2021 er antatt av Microsoft og NATO-land å være utført av en grrupper tilknyttet kinesiske myndigheter[1]. Gruppen brukte en zero day utnyttelse i Exchange. Microsoft sier at denne gruppen har hatt som mål å innhente innformasjon innenfor en rekke områder både i privat og offentlig sektor. Denne type angrep er altså ansett for å være spionasje. Gruppen Hafnium, som er antatt å stå bak angrepet, regnes som en APT-gruppe som typisk vil forsøke å unngå å bli oppdaget slik at de kan ha tilgang så lenge som mulig. Selskapet Volexity var det andre selskapet som rapporterte svakheten til Microsoft. Volexity sier at de så en endring i oppførsel etter oppdatering kom fra Microsoft hvor angriperne som før kun hadde eksfiltrert e-mailer nå forsøkte å bevege seg videre og ta kontroll over flere systemer. Det øker risikoen for å bli oppdaget, men som Volexity sier så er det irrelevant siden de vet at det uansett vil bli oppdaget innen kort tid.[35]. De startet også å scanne internet for å finne flest mulig mål å angripe som betyr at selv selskap som oppdaterte samme dag Microsoft kom med oppdatering ble rammet. [6]

Typisk vil en slik svakhet miste verdien etter sikkerhetsoppdatering og kanskje ende opp i et exploit-kit på et senere tidspunkt. Det at grupper som driver med eksempelvis ransomware har mer penger og at det blir observert at zero-day svakheter selges på forum for cyberkriminelle betyr at disse statlige APT-gruppene ikke bare kan selv endre taktikk og prøve å få mer kontroll over systemer men også selge koden de bruker for å utnytte svakheten. Det er vanskelig å vite akkurat hva som skjedde i dette tilfellet, men vi vet at det var en stor økning i angrep mot Exchange-servere etter Microsoft publiserte svakheten. I praksis var det et veldig kort tidsrom på 24 timer på å oppdatere eller mitigere denne svakheten for å beskytte seg mot angrep fra vinningskriminelle. Angrep fra Hafnium derimot skjedde før og rett etter oppdatering ble kjent.

Selskapet Acer ble angrepet 5. Mars av ransomware-gruppen REvil med krav om $50 millioner.[1] Det er fult mulig at denne gruppen har funnet ut hvordan de kan utnytte svakheten basert på CVE-rapporten fra Microsoft, som og er grunnen til at den ikke blir publisert før Microsoft hadde fikset problemet. En slik kode med noen feil ble og publisert på Github av en sikkerhetsforsker den 10. Mars som viser at det var mulig å oppnå på kort tid. Det er derimot ingenting som tilsier at Hafnium ikke kunne lagt ut og solgt denne svakheten som et exploit-kit med en gang Microsoft publiserte sin oppdatering. Det er ikke viktig om REvil selv skrev kode for å utnytte svakhet eller om den ble kjøpt. Problemet er at ransomware-grupper er observert aktive på forum klar til å betale mye penger for slike svakheter. Det åpner jo og for angrep før 24 timer.



Figur 2.6: Trusselaktør som tilbyr penger for diverse svakheter fra Digital Shadows undersøkelser[68]

Det er også observert diskusjon rundt å lære fra den komersielle sektoren og tilby det som Exploit-as-a-service. Det er usikkert hvordan det skal fungere i praksis, men det viser et større fokus på å i større grad selge svakheter. Her kan det også være at en gruppe oppnår tilganger i et system og selger tilgangen videre til noen som da står fritt til å installere skadevare som ransomware, botnet, cryptominer osv. Det kan også være industrispionasje[25]. Effekten er uansett at det blir lettere for angripere å utføre angrep. Spesielt for angripere som gjerne mangler teknisk kunnskap til å gjennomføre mer avanserte angrep. Det kan øke både mengden av denne typen angrep. Økninger in-

nen cyberkriminalitet kan gi veldig store utslag, at angrep mot autorisasjon steg første år under korona er et eksempel på det. Det har vært flere angrep som denne Exchange svakheten og SolarWinds som raskt kunne forårsaket mye mer direkte økonomisk tap om angrepene sitt primærmål var å distribuere ransomware eksempelvis. Nettselskaper kan her risikere både å bli tilfeldige mål i større grad, men også at denne typen angrep rettes mot infrastruktur fordi angripere vet at infrastrukturleverandører forvalter store verdier og har stort tidspress når det kommer til tilgjengelighet. Et eksempel er angrepet på Colonial Pipes i USA [8] hvor løsepenger ble betalt innen få timer etter filer ble låst og oljeledninger ble stengt. Hvis zero day svakheter benyttes i økende grad til å tjene penger i tillegg til spionasje vil det øke risiko for kostbare hendelser i strømnettet.

Del III

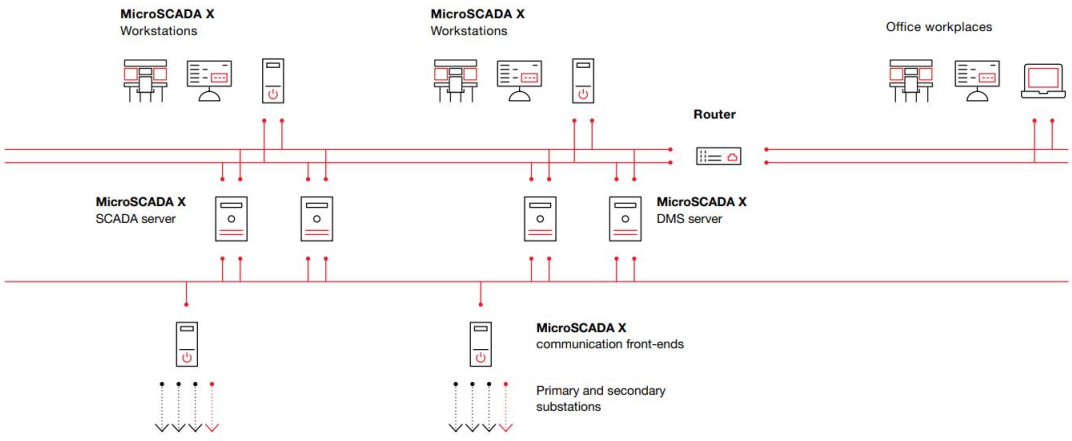
Risikovurdering

Kapittel 3

Systembeskrivelse

3.1 Løsninger og systembeskrivelse fra leverandører

Produkter som blir tilbudt av Hitachi ABB Power Grid:
MicroSCADA X er en løsning som primært kombinerer SCADA med DMS, men løsningen er samtidig modulær og benytter seg av internasjonale standarder for kommunikasjon. Det vil dermed ikke være et problem å integrere flere løsninger, f.eks Head-end system for AMS målere. Det finnes en segregering mellom PCer på kontoret og systemet ellers. Det er illustrert med en brannmur, og det er også dette som beskrives i brosjyre til systemet som sikkerhetstiltak. Det står at data som mange trenger tilgang til kan plasseres utenfor DMS-SCADA domenet slik at du kan begrense antall ansatte med tilganger i DMS-SCADA system.[23]

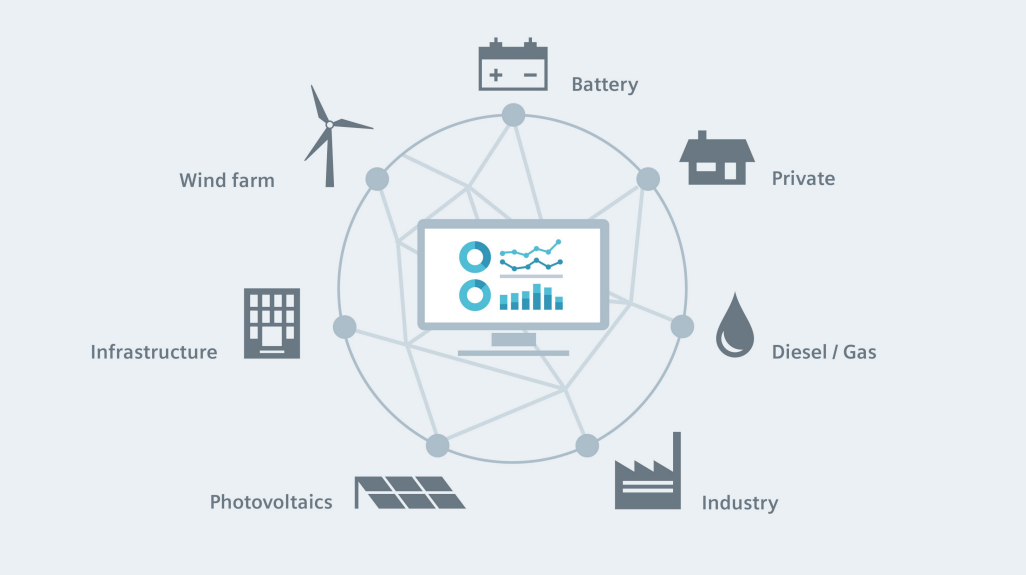


Figur 3.1: Hitachi ABB MircoSCADA X plantegning for nettverkstopologi([23], s. 10)

Det er levert en slik type transformator med denne type programvare installert i Norge[21] Her er det ikke brukt annen programvare enn det de tilbyr for overvåking og status for selve transformatoren. Bare med den type programvare vil det sendes betraktelig mer data inn til en sentral database og data vil her bli prosessert. Det vil og være veldig enkelt for Tensio TN å utvide funksjonalitet og koble denne trafoen mot andre systemer, eller bruke DMS programvare fra ABB hvor de importerer data fra andre transformatorer. ABB har en produktlinje som heter SAM600 som kan konvertere data innsamlet fra det de beskriver som konvensjonelle måleenheter til IEC 61850-9-2 standard som muliggjør sending av data fra ikke-digitale trafoer inn til DMS server.[31] [24]

ABB tilbyr og produkter som Lumada APM[22] Denne programvaren samler inn data og basert på det gir prognoser på når noe kan gå galt, eller hva som kan skje som følge av en handling samtidig som det gir diagnose for utstyr. Programvaren har også et "Open Model Interface" som gir tilgang til integrasjon fra 3. part.

Produkter som blir tilbudt av Siemens:
Siemens har på sine nettsider mye fokus på microgrids. Programvaren Spectrum Power er og markedsført som det, samtidig så påstås den å være både skalerbar og ha integrering av både digitale trafoer og SCADA systemer[56] så det er uklart om den også kan brukes av et kraftselskap for hele infrastrukturen. Beskrivelsen Siemens oppgir er ikke veldig ulik prosjektet Elnett21[15] og akkurat som i Elnett21 er også fjernvarme med i systemet her i tillegg til ren strøm.



Figur 3.2: Siemens Microgrid systembeskrivelse[57]

Her har også Siemens lagt til private husstander som en del av nettverket. Her vil AMS målere i private husstander være måten nettet kan kommunisere i begge retninger med

private husstander. Systemet er basert rundt et datasenter som tar inn store mengder informasjon både fra komponenter i nettet og større bruk av IoT for å samle inn flere målinger, men også data eksternt. Eksempelvis vil meteorologiske data som kan hentes fra API være relevant her. Det gjøres anslag for både kraftproduksjon og forbruk og så lages en optimalisert plan i forhold til fordeling av strømforbruk. I Elnett21 er både utenriksterminal for skip, Fiskepiren hvor alle båter for person/bil-transport fra Stavanger går fra samt Sola lufthavn en del av prosjektet så her er det og mulighet for å se på rutetider. Avinor har mål om at alle innenlands flyvninger skal være elektriske innen 2040 med estimert 2.5 MW per ladepunkt og Fiskepiren sitt estimerte behov er 8 MW. [38]

Det er slike behov sammen med en sterk økning i fornybar energi hvor en ikke kan kontrollere produksjon samt en kraftig reduksjon i priser på batterier som Siemens bruker som argument for å velge slike løsninger.

I Statnett sin digitalisering og automasjon av nettet holder de på å utvikle et åpent marked for kjøp og salg av aFRR [61] Her vil et system som beskrevet av Siemens her kunne ta med priser for salg av reservekapasitet i nettet tas med i kalkulasjoner for hva som er optimal fordeling og forbruk av strøm. I Nordflex prosjektet til Statnett er det for private husholdninger beskrevet spesielt varme og lading som områder som kan kobles ut i korte perioder og selges som reservekapasitet. Det vil gi fordel i form av mindre belastning i nettet, lavere strømregning for strømkunder da strømkutt skjer typisk i periode med høyt forbruk som også vanligvis er fulgt av høy strømpris. Samtidig kan og kraftselskap få betalt for å ha tilgjengelig automatisk reservekapasitet til å stabilisere nettet.

3.2 Leverandører kommuniserer udokumenterte påstander om sikkerhet ved produkter

Økt digitalisering av infrastruktur og sammenkobling av systemer gir økt eksponering til internett samt at mens en tranformator før ikke var koblet til internett i det hele tatt kan den nå bli det. En sammenkobling mellom systemer betyr ofte, men ikke nødvendigvis at en åpning i et system kan føre til at alle systemer blir kompromittert. Dette er selvfølgelig avhengig av hvilket system og barrierer som eksisterer mellom systemer.

Siemens skriver spesielt mye om sikkerhet på sine nettsider. De hevder også at deres system med microgrid er sikrere, men ikke i forhold til hva [58] Det argumenteres med at om du har det rette kontrollsystemet så er du mer beskyttet, men ingen argumenter for hvorfor deres kontrollsystem er sikrere. Det er også slik at både redundans i forhold til servere og det Siemens kaller "Advanced cyber security" er valgfrie ekstravalg for deres Spectrum Power programvare. I forhold til IT-sikkerhet så burde all programvare leveres konfigurert for høyest mulig sikkerhet. Det vil i dette tilfellet si at valgfri ekstra

redundans og sikkerhet skal være standard, mens ekstra funksjonalitet er deaktivert og en har en vurdering i forhold til risiko før en beslutter å aktivere mer funksjonalitet. Siemens skriver også om sertifiseringer de har oppnådd for diverse standarder innenfor innformasjonssikkerhet som ISO/IEC 27000, slik sertifisering sier bare noe om at de følger en standard for hvordan de jobber med IT-sikkerhet og ikke egentlig noe om hvor sikkert systemet er. Siemens opplyser ikke om at disse sertifikatene ikke i seg selv er noe sertifikat for hvor sikkert systemet er.

Fra leverandøren sin side er det altså ikke opplyst noe om ekstra sikkerhetsutfordringer ved integrasjon av disse systemene. Det finnes heller ingen vurderinger for risikomomenter ved disse produktene. Det finnes heller ingen argumenter for hvorfor deres system skal være sikrere mot angrep over internett. En stor beskymring er jo og supply-chain angrep hvor konsekvensen kan øke om flere systemer er koblet sammen. I SolarWinds angrepet hadde Orion-programvaren i noen tilfeller tilgang til Active Directory fordi den var ansett som programvare som en kunne stole på. Det gav angriperne tilgang til disse alle kontoer for domenet [26]. Tilsvarende for et DMS-system som bruker Active Directory så kan en se for seg noe lignende hvor angriper da kan logge inn som administrator i kontrollsystemet. De vil da også kunne oppnå denne tilgangen i alle andre systemene også inkludert SCADA. I dette tilfelle vil Siemens sin eksterne sikkerhet ikke kunne klare å beskytte mot angrepet. En av funksjonene Siemens spesielt trekker frem er deres tjeneste for å generere digitale sertifikater. Med sentral automatisk generering av sertifikater følger det derimot også at serveren som kjører denne programvaren må være godt sikret, med SolarWinds så kom den skadelige koden rett fra deres servere og var signert.[69] Et digitalt sertifikat er altså ingen garanti for at det ikke inneholder skadelig kode.

Også ABB Powergrids sitt system er veldig avhengig av ekstern sikring. Her trekkes og autorisasjon frem som et viktig element. De har satt opp en liste med IT-sikkerhetstiltak:

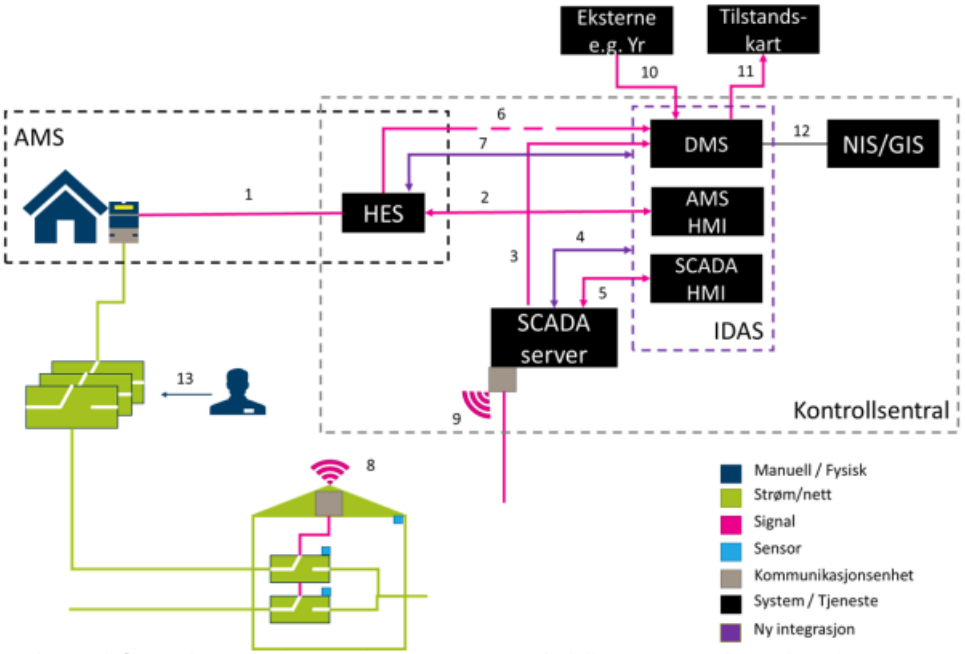
- Autentisering av bruker og ansvarsområde
- Sentralisert håndtering av brukere
- Fleksibel autorisasjon av brukere
- Tidsbegrensede tilganger
- Kryptering av kommunikasjon
- Logging av hendelser og bruker-aktivitet
- Rapportering

De skriver videre at MicroSCADA X kan utstyres med det de kaller industristandard malware og IPS løsninger. Eksempel på dette er virusbeskyttelse og liste over godkjente programmer([23], s. 10-11). Selv om de mener disse løsningene er

industri-standard er det altså ikke standard for deres produkt, men tillegsvalg. Ellers er det veldig lignende Siemens sine løsninger hvor en plasserer sikkerhet i brannmur for å beskytte mot et ekstern angrep og mener det er tilstrekkelig. Videre skriver de "Modern security technologies, such as commercial firewalls ensure continuous system security and prohibit malicious attacks and unauthorized access". Her er det klart at de mener brannmurer fra andre leverandører gjør at angrep ikke kan skje og at ingen som ikke skal får tilgang til systemene. Akkurat som med Siemens blir ikke sikkerhetsutfordringer ved integrering nevnt. Det er heller ingen grunnlag for påstander om at brannmur er tilstrekkelig. Som de selv nevner er jo disse brannmurene og løsningene kommersielt tilgjengelig og blir brukt av virksomheter i dag, likevel opplever virksomheter datainnbrudd. Her mangler det forklaring på hvordan bruk av de samme løsningene skal kunne beskytte strømnettet.

