Logging og logganalyse i energiforsyningen

Studentrapport

Kristoffer Hovland, student ved Høgskolen i Oslo og Akershus

1
2017

RAPPORT

Rapport nr 1-2017
Logging og logganalyse i energiforsyningen

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør:

Forfattere: Kristoffer Hovland, student ved Høgskolen i Oslo og Akershus

Trykk: NVEs hustrykkeri
Opplag: 100
Forsidefoto: Wikipedia Commons
ISBN 978-82-410-1549-6
ISSN 1501-2832

Sammendrag: Energiforsyningen står ovenfor en stor utfordring i forbindelse med trusselbildet når det gjelder IKT-sikkerhet. Logging og logganalyse er en metode som brukes for å kunne etterforske hendelser med uønsket tilgang, men også for å kunne detektere indikatorer på uønsket adgang. Denne rapporten er initiert av NVE som en del av et kontinuerlig arbeid med å revidere og oppdatere beredskapsforskriften.

Emneord: Logging, IKT-sikkerhet, sårbarheter, IKT-hendelseshåndtering, beredskap

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

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

2017

Innhold

Forord **6**

Sammendrag **7**

1 Innledning **8**

1.1 Bakgrunn 8
1.2 Problemstillinger 9
1.3 Metode 10

2 Rammeverk for cyber-angrep **11**

2.1 «The Cyber Kill Chain» mot industrielle kontrollsystemer 11
2.1.1 Steg 1: Innbrudds-forberedelser og utførelse 11
2.1.2 Steg 2: Angrepsutvikling og utførelse 13

3 Kjente hendelser **14**

3.1 Stuxnet (2010) 14
3.2 Ukraina (2015) 15

4 Kontrollsystemer og loggmuligheter **16**

4.1 Kort om kontrollsystemer 16
4.2 Kort om industrielle nettverk 17
4.3 Loggformat 18
4.4 Loggverktøy 19
4.4.1 Logginnsamlingsverktøy 19
4.4.2 Logganalyseverktøy 20
4.5 Komponenter i industrielle kontrollsystemer 21
4.5.1 Historikk-database og loggserver 22
4.5.2 PLS/RTU/ IED 22
4.5.3 Servere og HMI 22
4.6 Nettverk 23
4.6.1 Modem, pakkeomformere/linker og fjerntilgangspunkter 23
4.6.2 IDS og IPS 24
4.6.3 Brannmur 24
4.6.4 Fieldbusnettverk 24
4.6.5 TCP/IP-baserte protokoller 25

5 Strategier for å benytte logger **25**

5.1 Eksempler på loggbare hendelser 25
5.2 Logging som verktøy for å detektere hendelser 26
5.3 Logging som respons etter hendelser 28

6 Vurderinger **29**

6.1 Muligheter for logging i industrielle nettverk 29
6.2 Hvordan benytte de forskjellige loggdataene 29
6.3 Hvordan sikre loggdata 30
6.4 Logging i nye teknologier og grensesnitt 30

7 Konklusjoner **30**

7.1 Muligheter for logging i industrielle nettverk 30
7.2 Logging for økt sikkerhet 31
7.3 Sikring av loggdata 31

7.4 Nye teknologier og grensesnitt 32

8 Anbefalinger 33

8.1 Holdningsarbeid og kompetansebygging 33
8.2 Kjenn dine systemer og følg med på trusselsituasjonen 33
8.3 Bruk logger, og analyser loggene 34
8.4 Inntrengningstesting 34

9 Videre arbeid 35

9.1 Trendlinjer etter forskjellige forhold 35
9.2 Analysemuligheter 35
9.3 Standardisering av loggformat 35
9.4 Eksterne sikkerhetsleverandører 35
9.5 Skytjenester 36

10 Ordliste med forklaring 37

11 Kilder 38

Forord

IKT er i dag en viktig bidragsyter for å kunne tilfredsstille samfunnets krav til forsyningssikkerhet og effektiv drift hos selskaper i energibransjen. Med økt digitalisering og økt integrasjon av ulike systemer følger også økt risiko i form av både utilsiktede og tilsiktede IKT-hendelser. Hendelsene i Ukraina i 2015 og advarsler fra Nasjonal sikkerhetsmyndighet tilsier at angripere kan ha tilgang til systemene i månedsvis uten at de blir oppdaget. I følge Richard H. Ledgett Jr., Deputy Director for National Security Agency, kommer det hver dag en million nye virus (skadevare), og alle med en internettforbindelse og litt kunnskap kan utgjøre en trussel mot individer, virksomhet, en by eller en nasjon. Industrikontrollsystemer er i økende grad utsatt for angrep.[1]

Dersom virksomhetene skal kunne oppdage hva som skjer i systemene, må aktivitet logges og loggene må bli analysert og tolket. I beredskapsforskriften[2] er det satt krav til logging i driftskontrollsystemet hos alle klasse 2 anlegg. Kravet gjelder også for klasse 3 anlegg, men det finnes ikke slike krav for klasse 1 anlegg. Et skriftlig tilsyn utført av Norges vassdrag og energidirektorat (NVE) i 2015 ga flere avvik på kravet om logging enn på andre krav.

I april 2016 satte NVE i gang et prosjekt der NVE ser nærmere på behovet for endringer i dagens regelverk, beredskapsforskriften, spesielt kapittel 6 og 7, samt måle- og avregningsforskriftens § 4.2 med veiledere.

Som ledd i gjennomgangen av IKT-regelverket engasjerte NVE sommeren 2016 en sommerstudent, Kristoffer Ervik Hovland, bachelorstudent ved Høgskolen i Oslo og Akershus, for å bistå i arbeidet om logging. Denne rapporten er et resultat av arbeidet. Rapporten bygger på en workshop gjennomført ved NVE i juni der representanter fra bransjen og leverandørene deltok, samt flere møter og intervjuer med sikkerhetseksperter i og utenfor energisektoren.

Vi takker alle som har bidratt med kunnskap og innspill til rapporten.

Oslo, 14. november 2016

Ingunn Åsgard Bendiksen

Ingunn Åsgard Bendiksen
Avdelingsdirektør Tilsyn og beredskap

[1] Vergun, D., "Critical Infrastructure Vulnerable to Attack, NSA Leader Says", *Army News Service* (April, 2016), URL: http://www.defense.gov/News/Article/Article/740177/critical-infrastructure-vulnerable-to-attack-nsa-leader-says, besøkt 10.08.2016.

[2] Norges Vassdrag og Energidirektorat, «Forskrift om sikkerhet og beredskap i energiforsyningen» - §7.14c, *Lovdata* (2013), URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157 , besøkt 10.08.2016

Sammendrag

Energiforsyningen benytter industrielle kontrollsystemer (kalt driftskontrollsystemer) for driften av sine distribusjons-, regional- og sentralnett og for balansering av produksjon og forbruk. Kontrollsystemene er sammensatt av spesialiserte komponenter og applikasjoner som kommuniserer over store avstander via egen kommunikasjonsinfrastruktur eller internett. Med den store digitaliseringen av bransjen følger sårbarheter. Angripere kan skaffe seg tilgang til systemene om de har ressurser og vilje til dette. «The Cyber Kill Chain», et rammeverk, som ble definert av analytikere på Lockheed-Martin i 2011, beskriver hvordan en angriper typisk vil gå frem for å få tilgang til datasystemer. SANS har beskrevet dette rammeverket i sin rapport «The ICS Cyber Kill Chain». Rammeverket beskriver to hovedsteg, 1) «Innbrudds-forberedelser og utførelse» og 2) «Angrepsfremgang og utførelse». Det har de siste årene vært flere hendelser rettet mot kontrollsystemer. De to mest kjente er Stuxnet-viruset som ble oppdaget av sikkerhetsfirmaet VirusBlokAda i midten av Juni 2011, og angrepet mot den ukrainske energiforsyningen i desember 2015. Anriperne benyttet her metoder som var veldig konsistent med «The ICS Cyber Kill Chain».

Det er viktig å sikre de industrielle kontrollsystemene mot hendelser som dette, og et viktig tiltak er overvåking og logging. Logger er data som blir opprettet og lagret sekvensielt når systemer og komponenter endrer status. Formålet er å oppdage, eller å hindre hendelser, samt å sikre bevis i etterkant av hendelser. For å kunne ha nytte av logger må det benyttes loggforsendelsesverktøy, som støtter en standard. En slik standard er syslog. Syslog støtter sending av loggmeldinger fra forskjellige komponenter slik at de kan samles på et sted, f.eks. på en server. Etter å ha samlet loggdata, kan logganalyseverktøy som Splunk eller Elastic Stack (ELK-stakken) brukes for å endre loggformat, korrelere og analysere data.

Å kartlegge alle muligheter det finnes for logging i industrielle kontrollsystemer og nettverk kan være krevende, da de fleste nettverk er unike i sammensetting og konfigurasjon. De forskjellige komponentene har forskjellige loggmuligheter, og ikke alle komponenter har muligheter for å sende loggmeldinger. Der det finnes muligheter for å sende loggmeldinger, er den essensielle informasjonen: hvem eller hva som har utført en handling, hva er gjort, når ble det gjort, og hva var utfallet av handlingen.

Loggbare hendelser er knyttet til autentisering, nettverksaktivitet, ressurstilgang, skadevare-aktivitet, system- og dataendringer og feilmeldinger. Disse dataene kan brukes til å detektere hendelsene i det øyeblikket det skjer, og til å etterforske hendelsesforløpet i etterkant. I en etterforskning etter en hendelse benyttes alle tilgjengelig data for å kunne rekonstruere hendelsesforløpet i størst mulig grad.

For hver enkelt virksomhet er det viktig å kartlegge alle muligheter som finnes for logging, og identifisere hvilke loggdata som er relevant i en sikkerhetssammenheng. Loggdata bør beskyttes mot tilgang fra uautoriserte brukere, sikres mot uautorisert endring og sletting, og tas sikkerhetskopi av. Deteksjonstiden for cyberangrep kan variere stort, og i enkelte situasjoner er det nødvendig å lagre loggene i flere år. Rapporten anbefaler lagring i to år dersom målsettingen er å oppdage aktivitet fra avanserte og kompetente trusselaktører. Rapportens anbefaling er videre at virksomhetene bygger kompetanse på logging og logganalyse og holder seg oppdatert på hvilke muligheter som finnes for logging, samt har en plan for implementering av nytt utstyr i nye og eksisterende systemer.

1 Innledning

1.1 Bakgrunn

Driften av energiforsyningen i Norge er i dag i stor grad digitalisert. I driften av sentral- og regionalnettet benyttes driftskontrollsystemer. Driftskontrollsystem omfatter alle komponenter som ivaretar overvåking og styring i energiforsyningen, herunder driftssentraler, sambandsanlegg, servere med programvare som benyttes til overvåking og styring av anlegg, infrastruktur som fører signaler i driftskontrollsystemet og system, infrastruktur og sambandsanlegg som kan styre eller programmere vern med tilhørende komponenter enten gjennom driftskontrollsystemet eller gjennom andre kommunikasjonskanaler (direkte tilknytning).[3] Et annet begrep som ofte brukes er Supervisory Control and Data Acquisition (SCADA). SCADA er et industrielt kontrollsystem (ICS) som overvåker og kontrollerer en prosess. I energiforsyningen overvåkes og kontrolleres nettstasjoner, transformatorer og andre elektriske komponenter, som eksempelvis brytere og vern.

Bruken av informasjons- og kommunikasjonsteknologi (IKT) for overvåkning, styring og kontroll av kraftnettet vil bare øke etter hvert som gammel teknologi byttes ut med ny. Det norske strømnettet er en kritisk infrastruktur for landet, og denne infrastrukturen er i dag kontrollert av sentraliserte driftssentraler som er knyttet mot lokale kontrollanlegg med industrielle nettverk. Overgangen til IKT-basert overvåkning og styring av energiforsyningen har gitt store effektivitetsgevinster for selskapene, men også en større risiko for at antall uønskede IKT hendelser kan øke. Slike hendelser vil kunne påvirke prosesstyringen og forsyningssikkerheten. I tillegg er introduksjon av ny teknologi og nye leverandører sikkerhetsmessig og regulatorisk utfordrende[4].

I rapporten «Helhetlig IKT risikobilde 2015»[5] beskrives det som Nasjonal Sikkerhetsmyndighet (NSM) mener er trusselbildet mot norske interesser. Her er det fokusert stort på nettopp kritisk infrastruktur, og energiforsyningen er naturligvis et av punktene. I rapporten fra NSM ble det blant annet nevnt et eksempel fra 2014, hvor flere norske virksomheter i olje- og energiforsyningen ble angrepet ved at utvalgte ansatte mottok eposter[6] med infiserte vedlegg. Ansatte som åpnet infiserte vedlegg var også inngangsporten til systemene som ble angrepet i Ukraina ved årsskiftet 2015/2016[7]. Å sikre seg mot slike hendelser er noe norsk energisektor allerede fokuserer på. I 2014 ble for eksempel KraftCERT etablert for å gi sektoren et dedikert respons- og varslingsmiljø for IKT-hendelser.

---

[3] Skapalen, F. og Gåserud, Ø, Kapittel 7, Beskyttelse av driftskontrollsystem, Foredrag på seminar om beredskapsforskriften 13. februar 2013, http://docplayer.me/1555204-Kapittel-7-beskyttelse-av-driftskontrollsystem.html, besøkt 30.08.2016.

[4] Det kongelige olje- og energidepartement, «Kraft til endring – Energipolitikken mot 2030», *Meld. St. 25* (2015 – 2016) URL: https://www.regjeringen.no/contentassets/31249efa2ca6425cab08130b35ebb997/no/pdfs/stm201520160025000dddpdfs.pdf, besøkt 10.08.2016

[5] Nasjonal Sikkerhetsmyndighet, «NSM Helhetlig risikobilde 2015», *Nasjonal Sikkerhetsmyndighet* (August 2015), URL: https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf, besøkt 10.08.2016

[6] FireEye Inc, "Cyber Threats to the Nordic Region", *Fireye* (Mai 2015), URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf, besøkt 10.08.2016

[7] Johansen, P.A., «De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet», *Aftenposten* (Januar 2016), URL: http://www.aftenposten.no/verden/De-sa-det-var-umulig-Na-klarer-russiske-hackere-a-sla-av-stromnettet-13199b.html, besøkt 10.08.2016

Overvåking og logging er blant tiltakene som benyttes i sikringen av driftskontrollsystemene. Formålet er å korte ned en eventuell deteksjonstid eller å forhindre hendelser, samt å sikre bevis i etterkant av hendelser. Dersom virksomhetene definerer hvilke hendelser som er uønsket og definerer mottiltak, vil analyse av logger også kunne bidra til å oppdage trusler og trender, og å forbedre sikkerheten i systemene. Denne rapporten tar for seg logging som verktøy, og ser på forskjellige problemstillinger rundt bruk av loggdata og logganalyse.

Gjeldende sikkerhetsbestemmelser for energiforsyningen er «Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen» (beredskapsforskriften), med tilhørende veiledning[8]. Den er utgitt av Norges vassdrag og energidirektorat (NVE). For å sikre at forskriften er oppdatert og relevant i forhold til dagens teknologi og utfordringer, jobbes det med forbedringer i beredskapsforskriften.

I 2016 fikk NVE ved beredskapsseksjonen innvilget interne forskningsmidler til et prosjekt – «Regelverksutvikling innen IKT-sikkerhet av betydning for energiforsyningens ivaretakelse av forsyningssikkerhet». Målet med prosjektet er å vurdere hvorvidt det er hensiktsmessig å innlemme nye sikkerhetskrav til IKT-system i beredskapsforskriften. Dette for å sikre helhetlig sikkerhetstankegang og –arkitektur, som er gjennomgående for driftskontrollsystemer, AMS, DMS og andre typer IKT-system. Rapporten gir innspill til NVEs arbeid med å gjennomgå beredskapsforskriften[9].

1.2 Problemstillinger

Rapporten diskuterer følgende spørsmål:

- Hvilke muligheter finnes det for logging i industrielle nettverk, og hvor finnes de forskjellige loggdataene?
- Hvordan kan de forskjellige loggdataene brukes for å øke sikkerheten mot uønsket adgang til systemene?
- Hvilke loggdata bør sikres, hvor lenge og hvordan?
- Hvordan håndtere logging i nye teknologier og grensesnitt?

En oversikt over hvilke loggmuligheter som finnes i industrielle nettverk er grunnlaget for å vurdere hvilke loggdata som er mest relevante for sikkerhet. Ved å se på hvordan de forskjellige loggdata benyttes for å øke sikkerheten mot uønsket adgang, vil det være muligheter for å utlede hvilke loggdata som er relevante å bruke og som bør sikres.

Siden innsamling og lagring av loggdata kan kreve store ressurser hos en bedrift, er det stilt spørsmål til hvilke loggdata som bør sikres, hvor lenge, og hvordan disse bør sikres.

Til slutt diskuteres spørsmålet om å håndtere logging i nye teknologier og grensesnitt.

[8] Norges Vassdrag og Energidirektorat, «Veiledning til forskrift om sikkerhet og beredskap i energiforsyningen», *Norges vassdrag og energidirektorat* (2013) URL: http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf , besøkt 10.08.2016

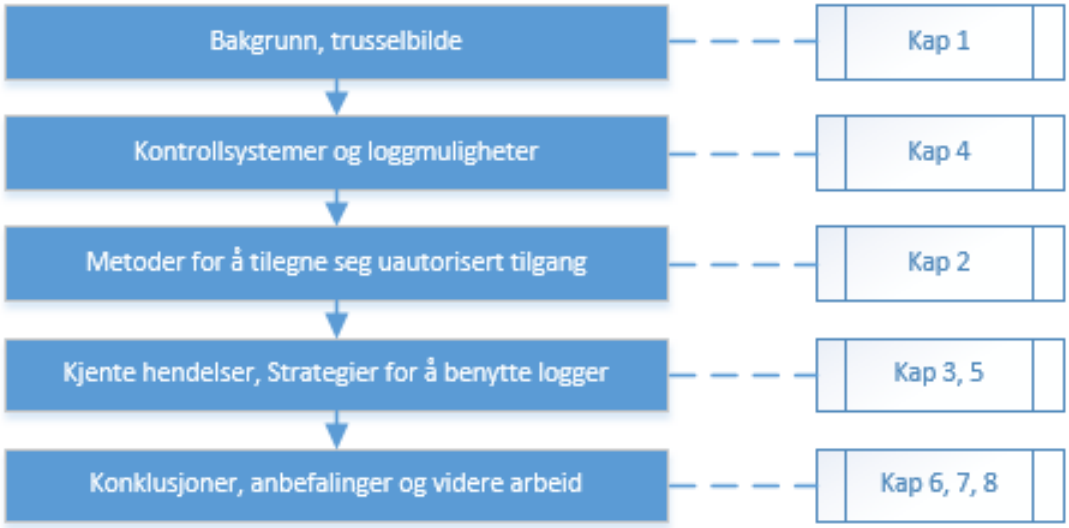
[9] Norges Vassdrag og Energidirektorat, «Forskrift om sikkerhet og beredskap i energiforsyningen», *Lovdata* (2013), URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157 , besøkt 10.08.2016

1.3 Metode

Prosjektet har innhentet data gjennom litteratursøk og gjennom:

- Epost til bransjen med spørsmål
- Telefonintervjuer og intervjuer med fagpersoner innen energiforsyningen, leverandører av industrielle kontrollsystemer, myndigheter og sikkerhetskonsulenter
- Workshop i NVE om logging 15. Juni 2016

Arbeidet er gjennomført i trinn, se Figur 1-1.



Figur 1-1 Arbeidsmetode

Arbeidet er gjennomført av et team i NVE bestående av:

- Avdelingsingeniør Kristoffer Hovland, NVE Beredskapsseksjonen og student ved Høgskolen i Oslo og Akershus
- Sjefsingeniør Janne Hagen, NVE Beredskapsseksjonen
- Overingeniør Jon-Martin Pettersen, NVE Beredskapsseksjonen

Rapporten er skrevet av Kristoffer Hovland.

2 Rammeverk for cyber-angrep

Selv om det finnesmange forskjellige metoder for cyber-angrep på industrielle kontrollsystemer er det nyttig å ha et rammeverk for å se på logging for IKT-sikkerhet. «The Cyber Killchain»[10] ble definert av Lockheed-Martin-analytikere i 2011 for å enklere kunne oppdage og respondere på innbrudd i IKT-systemer. Escal Institute of Advanced Technologies (SANS)[11] har laget en egen versjon kalt «ICS Cyber Kill Chain» [12], der beskrivelsene er omarbeidet til å rette seg mot industrielle kontrollsystemer.