3.3 Systembeskrivelse fra Sintef-rapport om integrasjon av AMS, DMS og SCADA

Sintef har i sin rapport til NVE laget en skisse av et system som integrerer NIS/GIS i DMS, samt at HES og SCADA også blir integrert.[19] Dette er en integrering som rapporten beskriver finnes enkelte steder i Europa. Leverandører har også løsninger for dette som de ønsker å selge som tidligere beskrevet. Her er DMS integrert med grensesnitt for styring av AMS og SCADA-server. Det gir en sentral styring av alt i nettet hvor leder for kobling som sitter i driftssentral hos nettselskap også kan gjøre endringer i SCADA-system og AMS-målere. Fordelen her er at all informasjon samles og kan behandles et sted. Det vil både gi god situasjonsforståelse og mulighet til å styre alt i nettet fra samme sted. Det åpner også for automatisering i nettet siden all informasjon er tilgjengelig.



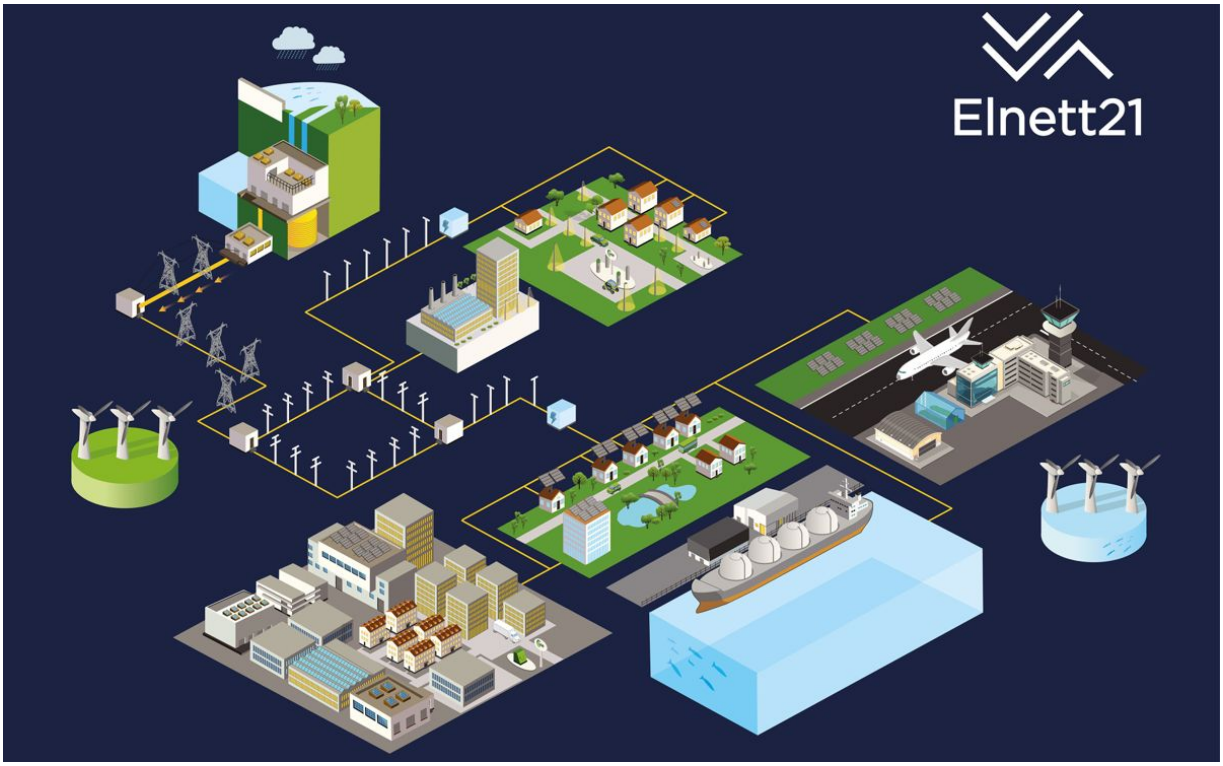
Figur 4 Høynivåbeskrivelse av integrasjonen mellom AMS, SCADA og DMS. De lilla pilene, samt den stiplede boksen som utgjør IDAS, viser den økte integrasjonen.

Figur 3.3: Systembeskrivelse fra Sintef-rapport

I denne figuren har DMS også flere integreringer enn tidligere for å modellere eksisterende tilkoblinger, men også nye tilkoblinger som kan komme. Her kan det være en del ulike løsninger som blir valgt spesielt når det kommer til tjenester som blir integrert.

3.4 Eksisterende og fremtidige smartgridløsninger fra nettselskap

Nettselskapene har også prosjekter for å forbedre nettet for å takle fremtidige utfordringer. Det er viktig å ta med hva nettselskapene ser for seg innen utvikling og hva de ønsker. AMS-målere både for husholdninger og bedrifter er veldig relevant i forhold til utviklingen. De har både en viktig rolle innenfor microgrid-løsninger og fleksibilitet. Et element i microgrid er lokal strømproduksjon som kan gå inn i nettet, dette finnes det allerede støtte for i AMS som kan automatisk selge overpdousksjon. I dag kan AMS-målere styres fra et HES, men DMS-systemet hvor en får inn informasjon og har kontroll over nettet har ikke mulighet for å sende styringssignaler til AMS. For å møte utfordringer som komme kan en slik integrasjon bli nødvendig.



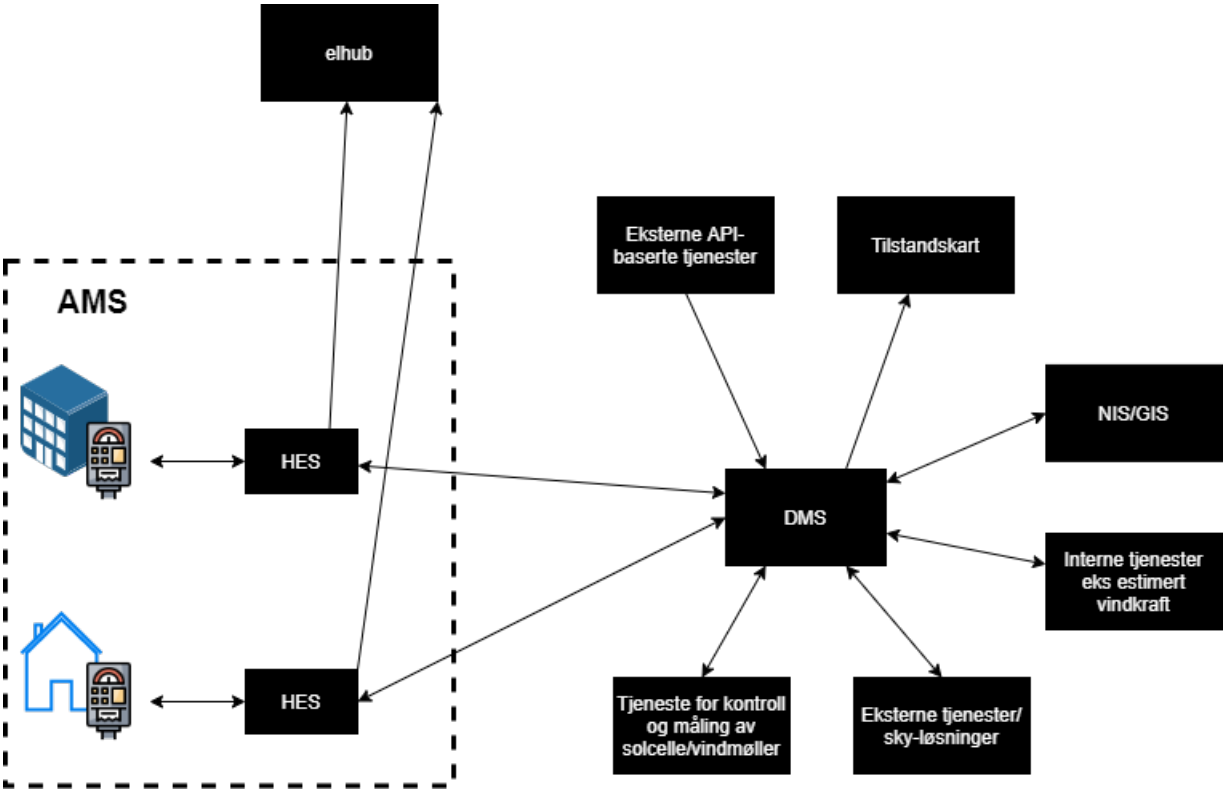
Figur 3.4: Figur fra Lyse sitt Elnett21 prosjekt som viser eksempel på microgrid-prosjekt som foregår på Nord-Jæren

I tilegg til integrasjon mot HES vil en gjerne ha behov for flere typer tjenester som integreres med DMS. Digitale transformatorer vil og være et viktig element i et slikt system. Tjenester kan inkludere programvare for å estimere produksjon lokalt fra fornybar energi både en dag i forveien og 1 time, 1 minutt osv og sette det opp mot estimert forbruk. Digitalisering vil gi mye tilgjengelig data som muliggjør maskinlæring som da kan kutte kostnader ved å optimalisere nettkontroll basert på disse estimatene. Samtidig vil det gi flere verktøy til å sørge for stabilitet når en introduserer mer vind og sol som har store svingninger i produksjon sammenlignet med vannkraftverk. Det er også her styring mot AMS målere i private hjem kommer inn. Det er allerede forsøk med forbrukerfleksibilitet i Norge for bedrifter hvor nettselskap kan begrense strømtilførsel i perioder. Basert på fremtidsutsikter legger jeg også inn at husholdninger i stor grad skal være en del av fleksibilitet. Enkelthusstander utgjør lite forbruk alene så automatisk frekvensrespons for husstander må bli automatisert. Smartstyring fra andre leverandører i private hjem som benytter data fra HAN-port i AMS måler og styrer etter optimal strømpris er ikke inkludert i systembeskrivelsen. Grunnen er at disse ikke styres av nettselskapene. Det kan likevel være mulig at de kan integreres med Statnet sitt marked hvor de kjøper fleksibilitet.

Elvia har identifisert fleksibilitet i lavspenningsnettet lokalt som et området de kan spare 1,1 milliarder over 10 år i sitt nett alene. [16] Varmtvannsbereder i artikkelen er derfor koblet til en Azure cloud-løsning for å hente informasjon om lokal transformator og overføringskapasitet.[33] Et slikt system vil være naturlig å integrer mot DMS, siden DMS kan hente inn målinger fra lokale digitale trafostasjoner og AMS-målere. Denne løsningen addresserer også utfordringer lokalt i lavspentnettet, mens Statnett kjøper fleksibilitet i prisområdene NO1-NO5. Slike løsninger fra nettselskap i samarbeid med andre aktører kan som Elvia sin kostnadsberegning viser bli viktige for smartgrid. Denne løsningen er ikke med i systembeskrivelsen jeg har laget. Her brukes hverken tilkobling til HES eller AMS fra DMS for å oppnå denne kontrollen. DMS kan her samle inn relevant informasjon, prossesere, og så laste opp resultatet. Det gir DMS en indirekte kontroll over enheter i husholdninger uten at DMS kan angripes fra disse kontrollenhetene. En slik modell gjør at det ikke er behov for DMS å kunne sende kontrollsignaler til AMS-målere. Jeg kommer derfor til å diskutere dette alternativet i konklusjonen.

3.5 Systemmodell for sårbarhets og risikoanalyse

Systemmodell valgt for denne oppgaven:



Figur 3.5: Systembeskrivelse for risikovurdering

I systembeskrivelsen jeg har valgt er hovedforskjellen fra beskrivelse i Sintef-rapport at SCADA ikke er inkludert. Hovedgrunnen til dette er inspill fra nettselskap i InterSecure-prosjektet om at integrasjon av SCADA med DMS ikke er en del av plan for smartgrid. SCADA-systemer er sårbare og det finnes skadevare eksempelvis brukt mot Ukraina som er laget for å sette kraftverk ut av drift[36]. I forhold til smartgrid er ikke automatisk kontroll av vannkraftverk nødvendig for å løse utfordringer. Grunnen er at vannkraftverk ikke kan benyttes til øyeblikkelig frekvens-respons. Vannkraft kan fortsatt brukes til å stabilisere nettet for reserver som bruker lengre tid på å levere strøm til nettet. Det gjør det fult mulig å styre kraftverkene manuelt. Lovkrav om sikkerhet for SCADA system vil også gjelde for hele systemet som gjør at besparelsene må være store for at en slik integrasjon skal bli økonomisk.

Jeg har også lagt til flere tjenester som kommuniserer med DMS. Dette er eksempel på tjenester som kan brukes i smartgrid. Estimering av vindkraft vil eksempelvis være viktig for å jevne ut topper i forbruk og produksjon. Dette må sees i sammenheng med informasjon i DMS som har kontroll på linjekapasitet og topologi. AMS er visualisert som et system for husholdninger og et system for større kunder. Grunnen til det er at flere nettselskap har prosjekter sammen med bedrifter der nettselskap direkte kan kontrollere forbruk hos kunde, men ikke lignende hos private husholdninger. Sikkerhet

lagt til grunn for modellen er slik som er beskrevet av ABB og Siemens.

Del IV

Risikovurdering

Kapittel 4

Risikovurdering av systembeskrivelse

4.1 Metode for risikovurdering

Basert på dette vil jeg foreta en risikovurdering basert på ISO/IEC 27005. Det vil være en kvalitativ vurdering med sannsynlighet vurdert på en skala fra 1-4. Basert på systembeskrivelse vil det være en systemsentrisk risikovurdering. Risiko oppnås ved å legge sammen sannsynlighet og konsekvens og er mellom 2-8. Konsekvens på 4 betyr en stor andel eller alle kunder blir frakoblet strøm. Konsekvens 1 betyr mindre kostnader og ressursbruk for å fortsette drift. Sannsynlighet 4 betyr at det er stor grunn til å forvente at en hendelse skjer hvertfall en gang innen en tidsperiode på 1-3 år. Mal for vurdering er fra emnet IN5080 – Sikkerhets- og risikostyring ved UiO. [34]

Her finnes det argumenter for å ikke evaluere utifra frekvens for et angrep eller sannsynlighet for en hendelse i det hele tatt. Hvis en eksempelvis antar at en angriper via supply-chain angrep har tatt kontroll over et HES med kontroll over alle tilknyttede AMS målere og disse kan alle bli slått av er det en veldig alvorlig hendelse. Da blir det selvfølgelig et spørsmål om det er relevant om den årlige sannsynligheten er 1% eller 10%. Her kan det tenkes det kunne vært mer relevant å sette en sikkerhetsklasse for bryterfunksjonaliteten i AMS-målere heller en enn å basere sikkerhetstiltak på total risiko. En sikkerhetsklasse vil i praksis være ganske likt det som allerede eksisterer i kraftberedskapsforskriften om ekstra krav til det som regnes som driftskontrollsystem.

Nr.	Trussel	Sårbarhet	Sikkerhetshendelse på verdier	Konsekvenser	R-nivå		
					S	K	R
1	Ekstern kompromittering av programvare som brukes i nettet i dag, eksempelvis DMS og HES.	Et angrep mot en leverandør kan gi angriper mulighet til å legge inn skadelig kode i programvare som så blir sendt til kunde som oppdatering. Svakheter kan gi angripere muligheter til å angripe DMS eller HES direkte.	Tilgjengelighet i nettet er den viktigste verdien som kan bli berørt her. Kontroll over DMS og HES kan gi angriper mulighet til å utføre handlinger i nettet eller gjøre systemene utilgjengelige.	Ytterste konsekvens er at angrepet fører til delvis eller fullstendig nedstegning av nettet og at DMS og HES system blir gjort utilgjengelige. Det kan få juridiske konsekvenser og vil fø økonomiske konsekvenser knyttet til gjennoppretning av system og KILE.	4	4	8
2	Ekstern kompromittering av ny programvare som integreres i internnettet, eksempelvis programvare basert på maskinlæring for estimering av forbruk og produksjon.	Et angrep mot en leverandør kan gi angriper mulighet til å legge inn skadelig kode i programvare som så blir sendt til kunde som oppdatering. Svakheter kan gi angripere muligheter til å angripe direkte.	Tilgjengelighet for sekundære tjenester kan bli brutt, det samme gjelder integriteten til informasjon fra disse tjenestene.	Integrering av diverse tjenester internt sammen med DMS og HES vil gi angriper mulighet til å også fortsette angrep internt og oppnå kontroll over DMS og HES. Her blir konsekvens det samme selv om konsekvensen av angrep mot sekundærtjenester i seg selv ikke er like alvorlig.	4	4	8
3	DDoS angrep som gjør at HES/DMS ikke klarer å kommunisere eksternt mot internet og AMS, digitale transformatorer.	Alt som er koblet til Internet kan bli offer for et DDoS angrep	Tilgjengelighet av tjenester som elhub, vær-API osv. samt sensorer og målere.	Mangel på informasjon kan gi noe mindre optimalisering av nett og produksjon. Elhub har frist på 24 timer for innlevering av forbruk fra AMS måler.	2	1	3
4	IT systemer og IoT har kortere levetid enn det elektromekaniske når det kommer til sikkerhet som gir mange nye angrepsflater inn mot DMS hvis det ikke holdes oppdatert.	IT systemer baserer seg på teknologi som er i rask endring og kan bli utdatert, eksempelvis kan kryptering som blir benyttet ikke være tilstrekkelig lengre om 10-25 år. Samtidig vil det elektromekaniske vare 30-70 år og IoT enheter kan ende opp med å ikke bli oppdatert eller byttet før de blir en sårbarhet.	Både tilgjenglighet av IoT enheter i nettet, tilgjengelighet av transformatorer og integriteten til informasjon som blir sendt kan bli brutt. Kommunikasjon fra AMS måler kan også bli dekryptert og er da brudd på konfidensialitet og personvern.	En IoT enhet med en svakhet kan gi en angriper tilgang til en transformator eller kun enheten i seg selv. Feil informasjon kan føre til at transformator blir tatt ut i drift for inspeksjon for å hindre skade på transformator. Tiltak som utbyttbar kommunikasjonsdel på AMS målere senker konsekvens betydelig. Ytterste konsekvens er at IoT enheter brukes til å angripe DMS systemet.	4	4	8

Figur 4.1: Tabell av risikovurdering del 1

Nr.	Trussel	Sårbarhet	Sikkerhetshendelse på verdier	Konsekvenser	R-nivå		
					S	K	R
5	Brudd på autorisasjon som gir tilganger i internnettet	Hvis angriper klarer å autorisere seg som en eksisterende bruker kan de få tilgang i internnettet hvor de videre kan bevege seg og oppnå flere tilganger.	Hvis angriper får systemtilgang overalt vil det være brudd på alle verdier.	Hvis en angriper klarer å omgå autorisering og oppnå tilganger til DMS og/eller HES så vil det ha alvorlige konsekvenser. Avhengig av hvilke tilganger som oppnås kan det bli like store konsekvenser som hvis programvaren sin kildekode er kompromittert	3	4	7
6	Ekstern tjeneste kompromittert, eksempelvis programvare som kjører i en skyløsning og kommuniserer med DMS	Ekstern tjeneste kan bli angrepet og modifisert informasjon kan bli sendt til DMS. Informasjon kan også være utilgjengelig hvis ekstern tjeneste eksempelvis blir rammet av ransomware.	Tilgjengelighet for ekstern tjeneste og integritet av informasjon kan bli brutt.	Hvis en tjeneste som estimerer strømforbruk eller behandler informasjon og gir tilbakemelding om vedlikehold i nettet enten blir utilgjengelig eller informasjon blir modifisert så vil det ha mindre effekt på drift av nettet.	2	2	4
7	Utro tjener	Ansatte kan av ulike grunner hjelpe en angriper å oppnå tilganger i systemet som kan utnyttes.	Her vil spesielt konfidensialitet i form av spionasje eller industrispionasje være relevant. Sabotasje som går utover tilgjengelighet i nettet er også et mulig mål.	Konsekvens vil være avhengig av hvilke tilganger utro tjener har. Hvis det er noen med tilgang til DMS system så kan konsekvens blir svært alvorlig	2	4	6
8	Kompetansemangel for gamle styringssystemer og teknologier.	Kompetansemangel for system og teknologier kan gjøre arbeid med å konfigurere og sikre eldre deler av nettet vanskelig. Det kan også være en utfordring hvis system må gjenoprettes etter et angrep.	Her vil spesielt tilgjengelighet for systemer være påvirket.	Mangel på kompetanse kan resultere i feilkonfigurasjon og manglende sikring av eldre styringssystem og teknologier. Det kan også gjøre kostnad ved å gjennopprette systemer etter et angrep høyere. Dette gjelder spesielt på grunn av KILE-kostnader.	2	3	5

Figur 4.2: Tabell av risikovurdering del 2

4.2 Grunnlag for risikovurdering

4.2.1 Supply chain og zero day sårbarheter, grunnlag for nr 1 og 2

Det har vært flere større angrep basert på enten supply chain som SolarWinds eller zero day som i Outlook. Utifra dagens trusselbilde er det heller ingenting som tilsier at det blir mindre av den type angrep. Det er umulig å spå fremtiden, men så langt er trenden stadig økning i antall angrep. Det kan og være snakk om økning i størrelsesorden 50-100% slik det var mot autorisasjon første år med korona. Sannsynligheten for at en hendelse skjer er her satt til øverste nivå 4. Det vil ikke bare gjelde systembeskrivelse jeg har lagt frem her, men også for dagens systemer. I min systembeskrivelse vil det i praksis være lite forskjell på trussel 1 og 2 her. Grunnen er at det ikke er lagt inn noe intern sikkerhet eller segregering i modell, likt det som blir presentert av Siemens og ABB power Grids. Konsekvens er her altså lik og på høyeste nivå for begge. Det er både fordi utkobling i hele eller deler av nettet er alvorlig i seg selv for kunder men også rent økonomisk for nettselskap i stor grad på grunn av KILE fra forskrift om kontroll av nettvirksomhet paragraf 9 [30].