2.1 «The Cyber Kill Chain» mot industrielle kontrollsystemer

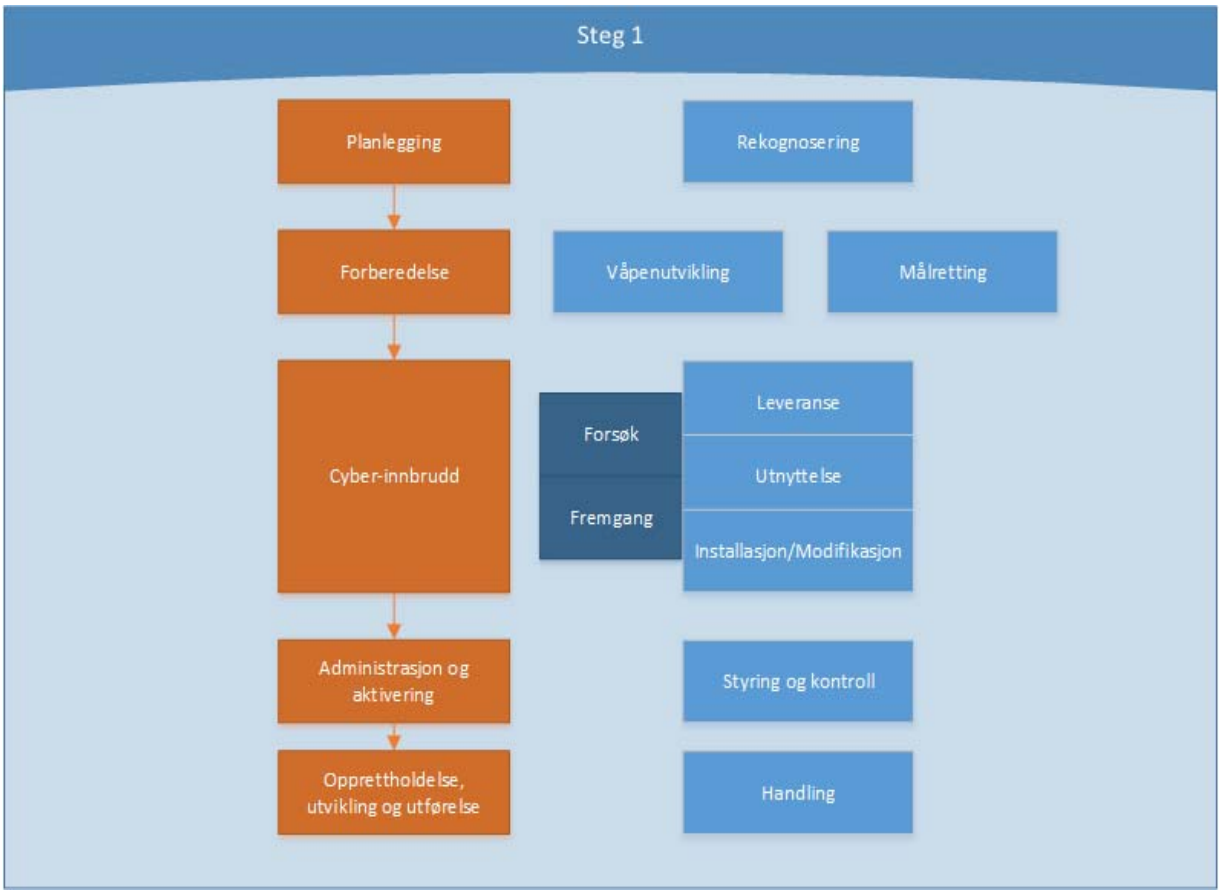
2.1.1 Steg 1: Innbrudds-forberedelser og utførelse

Det første steget er best kategorisert som aktiviteter som tradisjonelt ville blitt beskrevet som spionasje og informasjonsinnhenting. Formålet er å få tilgang til informasjon om systemet som skal angripes; lære seg systemet, levere mekanismer som kan omgå interne beskyttelser, og å få tilgang til produksjonsmiljøet.

[10] Hutchins, E.M., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Lockheed-Martin* (2010), URL: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf , besøkt 10.08.2016

[11] Escal Institute of Advanced Technologies (SANS), URL: http://www.sans.org

[12] Assante, M.J., Lee, R.M., "The Industrial Control System Cyber Kill Chain", *SANS Institute* (2016), URL: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297 , besøkt 10.08.2016



Figur 2-1 Steg 1 i ICS cyber-angrep

- Planlegging: I denne fasen gjøres det rekognosering/kartlegging av målet. Her er formålet å få nok informasjon til å avdekke svakheter i system og organisasjon til å utføre et vellykket angrep mot disse. Nyttig informasjon kan være nettverk, adresser for servere, brukerkontoer, protokoller, prosedyrer og mye mer. For industrielle kontrollsystemer kan denne fasen også inkludere studier for å finne tekniske sårbarheter og funksjoner, eller få en forståelse for hvordan prosesser og operasjonsmodeller kan være mulig å utnytte.
- Forberedelse: Etter at nok informasjon er hentet inn om målet, vil neste fase være å utvikle våpen som kan leveres til de valgte målene. Disse våpnene er oftest en form for fil som er injisert med skadelig programvare. De mest brukte filtypene for dette er PDF-filer og Word-dokumenter. Det blir også valgt ut mer spesifikke mål for å avdekke hvilke personer/systemer og hvilken metode som har størst sjanse for å gi et vellykket angrep.
- Cyberinnbrudd: For å få første tilgang til systemet gjøres det forsøk på å levere det utviklede våpenet, for eksempel ved såkalt «phishing» og «spear phishing»-eposter, eller ved å få koblet til infiserte minnepinner (USB). Angriperen ønsker her å få kjørt den skadelige programvaren, for å deretter utnytte svakheter i systemet. En annen metode kan være å forsøke å levere denne programvare via kontoer som er funnet, som har VPN-tilgang (Virtuelle private datanettverk). Forskjellen[13] på phishing og spear-phishing er at det i første tilfellet blir en melding eller epost med skadelig programvare sendt til enhver tilfeldig epostkonto i organisasjonen, mens i tilfellet med spear

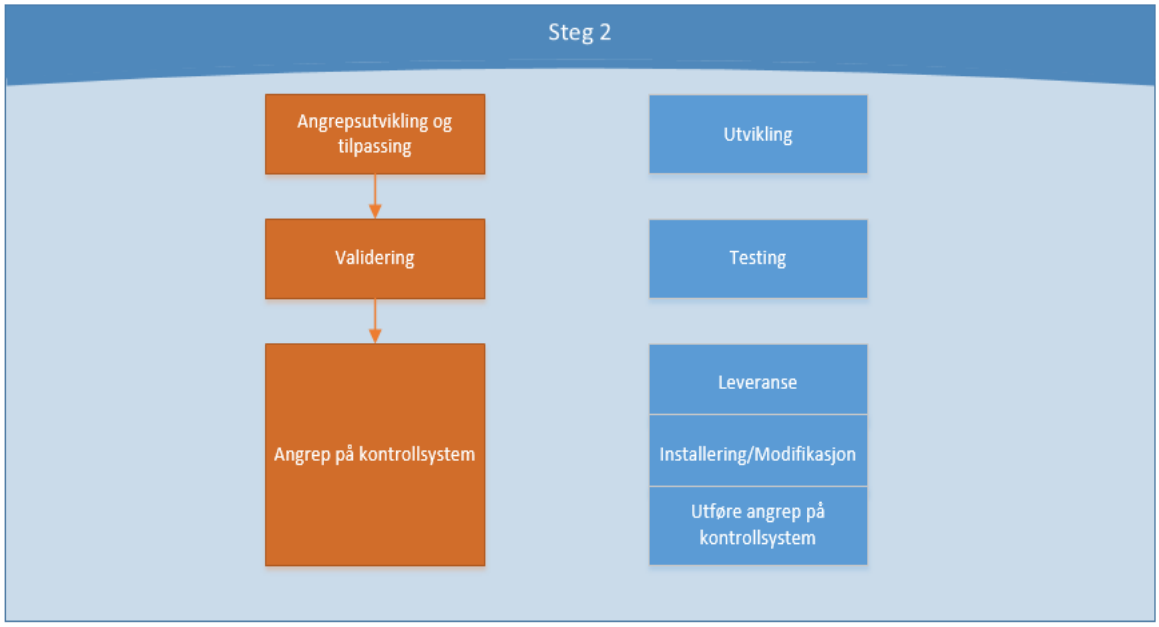
[13] Zetter, K., "Hacker Lexicon: What are phishing and spear phishing?", *Wired* (Juli 2015), URL: https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/ , besøkt 10.08.2016

phishing-eposter er meldinger laget for å fremstå som en melding fra noen mottakeren kjenner og stoler på. Når filen åpnes av mottaker får angriperen tilgang ved at det blir installert f.eks. en trojaner som gir mulighet for fjerntilgang, eller ved at tilgjengelige systeminnstillinger blir modifisert.

- Administrasjon og aktivering: Ved å utnytte tilgang gjennom alle identifiserte veier inn i systemet, prøver så angriperen å opprette styring og kontroll fra en maskin utenfor virksomheten (C2 – Command and Control). Det finnes mange forskjellige metoder å gjøre dette på, og ofte prøver angriperen å åpne flere bakdører inn i systemet. For å unngå deteksjon kamuflerer angriperen gjerne tilkoblingen ved å kommunisere via virksomhetens normale trafikkanaler.
- Opprettholdelse, utvikling og utførelse: Denne fasen inneholder mange forskjellige mål som en angriper kan ha, og det er i denne fasen angriperen begynner å manipulere systemet for å styrke fotfestet sitt. Vanlige aktiviteter inkluderer å identifisere tilknyttede systemer, og å forsøke å navigere uoppdaget rundt i nettverket for å finne nye tilganger som kan utnyttes. Et eksempel på slik aktivitet kan være å fange (sniffe) datapakker som sendes over nettverket, og få tilgang til brukerdata og lignende. For å unngå å bli oppdaget benyttes det også metoder for å fjerne alle spor, som å slette logger og andre data som kan avsløre den uønskede tilgangen.

2.1.2 Steg 2: Angrepsutvikling og utførelse

I dette steget bruker angriperen den den tilegnede kunnskapen til å utvikle og teste innbruddsverktøy (programvare).



Figur 2-2 – Steg 2 i ICS cyber-angrep

- Angrepsutvikling og tilpassing: Først vil angriperen utvikle og tilpasse nye skreddersydde verktøy som er ment å påvirke spesifikke områder i kontrollsystemet. Denne utviklingen vil mest sannsynlig skje ved bruk av informasjon angriperen fikk fra forrige steg. Som oftest vil dette skje på systemer utenfor virksomheten, noe som gjør denne fasen veldig vanskelig å oppdage. I utviklingsfasen kan det gå veldig lang tid.
- Validering: Etter at verktøyene er utviklet må angriperen teste om de fungerer. Dette gjøres på lignende eller identisk konfigurerte systemer, for å sikre at verktøyene har en signifikant og pålitelig påvirkning.

- Angrep på kontrollsystem: Her vil angriperen levere verktøyene via tilgjengelige kanaler, installereprogramvare, eller modifisere eksisterende systemfunksjoner. Til slutt utføres angrepet på kontrollsystemet. En angriper kan for eksempel sette parametre som manipulerer et gitt punkt i prosessen og forfalske prosessinformasjon for å lure operatører til å tro at alt er normalt.

3 Kjente hendelser

Det har de siste årene vært noen større angrep på driftskontrollsystemer som har fått stor oppmerksomhet internasjonalt. Disse hendelsene viser hvor viktig overvåking og logging i driftskontrollsystemer er.

3.1 Stuxnet (2010)

Et av de mest kjente cyberangrepene er Stuxnet-viruset som ble oppdaget av sikkerhetsfirmaet VirusBlokAda i midten av Juni, 2010.[14] Viruset inneholder en veldig spesialisert skadevare rettet mot industrielle nettverk. Stuxnet var det første viruset som inneholdt et rootkit rettet mot industrielle kontrollsystemer (et rootkit er en samling av dataprogrammer designet for å gi uautorisert tilgang til datamaskiner eller programmer), og inneholdt programvare som spionerte på industrielle nettverk. Etterforskning antyder at viruset rettet seg mot atomanlegg i Iran, og at målet var å slå ut Bushehr-anlegget, et atomanrikningsanlegg som ligger ved Persiabukten[15].