4.2.2 DDoS-angrep

Et DDoS angrep er noe som både kan utføres av aktører med eksempelvis IoT botnet som Mirai[5] men det tilbys også som en tjeneste mot betaling. Det gjør at DDoS er svært tilgjengelig og blitt et vanlig angrep for tjenestenekt. Derimot er de aller fleste DDoS angrep både små og varer kun kort tid. Ifølge Clouflare er 97% av angrep under 500 Mbps og 98% varer kortere enn en time av nettverk DDoS-angrep mot lag 3/4 i OSI modellen. [76]

Selv om denne typen angrep altså både er svært vanlige og tilgjengelige så trengs det ikke mye beskyttelse for å mitigere effekten av de angrepene med lavt volum. Selv om angrep skulle være velykket vil heller ikke tjenestenekt på 1 time være problematisk siden AMS målere lagrer data og HES ikke behøver å sende inn data til Elhub med en gang de blir mottatt. Det kan ha større konsekvenser for digitale transformatorer hvis disse er eksponert mot internet. Samtidig har ikke-digitale transformatorer aldri kontakt med DMS og det vil naturligvis være rutiner som sikrer drift av nettet om en mister kontakt av naturlige årsaker som også kan brukes ved eventuelt DDoS angrep. Konsekvensen blir også begrenset her fordi nettselskap kan alliere seg med andre, eksempelvis internettleverandør for å håndtere et angrep. Hvis angrep likevel skulle overskride kapasitet til internettleverandør er det mulig å få hjelp av selskap som Cloudflare som har mitigert verdens største DDoS angrep uten avbrudd i tjeneste hos kunder[75]. Jeg har vurdert sannsynlighet til 2 fordi det finnes flere store botnet som brukes aktivt. Sannsynlighet er her basert på et større angrep som varer flere timer eller dager. Små eller korte DDoS-angrep er mye vanligere men med litt tiltak vil de ikke påvirke drift. Jeg har satt konsekvens til 1 fordi det ikke er realistisk at et angrep vil føre til stor skade eller ekstrakodstnader. Det gjelder spesielt siden angrep ofte er veldig tidsbegrenset.

Det finnes også løsninger som kan fullstendig mitigere om det skulle bli et problem.

4.2.3 IT og IoT-systemer har kortere levetid enn elektromekaniske

Elektromekaniske systemer har levetid på 40-70 år[66], men det samme gjelder ikke for IT systemer. Det største problemet er mangelen på oppdateringer hvor en kan se til eksempelvis Windows XP[74] hvor sikkerhetsoppdateringer var tilgjengelige i 13 år. En stor del av grunnen til at sikkerhetsoppdateringer fortsatte 6 år etter siste versjon var nettopp at mange bedrifter og det offentlige hadde diverse systemer hvor en så for seg lengre levetid enn både 7 og 13 år. Eksempelvis så både den britiske og nederlandske regjering seg nødt til å betale Microsoft ekstra for utvidet støtte. Problemet er enda større om både operativsystem og programvare slutter å få sikkerhetsoppdateringer men er nødvendige for drift i en fabrikk eller strømnett osv hvor en kan måtte bytte ut elektromekaniske deler av nettet om en skal bytte IT-system som fort gjør at det ikke er økonomisk å bytte disse. Det behøver heller ikke å være et problem om disse PCene ikke er tilkoblet internet og har god fysisk sikkerhet.

Grunnen til at både sannsynlighet og konsekvens er satt til 3 her er gitt en utviklet hvor en digitaliserer mer, samt integrerer flere systemer. Spesielt når en legger til IoT enheter som en da integrerer med det elektromekaniske. AMS målere er jo eksempel på dette og hvis de skulle måtte byttes ut eksempelvis etter 15 år pga en svakhet, mangel på oppdatering ol. Installasjonen kostet 9 milliarder kroner på landsbasis. [78] Bare en av trafostasjonene i Lnett sitt prosjekt for å utbedre overføringskapasitet koster 200 millioner med 3 transformatorer. Totalt er prosjektet beregnet til 10 milliarder kroner.[67] Det er gjort tiltak i dag for AMS målere fra Aidon eksempelvis hvor kommunikasjonsdel er mulig å erstatte da den er ansett til å ha kortest levetid slik at måleren får forlenget levetid med en mindre kostbar ettermontering. [2]

Likevel er det en del utfordringer knyttet til ulik forventet levealder, en uskifting av kommunikasjonsdel avhenger eksempelvis av at Aidon har den klar hvis det skulle bli behov for det. Det er og en mulig utfordring med at mens Aidon har kunder innen bransjen og er klar over forventninger til levetid så lager eksempelvis ikke Microsoft operativsystem basert på støtte i 30 år. Det kan også bli en utfordring med nye aktører som er mer fokusert på teknologi og ikke er tradisjonelle leverandører av elektromekaniske deler slik ekempelvis Siemens og ABB er. Samlet sett gjør det at både sannsynlighet og konsekvens her blir relativt høy og jeg har satt både sannsynlighet og konsekvens til 4. Konsekvens er satt til 4 fordi systembeskrivelsen min ikke har noen intern sikkerhet. En utdatert IoT enhet med kjent sårbarher vil da kunne bli en dør for angriper for å ta kontroll over DMS. Her kan det og være PCer internt i nettet som kjører utdatert OS eller programvare som gjør det lett for angriper å bevege seg internt. Sannsynlighet er basert på ny sårbarhet for noe i nettet oppstår som det ikke finnes oppdatering eller

mulighet til å fikse uten høy kostnad.

4.2.4 Angrep mot autorisasjon

Autorisasjon av brukere er et veldig viktig prinsipp innen IT-sikkerhet, samtidig er det veldig vanskelig å garantere at noen får tilganger de ikke burde hatt. Det kan gå på rutiner i systemet hvor tilganger kan gis til store grupper og inkludere personer som ikke burde hatt tilgang. Det kan og være tilganger som har blitt gitt tidligere men burde vært trukket tilbake. Det største problemet derimot er å kunne garantere at noen er den de utgir seg for. Økt bruk av hjemmekontor under korona har ført til at det enten har blitt opprettet eller stor økning i bruk av eksempelvis VPN tjeneste for å koble til internnett hvor en har tilgang til de programmer og data en trenger for jobb. Angrep mot autorisasjon på hjemmekontor er selvfølgelig ikke noe som rammer interne systemer hvor en må være på kontoret for å ha tilgang, men kan gi angriper et fotfeste i internnettet hvor de kan angripe fra. Gitt systembeskrivelse med ingen intern sikkerhet må konsekvens bli 4. Sannsynlighet er basert på at en slik hendelse skjer, forsøk på dette som phising er enda vanligere. Selv 2-faktor autentisering som blir lagt til grunn her vil ikke forhindre angrep, men gjør at sannsynlighet for en hendelse blir lavere.

4.2.5 Eksterne tjenester

Her vil det være en del ulikheter i risiko med integrasjkon av nye tjenester basert på hvordan det blir gjort. Eksempelvis vil det ikke være risikabelt med API spørringer til yr.no gitt at all annen kommunikasjon er sperret og data blir verifisert på samme måte en gjør ved lagring i en databse. Derimot vil både tjenester som er installert internt eller tjenester hvor en ikke har så restriktiv kommunikasjon som mot et API gi økt angrepsflate for å omgå autorisering i internnett til DMS og HES og gi angriper tilganger i disse systemene. Interne systemer her kan være systemer som ikke er så sikkerhetskritiske i den forstand at konsekvensen av et angrep mot denne tjenesten alene ikke er stor og det derfor er mulig å få tilgang til denne tjenesten eksternt.

Eksterne tjenester som leverer data i form av API spørring eller som XML-filer eksempelvis hvor data saniteres vil ikke ha mulighet til å få tilgang til eller gjøre noe i internnett. De er derfor ikke en direkte trussel for å ta kontroll over nett. Derimot kan det bli et problem om disse tjenestene blir angrepet og tilsynelatende opererer som vanlig men informasjon som blir oversendt er endret. Dette kan selvfølgelig også skje ved at å angripe selve kommunikasjonen. Hvis en eksempelvis da bruker en ekstern tjeneste for å beregne strømforbruk eller produksjon av vindkraft for de neste 24 timene og får feil informasjon tilbake kan dette få følger for styringen av nettet som kan gå utover stabilitet. Konsekvens er satt til 2 her da det er usannsynlig at feilaktig informasjon vil føre til store utkoblinger i nettet. Det er basert på at all kontroll ikke er automatisert, noe Statnett har nevnt som en mulighet. Konsekvensene kan da bli større.

4.2.6 Utro tjener

Utro tjener vil alltid være en IT-sikkerhetsrisiko. Det kan være ulike motivasjoner som ligger bak og kan være vanskelig å oppdage. Konsekvens av utro tjener vil og være veldig ulik avhengig av hva målet er. Her har jeg tatt utgangspunkt i utro tjener som forsøker å utgjørde en trussel mot nettet. Det kan være spionering som legger til rette for angrep eller det kan være sabotasje. I 2020 ble en ansatt i DNV GL arrestert av PST siktet for spionasje for Russland. [47] Artikkelen trekkes frem momenter fra PST sin trusselvurdering for 2020 der PST regner spionasje som en alvorlig trussel og skriver at plassering av spioner på innsiden av norske virksomheter er kjerneoppgavefor utenlandsk ettertening. Det kan også ses i sammenheng med APT-grupper som er knyttet til etteretningstjenester i diverse land. Det er derfor fult mulig at informasjon kan bli sendt til disse gruppene for å gjøre det lettere for dem å angripe virksomheten. Jeg har satt sannsynlighet til 2 siden det krever en del arbeid og ressurser å få til. Her er det derimot et viktig moment at mål ikke vil være tilfeldige så om en virksomhet er valgt ut som mål vil nok sannsynlighet for at en hendelse opstår som følge av utro tjeneste høyere. Konsekvens er satt til øverste nivå, mest fordi eksempelvis leder for kobling kan være den utro tjeneren og da ha kontroll over DMS, HES og alle AMS-målere. Siden det heller ikke er intern sikkerhet i systembeskrivelse vil noen som jobber på kontor kunne ta med USB med malware som videre kan gi kontroll.

4.2.7 Kompetansemangel

Kompetansemangel når det kommer til eldre styringssystemer og teknologier kan og være et problem. Typisk vil de som har kompetanse på dette gå av med pensjon og det vil være vanskelig å finne noen med kompetanse siden det er veldig gamle systemer. Kompetanse når det kommer til styringssystemer og teknologier er viktig for å også kunne sikre disse. Det er også den mest utsatte delen av nettverket og kan ha kjente sårbarheter, være laget med lite eller ingen sikkerhet eller lignende. Da er det viktig å vite hvordan de fungerer for å kunne sikre dem. Det er også viktig i forhold til å unngå feilkonfigurasjon. Styringssystemer og andre systemer som ikke er systemer som lagrer data kan også gjenopprettes etter et angrep ved å installere på nytt og konfigurere til original tilstand. Det krever at noen vet hvordan det skal gjøres, og kan gjøre det raskt sånn at det ikke tar flere uker å gjennoprette et styringssystem. Med mer IT i nettet så vil det også bli flere nye teknologier. Det kan også være nye teknologier som kan raskt bli utdatert som gjør at kompetansemangel kan oppstå innen få år og ikke tiår. Budsjetter er jo og begrensede og mange nye teknologier kan gi utfordringer med å ha kompetanse for alt blant ansatte. Her har jeg satt sannsynlighet til 2. Kompetansemangel kan til en viss grad planlegges for av nettselskap som er grunnen til at jeg ikke har satt den høyere. Her vil det nok være lettest for det enkelte nettselskap å selv sette sin egen verdi basert på hvilke teknologier de benytter, planlegger å bruke, samt kompetanse og alder blant ansatte. Konsekvens er satt til 3 på grunn av at kompetansemangel kan føre til manglende sikring/feilkonfigurasjon samt løpende KILE kostnader kan bli forlenget ved en hendelse som påvirker leveranse av strøm til kunder.

4.3 Samlet risiko

Samlet sett gir en slik endring med mer digitalisering og integrasjon av tjenester en klar økning av total risiko i nettet. Noen trussler eksisterer allerede i dag som supply chain-angrep, derimot vil naturligvis angrepsflaten bli betydelig større om antall programmer som kjører på internett øker. Digitalisering gir naturligvis helt nye angrepsflater i tillegg til at disse integreres inn i et felles system. Integrering øker jo sannsynlighet for å bli rammet av et angrep, men også konsekvens av angrep blir angrepet pga økt digitalisering da større deler av nettet kan kontrolleres. Flere målepunkter og informasjon om nettet er positivt for drift, men vil og utgjøre en ny sårbarhet hvis denne informasjonen modifiseres slik at det blir tatt beslutninger på feil informasjon som kan gå utover stabilitet og tilgjengelighet av strøm.

Del V

Nye angrepsmetoder krever endringer innen cybersikkerhet

Kapittel 5

Introduksjon av zero trust prinsipp

5.1 Argumenter for bruk av zero trust

For å bøte på endringer i måten angrep blir utført og også nye utfordringer er det flere som mener at en må tenke annerledes når det kommer til sikkerhetsarkitektur. Spesielt i USA så har blant annet CISA tatt til ordet for å gå over til en zero trust modell. Denne modellen er nå vedtatt at skal være implementert på føderalt nivå innen slutten av 2024[20]. Selv om ikke zero trust ikke er nytt så har modellen kommet i søkelyset i 2021 etter omfattende angrep mot både føderale myndigheter i USA og store selskaper. Angrepene skal ifølge amerikanske myndigheter være utført av grupper tilknyttet russisk etteretning[26]. Omfang av angrep alene gir ikke grunnlag for å endre sikkerhetsmodell, men alle angrepene benyttet enten svakheter i programvare fra Microsoft og VMWare eller i tilfellet med SolarWinds hvor en oppdatering til Orion programvaren ble modifisert til å inneholde verktøy for fjerntilgang. Denne typen angrep som går på leverandør av programvare og tjenester er veldig vanskelig å sikre seg imot siden angrepet skjer utenfor de systemer selskaper eller myndigheter har direkte kontroll over.

Zero Trust er en sikkerhetsfilisofi som hovedsaklig bygger på tre prinsipper:

- Ensure that all resources are accessed securely regardless of location: It is necessary to assume that all network traffic poses a potential threat until it has been authorised, inspected, and secured.
- Adopt a least privilege strategy and strictly enforce access control: Each user on the network must be restricted to having the minimal privileges necessary to perform their job, and access to sensitive resources is strictly controlled.
- Inspect and log all traffic: To ensure that users granted network access are not behaving badly, traffic must be logged, inspected, and acted upon in real-time.

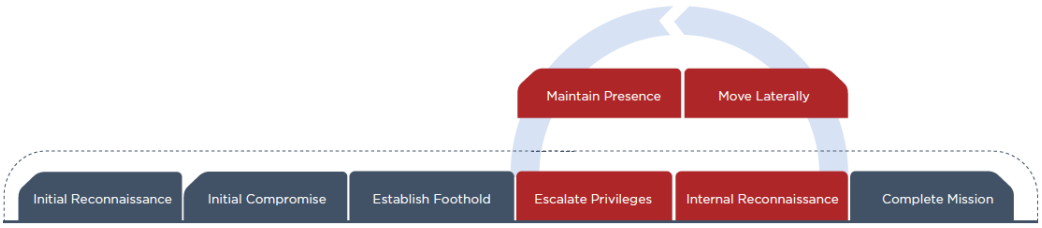
[7]
I motsetning til det Siemens presenterer der fokus er å integrere alt til et sikkert system

som da bygger mye på å sikre de yttre delene av systemet mot angrep så vil ikke dette regnes som god beskyttelse med en zero trust tankegang. I forbindelses med Senatshøringer i USA etter SolarWinds-angrepet ble administrerende direktør for sikkerhetsselskapet FireEye spurt om han annså brannmurer som effektive for å hindre angrep hvor han svarte at de hadde utført 600 red-team angrep, altså deres sikkerhetseksperter forsøker å angripe og kompromittere selskaper i en sikkerhetstest. Ikke en gang hadde brannmur stoppet angrep. [73]

I forbindelse med SolarWinds så er det flere punkter hvor en zero trust modell kunne begrenset omfanget av angrepet. Programvaren som ble kompromisert blir brukt til overvåkning og til dels styring av nettverksressurser, men siden programvaren kjører internt og ble regnet som programvare som en kan stole på så var det ikke hos alle begrensninger på tilganger til denne programvaren. Heller ikke kommunikasjon med Internet var hindret som gjorde at når malware var installert kunne den ringe hjem". Eksempler på tilganger som ble opnådd i noen bedrifter var kompomittering av mailservere og autentifikasjonstjenester som gjorde at de fikk både brukernavn, passord og session-id cookies som de kunne bruke til å unngå to-faktor autentifisering for Microsoft domene-kontoer.[3] Et av hovedmålene med zero trust er å kunne sterkt begrense tilganger og segregere ulike systemer slik at om SolarWinds sin Orion programvare eksempelvis vil kommunisere med andre tjenester så vil det begrenses. Samtidig vil alt også logges og overvåkes, ideelt vil det bli fanget opp at Orion programvaren forsøkte å få tilgang til en tjenesten den ikke var autorisert i å få tilgang til som igjen fører til nøyere inspeksjon av selve programvaren.

Løsningen for tradisjonell cybersikkerhet her er å kunne oppdage at oppdateringen fra SolarWinds inneholder malware, med en brannmur som har IDS/IPS som kan analysere oppdatering i sanntid og potensielt stoppe dem. ABB Powergrids nevner i sitt materiale at systemet deres kan utstyres med en slik beskyttelse mot malware og virus. Videre skriver de også at de kan lage liste over godkjent programvare.([23], s. 10-11) Det er veldig usannsynlig at alle selskapene som ble rammet ikke hadde et slik IPS-system aktivert, og om bedrifter opererte med lister over godkjent programvare ville naturligvis hatt programmer som Orion og Outlook på den listen. I realiteten ser vi altså at angrep ikke alltid blir stoppet og flere eksperter som mener at brannmur aldri vil være godt nok. Økende grad av kryptering gjør det også vanskeligere for en brannmur da mindre informasjon om trafikk er tilgjengelig. Bruk av ny-utviklet malware gjør det også svært vanskelig for en brannmur å oppdage. Det kan og gjelde eksisterende malware med små modifikasjoner[51]. Zero trust er en filisofi som bygger på at slike angrep ikke alltid kan blokkeres og du får i tilegg et fokus på hvordan du kan begrense skadeomfang og oppdage angrep tidlig slik at selv om en angriper skulle komme seg inn vil sakdeomfang være begrenset. Ofte i slike supply-chain angrep er det ikke programvaren som blir kompromittert som er interessant for angriper, men hvilke system som kan nås etter å ha benyttet den programvaren til å komme inn på

internnett. Det gir god mulighet til å både separere og mer tid til å oppdage angrep før det når et punkt der konsekvensen blir høy. Et av selskapene som ble angrepet var FireEye der de oppga at dehadde blitt frastjålet red-team verktøy. Orion var bare brukt til å få et fotfeste innenfor nettverket. Hvis det her hadde vært en separering mellom Orion programvare og database som inneholder viktige verktøy ville angrepet mot muligens FireEye mislykkes. FireEye har selv en modell for hvordan de utøver sine angrep som viser hvordan et slik angrpe kan foregå:



Figur 5.1: Prosses for cyberangrep[32]

5.2 Angripere endrer metodikk for å omgå tradisjonell IT-sikkerhet

I SolarWinds angrepet ble det brukt mange teknikker for å ikke bli oppdaget. Teknikker som gjør at tradisjonelle sikkerhetstiltak ikke vil kunne klare å hverken stoppe eller oppdage et slikt angrep. Det var helt klart et APT angrep der første aktivitet skjedde i September 2019 [69]. Det var kun en test, men viser at de allerede på et veldig tidlig stadium hadde klart å få sin kode inn i Orion programvaren slik at den ble signert og sendt ut som oppdatering. Det ble tatt i brukt mange taktikker for å skjule koden også etter at den ble installert av kunder. Det var eksempelvis logikk for å oppdage programmer og drivere som kunne indikere at koden kjørte på en PC hvor en hadde verktøy for å undersøke og finne skadelig kode.[72] Hvis en kunde da først installerer Orion-oppdatering i et test-miljø for å se om den gjør noen den ikke burde så vil den skadelige koden ikke går over til trinn 2. Når den senere installeres i det faktsike systemet derimot vil den ikke finne noen av disse prossesene sannsynligvis og går til trinn 2 hvor den laster ned malware. Sikkerhetsselskapet FireEye har dokumentert bruk av 17 teknikker fra MITRE sitt ATT&CK rammeverk.[18] Angriperene har også laget en egen måte å kommunisere på samt å leie servere fra Amazon slik at IP-adresser som blir benyttet ikke blir flagget som mistenkelige. Slik kommunikasjon inn og ut av nettet går gjennom brannmurer som ofte har mye inspeksjon og muligheter til å sende advarsler eller blokkere trafikk. Måten angriperene kommuniserer på her gjorde at brannmurene ikke klarte å skille denne kommunikasjonen fra normal kommunikasjon.

Figur 5.2: Figur fra FireEye som viser taktikker brukt i trinn 2[18]

SolarWinds-angrepet er spesielt viktig, ikke fordi en ikke trodde et slikt angrep kunne skje, men at det viste at det var mulig. Konsekvensene var så omfattende i USA som kan virke som hovedmålet, at både myndigheter og bedrifter på toppnivå måtte ta stilling til problemet. Når myndighetene i USA presenterte sin zero trust strategi påpekes det og der at det største hinderet for modellen er å få med ledelsen på overgangen.[12] Som Microsoft skriver så er ikke prinsippet nytt, begrepet ble først brukt i 2010. Det er derimot først etter dette angrepet at det ble mye fokus på denne modellen.

Dette angrepet var veldig omfattende og Microsoft har estimert at minst 1000 engineers"har jobbet med angrepet.[71] Det er en veldig vag estimering av ressursbruk, men tyder likevel på at Microsoft mener det er lagt store ressurser i angrepet. Et angrep

trenger derimot ikke å være på nivå med dette for å omgå tradisjonell IT-sikkerhet. Dette angrepet var delvis rettet mot firma som leverer sikkerhetsløsninger som FireEye, Cisco og Microsoft, samt Departement of Homeland Security i USA. Angrep mot mål med mindre sikkerhet vil ikke behøve like stor ressursbruk.

IoT i strømnettet er et problem når det kommer til sikkerhet, samtidig er det også et problem i private husholdninger. Det finnes allerede store botnet basert på IoT som Mirai. IoT i hjem kan leveres helt uten sikkerhet eller oppdateringer og være lette mål som en angriper eksempelvis kan bruke som proxy i et angrep for å få IP adresse i samme land. Det kan tom tenkes at angriper med litt ekstra jobb kan angripe IoT enhet til en ansatt i selskapet. Med zero trust vil en derfor aldri regne en IP-adresse som noe en kan stole på. Selv om dette er en IP-adresse den ansatte stadig bruker så vil antagelsen være at det kan være en ondsinnet aktør som forsøker å kommunisere. Den beskyttelsen i brannmur mot malware med IDS som inspiserer all trafikk og ser etter signaturer kan og omgås uten å gjøre det like avansert som SolarWinds-angrepet. Signaturbasert beskyttelse fungerer bra mot angrep som bruker kjente metoder og kjent skadevare, men mer avanserte angrep vil benytte en ny svakhet, modifisert eller obfusert skadevare som brannmuren ikke klarer å oppdage. Krypterte forbindelser inn i internnett er også et problem om det ikke blir dekryptert i brannmur men på enheter inne i nettet. Med zero trust så er selvfølgelig tradisjonell perimetersikring med brannmur og autorisering for å logge inn like viktig som før. Christopher Kreb som var ansvarlig for sikkerhet hos DHS anslår at 90-95% av trussler er basert på kjente teknikker.[69] Disse løsningene vil altså fortsatt kunne oppdage og blokkere det klare flertallet av angrep. Zero trust er viktig for å mitigere den 5%-10% andelen som ikke blir oppdaget. Det er selvfølgelig et fortsatt mål om å stoppe intregningen om mulig. Hovedforskjellen er at zero trust også har stort fokus på intern og kontinuerlig sikkerhet samt overvåkning. I SolarWinds angrepet så ble aldri trinn 2 iverksatt nettopp hvis den oppdaget verktøy som kunne overvåke hva som skjedde på PCen. Det viser at angriperene til tross for å bruke veldig mange helt nye taktikker ikke ville risikere et angrep om de trodde systemet var under overvåkåning.

5.3 Zero trust for å beskytte seg mot angrep i leverandørkjede

En stor del av grunnen til at leverandører har blitt et større mål spesielt mot selskaper som forvalter større verdier og dermed i det minste har større verdi av å øke egen sikkerhet er at det oftest er viktig å komme inn et sted i nettet. Har angriper kommet inn er det mindre sikringer og om de da har lite tilganger brukes gjerne interne svakheter for å flytte seg internt og oppnå flere tilganger i systemet. Akkurat hvilke tilganger handler om typen angrep. Angrepene mot føderale myndigheter og store selskaper i USA siktet seg eksempelvis inn på å oppnå tilganger til skytjenester hvor mye informasjon som angriperene var ute etter er lagret. Her har altså angriper sett på hele verditjenesten og

bestemt at istedenfor å forsøke å finne en svakhet i selve skytjenesten, og angripe disse direkte, så var det lettere å angripe leverandører av programvare. Deretter fant de en leverandør til målene en ville angripe og bruke en inngang til å komme seg videre til målet sitt. Her ligger også grunnlaget for mulighet til å begrense skadeomfang i strømnettet. Hvis hovedmål er å beskytte DMS-systemet og det eksempelvis er en svakhet eller skadevare i program som brukes for e-post kan i det tilfelle angrepet begrenses og vil ikke nå DMS. Det å sette begrensninger er hverken nytt eller unikt ved zero trust. Zero trust setter derimot krav om at det skal være gjennomgående, altså ikke spesielle tiltak for å skjerme DMS, men alt internt skal skjermes der det er rimelig å gjøre det. Samtidig får du og mulighet for å overvåke trafikk mellom tjenester på internnettet. I praksis vil det bety brannmurer også internt mellom tjenester og enheter.

Grunnen til at nettselskap, eller andre selskap, ikke kan sjekke programvare og oppdateringer fra leverandører er ressubruken som er nødvendig for å få dette til. Orion ble levert med den skadelige koden som del av ferdig kompilert maskinkode.[69] Angriperene opprettet en midlertidig fil akkurat når kompilering ble iverksatt slik at deres kode aldri var i SolarWinds sin kildekode. Det gjorde at FireEye og CrowdStrike måtte bruke CrowdStrike sin programvare for å forsøke å gjennskape kildekode og gå gjennom alt for å finne den delen som inneholdt skadelig kode. Det er svært ressurskrevende arbeid som i praksis er umulig å gjennomføre for alle oppdateringer av all programvare. I artikkelen fra NPR kommer det også frem at SolarWinds hadde en lang liste med kunder, som gjorde det lett å identifisere dem som et viktig ledd i leverandørkjede. Dette uttaler SolarWinds at er normalt. Det gjør det ikke til et mindre problem, heller motsatt. Første steg for en angriper er å innhente informasjon, mens det her påpekes at prioritering for leverandører er å markedsføre sitt produkt. Ian Thornton-Trump som var tidligere ansatt i SolarWinds uttaler også at selskapet ikke var interessert i å bruke tilstrekkelig med penger på IT-sikkerhet. Det er en person sin vurdering og betyr ikke at sikkerhet var dårlig hos SolarWinds. Det er derimot et klart problem når leverandører ikke prioriterer IT-sikkerhet. Et motivasjonsproblem er at samtidig som SolarWinds ble angrepet har de i liten grad selv vært påvirket. Kundene deres sitter på samlede verdier som langt overstiger det SolarWinds gjør, men som leverandør trenger ikke å ta hensyn til det. Hvis det eksempelvis hadde vært ransomware-angrep er det kundene som hadde måttet betale løsepenger og ikke leverandør. Her kan det alstå lett oppstå en situasjon hvor en leverandør ikke er klar over verdiene hos kunde og har langt dårligere sikring av sine systemer. Det gir god grunn til å ikke stole fullstendig på programvare fra leverandører. Det betyr i praksis å ta høyde for at programvaren kan inneholde en svakhet eller skadelig kode og ta høyde for det når en ser på IT-sikkerhet for systemet.

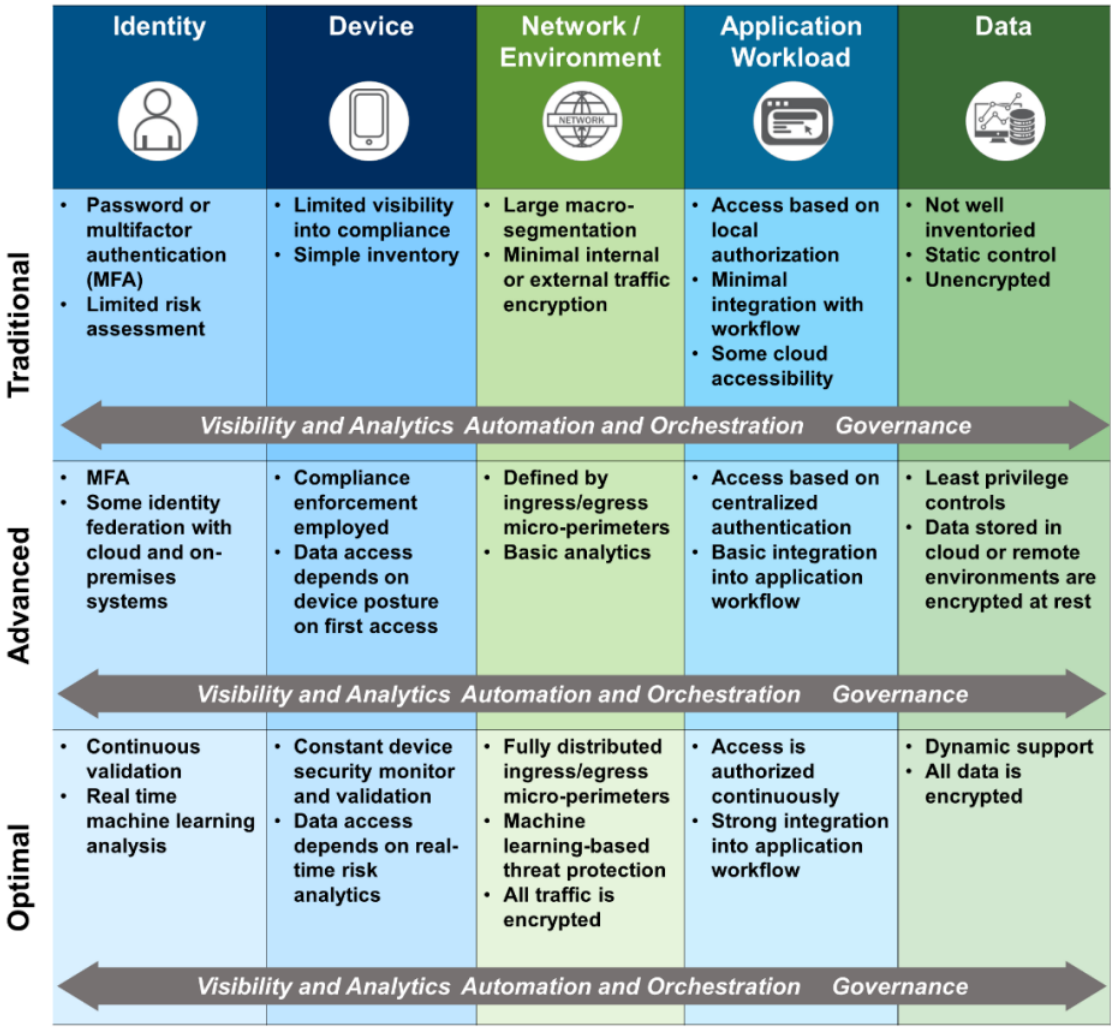
5.4 Zero trust innenfor strømnett

Zero trust i strømnett kan være med på å mitigere økt risiko for angrep mot stadig mer digitale strømnett og stømnett hvor stadig flere tjenester og programvare blir integrert. En av de største utfordringene med å gjøre flere komponenter i systemet digitalt og legge til flere IoT enheter, samt integrere flere systemer er flere angrepsvektorer. Hvis en tenker seg at programvare for distribusjonsnettet benytter seg av programvare for å gi prognoser for strømproduksjon og strømforbruk vil dette være en mulig angrepsvektor om dette er integrert i et system som MicroSCADA X eller Spectrum. Her finnes det derimot mulighet for å separere systemene, selv om begge tjenester kjører på samme datasenter kan prognosetjenesten eksempelvis kjøres viritualisert og begrenses slik at den kan levere prognoser, men ellers er kommunikasjon blokkert. Adgangskontroll kan da også konfigureres til å lage roller som kun har tilgang til denne tjenesten.

I et scenario hvor AMS-målere både for bedrifter og private husholdninger blir integrert mot DMS via HES finnes det også flere mulige segmenteringsstrategier. En brannmur mellom DMS og HES vil være naturlig. Avhengig av hvordan AMS målere er koblet opp mot DMS er det potensielt mulighet for å sette en gruppe AMS-målere bak en brannmur også, eller ha en programvarebasert segregering i HES. Hvis en antar at all trafikk inn mot HES er potensielt skadelig vil det være viktig å kunne logge alt, samt å raskt kunne oppdage og begrense omfang av et angrep. Det er selvfølgelig en utfordring å se på all trafikk for en analytiker og finne ut hva som er skadelig. I dette tilfellet er det derimot klart definert hvordan målere kommuniserer med HES og det vil være lett å se om det er trafikk som avviker fra vanlig kommunikasjon selv om det er snakk om mye data. Det gjør også automatisering enklere når systemet er så avgrenset og den vanlige trafikken er samme type som repeteres. Det kan også gjøres mot digitale transformatorer.

5.5 Zero trust modell fra CISA

CISA har publisert en model der de har en kort oppsumering av deres grunnpillarer i zero trust og sammenlignet mot tradisjonel sikkerhet. Zero trust er ikke entydig definert som internasjonal standard. Derimot er det CISA har utviklet en definisjon og en standard som gjelder for føderale myndigheter i USA. Derfor har jeg valgt å benytte meg av deres modellering fremfor egen modell eller modell fra kommersiell aktør da de modellene kan være tilpasset aktørens eget sortiment og ikke nødvendigvis det som sikrer systemet på best mulig måte. Dette er et utkast fra CISA, endelig modell kan derfor inneholde endringer. [4]



Figur 5.3: CISA-modell for implementasjon av zero trust [4]

5.5.1 Identitet

Hovedprinsippet i zero trust er å anta atalle brukere, enheter, trafikk i nett osv er ondsinnet. Det kommer frem her i tabellen som en klar forskjell. For identitet brukes MFA av mange i dag for å være sikker på at den som logger seg inn er den de utgir seg for. Det kan også være noen parameter lagt inn typisk geo-IP hvor det kan gis varsel hvis bruker logger seg inn fra en annen lokasjon enn normalt. I kategorien for optimal zero trust derimot vil du hele tiden følge med og overvåke både for å verifisere at personen er den personen utgir seg for å være. Her spesielt kommer maskinlæring inn som et fremtidig virkemiddel for å kunne raskt oppdage urettmessigheter. Det kan og være enklere faktorer eksempelvis om en ansatt er logget inn på 2 mobiltelefoner når de i utgangspunktet bare skal ha en jobbtelefon[9]. Et slik tilfelle vil det være naturlig at det enten kommer et varsel eller at handling automatisk blir tatt og den identiteten blir avlogget alle systemer. Identitet omhandler også tilganger. Kontoer vil bli administrert med mer informasjon om eksempelvis tilhørighet i grupper, prosjekter osv for å gi veldig spesialiserte tilganger til akkurat de som skal ha dem og ingen andre. En større grad av automatisering er også nødvendig for hvis en gir og trekker inn tilganger skal det ikke mye til før ansatte har tilganger de ikke lenger burde hatt. Her bør det også brukes såkalte "akkurat i tidetilganger som i et prosjekt vil da være en tilgang som blir gitt morgenen når prosjektet starter og automatisk satt til å bli fratatt sluttdato for prosjekt. En større oppdeling av nettet vil også bety en økning i avgrensede områder og da mer findeling av tilganger. Større grad av automatisering vil ikke altså bare være nødvendig for å unngå svikt i rutiner eller menneskelige feil, men og fordi antallet tilganger som må gis og fratas vil øke. Hovedmålet for innstramning i tilganger er å forsterke prinsippet om å gi akkurat nødvendige tilganger og ikke mer.

5.5.2 Enhet

Sikring og kontroll av enheter i nettet vil også bli viktigere. Det gjelder alt fra jobbtelefon til IoT enheter i nettet. Dette punktet inkluderer blant annet å sette krav til sikkerhet for alle enheter og sjekke at disse blir fulgt av alle enheter. Selv om du er logget inn på en enhet vil tilgang til data og bli vurdert utifra informasjon om enheten. Dette kan eksempelvis være fra eksempelet om 2 telefoner så bør det være en liste å sjekke mot som viser at to av dem ikke eksisterer. Den ansatte vil da få tilgang fra sin mobil, men angriperene sine telefoner vil ikke få tilgang til data. En mer avansert versjon vil automatisk søke etter enheter i nettet hele tiden for å raskt oppdage om det er enheter koblet til nettet som ikke skal være der. Et resultat av å fullstendig følge dette blir jo at utdaterte enheter ikke vil oppfylle krav. Det er jo selvfølgelig et problem uansett modell, men på grunn av kostander er det ikke sikkert at det lar seg gjennomføre.