Stuxnet[16] infiserte systemer via en USB-minnepenn (når USB-minnepenner kobles til datamaskiner utveksles det en protokoll for å identifisere minnepennen, denne protokollen kan manipuleres til å laste opp et virus på datamaskinen[17]), og fortsatte så å infisere alle datamaskiner på det tilkoblede nettverket, som kjørte operativsystemet Microsoft Windows. Ved å benytte et digitalt sertifikat, som så ut til å komme fra en pålitelig kilde, lyktes Stuxnet å unngå å bli oppdaget av deteksjonssystemet. Etter å ha infisert systemene sjekket det så om maskinene var en del av det industrielle kontrollsystemet, som inneholdt programvare levert av Siemens. Hvis komponentene ikke var en del av kontrollsystemet, gjorde Stuxnet ingenting. I motsatt fall ville det prøve å få tilgang til internett. Via internett lastet Stuxnet ned en mer oppdatert versjon av seg selv hvis datamaskinen oppfylte kriteriene. Deretter infiserte Stuxnet de forskjellige kontrollerne. Stuxnet utnyttet sårbarheter i programvare som ikke hadde blitt oppdaget av sikkerhetseksperter på tidspunktet. Etter at Stuxnet hadde infisert kontrollerne, lå det uoppdaget over en periode og logget all aktivitet i systemet. Dette utnyttet Stuxnet til slutt ved å forfalske data tilbake til operatør-terminaler, mens det gjorde endringer i signaler til aktuatorer. Denne metoden forlenget tiden fra viruset begynte å gjøre endringer som var

---

[14] Kaspersky, E., "The Man Who Found Stuxnet – Sergey Ulasen in the spotlight", *Nota Bene* (November 2011), URL: https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/, besøkt 10.08.2016.

[15] Schneider, B., "The Story Behind The Stuxnet Virus", *Forbes* (Juli 2010), URL: http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html, besøkt 10.08.2016 og Anderson, N, «Confirmed: US and Israel created Stuxnet, lost control of it", URL: http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/, besøkt 19.09.2016.

[16] Kushner, D., "The Real Story of Stuxnet", *IEEE Spectrum* (Februar 2013), URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, besøkt 10.08.2016

[17] Rafter, M.V., "New Security Risks from USB Flash Drives", *Norton (Ukjent dato)*, URL: http://us.norton.com/yoursecurityresource/detail.jsp?aid=usbdrives, besøkt 10.08.2016

skadelige for prosessene til det ble oppdaget. Skadepotensialet ble dermed mye større. Konsekvensen ble at utstyr i anrikningsprosessen ble ødelagt.

Stuxnet endret hvordan verden så på IKT-sikkerhet. Angrepet viste at industrielle kontrollsystemer er sårbare for cyberangrep, blant annet som følge av økt bruk av tilkoblinger til andre systemer, og til internett.

3.2 Ukraina (2015)

Den 23. desember 2015 var det et større strømbrudd[18] i Ivano-Frankivsk Oblast, en region i de vestlige delene av Ukraina. Det viste seg i ettertid at strømbruddet var et resultat av et lenge planlagt cyber-angrep. Målet var å slå ut strømnettet med størst mulig virkning. Metodene aktørene benyttet i dette angrepet er konsistent med «The Cyber Kill Chain», beskrevet i kapittel 2.

Først ble de forskjellige strømleverandørene identifisert som mål. Angriperne benyttet automatiserte systemer i stor skala. Det ble utviklet og sendt ut spear-phishing-eposter. Epostene inneholdt Microsoft Office filer med skadevare skjult i makroer. (De benyttet en versjon av BlackEnergy 3-skadevare)[19].

Skadevaren inkluderte programvare som logget alle tastetrykk, og på denne måten fikk angriperne tilgang til informasjon som de kunne benytte til å gjøre endringer på brukerkontoer. På dette punktet hadde angriperne lykkes å sikre seg tilgang via VPN. Med den tilgangen siktet de seg så inn mot nettverkene hvor kontrollsystemene lå. Det er sannsynligvis brukt tid på å hente ut informasjon om systemene for å kunne skreddersy og utvikle programvare som så ble brukt i neste del av angrepet.

Da selve angrepet ble utført, var det gått et år siden phishing-epostene ble sendt. Angriperne benyttet metoder for å låse operatører ute fra kontrollsystemene, og de brukte leverandør-programvare til å levere kommandoer til kontrollsystemene via lokale kaprede konsoller. Disse kommandoene gikk i hovedsak ut på å lukke brytere, som kunne fjernstyres for å skape større strømbrudd. Minst 27 transformatorstasjoner mistet kontakt med nettet, og rundt 225 000 kunder ble uten strøm. Samtidig ble det lastet opp skadelig fastvare til pakkeomformere (Gateways) i stasjonene, noe som gjorde at det ikke lenger var mulig å kommunisere med dem via kontrollsystemet. Det ble også utført en aksjon mot telefonsentralene til virksomhetene under angrep; dette ble utført ved å kontinuerlig ringe til alle relevante telefoner fra datamaskiner med egnet programvare.[20] Det er svært sannsynlig at rekognosering ble foretatt på et tidspunkt, da den endelige angrepsmetoden var meget godt koordinert.

---

[18] Zetter, K., "Everything we know about Ukraine's power plant hack", *Wired* (Januar 2016), URL: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/, besøkt 10.08.2016

[19] Samani, R., "Updated BlackEnergy Trojan Grows More Powerful", *McAfee* (Januar 2016), URL: https://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/, besøkt 10.08.2016

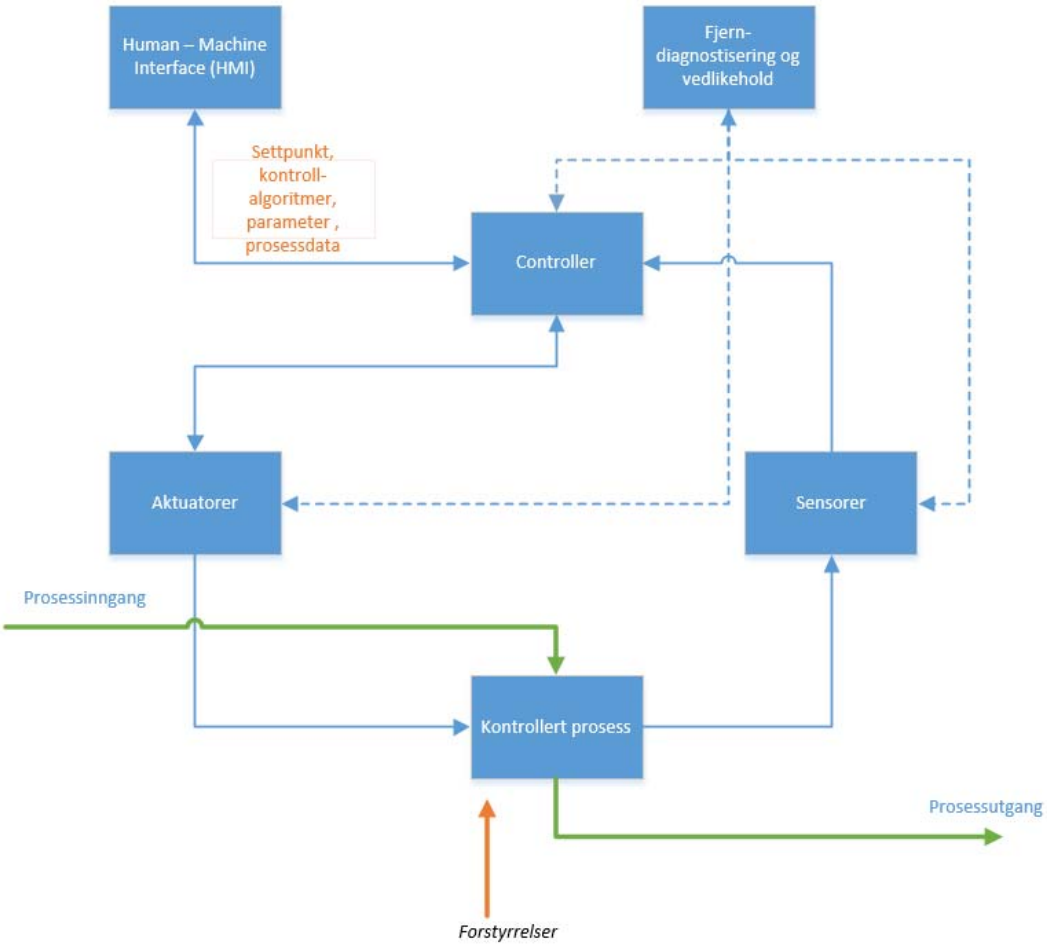
[20] Lee, R.M., "Analysis of the Cyber Attack on the Ukranian Power Grid", *SANS* (Mars 2016), URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, besøkt 10.08.2016

4 Kontrollsystemer og loggmuligheter

Dette kapittelet beskriver industrielle kontrollsystemer (ICS), og noen av loggmulighetene som finnes i de forskjellige komponentene og nettverkene. Kapittel 5 omtaler hvilke loggpunkter som kan knyttes opp mot sikkerhet.

4.1 Kort om kontrollsystemer

Elektrisk strøm blir produsert og konsumert i samme øyeblikk. Kontrollsystemer benyttes for å regulere produksjonen og overføringen av strøm til forbrukerne. Prinsipielt foregår ofte reguleringen som vist i figur 4-1. Dette prinsippet gjelder for øvrig for all regulering.



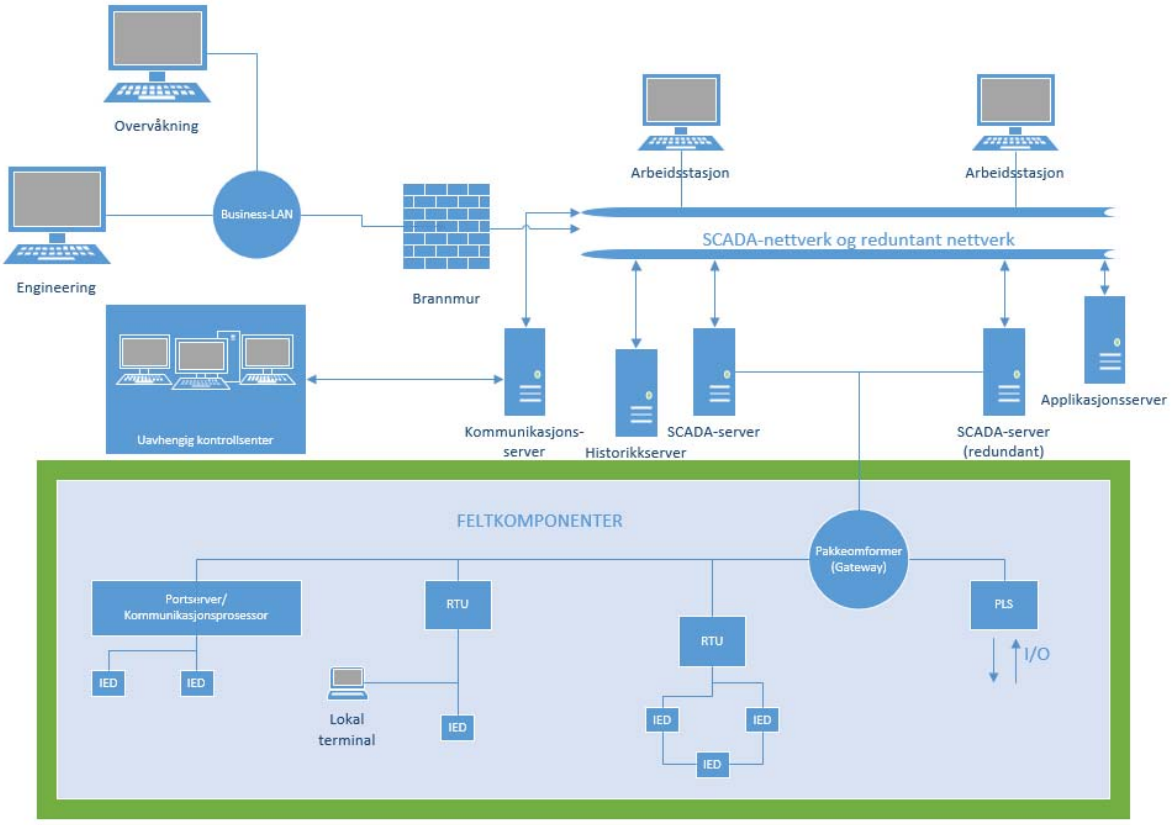
Figur 4-1 – Prinsipper for regulering i kontrollsystemer

Prosessen blir målt av sensorer av forskjellige typer som gir tilbakemelding til en kontroller, denne stilles inn via en HMI (Human Machine Interface). Kontrolleren sender deretter signal til en aktuator[21], som påvirker prosessen. Denne tidskonstante prosessen vil kjøre i sanntid, og korrigerer med aktuatorer for å hele tiden prøve å nå settpunktet.

[21] Aktuator er en komponent som gjør om elektrisk strøm (strømstyrt) eller elektrisk spenning (spenningsstyrt) til mekanisk bevegelse. Den mekaniske bevegelsen kan brukes direkte, eller til å styre hydrauliske eller pneumastiske ventiler (kilde wikipedia).

I energiforsyningen pågår denne tekniske reguleringen lokalt på et anlegg og over stor geografisk spredning. Det benyttes derfor industrielle kontrollsystemer og SCADA for å samkjøre reguleringen på et overordnet nivå.

4.2 Kort om industrielle nettverk



Figur 4-2 Prinsipptegning for industrielt nettverk

Industrielle nettverk er sammensatt av spesialiserte komponenter og applikasjoner der hovedkomponentene er kontrollere, lokale styringssystemer og SCADA[22]. I denne rapporten er industrielle nettverk en betegnelse på nettverk for kommunikasjon i automatiserte styringssystemer.

SCADA er en betegnelse som brukes mye i energiforsyningen for sentraliserte systemer som overvåker og kontrollerer prosesser over forskjellige typer nettverk. SCADA er industrielle kontrollsystemer som kan benyttes over et stort geografisk område.

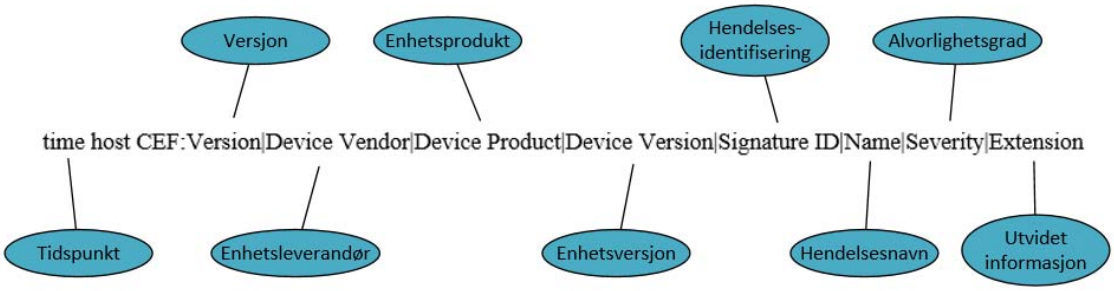
Prinsipielt deles gjerne nettverket (Figur 4-2) opp i 3 deler; virksomhetens vanlige nettverk (kontornettverk), SCADA-nettverk og feltkomponenter. SCADA-servere sørger for kommunikasjon mellom SCADA-nettverket og feltkomponentene, og i tillegg finnes det flere servere med forskjellige funksjoner koblet på det samme nettverket. Feltkomponenter kommuniserer med nettverket via en pakkeomformer, også kalt gateway. Pakkeomformere gjør

[22] OpenSecurityArchitechture, "SP-023: Industrial Control Systems", *OSA* (Ukjent dato), URL: http://www.opensecurityarchitecture.org/cms/library/patternlandscape/293-sp-023-industrial-control-systems, besøkt 10.08.2016

om de forskjellige fieldbus-protokollene til en protokoll som kan kommunisere via vanlige IP protokoller og omvendt. Det er forskjellig utstyr som brukes i industrielle nettverk, og kapittel 4.5 og 4.6 forklarer litt om noen av de vanligste komponentene og protokollene som benyttes, samt hvilke loggmuligheter disse har.

4.3 Loggformat

Definisjonen på et loggformat er måten en loggmelding er satt opp, og formatet avgjør hvordan meldingen tolkes. I industrielle kontrollsystemer sendes/lagres loggmeldinger i flere ulike loggformater. Formatet gir en struktur for lagring av loggpunkter. Noen eksempler er CEF (Common Event Format), CLFS (Common Log File System), CIM (Common Information Model) og CEE (Common Event Expression).Det sist omtalte formatet er for øvrig ikke lenger under utvikling[23]. Siden det ikke finnes en universell standard, er det i denne rapporten tatt utgangspunkt i et av de vanligste loggformatene som benyttes, CEF[24]. I en loggmelding som benytter CEF finnes følgende informasjon:



Figur 4-3 – Common event format

- Tidspunkt – Avhengig av hvordan en eventuell forsendelsesmetode er satt opp, vises tidspunktet her i valgt format
- Versjon – Dette identifiserer hvilken versjon av CEF formatet som benyttes. Denne informasjonen brukes deretter for å tolke hva de følgende punktene representerer
- Enhetsleverandør, produkt og versjon – Tekst som unikt identifiserer hvem eller hva som sendte loggmeldingen
- Hendelses-identifisering – Viser hvilken kategori hendelsen som ble rapportert er i. Dette kan være for eksempel være sikkerhet, egendefinert sikkerhet, brannmursikkerhet og systemsikkerhet[25]
- Hendelsesnavn – Dette er en kort beskrivelse av hendelsen
- Alvorlighetsgrad – Indikerer alvorsgraden av hendelsen. For CEF vises dette i tall fra 0-10, hvor 10 er den mest alvorlige

[23] Mitre Corporation, "Common Event Expression", *Mitre* (November 2014), URL: https://cee.mitre.org/, besøkt 10.08.2016
[24] ArcSight Inc, "Common Event Format", *McAfee* (Juli 2010), URL: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/78000/KB78712/en_US/CEF_White_Paper_20100722.pdf, besøkt 10.08.2016
[25] ArcSight Inc, "SecuSphere Configuration Guide", *Imperva* (April 2009), URL: https://www.imperva.com/docs/SB_Imperva_SecureSphere_CEF_guide.pdf, besøkt 10.08.2016

- Utvidet informasjon – Her finnes detaljer om hendelsen, og er den største delen av loggpunktet.

Det er som regel ikke mulig for alle komponenter å sende meldinger i samme format, derfor benyttes ofte loggverktøy for å konvertere meldingene til et felles format. Dette kommer det mer om i kapittel 4.4.

4.4 Loggverktøy

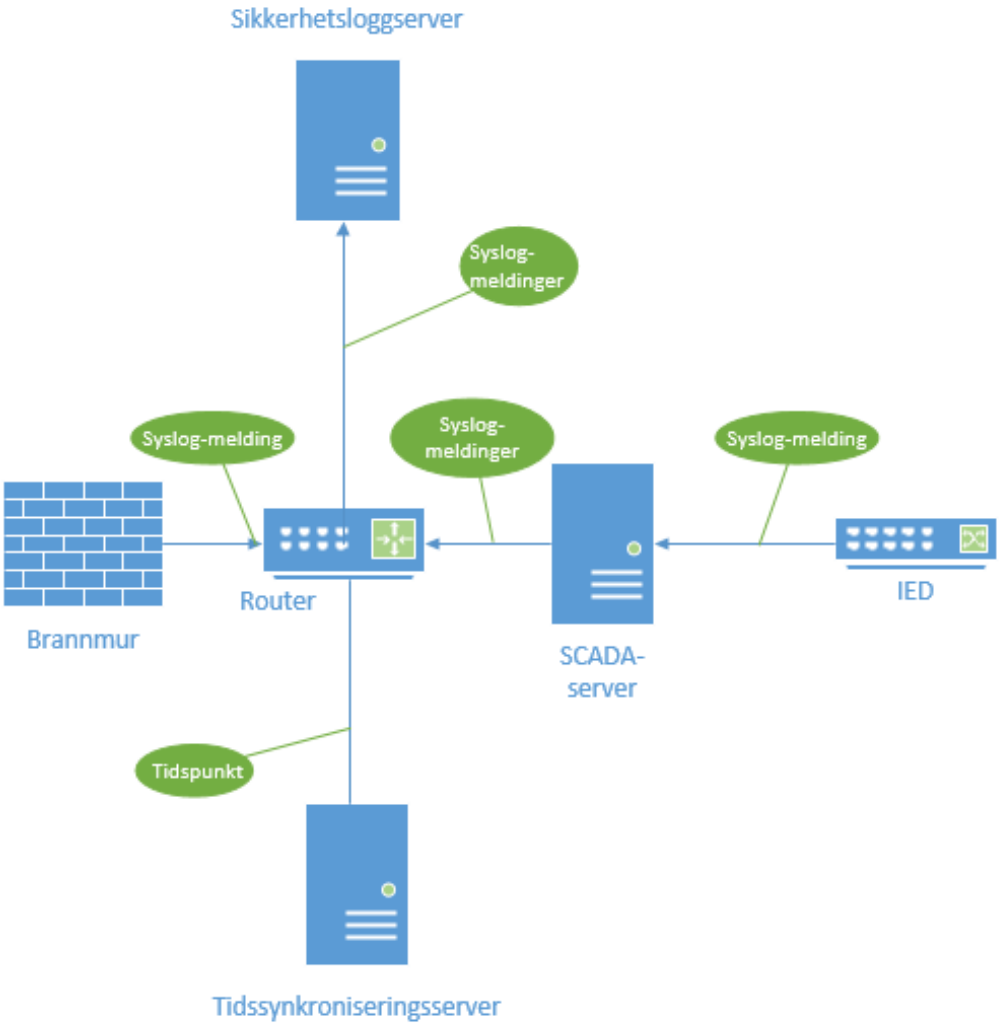
4.4.1 Logginnsamlingsverktøy

For å slippe å hente ut loggdata manuelt fra hver enkelt komponent, og å enklere behandle loggdata, benyttes det ofte et logginnsamlingsverktøy. Slike verktøy samler relevante data på en server. Et av de mest kjente standardene som benyttes til dette er syslog[26]. Syslog gjør det mulig å dele loggmeldinger med andre systemer som kan overvåke, lagre og analysere loggmeldingene, gjerne på en dedikert server.