5.5.3 Nettverk

Innenfor nettverk vil det være en del endringer i nettverskarkitektur fordi denne delen er svært viktig for å begrense konsekvens. Når en ser på angrep av typen supply-chain så er det ikke lett for et nettselskap å påvirke sannsynlighet, derimot vil det være mulig å påvirke konsekvens av et slik angrep. Det består i det CISA beskriver som mikro-perimeter som kan være å ha en brannmur mellom epost-server og resten av systemer. Det vil og bety at både HES og DMS ligger innenfor en slik mikro-perimeter i internnettet. Videre kan en også avgrense programmer fra hverandre innenfor samme mikro-perimeter. Det er også lagt opp til en oppgradering av dagens IDS i brannmurer, hvor målet er det som kalles Next Generation Firewallssom også skal kunne bruke maskinlæring til å eksempelvis finne skadevare vi enda ikke vet eksisterer. Dette er derimot veldig avhengig av leverandører som kan levere et slik produkt og er enda i en veldig tidlig fase av utviklingen. Det en og får ved å lage mikro-perimetere er god oversikt og logging av all trafikk mellom disse. Det kan være veldig nyttig for å oppdage inntregning tidlig. Veldig mye[**morketall-2020-18**] inntregning i systemer oppdages enten ved tilfeldighet eller en sjekk av systemer. Hvis det var konstant overvåkning kunne det blitt oppdaget før noe skade var skjedd. Både segmentering og tilgangskontroll gir og mer informasjon og mulighet til å avdekke.

5.5.4 Programvare

På grunn av segmentering av nettverk og endringer i autorisering og verifisering av enheter bør flere programmer bli tilgjengelig direkte over Internet istedenfor å være kun tilgjengelig internt via VPN. Dette kan jo ikke gjelde for noen tilganger til DMS, som heller ikke er tilgjengelig via VPN i dag. Det er også lovkrav som gjør dette umulig. Her må det også gjøres vurderinger siden angrepsflaten vil øke med flere programmer direkte tilgjengelige. Samtidig vil noen som kobler eksternt være koblet til det programmet og ikke ha tilgang til internnett som de ville hatt med VPN og det mest sikkerhetskritiske vil fortsatt være tilgjengelig kun fysisk ved kontoret. Det bygger også på at krav i pillarene for identitet, enhet og nettverk er oppfylte. Ellers vil angriper enkelt kunne ta seg videre fra tjenesten inn i internnett. Videre i denne pillaren så er det fokus på å teste og overvåke programvare. Testing og sikkerhet i kode er jo noe som hovedsakelig ligger hos leverandør. Her vil det nok være mest naturlig med krav og kontroll av leverandør for å oppnå dette. Overvåkning av programvare med logging av hendelser for å ha oversikt over hva programvare gjør er derimot mulig å gjøre hos nettselskap. Det er spesielt relevant for programvare som blir modifisert til å inneholde skadelig kode. Da er det viktig å logge hendelser for å kunne oppdage om programvaren gjør noe den ikke pleier og ikke burde gjøre.

5.5.5 Data

For data er tilgang der flere faktorer blir vurdert som beskrevet i identitet og enhet viktig. Det stilles og krav til kontroll over og kategorisering av data slik at det finnes en oversikt over hva som skal være der. Tilganger gjort entel til alt av data eller kun data som blir ansett som av ekstra verdi vil også bli loggført. Både loggføringer av tilgang og oversikt over data vil gjøre det lettere å oppdage angrep og lettere å gå tilbake og se hvilke data som er lest, slettet eller endret. Lagret data bør også alltid krypteres.

5.5.6 Microsoft sin modell

Selv om jeg har valgt å bruke CISA sin modell som grunnlag i oppgaven så har også Microsoft en modell som har en del likheter og vil være naturlig å sammenligne med. Microsoft er jo selvfølgelig også en leverandør for føderal sektor som da må levere på CISA sine punkter. Micrrosoft har både tabell i samme stil som CISA samt en modell for arkitekturen til et system som benytter zero trust:

Maturity Model table, part 1 of 2

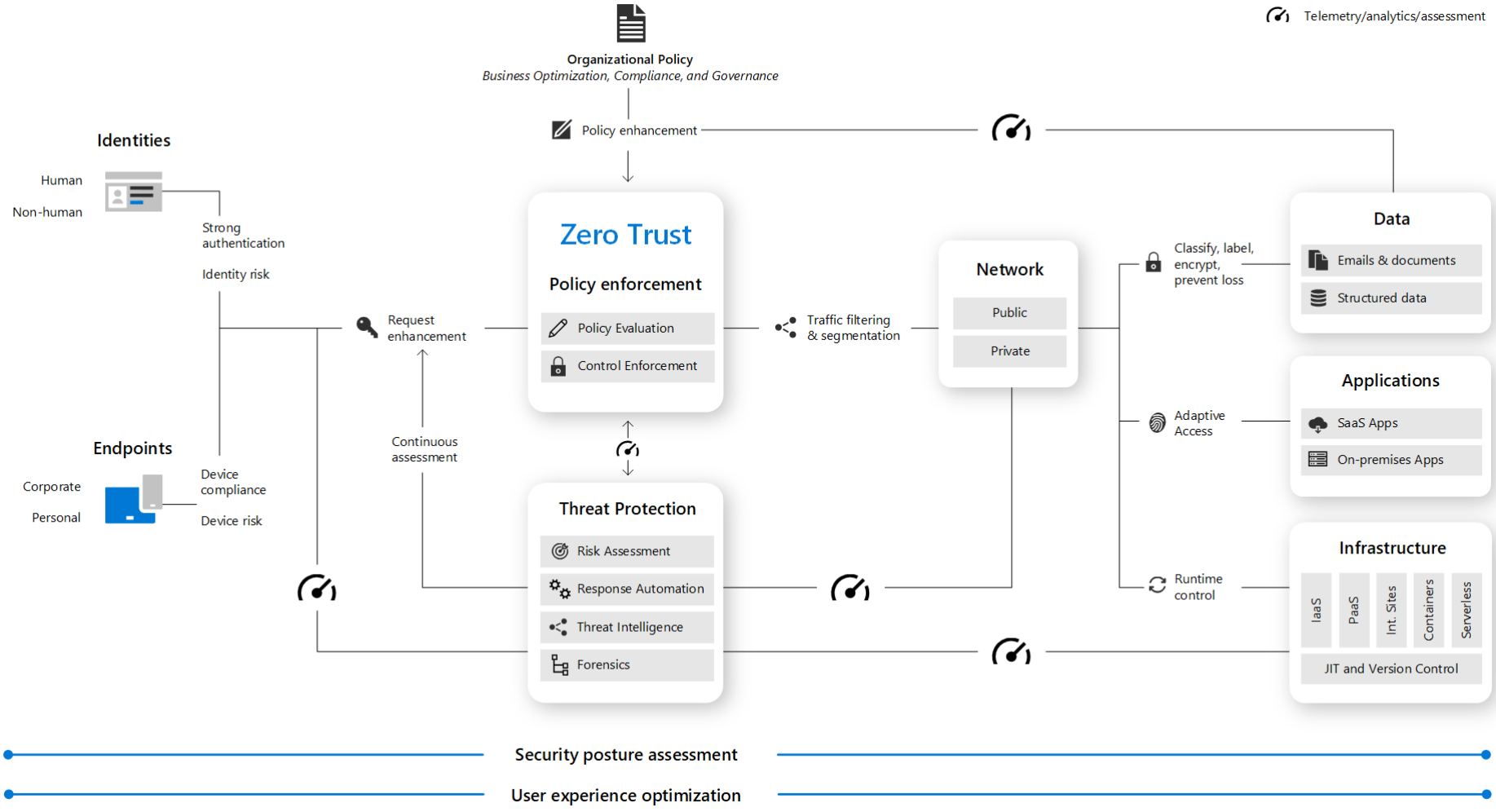
	Getting Started	Advanced	Optimal
Identity	• Authentication using a weak credential such as password • Cloud identity federates with on-premises system and some apps connected with the cloud identity provider • Manual provisioning, governance, and limited visibility into risk	• Authentication using strong authentication such as MFA • Most apps are federated with cloud identity for authentication, authorization, provisioning, and deprovisioning • Visibility into identity and session risk	• Authentication using passwordless and phishing resistant methods • All apps are modern and federated with cloud identity for authentication, authorization, provisioning, and deprovisioning • Automated access reviews ensure proper management of group memberships, access to apps, and role assignments
Endpoints	• On-premises management using basic endpoint protection (EPP) • Configuration settings managed with Group Policy • Limited visibility into compliance	• On-premises management connected to cloud MDM for security configuration and devices registered with cloud identity • Compliance enforcement based on device posture on first access • EPP + EDR to include post-breach monitoring and response coverage, basic automatic remediation playbooks	• Device health, antimalware status, and security are constantly monitored and validated • Device security settings enforced with baselines across all devices • EPP + EDR + TVM for posture management, advanced automatic remediation playbooks, and XDR integration
Network	• Permissions are manually managed and static • Some internet resources are accessible to users directly; VPNs and open networks provide access to majority of resources. • Workloads are monitored for known threats and static traffic filtering; Some internal and external traffic is encrypted	• Permissions are managed with policy and adjusted based on recommendations • Access across sensitive workloads is isolated by session; cloud apps, internet resources, and sensitive private networks are accessible without location-assumed trust • Traffic is monitored; most internal and external traffic is encrypted	• Adaptive access policies explicitly check evolving permissions automatically to resources based on risk and usage • All sessions are continuously evaluated for policy violations and access is revoked dynamically, based on data signals powered by a cloud-based service • Traffic is monitored to identify potential threats and dynamic signaling; All data and network traffic is encrypted end-to-end
Applications	• Cloud shadow IT risk is assessed, and critical apps are monitored and controlled • Some critical cloud apps are accessible to users	• On-premises apps are internet-facing • Cloud apps are configured with SSO	• All apps are available using least privilege access with continuous verification • Dynamic control is in place for all apps with in-session monitoring and response

Figur 5.4: Microsoft modell for zero trust del 1 ([42], s. 7)

Maturity Model table, part 2 of 2

	Getting Started	Advanced	Optimal
Data	• Rule-based and keyword methods are used to discover and classify sensitive data across some locations, apps, services • Access is governed by perimeter control, not data sensitivity • Sensitivity labels are applied manually, with inconsistent data classification	• Automated discovery and classification across all locations, apps, and services and heterogenous data types • Access is governed irrespective of perimeter or app boundary • Restricting flow of sensitive data	• Continuous discovery and correlation of signals using machine learning to identity data exfiltration risks • Access decisions are governed by a cloud security policy engine • Proactive data governance and risk assessment
Infrastructure	• Permissions are managed manually across environments • Configuration management of VMs and servers on which workloads are running	• Workloads are monitored and alerted for abnormal behavior • Every workload is assigned app identity • Human access to resources requires just-in-time	• Unauthorized deployments are blocked and alert is triggered • Granular visibility and access control are available across all workloads • User and resource access is segmented for each workload
Threat protection	• Reactive threat and vulnerability detection • Pre-breach protection using tools like AV for endpoints, EOP for email • Isolated or siloed security and response • Basic endpoint monitoring	• Proactive threat and vulnerability detection and post-breach response • Automated investigation and remediation (AIR) enabled for test groups and basic threats • XDR capabilities across at least two security pillars and some security information and event management (SIEM) integration	• AIR has been fully enabled • Actively using threat analytics, threat intelligence, and recommended mitigations to close vulnerabilities and misconfigurations • XDR capabilities applied across all pillars and fully integrated with SIEM for advanced threat hunting, detection, response, and prevention
Policy enforcement	• Access decisions are based on limited signals • Access decisions are not centralized • Access decisions are made at only the time of access and are not continuous	• Access decisions are based on signals from at least two pillars • Centralized policy engine used to make access decisions	• Access decisions are based on signals from all pillars • Decisions are continuously evaluated, and policy is enforced in real time • Real-time threat assessment used in access decision

Figur 5.5: Microsoft modell for zero trust del 2 ([42], s. 8)



Figur 5.6: Modell som viser arkitektur til en zero trust løsning fra Microsoft [54]

5.6 Praktiske utfordringer ved zero trust

Zero trust-modellen er både veldig omfattende på helhetsnivå der den berører alle aspekter i et IT system, men selv enkelttiltak alene kan være veldig omfattende. CISA sin modell har delt tiltak i tre kategorier som er tradisjonell god praksis, avansert og optimal zero trust. Optimal zero trust kan betraktes som et fremtidig optimalt scenario ettersom det blant annet er lagt inn teknologi som ikke er moden enda og sum av alle tiltak. Hvis en ser over tiltak for blant annet overvåkning er det og klart at i tilegg til inkjøp av alle løsninger så vil det også kreve en del ansatte til enhver tid. Så selv om forslagene i kategorien optimal gjerne teoretisk kan regnes som optimale er det ikke dermed gitt at kostandene ved disse tiltakene står i stil med mitigert risiko ved innføring av disse tiltakene.

5.6.1 CISA optimal zero trust

Et eksempel på teknologi som blir brukt i seksjonen optimal, men som enda ikke er skikkelig er utviklet er programvare basert på maskinlæring. Det finnes blant annet under trusselbeskyttelse i kategorien nettverk. I teorien skal en slik trusselbeskyttelse både kjøre på eksterne brannmurer istedenfor dagens IDS, men også internt. Her vil det også være naturlig å ta med overvåkningsdata for identitet og enheter. Ideen er at programvaren skal lære seg hva som er normalt og da kunne gi varsel og sette igang tiltak automatisk når den oppdager noe som er utenom det vanlige. På denne måten vil du kunne oppdage skadevare også om den ikke er kjent fra før av. Det er flere selskaper, eksempelvis Darktrace, som har løsninger de mener kan bruke maskinlæring til å oppdage selv helt ny skadevare eller svakheter.[10] Darktrace er også aktive i å gi konkrete eksempler for hva deres programvare kan klare som er grunnen til at denne programvare er valgt som eksempel her. De har blant annet en blogpost med flere nulldagshendelser i 2021.[37] Her beskriver de hvordan angrep ble oppdaget og hvilke varsler som ble sendt. De skriver derimot at angriper fortsetter å generere varsler i dager eller uker etter at mistenkelig aktivitet har blitt oppdaget. Det kan være flere grunner til det, men hvis en ser generelt på maskinlæring så er nøyaktighet en stor utfordring. Dette er også beskrevet på Darktrace sine nettsider hvor de hevder modellen vil få bedre nøyaktighet over tid. Hvis programvaren da settes til å blokkere alt den generer varsler for kan det da tenkes at mye legitim trafikk også blir blokkert, ansatte blir nektet adganger og lignende.

I Darktrace sine eksempler kan det virke som at bedriftene har satt programvaren til å generere varsler som så blir analysert av et menneske. Ser en på eksempelet med Github hevdes det at angrepet ble oppdaget med varsel om uvanlig forespørsel til en uvanlig IP. Likevel fortsatte angripers aktivitet, eksfiltrerte data og installerte cryptominer og gjorde server til del av botnet. Her kom varsler, men det ble enten ikke iverksatt tiltak eller tiltak iverksatt var ikke effektive. Det kan være flere grunner til det, spesi-

elt siden det var et prøveprosjekt. Hvis vi antar ingen automasjon så har varsler enten ikke blitt fulgt opp eller mengden varsler har vært for stor til å følge opp alt. Det finnes ingen informasjon om hvor mange varsler som blir generert og hvor stor andel av disse som viser seg å være riktige. Det som og kommer frem er at selve svakheten ikke er oppdaget, kun hendelser som regnes som uvanlige. Det kan altså være et godt utgangspunkt, men varslene er ikke satt i system automatisk. Ser en på Mnemonic som tilbyr en tjeneste hvor de overvåker kunder sine nett og analyserer så skriver de at de håndterer 4,5 milliarder hendelser hver dag for alle sine kunder i 2017.[60] Her skisseres problemstillingen med antall varsler som kan oppstå. Disse 4,5 milliarder hendelsene reduseres ved hjelp av datasystemer til 80-82 og analytikere til 2 per dag. Det er veldig viktig at slik sikkerhetsautomasjon faktisk kan redusere antall varsler tilstrekkelig til at det er rimelig mengde varsler for analytikere å gjennomgå. Nøyaktighet for disse er selvfølgelig også viktig.

Hvis en ser på eksempelet med Log4j fra Darktrace så skriver de at 6 unike varsler ble generert. Det ble blant annet gikk varsler om uvanlig forbindelse og varsel om uvanlig script fra sjelden ekstern forbindelse. Den type overvåkning er utvilsomt viktig, men ikke noe som er unikt ved maskinlæring. Det som er poenget med CISA sin anbefaling er ikke at overvåkning av trussler skal være basert på maskinlæring, men at vi med bruk av maskinlæring kan få funksjonalitet vi ikke har i dag. Det er fortsatt slik at nye svakheter og skadevare blir oppdaget av analytikere. Det som blir oppdaget av Darktrace er uvanlig aktivitet som kan hjelpe en analytiker å finne en svakhet. Den type beskyttelse faller da i praksis inn i CISA sin avansert-kategori. I tradisjonell-kategorien er det lagt inn en IDS tjeneste som kun baserer seg på statisk informasjon i form av lister med blokkerte IP-adresser, signatur av skadevare etc som blir utarbeidet sentralt hos leverandør. Kravet i avansert er en form for grunnleggende analyse for å oppdage angrep. Det kan eksempelvis være å se på uvanlige hendelser i nettverk, enheter, innlogging osv og gå inn å se om det er en del av et angrep eller ikke. Basert på varsler generert så vil automasjon være nødvendig for å kunne utføre slik analyse. Det kan også være et alternativ å kjøpe dette som en tjeneste. Det er en minimumskostnad knyttet til å ha noen på jobb 24/7 inkludert helligdager. Speseilt mer avanserte angrep kan basere seg på informasjon om når sikkerhetsanalytiker er på jobb og ikke som betyr at ideelt bør alltid noen være på jobb. Et problem med å sette det ut som en tjeneste vil er at det vil øke angrepsflate mot systemet, men det må gjerne sees opp imot risiko av å ikke ha noen på jobb natt til 1. juledag.