Hvis komponenter har funksjoner for logginnsamlingsverktøy i henhold til syslog, så er det mulig legge inn en mottaker, og deretter blir hver hendelse som er satt i funksjonen sendt umiddelbart til en loggserver definert som mottaker. I figur 4-4 er syslog-serveren blitt navngitt sikkerhetsloggserver, og i dette tilfellet ville det vært loggmeldinger relatert til sikkerheten i systemet som blir overført. Det er viktig å være klar over at syslog og andre standarder for logginnsamlingsverktøy kun definerer en forsendelsesmetode[27], og ikke utfører andre handlinger enn nettopp å oversende meldingene. Et annet vesentlig punkt er at ved å benytte tidssynkronisering, såkalt NTP (Network Time Protocol), så sikres det at alle loggbeskjedene som sendes til sikkerhetsloggserver har korrelerte tidsstempler, og dermed vil bli lagret i riktig tid og sekvens.

[26] Eaton, I., "The Ins and Outs of System logging Using Syslog", *SANS Institute* (2003), URL: https://www.sans.org/reading-room/whitepapers/logging/ins-outs-system-logging-syslog-1168, besøkt 10.08.2016

[27] Leskiw, A., «Understanding Syslog: Servers, Messages & Security», *Network Management Software* (Ukjent dato), URL: http://www.networkmanagementsoftware.com/what-is-syslog/, besøkt 10.08.2016

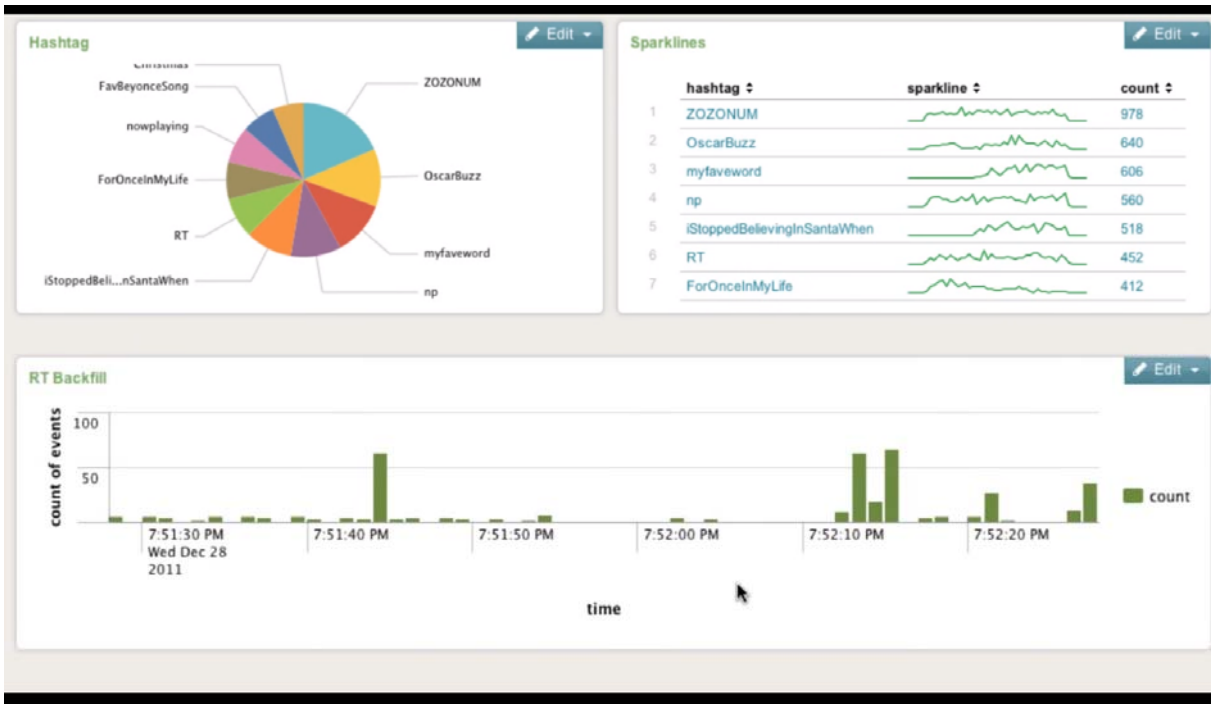


Figur 4-4 – Syslog eksempel: Alle komponenter sender, uavhengig av plassering, loggmeldinger til sikkerhetsloggserver

4.4.2 Logganalyseverktøy

Selv om loggdata er samlet på ett sted er det gjerne krevende å analysere og overvåke denne loggen. Det benyttes derfor forskjellige logganalyseverktøy, Security Information and Event Management-programmer (SIEM-programmer) for å forenkle dette arbeidet. To eksempler er Elastic Stack (ELK-stakken[28] (en samling av gratis programvare), og Splunk, et kommersielt program[29].

[28] Nasjonal Sikkerhetsmyndighet, «Systemovervåking ved bruk av ELK-stakken», *Nasjonal Sikkerhetsmyndighet* (April 2016), URL: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-11_systemovervaking_ved_bruk_av_elk-stakken.pdf, besøkt 10.08.2016, se også Elastic Stack, https://www.elastic.co/webinars/introduction-elk-stack, besøkt 30.08.2016.
[29] Klein, H., "What is Splunk and How Does it Work?", *Helgeklein.com* (September 2014), URL: https://helgeklein.com/blog/2014/09/splunk-work/, besøkt 10.08.2016



Figur 4-5 Skjermbilde fra Splunk demonstrasjonsvideo (trendanalyse)[30]

Programmer for loggbehandling muliggjør å:

- Samle
- Korrelere
- Kategorisere
- Søke
- Sette opp varslinger
- Analysere data

Programmene kan også konvertere loggdata fra ulike kilder til et felles format, indeksere, lagre data i en sentral database og, som vist i figur 4-5, presentere loggdata grafisk til bruker. Det kreves god kunnskap om systemene som skal analyseres og overvåkes for å ha fullt utbytte av slike programmer.

4.5 Komponenter i industrielle kontrollsystemer

Det er nødvendig for operatørene å ha en god oversikt over hvilke komponenter som benyttes i industrielle kontrollsystemer. Denne rapporten tar utgangspunkt i "National Institute of Standards and Technology" sin «Guide to Industrial Control Systems (ICS) Security»[31].

---

[30] Splunk, «Splunk 4.3 Demo» (Video), *Splunk* (Januar 2012), URL: http://www.splunk.com/view/SP-CAAAGNB, besøkt 10.08.2016

[31] Stouffer, K., "Guide to Industrial Control Systems (ICS) Security", *National Institute of Standards and Technology* (Juni 2011), URL: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, besøkt 10.08.2016

4.5.1 Historikk-database og loggserver

En historikk-database (Historian) er en sentralisert database som logger prosessinformasjon i et industrielt kontrollsystem. Data som er lagret her kan brukes for å gjøre forskjellige analyser for statistisk prosesskontroll.

Andre loggdata, som for eksempel sikkerhetsrelaterte logghendelser, går til egen dedikert loggserver. Loggserveren kan være plassert i prosessnettet, eller på en annen plassering (som et parallelt driftsnett eller en sentral server).

4.5.2 PLS/RTU/ IED

Programmerbar logisk styring (PLS) er en liten industriell datamaskin som er designet for å utføre logiske funksjoner, som blir til fysiske handlinger utført av elektrisk maskinvare (Reléer, brytere og mekaniske tellere/timere). PLS har utviklet seg til kontrollere med mulighet for å styre komplekse prosesser, og de er mye brukt i SCADA.

Remote terminal unit (RTU) er elektroniske komponenter med egen mikroprosessor som kan sende og motta signaler i SCADA-nettverket. De er feltkomponenter, noen ganger utstyrt med trådløst radiogrensesnitt for å kunne fungere i områder hvor kabelbasert kommunikasjon er utilgjengelig. Noen ganger er PLS implementert som feltkomponenter for å fungere som en RTU. I disse tilfellene blir ofte PLS referert til som RTU.

En Intelligent Electronic Device (IED) er en «smart» sensor/aktuator som har nok prosessorkraft til å hente data, kommunisere med andre komponenter og utføre lokal prosessering og kontroll. Den kan kombinere en analog sensor, analog utgang, kommunikasjonssystem og minne i en komponent. Bruk av IED i SCADA-systemer tillater automatisk styring på et lokalt nivå.

Ikke alle IED har muligheter for å sende loggdata til en loggserver, men teknologien utvikles i retning av flere muligheter for å benytte loggfunksjoner som støtter for eksempel syslog[32]. Siden IED, PLS og RTU er feltutstyr, så har de til dels de samme loggfunksjonene. Loggfunksjoner kan være:

- Innlasting og oppdatering av parametere og fastvare
- Påloggingsforsøk
- Tilkoblinger
- Oversikt over hvilke tilkoblingsporter som brukes
- Bytte av minnekort

4.5.3 Servere og HMI

Avhengig av konfigurasjon, kan et industrielt nettverk inneholde mange forskjellige servere. Noen av de vanligste betegnelsene er:

> Kontrollserver - kjører overordnede kontrollprogrammer og kommuniserer med kontrollere på lavere nivå. Den har tilgang på underordnede kontrollmoduler over et

[32] Intervju med leverandørselskap

industrielt nettverk. Kontrollserveren fungerer som «master» i et SCADA-system, og har mange kallenavn, deriblant SCADA-server og Master Terminal Unit (MTU).

Inngang/utgangsserver[33] er en komponent som er ansvarlig for å samle inn, bufre og gi tilgang til prosessinformasjon fra underkomponenter som PLS, RTU og IED. Serveren kan være felles med kontrollserveren, eller på en egen datamaskin. Den er også brukt som grensesnitt for tredjeparts komponenter, som HMI og fjerntilgang.

Human-Machine Interface (HMI) er en komponent med programvare og maskinvare som tillater personell å overvåke statusen av en prosess som blir regulert. HMI er ofte representert av en liten interaktiv skjerm som kan modifisere reguleringsinnstillinger, eksempelvis settpunkt, og manuelt overkjøre automatiske reguleringsoperasjoner i nødstilfeller. I tillegg viser den prosessens statusinformasjon, historikk, rapporter og annen informasjon. Plattform og grensesnitt på HMI varierer.

Konfigurasjonsstasjoner (Engineering workstation) er datamaskiner som benyttes for å vedlikeholde og feilsøke i applikasjoner og komponenter i nettverket.[34]

Arbeidsstasjoner er datamaskiner i sentraler som benyttes til daglig drift av kontrollsystemene, og som brukes til å overvåke og gjøre endringer på feltkomponenter.