5.6.2 Avansert zero trust er mer realistisk i forhold til ressursbruk

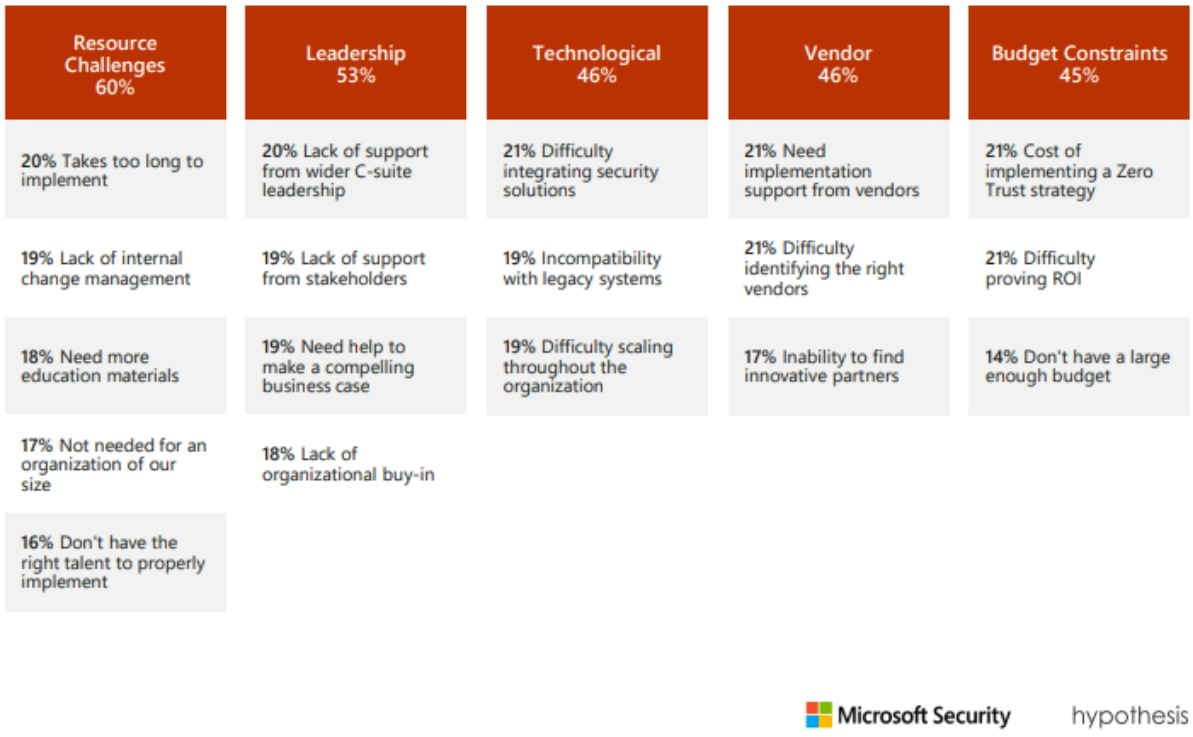
En annen stor utfordring med å implementere optimal zero trust er den totale kostnaden og tidsbruk for å implementere alt. Nøyaktig kostnad vil variere, men her kan fort kostand og krav til nok personell med kompetanse bli et støre problem og kostnad enn

det gir reduksjon av risiko. Her er det nytt utstyr som må kjøpes til mikro-perimeter. Det må bli opplæring i nye systemer og hvordan det fungerer. Mye er basert på automasjon som betyr innkjøp av en rekke tjenester. På toppen av dette vil det kreve flere ansatte både til analyse, men også til å raskt fikse problemer som oppstår når tilgangskontroll blir svært streng og ansatte eller programmer blir nektet tilgang de burde ha.

Videre i rapporten velger jeg derfor å se bort ifra CISA sin optimale kategori. Grunnlaget er som beskrevet over med at det er både urealistisk å oppnå i dag og er så omfattende at jeg ikke tror det er økonomisk forsvarlig sett i forhold til risiko. Istedenfor velger jeg å se på kategorien for et avansert system. Det er også slik at zero trust modellen inneholder en grad av modenhet. Grunnen til det er jo at en ser i praksis så tar det tid å implementere og få alt av ansatte og systemer over i ny modell. Jeg velger likevel å se på tiltak i en modell der alt er ferdig implementert. Prosjekter som å oppgradere nettlinjer, installere AMS-målere ol. er allerede prosjekter som har lange tidshorisonter. Vi har i dag testprosjekter med mer digitalisering og integrering i strømnettet som i praksis er en tidlig fase av å implementere et slik system som er beskrevet tidligere i oppgaven. Arbeid med implementering av en zero trust modell kan altså starte i en tidlig fase og være i sluttfase før en starter å integrere mer inn mot DMS eksempelvis.

5.6.3 Hva anser organisasjoner som utfordringer med zero trust?

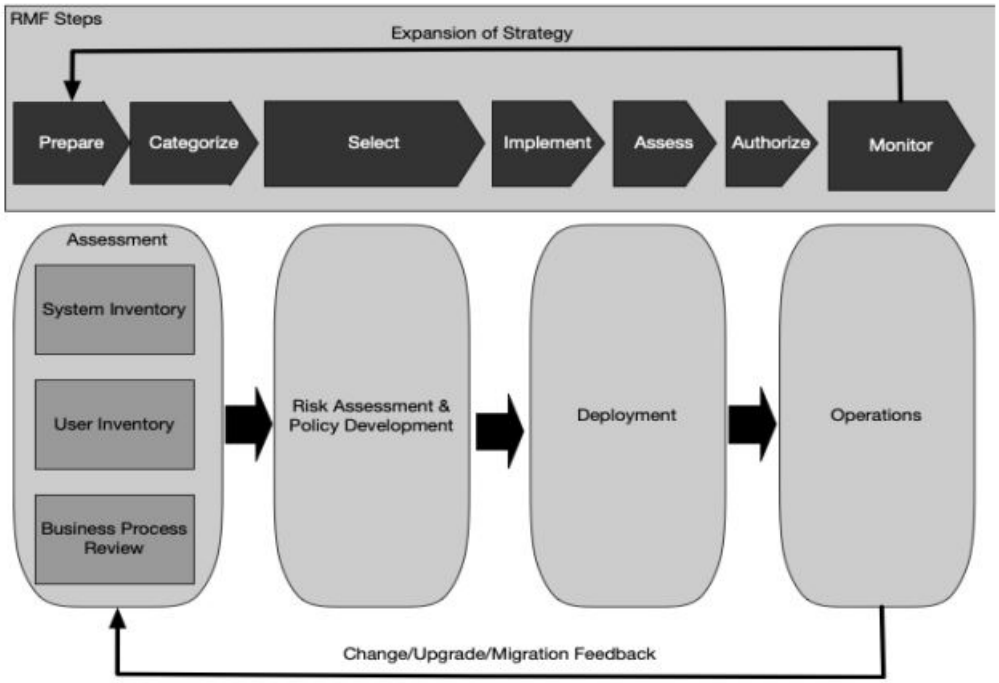
Microsoft har utført en undersøkelse for å finne ut hva deres kunder anser som utfordringer når det kommer til zero trust.



Figur 5.7: Utfordringer med zero trust basert på svar fra virksomheter[53]

Undersøkelsen viser at de to største utfordringene organisasjonene har er mangel på ressurser til å gå over til det nye systemet og problemer med å få med ledelse til å utføre endringer. Her kan det være sammenhen mellom mangel på støtte i ledelse i organisasjon og mangel på ressurser og budsjett. Det er og klart at teknologi og leverandører som kan tilby løsninger som zero trust krever er en utfordring. Det er derfor klart at det er viktig å se på hva leverandører kan levere og hvilke teknologier som finnes før en bestemmer seg for å implementere et av punktene i modellen. For strømnett kan inkompabilitet med eldre systemer klart være en utfordring. Modellen som er lagt opp her vil i utgangspunktet ikke ha noen utdaterte systemer eller enheter i nettet. Det er ikke sikkert det er gjennomførbart i praksis å fjerne disse. Siden zero trust har mye segmentering og sikring ellers internt så vil det være mulig å ta høyde for og sikre disse delene i nettet ekstra. Det kan derimot være et problem om leverandører ikke har løsninger som tar høyde for dette.

For å hjelpe bedrifter å gå over til zero trust har NIST skissert en prosses for å gradvis starte og utvide zero trust da det ikke er veldig realistisk å flytte alt over til en full zero trust modell i en omgang. En slik modell vil også gi nettselskap mulighet til å evaluere modellen opp mot andre metoder for å sikre systemer.



Figur 5.8: Prosses for zero trust [50]

Siden zero trust modellen fortsatt er veldig ny så kan en slik modell være fordelaktig. Det er fult mulig å starte hvor behovet anses som størst. Mer logging og overvåkning kan eksempelvis implementeres i nettverk og programvare alene. Dette kan vurderes og hvis resultatene er gode så kan nye tiltak implementeres. Best resultat vil nok oppnås når hele modellen er implementert, men tiltakene i seg selv vil alle ha positiv effekt. Mange av tiltakene beskrevet i modellen blir benyttet uten at en har en zero trust modell. Et eksempel på deter punktet "MFA, Some identity federation with cloud and on-premises systemsom mange leverandører av autorisering tilbyr til kunder uavhengig av zero trust.

Del VI

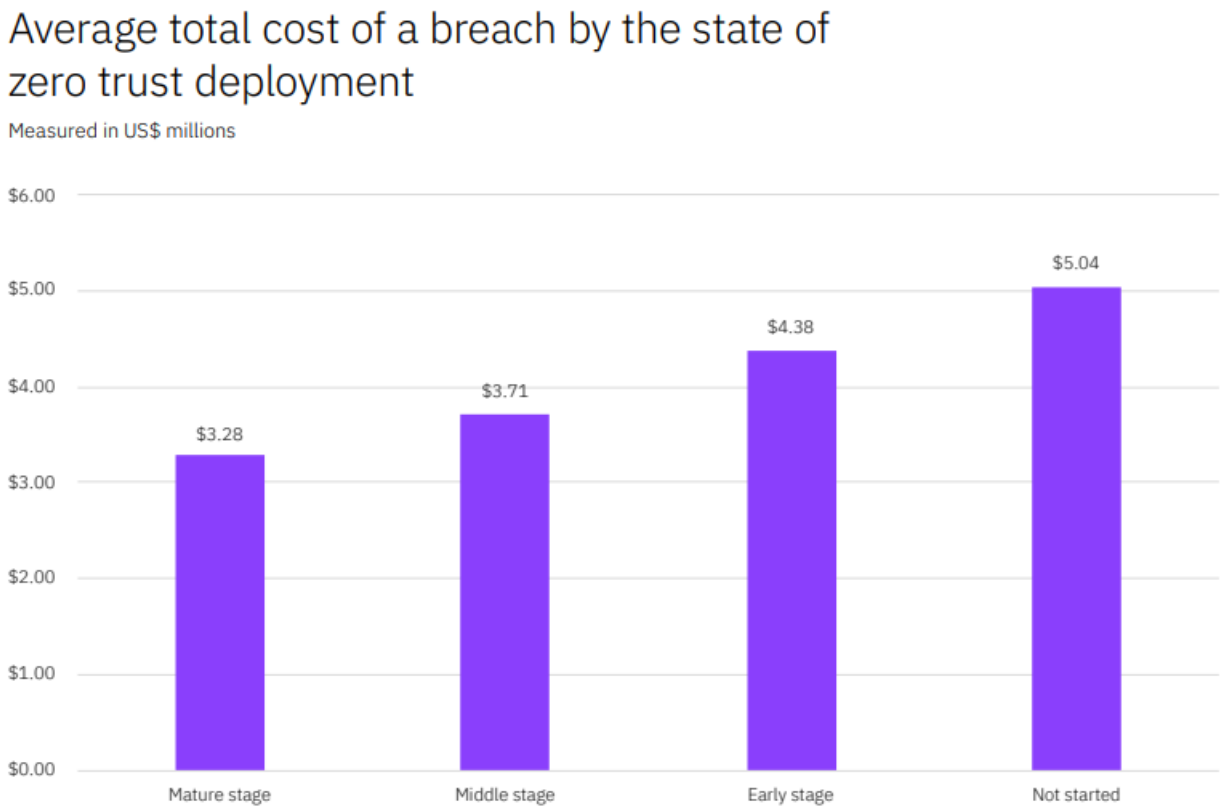
Tiltak for sikring av smartgrids

Kapittel 6

Anbefalinger for prioriterte tiltak fra zero trust-modellen

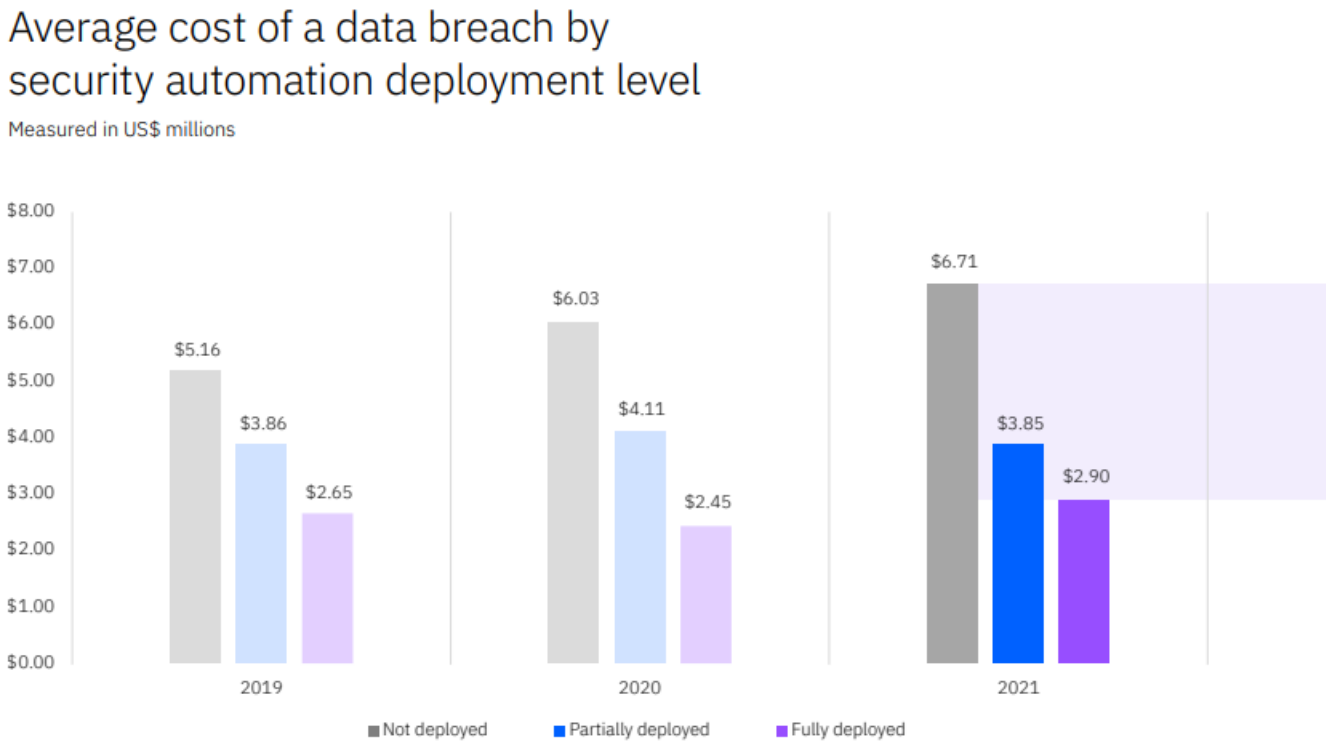
6.1 Tiltak som gir reduksjon i konsekvens av angrep fra IBM-rapport

IBM utgir årlig en rapport om kostnaden av angrep som rammer data. Rapporten baserer i hovedsak på kostnader relatert til områder som omhandler personlig informasjon. Tallene er basert på estimater fra de som deltok. Det er lignende Mørketallsundersøkelsen hvor en kan velge å svare og svar er anonyme og basert på hva deltagere selv rapporterer inn. Det er altså ikke helt dekkende for nettselskaper hvor behandling av personlig informasjon er begrenset. Energi-sektor utgjør og kun 6% av deltakere.([52], s. 63) Selv om tallene i seg selv ikke er representative så gir forskjellen i kostnad for ulike tiltak en indikasjon på hvor bra ulike tiltak fungerer.



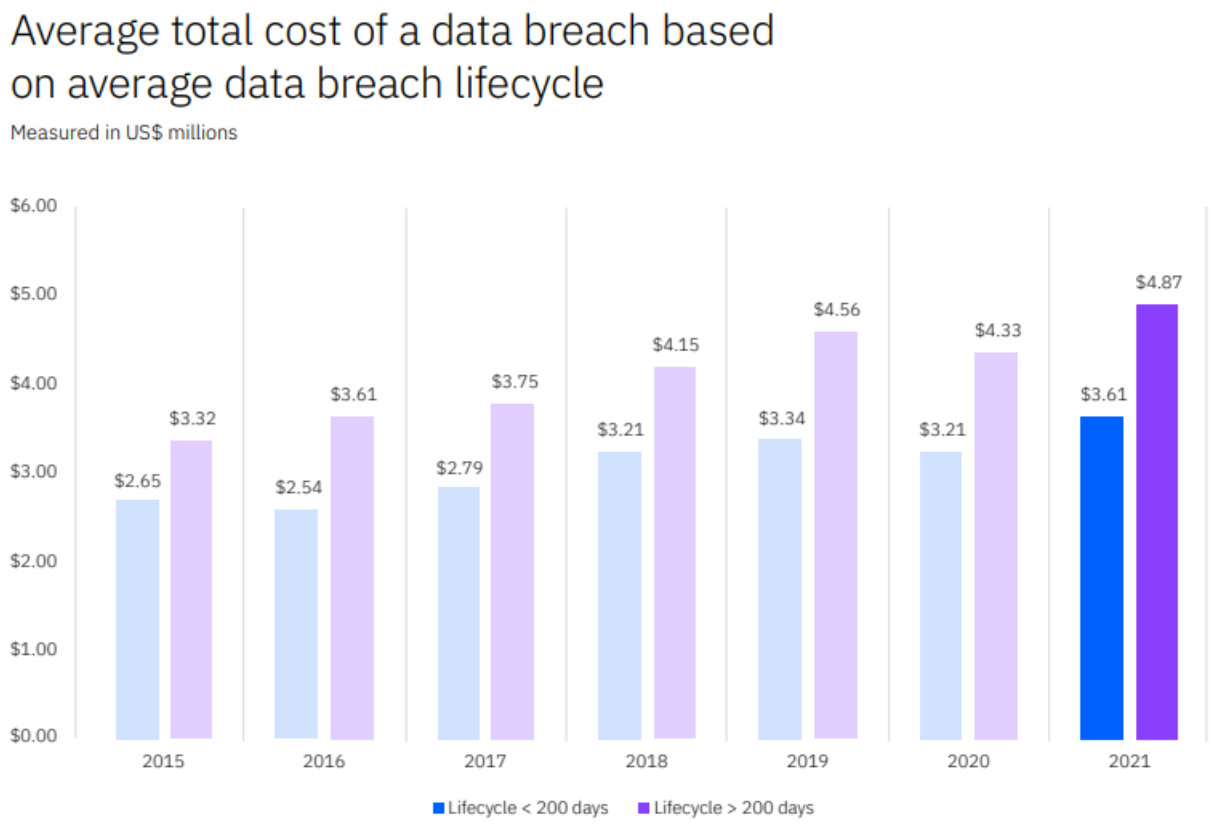
Figur 6.1: Påvirkning av zero trust på konsekvens etter hvor mye som er implementert ([52], s. 33)

Figuren viser en klar reduksjon på 42.3% i konsekvens ved selskaper som følger IBM sin definasjon av zero trust. Det er også en reduksjon selv for selskaper i en tidlig fase. IBM har også satt fokus på et spesielt punkt hvor de ser den største forskjellen og det er bruk av maskinlæring/automasjon for sikkerhet. Her ser de en reduksjon i konsekvens på 84.4%:



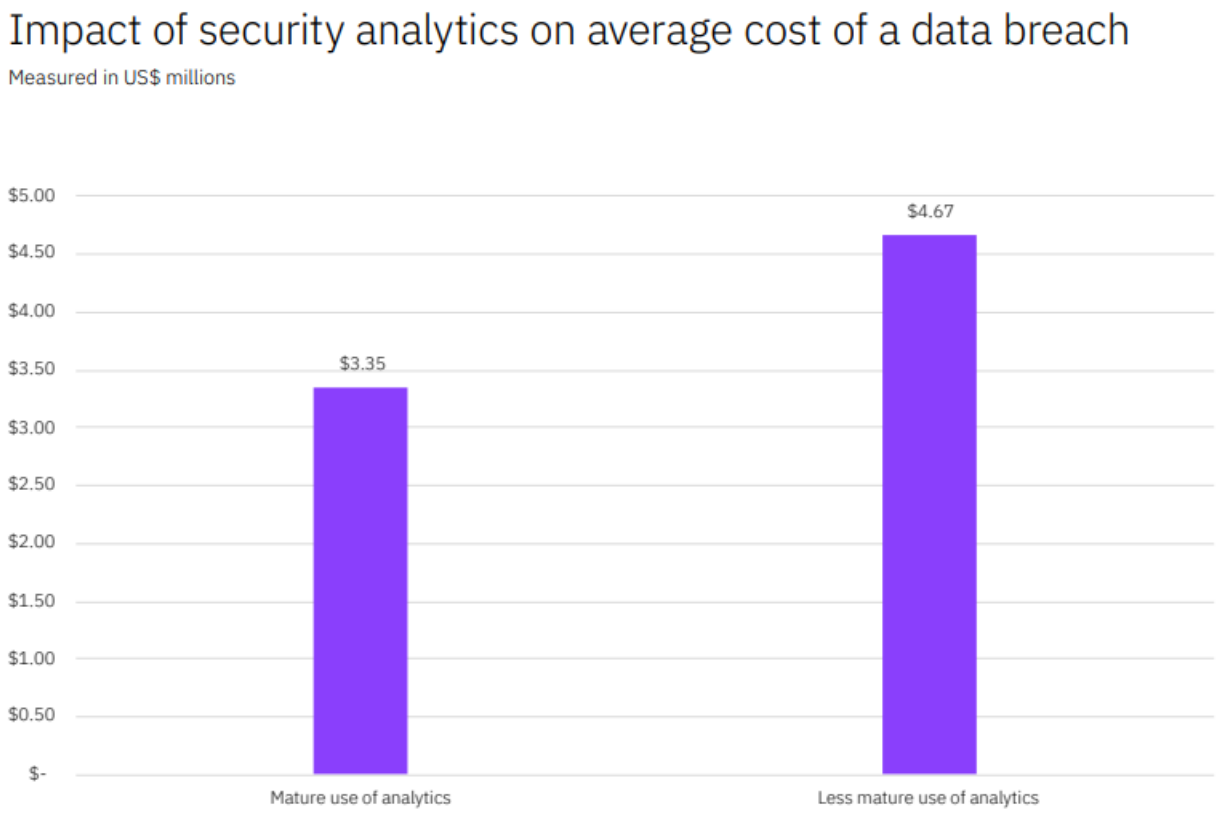
Figur 6.2: Påvirkning av sikkerhetsautomasjon på konsekvens av datainnbrudd ([52], s. 37)

Igjen så viser tallene her at en delvis implementasjon utgjør en stor forskjell. Hvis det er vanskeligheter med å eksempelvis integrere det i deler av nettverket så vil det fortsatt være nyttig å implementere for alt annet. For reduksjonen i konsekvens vises det spesielt til at det tar kortere tid å finne angrep og kortere tid å stoppe. Reduksjonen i denne kategorien utgjør den største reduksjonen i noen kategori i undersøkelsen.



Figur 6.3: Kostnad basert på lengde av datainnbrudd ([52], s. 24)

Figuren viser en sammenheng mellom hvor lang tid det tar å oppdage og håndtere en hendelse og konsekvensen av denne. Det kommer og frem at i gjennomsnitt tar dette 324 dager, men faller til 247 dager med automasjon. Hva de ulike nivåene av automasjon her betyr i praksis er ikke definert. Sikkerhetsautomasjon vil sannsynligvis inneholde en form for overvåkning internt og det er mulig at sammenligningsgrunnlaget i stor grad mangler dette. Dermed er det ikke sikkert utifra dette at automasjon alene har så stor effekt som vist. Samtidig vil sannsynligvis overvåkning internt av nettverkstrafikk og programvare inneholde automasjon siden datamengdene blir så store. Det finnes både gode argumenter for dette tiltaket og tall som kan indikere god effekt som vil være relevant i forhold til prioritering av tiltak. Her er og sikkerhetsanalyse assosiert med reduksjon i konsekvens:



Figur 6.4: Påvirkning i bruk av analyse av systemer på konsekvens av datainnbrudd ([52], s. 41)

6.2 Anbefalinger av tiltak basert på risikoanalyse av systembeskrivelse

6.2.1 Mikro-segregering i internnett

Jeg vil derfor se på primært tiltak sett i lys av risikovurdering gjort tidligere i rapporten. Her er det angrep av typen supply-chain angrep som er vurdert til å ha høyest risiko. Spesielt mikro-segmentering og overvåkning vil være gode tiltak her. Mikro-segmentering forutsetter at angrepet skjer i programvare i internnett men ikke er hovedmålet i seg selv. Det som gir størst utslag på konsekvens er hvis angriper når DMS eller HES system. Hvis mikro-segmentering kan hindre et angrep å nå DMS/HES vil det gi stor reduksjon i konsekvens for suply-chain angrep. Supply-chain angrep kan og forekomme mot leverandør av selve DMS eller HES. Her vil ikke segmenteringen ha effekt for å beskytte den programvaren i seg selv. Et angrep kan likevel påføre skade andre steder i virksomheten og her vil segmenteringen fortsatt kunne hjelpe.

6.2.2 Sikkerhetsmonitorering

Sikkerhetsmonitorering er noe som kan ha stor effekt på konsekvens. Klare virksomheten å oppdage angrepet før angriper for gjort videre skade vil konsekvenser at et angrep være begrenset til kostnader for å sikre systemer. Til tross for at angriperne brukte helt nye teknikker i SolarWinds angrepet så ville de ikke gå over til fase 2 og sende inn malware om de oppdaget kjente verktøy for monitorering. Selv om nye teknikker brukes så må uansett endringer bli gjort og det er en kommunikasjon ut til angriper. Mikro-segmentering gjør det mulig å logge og monitorere trafikk også internt mellom systemer. Det vil også være viktig å logge aktivitet fra brukere og se på hendelser for enheter i nettverket. Sikkerhetsmonitorering av programvare er også viktig spesielt med tanke på supply-chain.

6.2.3 Automasjon av sikkerhetsmonitorering

Sikkerhetsmonitorering kan bli veldig omfattende, spesielt når monitorering skal omfatte trafikk, brukere, enheter og programvare. Selv om det er ganske grunnlegende så vil jeg anbefale bruk av atomasjon til dette. Automasjon kan konfigureres både til å utføre enkelte handlinger på egenhånd, men også filtrere ut hendelser. Automasjon vil muliggjøre et høyere nivå av sikkerhetsmonitorering som vil være nødvendig for et smartgrid.

6.2.4 Synergi mellom monitorering og segmentering

Hvis en angriper kommer seg inn i nettverket og får tilganger vil de med mikrosegmentering måtte gjennom en brannmur for å bevege seg videre. Dette er en brannmur som vil være strengt konfigurert og ha samme IDS som en brannmur ut mot internet. Det å gjøre det vanskeliger å flytte seg internt betyr og at det kan ta mer tid for en angriper å oppnå flere tilganger. Det vil gi mer tid til å oppdage angrepet og ta grep før konsekvensene blir store.

6.2.5 Bruk av leverandører av sikkerhetsmonitorering

Selv med automasjon av monitorering så leverer strømnettet strøm 24/7 365 dager i året. Det er ikke vanskelig for en angriper å finne ut hvilke dager som er offentlige fridager, og når det er kveld. Ideelt bør det være noen på jobb til enhver tid for å monitorere systemet. Her kan det være vanskelig å både finne kompetansje og utfordring i forhold til kostnad ved et slik tiltak. Jeg ville anbefalt å se til sikkerhetsselskaper som tilbyr slike tjenester på dette punktet. Outsourcing i seg selv introduserer ekstra risiko og kompetansekrav for å vurdere leverandør. Samtidig vil leverandør kunne tilby både tekniske løsninger for monitorering og vil alltid ha ansatte på jobb og kan stille med ekstra ressurser om angrep blir oppdaget. For å hjelpe

virksomheter har NSM laget en kvalitetsordning for selskaper som tilbyr tjenester for å håndtere angrep. [46]

6.2.6 Tiltak for utdaterte enheter og programvare

Hvis en har programvare, operativsystemer eller blanding som er utdatert men ville krevd store kostnader ved å oppgradere, eksempelvis bytte hele transformatorstasjonen vil det ofte ikke være et alternativ. Da er det viktig å ha oversikt over hvor disse svakhetene i systemet er og så godt som mulig separere dem fra resten av systemet og kun tillate nødvendig kommunikasjon. Hvis en har oversikt over svakheter ved eldre IT systemer eller komponenter er det også mulig å overvåke aktivitet som samsvarer med utnyttelse av disse svakhetene. Det vil være lignende et honeypot system hvor en maskin med kjente svakheter settes opp og en overvåker og finner de som angriper og utnytter denne svakheten. Her er ikke målet å lure inn noen angripere. Hvis en angriper kommer seg inn i et system er det naturlig å først innhente informasjon. Finner de noe med kjente svakheter er det naturlig å forsøke å utnytte disse, men målrettet automatisk overvåkning av disse svakhetene vil gi mulighet til å oppdage et angrep raskt.

En utfordring her kan bli teknologier og leverandører. I CISA sin modell så er det på et optimalt nivå viktig at alle enheter og programvare oppfyller sikkerhetskrav. Hvis det ikke er mulig å oppnå i strømnettet vil det ikke samsvare med modell. Samtidig er modellen bygget opp slik at den ikke krever fullstendig samsvar med modell for å oppnå effekt. Jeg tror derfor det i seg selv ikke er et stort problem. Bevissthet og ekstra tiltak rundt ekstra sårbare enheter og programvare i nettet anser jeg å gi betydelig nok reduksjon i risiko til at det vil være mulig å beholde det i nettverket. Det vil likevel forbli en ekstra sårbar del av nettet. Hvis mulig kan det derfor være lurt å legge vekt på mulighet for bytte IT-del av elektromekaniske komponenter i nettet og legge vekt på sikkerhetsoppdateringer for programvare som bli benyttet. Hvis produsenten ikke tilbyr langvarig støtte kan nettselskap ende opp med enten høyere risiko eller ekstrakostnad for å sikre en ny sårbarhet selv.

6.2.7 Integritet av data fra eksterntjenester

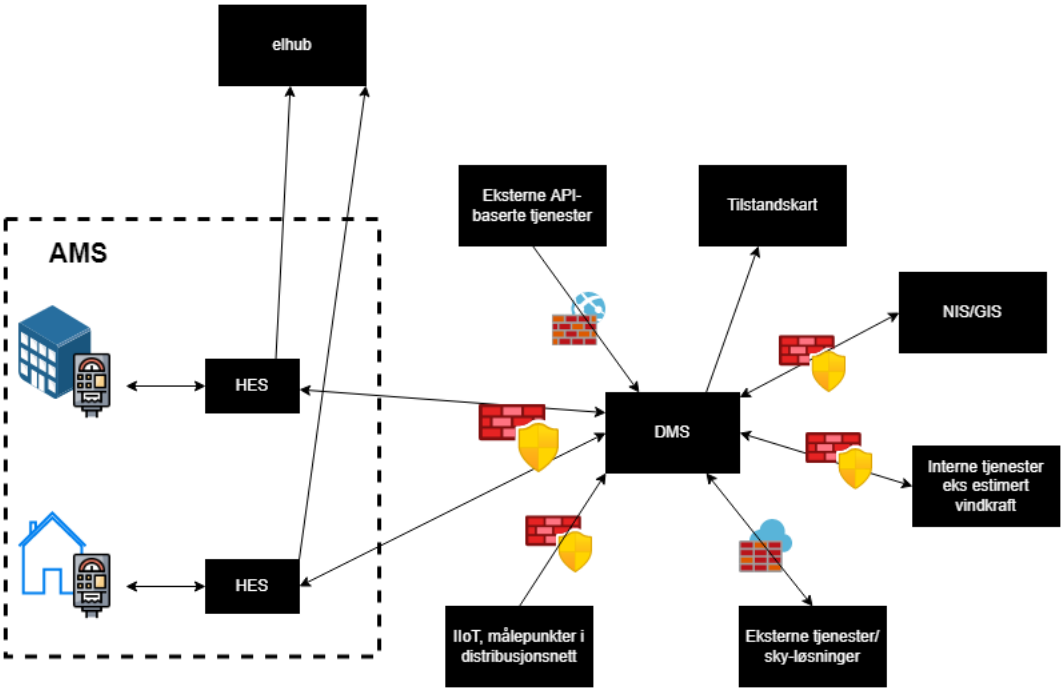
Det er vanskelig å beskytte seg mot å få tilsendt manipulert informasjon fra ekstern tjeneste som bli benyttet. Det kan være en ekstern skyløsning som nettselskapet kontrollerer, men det kan og være løsninger som er helt utenfor nettselskapet sin kontroll. Hvis en legger til grunn et veldig automatisert smartgridsystem som blant annet bruker værdata fra yr.no vil systemet da kunne gjøre feil beslutninger. Dette er ikke en type angrep som vil kunne bli oppdaget av sikkerhetsmonitorering. Mitt forslag til tiltak her vil være å presentere alt av beslutningsgrunnlag slik at det er lett for mennesker å sjekke det. En maskin har ingen mulighet til å vurdere hva som er rimelig. De som jobber og kjenner til nettet derimot vil kunne oppdage dette. Her tror jeg det er viktig at det ikke blir gjort beslutninger som kan ha høy konsekvens basert på

data fra eksterne kilder. Det kan sammenlignes med å ikke la en selvkjørende bil kjøre uten menneske med sertifikat til å passe på.

6.2.8 Autorisering

Tiltak for autorisasjon er noe ulikt for nettselskaper enn andre virksomheter. Grunnen er krav om fysisk sikring og fysisk tilstedeverlse for kontroll av DMS. Ekstern kontroll er derfor ikke mulig med mindre angriper får kontroll over maskiner som styrer DMS og tilganger. Angriper kan likevel fortsatt få tilganger til en ansatt inn i internnettet og bruke det som en måte å komme inn i systemet. Spesielt med økt bruk av hjemmekontor har angrep av denn sort for å oppnå tilganger økt veldig. Angrep kan eksempelvis skje via phishing som er både enkelt og billig å gjennomføre. Anbefalingen min her er bruk av MFA, også internt. Bruk av en sentralisert løsning for å administrere identitet gir god oversikt over alle brukere og tilganger. Bruk av grupper og roller, samt automatisering er viktig for å ha kontroll på tilganger, brukere og hindre at alle har kun nødvendige tilganger. Her bør det og brukes midlertidige tilganger som gis akkurat når de trengs. Det er ekstra viktig med et mer segregert nettverk for å hindre at en angriper får tilgang til store deler av nettverket hvis de klarer å ta over en bruker.

6.2.9 Ny systembeskrivelse



Figur 6.5: I den nye systembeskrivelsen har jeg lagt til brannmurer mellom ulike tjenester.

6.3 Risikovurdering etter tiltak

Nr.	Trussel	R-nivå før			Nye tiltak	R-nvå etter		
		S	K	R		S	K	R
1	Ekstern kompromittering av programvare som brukes i nettet i dag, eksempelvis DMS og HES.	4	4	8	Mikro-segmentering og brukt av automasjon og sikkerhetmonitorering for nettverk, enheter, brukeraktivitet og programvare.	4	4	8
2	Ekstern kompromittering av ny programvare som integreres i internnettet, eksempelvis programvare basert på maskinlæring for estimering av forbruk og produksjon.	4	4	8	Mikro-segmentering og brukt av automasjon og sikkerhetmonitorering for nettverk, enheter, brukeraktivitet og programvare.	4	2	6
3	DDoS angrep som gjør at HES/DMS ikke klarer å kommunisere eksternt mot internet og AMS, digitale	2	1	3	Ingen nye tiltak	2	1	3
4	IT systemer og IoT har kortere levetid enn det elektromekaniske når det kommer til sikkerhet som gir mange nye angrepsflater inn mot DMS hvis det ikke holdes oppdatert.	4	4	8	Fokus på løsninger der IT-del kan byttes separat, tiltak for å segregere, sikre, og overvåke ekstra på områder der det finnes kjente sårbarheter.	3	2	5
5	Brudd på autorisasjon som gir tilganger i internnettet	3	4	7	Bruk av MFA, sentralisert identitetsløsning, automatisering av roller, grupper. Findeling av tilganger og bruk av midlertidige tilganger som blir gikk akkurat i tide.	2	2	4
6	Ekstern tjeneste kompromittert, eksempelvis programvare som kjører i en skyløsning og kommuniserer med DMS	2	2	4	Bruk av manuell verifisering av tall og manuell kontroll slik at systemkontroll som kan gi negative konsekvenser i strømnettet ikke blir automatisk utført.	2	1	3
7	Utro tjener	2	4	6	Monitorering av brukeraktivitet og generelt mer monitorering og automasjon.	2	3	5
8	Kompetansemangel for gamle styringssystemer og teknologier.	2	3	5	Ingen nye tiltak	2	3	5

Figur 6.6: Tabell som viser ny risikovurdering etter tiltak

6.4 Grunnlag for ny vurdering

For sårbarheter og supply-chain angrep mot DMS eller HES programvare har jeg ikke endret risiko etter tiltak. Hvis disse angripes direkte og målrettet er det fult mulig at angriper også har spesiallaget malware som Industroyer med mål om sabotasje. Jeg anser sannsynligheten for å oppdage og stoppe angrepet som større, men tror fortsatt det er betydelig risiko ved et slik målrettet avansert angrep. For annen programvare derimot har jeg redusert konsekvens til 2. Sannsynlighet er uendret siden tiltakene ikke stopper hendelsen fra å skje, men reduserer risiko. Det er viktig å nevne at vurderingen baserer seg på at segmentering og monitorering stort sett har effekt, men det kan aldri utelukkes at noen fortsatt klarer å omgå de sperrene. En slik hendelse kunne vært i en underkategori med betydelig redusert sannsynlighet.

For trussel 4 så tror jeg bevissthet og løsninger for å unngå å ende opp med gamle teknologier og sårbare enheter vil ha noe effekt på sannsynlighet, men vil være veldig vanskelig å redusere sannsynlighet for at det skjer. Jeg regner med at slike sårbare enheter og gamle teknologier alltid vil være i strømnettet, sannsynlighet her er et mål på hvor sannsynlig det er en ny slik svakhet oppstårr i en tidsperiode på 1-3 år. Konsekvens tror jeg derimot kan reduseres til 2. Igjen gjelder samme forbehold som for trussel 2. Innenfor autorisasjon finnes det gode løsninger per i dag for å redusere risiko. Bruk av ganske omfattende autorisasjon tror jeg derfor vil kunne redusere både sannsynlighet og konsekvens. Segmentering bidrar også her til å effektivt skille ulike roller innenfor ulike systemer.

Jeg har satt ned konsekvens av angrep mot eksterne tjenester som gjør at systemet kan motta feil informasjon. Dette baserer seg på at det gjøres mange manuelle handlinger og minst mulig automatiseres. Hvis det blir vanskelig eller umulig å overlate mestepart av kontroll til manuel styring vil konsekvensen øke. Alternativt må det finnes løsninger for å verifisere tall. Eksempel på det kan være værmåling fra 3 ulike kilder. Andre kilder for informasjon kan bli vanskelige å verifisere. Hvis automasjon tar over svært mye eller all kontroll vil jeg anbefale redundans for data beslutninger blir basert på.