Loggmuligheter på arbeidsstasjoner, servere og HMI er avhengig av hvilken programvare den kjører og hvordan serveren er satt opp, men kan kategoriseres som[35]:

- Applikasjonslogg – Hendelser for alle bruker-program
- Sikkerhetslogg – Påloggingsforsøk, fil-endringer og annen informasjon (hvem, hva, når, etc.) relatert til sikkerhet
- Systemlogg – Driveroppdateringer, komponent-endringer. Hendelser som er relatert til selve komponentens tekniske tilstand

4.6 Nettverk

4.6.1 Modem, pakkeomformere/linker og fjerntilgangspunkter

For å tillate komponenter å kommunisere benytter en et modem som konverterer mellom seriell digital data og et signal passende for overføring over en telefonlinje. Modem blir ofte benyttet i SCADA systemer for å muliggjøre langdistanse seriell kommunikasjon mellom MTU og fjerntliggende komponenter.

En ruter er en komponent som overfører (ruter) datapakker mellom nettverk. Vanlig bruk av rutere inkluderer å koble et kablet nettverk til et trådløst nettverk, og å koble MTU og RTU til et større nettverk for SCADA-kommunikasjon. Pakkeomformere omformer fra en nettverksprotokoll til en annen.

Fjerntilgangspunkter benyttes for å konfigurere kontrollsystemer og hente ut prosessdata. Eksempler inkluderer å bruke et nettbrett til å hente data i et lokalt nettverk (LAN) gjennom et

[33] Omtalt som "Frontend".
[34] ICS-CERT, "Control System Engineering Workstation", *ICS-CERT* (Juli 2016), URL: https://ics-cert.us-cert.gov/Control_System_Engineering_Workstation-Definition.html, besøkt 10.08.2016
[35] Microsoft, "Event Logs and Channels in Windows Event Log", *Microsoft* (Juni 2012), URL: https://msdn.microsoft.com/en-us/library/aa385225.aspx, besøkt 10.08.2016

trådløst tilgangspunkt, og å bruke en datamaskin og modem for å logge inn på et industrielt kontrollsystem.

Loggmuligheter vil variere etter type utstyr og produsent, men et minimum vil som regel være[36]:

- Dato og tidspunkt
- Kilde-adresse og mål-adresse (IP)
- Handling (F.eks. om tilgang ble blokkert eller tillatt, brukerkonto pålogget mm.)

4.6.2 IDS og IPS

IDS og IPS står for, henholdsvis, Intrusion Detection System og Intrusion Prevention System[37]. Samlebetegnelsen er ofte IDPS. Dette er en komponent eller applikasjon som overvåker nettverk og systemaktiviteter for å avdekke, eller hvis det er en ren IPS, blokkere uønsket trafikk. IDPS analyserer både pakkehoder og innhold i pakker sendt over nettverket.

4.6.3 Brannmur

Brannmuren beskytter komponenter i et nettverk ved å overvåke og kontrollere kommunikasjons-pakkehoder i nettverkstrafikk mot forhåndsdefinerte filter. Brannmurer benyttes også for å segmentere industrielle nettverk, og nyere brannmurer har ofte innebygd IDPS.

Loggmuligheter i brannmurer kan være[38]:

- Brukt protokoll
- Port
- Pakkestørrelse
- Avsender/Mottakeradresse

4.6.4 Fieldbusnettverk

Fieldbusnettverket sørger for kommunikasjon mellom sensorer og andre komponenter til en PLS eller annen type kontroller. Bruk av fieldbusteknologi eliminerer behovet for direkte tilkobling mellom kontrolleren og hver komponent. Komponentene kommuniserer med kontrolleren ved hjelp av forskjellige protokoller, som krever spesialkabler og tilkoblinger (blant annet modbus og profibus). Pakkene som blir sent mellom komponentene og kontrolleren identifiserer hver unike komponent. Protokollene kan logges via IDS og IPS.

---

[36] Netgear, "How do i view the activity logs of my Nighhawk router?", *Netgear* (Februar 2016), URL: http://kb.netgear.com/app/answers/detail/a_id/24224/~/how-do-i-view-the-activity-logs-of-my-%20nighthawk-router%3F?cid=wmt_netgear_organic, besøkt 10.08.2016

[37] Scarfone, K., "Guide to Intrusion Detection and Prevention Systems (IDPS)", *National Institute of Standards and Technology* (Februar 2007), URL: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, besøkt 10.08.2016

[38] Microsoft, Interpreting the Windows Firewall Log, *Microsoft* (Ukjent dato), URL: https://technet.microsoft.com/en-us/library/cc758040(v=ws.10).aspx, besøkt 10.08.2016

Loggmuligheter i fieldbus-nettverk er blant annet [39]:

- Pakkestørrelser
- Funksjonskoder/kommandoer
- Trafikk på porter brukt til de forskjellige protokollene

4.6.5 TCP/IP-baserte protokoller

Det er veldig varierende hvilke protokoller som er brukt øvrige steder i SCADA-nettverk. Noen av de vanligste er ICCP/TASE.2, DNP3, IEC 60870-5-104 («104-protokollen»). 104-protokollen er en av de mest populære for å kommunisere via gateway til SCADA-server), og de kommuniserer via forskjellige komponenter i et WAN (Wide Area Network).

Loggmuligheter i nettverkstrafikk vil være bestemt av hvilket verktøy du bruker til å logge nettverkstrafikken med. IDS eller IPS som er plassert i nettverket er en metode å gjøre dette på i dag: [40]

- Pakkestørrelser
- Funksjonskoder/kommandoer
- Trafikk på porter brukt til de forskjellige protokollene

Bruk av IPS i prosesskontroll er lite utbredt siden slik programvare kan stenge ned prosesser og kople ut brytere.

5 Strategier for å benytte logger

Hovedformålet med sikkerhetslogging i industrielle nettverk i energiforsyningen er å:

- Korte ned deteksjonstiden og gjøre det mulig å forhindre hendelser slik at forsyningssikkerheten blir ivaretatt
- Sikre bevis i etterkant av hendelser
- Sikre informasjon for å kunne gjenopprette systemer til normal drift etter hendelser

I dette kapittelet vil rapporten gå litt nærmere inn i metoder som sørger for å oppfylle de overnevnte kriterier, samt gi noen eksempler på loggpunkter som er relevant for sikkerhet.

5.1 Eksempler på loggbare hendelser

Hva som blir logget er avhengig av hvordan loggene er satt opp, type utstyr, og hvordan utstyret blir brukt. Dermed blir det utfordrende å gi en beskrivelse av hva som blir logget, men noe av det som ofte[41] er relevant for sikkerhetslogging er presentert i Tabell 5-1.

---

[39] Knapp, E.D., (2011) *Industrial Network Security*, USA: Syngress
[40] Knapp, E.D., (2011) *Industrial Network Security*, USA: Syngress
[41] Czanik, P., "The 6 Categories of Critical Log Information", *SANS Institute* (Versjon 3.01), URL: http://www.sans.edu/research/security-laboratory/article/6toplogs, besøkt 10.08.2016

Autentisering	Nettverksaktivitet
Påloggingar og forsøk på påloggingar Tilgangsendringer i filer og lignende Installasjon av applikasjoner og oppdateringer	Interne tilkoblinger Eksterne tilkoblinger Trender
Ressurstilgang	**Skadevare-aktivitet**
Tilgang til ressurser på kritiske systemer Forsøk på å nå svartelistede domener All tilgang fra privilegerte brukere	Trend av all deteksjon av skadevare med utfall av hendelsen Alle interne tilkoblinger til kjente skadevare IP-adresser
System - og dataendringer	**Feilmeldingar og kritiske feil**
Endringer av brukerkontoer og brukergrupper Passordendringer og tilbakestilling av passord Endringer i nettverkstjenester Endringer i systemfiler og konfigurasjoner Endringer i tilgangsnivåer Installasjoner av programmer og oppdateringer gjort av system	Kritiske feil fra system og applikasjoner System og applikasjonskrasj, nedstenginger og omstarter Feil under kjøring av backup Kapasitetsproblemer fra minne, harddisk, prosessor og andre systemressurser