Til slutt har jeg redusert konsekvens fra 4 til 3 for utro tjener. Sikkerhetsmonitorering vil kunne oppdage uvanlig aktivitet fra en bruker. Spionasje kan derimot fortsatt gjøres med den ansattes tilganger. Reduksjonen fra 4 til 3 baserer seg på varsel fra sikkerhetsmonitorering. Igjen er det et forbehold her og i ytterste konsekvens vil det være mulig for utro tjener å gjøre stor skade fortsatt. For kompetansemangel har jeg ikke listet opp noen nye tiltak. Det kan likevel være lurt å være bevisst på dette både i forhold til nåværende ansatte men også i innkjøp av nye løsninger.

Del VII

Avslutning

Kapittel 7

Konklusjon og videre arbeid

Basert på prognoser for fremtidige endringer så er smartgrid nærmest nødvendig for fremtiden for å kunne nå klimamål. Uavhengig av klimamål så vil den pågående elektrifiseringen og økende grad av mer variabel strømproduksjon i energimiksen kreve tiltak i nettet. Smartgrid er en løsningen som utnytter ressursene på en effektiv måte og unngår overdimensjonering. Problemet er at det gikk samme sikkerhetstiltak øker risikoen i strømnettet. Det er ikke slik at det må være smartgrid for å innføre zero trust-modell. Økt digitalisering og økning i angrepsflate med flere programmer og tjenester vil dermed alltid øke risiko.

Samtidig som et smartgrid-system med sammenkoblet DMS og HES gir økt risiko så er strømnettet i dag også veldig utsatt for supply-chain og zero day. Selv om risikoen for et smartgrid et større gitt likt sikkerhetsnivå så vil et smartgrid med en zero-trust modell ha lavere risiko enn dagens modell med tradisjonelle sikkerhetstiltak. Det finnes mange argumenter for nettopp zero trust som modell her. Det jeg anser som mest tungtveiene er at det kommer med tiltak for de delene av systemet som har høyest risiko. Det er også blitt populært nettopp på grunn av nyere utvikling i trusselbilde. Likevel er adopsjonen veldig ny som betyr at erfaringer, inkludert eventuelt gevinst, er begrensede.

Selv om min risikoanalyse viser reduksjon i risiko som kan gi lavere systemrisiko enn nåværende system med tradisjonell sikkerhet så er bryterfunksjonalitet i AMS fortsatt en beskymring. Bryterfunksjonaliteten er ikke nødvendig for å oppnå forbrukerfleksibilitet. Det åpner derimot for at et angrep kan koble ut både virksomheter og husholdninger, potensielt i stor skala. Dette vil være svært alvorlig. Her kan en bedre løsning være slik som Elvia sitt prosjekt der enhet som styrer varmtvannsbereder henter innformasjon fra en sky-løsning fra Elvia. Styring av målere fra DMS vil da ikke være nødvendig og HES kan være segregert og kun sende målerinfo til DMS slik som i dag. Samtidig oppnås forbrukerfleksibilitet i nettet. Konsekvens av at en angriper får tilgang til informasjon tilgjengelig i sky-løsning er veldig liten. Det vil derimot være nødvendig med tiltak for enheter installert i husholdninger. En svakhet kan gi angriper mulighet til å ta kontroll over alle slike enheter i nettet. Her må det ses på løsningen, men jeg

tror likevel det vil innebære mindre risiko enn å integrere AMS-målere. For å eksponere AMS målere til økt risiko bør det være en stor gevinst, men her finnes det andre måter en kan oppnå målene i smartgrid uten å eksponere AMS målere for slik risiko. Jeg vil derfor anbefale å heller se mot den type løsninger og unngå en integrasjon som gir DMS kontroll over AMS-målere.

Bibliografi

[1] *2021 Microsoft Exchange Server data breach*. URL: https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach. (accessed: 15.05.2022).

[2] Aidon. *Energy Service Devices (ESD)*. URL: https://www.aidon.com/nb/vare-losninger/#energy-service-devices-esd. (accessed: 13.04.2021).

[3] Britive. *Securing Privileged Cloud Credentials: The SolarWinds Cyber Attack*. URL: https://www.britive.com/news/solarwinds-cyber-attack/. (accessed: 13.04.2021).

[4] Cisa. «Zero Trust Maturity Model». I: (2021), s. 5–14. URL: https://www.cisa.gov/zero-trust-maturity-model.

[5] Cloudflare. *What is the Mirai Botnet?* URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. (accessed: 13.04.2021).

[6] Kevin Collier. *'Really messy': Why the hack of Microsoft's email system is getting worse*. URL: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/. (accessed: 15.05.2022).

[7] Zachary A. Collier og Joseph Sarkis. «The zero trust supply chain: Managing supply chain risk in the absence of trust». I: *International Journal of Production Research* 0.0 (2021), s. 1–16. DOI: 10.1080/00207543.2021.1884311. eprint: https://doi.org/10.1080/00207543.2021.1884311. URL: https://doi.org/10.1080/00207543.2021.1884311.

[8] *Colonial Pipeline ransomware attack*. URL: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack. (accessed: 15.05.2022).

[9] Bruceb Consulting. *The Great Russia Hack 4: How Did They Get Caught?* URL: https://www.bruceb.com/2021/02/the-great-russia-hack-4-how-did-they-get-caught/. (accessed: 13.04.2021).

[10] Darktrace. *Self-Learning AI learns your business from the ground up to stop cyber disruption*. URL: https://www.darktrace.com/en/self-learning-ai/. (accessed: 13.04.2021).

[11] Jason Deign. *Germany's Maxed-Out Grid Is Causing Trouble Across Europe*. URL: https://www.greentechmedia.com/articles/read/germanys-stressed-grid-is-causing-trouble-across-europe. (accessed: 13.05.2022).

[12] Steve Dispensa. *The federal Zero Trust strategy and Microsoft's deployment guidance for all*. URL: https://www.microsoft.com/security/blog/2022/02/22/the-federal-zero-trust-strategy-and-microsofts-deployment-guidance-for-all/. (accessed: 13.04.2021).

[13] Elhub. *Elhubs Personvernerklæring*. URL: https://elhub.no/personvern-og-sikkerhet/elhubs-personvernerklaering/#personopplysninger. (accessed: 13.04.2021).

[14] Elnett21. *Havnen fortsetter elektrifiseringen – bygger eget el-nett i Risavika*. URL: https://www.elnett21.no/nyheter/havnen-fortsetter-elektrifiseringen-bygger-eget-el-nett-i-risavika. (accessed: 15.05.2022).

[15] Elnett21. *Ingen*. URL: https://www.elnett21.no/. (accessed: 13.04.2021).

[16] Elvia. *Smarte varmtvannsberedere vil redusere ressursbruken*. URL: https://www.elvia.no/drift-og-vedlikehold/utbygginger-og-prosjekter/smarte-varmtvannsberedere-vil-redusere-ressursbruken/. (accessed: 15.05.2022).

[17] Agder Energi. *Vellykket test av fleksibilitetshandel*. URL: https://www.ae.no/aktuelt/nyheter/vellykket-test-av-fleksibilitetshandel/. (accessed: 16.05.2022).

[18] FireEye. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. URL: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor. (accessed: 13.04.2021).

[19] Christian Frøystad mfl. «Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA». I: (2018), s. 1–35. URL: https://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf.

[20] Eric Goldstein. *MATURING ENTERPRISE MOBILITY TOWARDS ZERO TRUST ARCHITECTURES*. URL: https://www.cisa.gov/blog/2022/03/04/maturing-enterprise-mobility-towards-zero-trust-architectures. (accessed: 13.04.2021).

[21] Hitachi ABB Power Grids. *Hitachi ABB Power Grids and Tensio TN AS to deliver Norway's first fully digital, eco-efficient substation*. URL: https://www.hitachiabb-powergrids.com/no/no/news/global-news/press-releases/hitachi-abb-power-grids-and-tensio-tn-as-to-deliver-norway-s-first-fully-digital-eco-efficient-substation. (accessed: 13.04.2021).

[22] Hitachi ABB Power Grids. *Lumada APM Asset performance management, from field data to fleet optimization.* URL: https://search.abb.com/library/Download.aspx?DocumentID=9AKK106930A8037&LanguageCode=en&DocumentPartId=A4-web&Action=Launch. (accessed: 13.04.2021).

[23] Hitachi ABB Power Grids. *One vision MicroSCADA X*. URL: https://search.abb.com/library/Download.aspx?DocumentID=1MRS756253&LanguageCode=en&DocumentPartId=LoRes&Action=Launch. (accessed: 13.04.2021).

[24] Hitachi ABB Power Grids. *We are bridging the gap. Enabling Digital Substations.* URL: https://search.abb.com/library/Download.aspx?DocumentID=4CAE000290&LanguageCode=en&DocumentPartId=LoRes&Action=Launch. (accessed: 13.04.2021).

[25] Martin Gundersen. *Sporet datainnbrudd til sin største konkurrent*. URL: https://nrkbeta.no/2022/03/08/sporet-datainnbrudd-til-sin-storste-konkurrent/. (accessed: 15.05.2022).

[26] Ingen. *2020 United States federal government data breach*. URL: https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach. (accessed: 13.04.2021).

[27] Ingen. *Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv*. URL: https://lovdata.no/dokument/SF/forskrift/1999-03-11-301/KAPITTEL_4#%5C%C2%5C%A74-2. (accessed: 13.04.2021).

[28] Ingen. *Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv*. URL: https://lovdata.no/dokument/SF/forskrift/1999-03-11-301/KAPITTEL_4#%5C%C2%5C%A74-3. (accessed: 13.04.2021).

[29] Ingen. *Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv*. URL: https://lovdata.no/dokument/SF/forskrift/1999-03-11-301/KAPITTEL_4#%5C%C2%5C%A74-4. (accessed: 13.04.2021).

[30] Ingen. *Forskrift om økonomisk og teknisk rapportering, inntektsramme for nettvirksomheten og tariffer*. URL: https://lovdata.no/forskrift/1999-03-11-302/%C2%A79-2. (accessed: 13.04.2021).

[31] Ingen. *NEK IEC 61850-serien*. URL: https://www.nek.no/manedens-standard-april-2016-nek-iec-61850-serien/. (accessed: 13.04.2021).

[32] Ingen. *Red Team Assessment*. URL: https://www.mandiant.com/services/technical-assurance/red-team-assessment. (accessed: 13.04.2021).

[33] Microsoft IoT. *OSO Hotwater boosts sustainability with connected water heaters powered by Azure Sphere*. URL: https://www.youtube.com/watch?v=ZrOLjgat23E. (accessed: 15.05.2022).

[34] Audun Jøsang. *dokumenter*. URL: https://www.uio.no/studier/emner/matnat/ifi/IN5080/v21/dokumenter/. (accessed: 16.05.2022).

[35] Brian Krebs. *At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software*. URL: https://www.nbcnews.com/tech/security/really-messy-hack-microsofts-email-system-getting-worse-rcna377. (accessed: 15.05.2022).

[36] Robert Lipovsky og Anton Cherepanov. *Industroyer: Den største malwaretrusselen mot kritisk infrastruktur siden Stuxnet*. URL: https://www.eset.com/no/industroyer/. (accessed: 15.05.2022).

[37] Sam Lister. *Walking through the front door: Compromises of Internet-facing systems*. URL: https://www.darktrace.com/en/inside-the-soc/walking-through-the-front-door-compromises-of-internet-facing-systems/. (accessed: 13.04.2021).

[38] Lyse. *-Sammen utvikler vi Norge som energinasjon*. URL: https://www.elnett21.no/nyheter/sammen-utvikler-vi-norge-som-energinasjon. (accessed: 13.04.2021).

[39] Lyse. *Styring av forbruk*. URL: https://www.lysekonsern.no/virksomhet/elnett/styring-av-forbruk/. (accessed: 15.05.2022).

[40] Anne-Kari Valdal Marie Røyksund. *Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning*. URL: https://publikasjoner.nve.no/eksternrapport/2020/eksternrapport2020_02.pdf. (accessed: 13.04.2021).

[41] Ståle Grut Martin Gundersen. *Europeisk datatilsyn åpner granskning etter NRKbeta-avsløring*. URL: https://nrkbeta.no/2020/12/11/europeisk-datatilsyn-apner-granskning-etter-nrkbeta-avsloring/. (accessed: 13.04.2021).

[42] Microsoft. «Evolving Zero Trust». I: (2021), s. 7–8. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT.

[43] Mnemonic. «2021 Security report». I: (2021), s. 28–29. URL: https://www.mnemonic.io/globalassets/resources/security_report_2021.pdf.

[44] Sonja van Renssen Nick Ferris. *Cybersecurity threats escalate in the energy sector*. URL: https://www.energymonitor.ai/tech/digitalisation/cybersecurity-threats-escalate-in-the-energy-sector. (accessed: 15.05.2022).

[45] Jannicke Nilsen. *Lyse går for AMS-måler med spenningsovervåking og smarthusmuligheter*. URL: https://www.tu.no/artikler/lyse-gar-for-ams-maler-med-spenningsovervaking-og-smarthusmuligheter/228176. (accessed: 13.04.2021).

[46] NSM. *Kvalitetsordning for leverandører som håndterer IKT-hendelser*. URL: https://nsm.no/fagomrader/sikkerhetsstyring/leverandorforhold/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser. (accessed: 13.04.2021).

[47] NTB. *Ingeniør pågrepet av PST: Skal ha overlevert informasjon til Russland*. URL: https://www.tu.no/artikler/ingenior-pagrepet-av-pst-for-a-ha-overlevert-informasjon-til-fremmed-stat/497586. (accessed: 15.05.2022).

[48] Hitachi ABB Powergrids. *MicroSCADA X*. URL: https://www.hitachiabb-powergrids.com/offering/product-and-system/scada/microscada-x. (accessed: 13.04.2021).

[49] Renergy. *Mer vindkraft kan gi slitasje på vannkraftverkene*. URL: https://renergycluster.no/2019/mer-vindkraft-kan-gi-slitasje-pa-vannkraftverkene/. (accessed: 15.05.2022).

[50] Scott Rose mfl. «Zero Trust Architecture». I: (2020), s. 37. URL: https://doi.org/10.6028/NIST.SP.800-207.

[51] James Scott. «Signature based malware detection is dead». I: *Institute for Critical Infrastructure Technology* (2017).

[52] IBM Security. «Cost of a Data Breach Report 2021». I: (2021), s. 1–73. URL: https://www.ibm.com/downloads/cas/OJDVQGRY.

[53] Microsoft Security. «Evolving Zero Trust». I: (2021), s. 20. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha.

[54] Microsoft 365 Security. *Microsoft 365 Zero Trust deployment plan*. URL: https://docs.microsoft.com/en-us/microsoft-365/security/microsoft-365-zero-trust?view=o365-worldwide. (accessed: 13.04.2021).

[55] Siemens. *Advanced Control for Onsite Energy Optimization*. URL: https://assets.new.siemens.com/siemens/assets/api/uuid:221822430df8e588a19ca62996f7e160b9b3af76/mgms-advanced-control-brochure.pdf. (accessed: 13.04.2021).

[56] Siemens. *Spectrum Power, the open and scalable platform for high, medium and low-voltage grid operation*. URL: https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-control.html. (accessed: 13.04.2021).

[57] Siemens. *Spectrum Power™ MGMS*. URL: https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/microgrid/spectrum-power-mgms.html. (accessed: 13.04.2021).

[58] Siemens. *Why microgrids are the future of energy management*. URL: https://assets.new.siemens.com/siemens/assets/api/uuid:fe665c240522441d27392dca1934df39cc06677f/microgrid-infographic-en-final.pdf. (accessed: 13.04.2021).

[59] Næringslivets sikkerhets-råd. «Mørketallsundersøkelsen 2020». I: (2020), s. 1–70. URL: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen.

[60] SMT. *Finding a straw in a haystack*. URL: https://www.smtware.com/en/knowledge-base/cyber-security-finding-straw-in-a-haystack/. (accessed: 13.04.2021).

[61] Statnett. *aFRR - sekundærreserve*. URL: https://www.statnett.no/for-aktorer-i-kraftbransjen/systemansvaret/kraftmarkedet/reservemarkeder/sekundarreserver/. (accessed: 13.04.2021).

[62] Statnett. «Fast Frequency Reserves 2018». I: (2018), s. 16–22. URL: https://www.statnett.no/globalassets/for-aktorer-i-kraftsystemet/utvikling-av-kraftsystemet/nordisk-frekvensstabilitet/fast-frequency-reserves-pilot-2018.pdf.

[63] Statnett. *NORFLEX*. URL: https://www.statnett.no/om-statnett/fou-og-teknologiutvikling/vare-sentrale-prosjekter/norflex/. (accessed: 13.04.2021).

[64] Statnett. «Systemdrifts- og markedsutviklingsplan 2022-2030». I: (2022). URL: https://www.statnett.no/globalassets/for-aktorer-i-kraftsystemet/utvikling-av-kraftsystemet/smup/systemdrifts--og-markedsutviklingsplan-2022-2030.pdf.

[65] Statnett. *Veien mot nullutslipp*. URL: https://www.statnett.no/contentassets/94e165aba0e94c9eb0b6eeacbd017028/langsiktig-markedsanalyse-2020-2050---veien-mot-nullutslipp---anders-kringstad.pdf. (accessed: 13.05.2022).

[66] Birger Stene, Tor Morten Sneve og Karstein Brekke. «Aldersfordeling for komponenter i kraftsystemet». I: (2005), s. 39. URL: https://publikasjoner.nve.no/rapport/2005/rapport2005_08.pdf.

[67] Geir Sveen. *Dette spadestikket koster mer enn det nye sykehuset: 10 milliarder kroner*. URL: https://www.aftenbladet.no/lokalt/i/lAnWGG/dette-spadestikket-koster-mer-enn-det-nye-sykehuset-10-milliarder-kroner. (accessed: 13.04.2021).

[68] Photon Research Team. *Vulnerability Intelligence: What's The Word In Dark Web Forums?* URL: https://www.digitalshadows.com/blog-and-research/vulnerability-intelligence-whats-the-word-in-dark-web-forums/. (accessed: 15.05.2022).

[69] Dina Temple-Raston. *A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*. URL: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack?t=1652290033056. (accessed: 15.05.2022).

[70] Tibber. *Lad elbilen smartere*. URL: https://tibber.com/no/smart-styring/elbillading. (accessed: 15.05.2022).

[71] Liam Tung. *Microsoft: SolarWinds attack took more than 1,000 engineers to createl*. URL: https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create/. (accessed: 13.04.2021).

[72] Fabio Viggiani. *The SolarWinds Orion SUNBURST Supply Chain Attack*. URL: https://www.truesec.com/hub/blog/the-solarwinds-orion-sunburst-supply-chain-attack. (accessed: 13.04.2021).

[73] Brad D. Williams. *NSA Urges Defense Sector to Adopt Zero-Trust Model After SolarWinds Hack*. URL: https://breakingdefense.com/2021/03/after-solarwinds-hack-nsa-pushes-zero-trust-model/. (accessed: 03.05.2021).

[74] *Windows XP*. URL: https://en.wikipedia.org/wiki/Windows_XP. (accessed: 13.04.2021).

[75] Omer Yoachimik. *DCloudflare thwarts 17.2M rps DDoS attack — the largest ever reported*. URL: https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/. (accessed: 13.04.2021).

[76] Omer Yoachimik og Vivek Ganti. *DDoS Attack Trends for Q4 2021*. URL: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/. (accessed: 13.04.2021).

[77] Andra Zaharia. *How Automation is Changing Cyber Crime: Exploits as a Service*. URL: https://heimdalsecurity.com/blog/exploit-kits-service-automation-changing-face-cyber-crime/. (accessed: 15.05.2022).

[78] Rikke Åserud. *Smartmålerne: Når blir de lønnsomme?* URL: https://www.huseierne.no/hus-bolig/tema/okonomi/smartmalerne-nar-blir-de-lonnsomme/. (accessed: 13.04.2021).