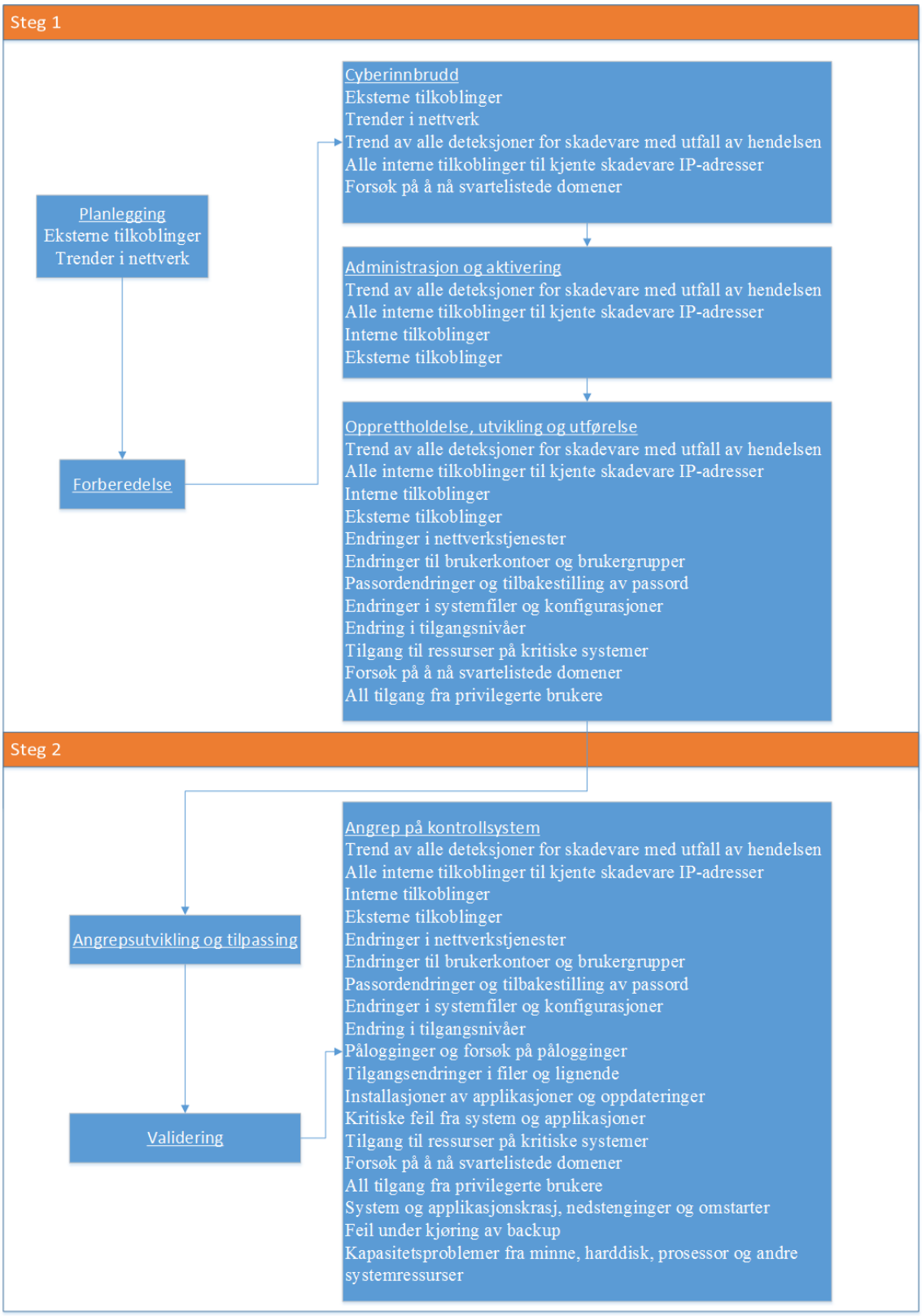
Tabell 5-1 - Sikkerhetshendelser

5.2 Logging som verktøy for å detektere hendelser

For å hindre stor skade er det viktig å oppdage en uønsket hendelse så tidlig som mulig. Her er det vesentlig at virksomheten har kartlagt alle muligheter for logging i systemene og kartlagt hvilke loggdata som er relevante å analysere. Det bør etableres en overvåkning av loggene som kan gjenkjenne avvik i logghendelser. Avvik kan indikere at det er en pågående uønsket hendelse. Denne overvåkningen kan være manuell dersom det er etablert gode rutiner for å analysere loggene periodisk. For automatisk overvåkning benyttes SIEM-programmer[42], som gjennomgår loggene i nåtid, og analyserer etter forhåndsdefinerte mønstre[43]. For SIEM-programmer kan det settes opp forskjellige regler for hvilke hendelser og grenseverdier som kan gi en alarm.

SIEM-programmer kan ofte settes opp slik at hendelser fra de forskjellige komponentene blir sammenlignet (korrelert). Når grenseverdier blir overskredet, trigger det alarmer.

[42] Swift, D., "A Practical Application of SIM/SEM/SIEM Automating Threat Identification", *SANS Institute* (Desember 2006), URL: http://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781, besøkt 10.08.2016
[43] Intervju med sikkerhetsorgan



Figur 5-1 Eksempel på loggmuligheter i ICS Cyber Kill Chain

Det finnes for øvrig mange indikatorer på at en uønsket hendelse pågår (se Figur 5-1). Siden angrepsmetoder varierer, kan virksomheten på forhånd simulere forskjellige angrepsscenarioer for å avdekke mulige svakheter.

Automatisert overvåkning må være satt opp riktig av personell med kompetanse på området før det kan gi alarm til vanlige brukere. Brukere kan deretter varsle om det skulle oppstå hendelser. Det er viktig at man velger seg en generell SIEM-løsning som kan korrelere på tvers av utstyr fra ulike leverandører, alle nettverkssoner, samt applikasjonene og systemene som selskapet har. Da kan selskapet spore hendelser gjennom hele nettverket.

Det kan være hensiktsmessig å sammenligne rammeverk og loggmuligheter, og Figur 5-1 er et eksempel på hvordan de forskjellige fasene i ICS Cyber Kill Chain kan logges og detekteres. Noen av fasene er uten loggpunkter fordi dette er faser hvor det normalt ikke er noe kontakt mellom angriper og virksomhet.

5.3 Logging som respons etter hendelser

I etterkant av en hendelse vil det som regel bli gjort en etterforskning[44]. Dette har flere formål:

- Isolere den aktive programvaren som forårsaker hendelsen raskest mulig for å få færrest mulig negative konsekvenser for virksomheten
- Kunne gjenopprette systemet til den tilstand det hadde før hendelsen
- Sikre bevis for en eventuell anmeldelse
- Identifisere tiltak for å forhindre at lignende scenarioer kan inntreffe igjen

Å benytte loggdata er bare en del av en etterforskning. Det er ønskelig å få all tilgjengelig informasjon om systemet etter en hendelse, og dette inkluderer å hente ut all informasjon og konfigurasjoner av alt tilgjengelig utstyr i størst mulig grad. Når all informasjon er hentet ut, er målet å gjenskape et detaljert hendelsesforløp. Her benyttes det i hovedsak vitenskapelige metoder[45], slik at etterforskningen er etterprøvbar. Det er ofte enorme mengder loggdata som må analyseres, så når en forsøker å gjenskape hendelsesforløpet, vurderes relevansen av forskjellige data før det gjøres nærmere analyser. For å gjenskape hendelsesforløp er det vesentlig å vite tidspunkt og metode for den første indikatoren, slik at en vet hvilket punkt systemet skal gjenopprettes til. Her vil det være uheldig om det ikke har vært benyttet tidssynkronisering på alle komponenter som har sendt loggdata.

I situasjoner etter en hendelse oppstår det dilemma: Ønskes det å gjenopprette systemet til normal drift så raskt som mulig, eller å gjøre en grundig etterforskning[46]? En grundig etterforskning forutsetter gjerne at systemet «fryses» ned til all nødvendig informasjon er lagret, og deretter kan det gjenopprettes. I driftskontrollsystem i energiforsyningen vil det ikke være aktuelt å fryse systemet, da det vil være essensielt å gjenopprette så snart som mulig. Utvidet bruk av logging i et system kan være med på å korte ned denne nedetiden siden det ikke i samme grad vil være behov for å hente ut data manuelt.

---

[44] Folkerth, L., "Forensic Analysis of Industrial Control Systems, *SANS Institute* (September 2015), URL: https://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-industrial-control-systems-36277, besøkt 10.08.2016

[45] Andersen, H., "Scientific Method", *Stanford* University (November 2015), URL: http://plato.stanford.edu/entries/scientific-method/, besøkt 10.08.2016

[46] Kral, P., "The Incident Handlers Handbook", *SANS Institute* (Desember 2011), URL: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901, besøkt 10.08.2016

6 Vurderinger

6.1 Muligheter for logging i industrielle nettverk

Det som har blitt presentert av loggmuligheter i rapporten er funnet gjennom litteraturstudier. I kapittel 4.5 og 4.6 er det blitt presentert en del loggmuligheter på forskjellig utstyr som benyttes i dag, både i nettverk og i feltkomponenter. De forskjellige komponentene som er tatt med her i rapporten er de som typisk blir brukt i kontrollsystemer, men dette er ikke er uttømmende liste. I løpet av prosjektet har det blitt avdekket at industrielle kontrollsystemer benytter en stor variasjon av utstyr og konfigurasjoner.

Det ble grunnet denne variasjonen lite hensiktsmessig å gjennomgå komponent for komponent under gjennomføring av intervjuene. De fleste virksomheter logger i dag trafikk i sine nettverk og hendelser på servere og arbeidsstasjoner, mens noen også logger feltkomponenter som støtter syslog-funksjoner. Det har kommet frem i intervjuene at produkter med samme funksjoner, men forskjellige leverandør og modell, kan ha vidt forskjellige loggmuligheter. Derfor kan ikke loggmulighetene beskrives nøyaktig.

Et logginnsamlingsverktøy gjør det mulig å bruke logging aktivt i industrielle nettverk. Dersom utstyr ikke støtter f.eks. syslog vil det være vanskelig å gjøre seg nytte av de forskjellige loggdata.

6.2 Hvordan benytte de forskjellige loggdataene

For å kunne få fullt utbytte av overvåkningsverktøy må det være investert tilstrekkelig tid i å etablere en grunnlinjeovervåkning (baseline), for å vite hva som er normal oppførsel i et kontrollsystem. Når det gjelder nettverkstrafikk i SCADA-systemer så er trafikken til en viss grad statisk, og det skal med tilstrekkelig kompetanse være gode muligheter for å etablere en baseline rundt denne. [47]

Det er vist i figur 5-1 hvordan hendelser kan detekteres i de forskjellige fasene av ICS Cyber Kill Chain ved hjelp av loggdata. Dette er bare et eksempel. Logghåndteringsverktøyene presentert i underkapittel 4.4.2 er noen av de vanligste som benyttes av sikkerhetspersonell.

Logging og analyse av logger krever ressurser i form av teknologi og bemanning. Det har blitt nevnt i flere av møtene i løpet av prosjektet at fokuset i virksomheter er rettet mot driftslogging, og i liten grad mot sikkerhet. Dette bekrefter/viser at det kan være utfordrende for virksomheter som ikke har hatt noen kjente hendelser å ha fokus på sikkerhet.

SANS (2010) har utgitt anbefaling til loggstrategi[48]. De anbefaler følgende:

- Logg sentralt alle hendelser fra prioriterte hendelsestyper og utvalgte komponenter. Eksempler kan være administratoraktivitet og feiltilstander
- Bestem og dokumenter bredden i loggingen, dette inkluderer komponenter og systemer som inngår i det nettverket som skal beskyttes, samt definer plassering og lagringstid

[47] Intervju med sikkerhetsorgan
[48] Swift, D, *Successful SIEM and Log Management. Strategies for Audit and Compliance*. SANS Institute InfoSec Room, November 4, 2010.

- Revider loggene regelmessig, definer uønskede hendelser for oppfølging. Pass på å utvikle nødvendige prosedyrer for å følge opp hendelsene
- Lag en revisjonsplan for loggene, dokumenter hva loggene viser og om det er i samsvar med regelverket

6.3 Hvordan sikre loggdata

Vurderinger av hvilke loggdata som bør sikres, lagringstid og hvordan loggdata bør sikres er tatt med utgangspunkt i litteratursøk og workshop hos NVE den 15. Juni 2016, hvor flere representanter fra energiforsyningen og leverandørbransjen var tilstede. Samtidig er det vanskelig å sette konkrete tekniske krav til logging i forskrifter. Virksomhetene risikerer å utelate muligheter for logging i sine systemer hvis kravene blir for konkrete, og siden forskriftene er offentlige, kan dette også utnyttes av kompetente angripere for å finne smutthull.[49] Funnene viser at det varierer fra system til system hvilke loggdata som er relevant for sikkerheten, og at mye avhenger av sikkerhetsarkitekturen til kontrollsystemene. Når det gjelder sikringen av loggdata derimot, så er det åpenbart at de må sikres mot uautorisert endring, siden upålitelige loggdata verken kan benyttes for deteksjon eller til etterforskning.

Om en ser på kjente hendelser som er beskrevet i denne rapporten, kan det gå lang tid før et avanserte målrettet angrep eventuelt blir oppdaget. Ved angrepet på energiforsyningen i Ukraina i desember 2015 kom det frem at angripere hadde tilgang til systemet minst et år før selve angrepet ble gjennomført. Slike hendelser må tas med i vurderingen når lagringstiden av logger skal defineres.

6.4 Logging i nye teknologier og grensesnitt

En stor utfordring med utviklingen i teknologien og hastigheten utviklingen skjer i, er at det kan være vanskelig å holde oversikten over hva som er angrepsflaten til kontrollsystemet. Flere og flere komponenter får funksjoner som gjør at de kan integreres mot andre systemer, og dette fører igjen til en større angrepsflate. Fordelen er at flere komponenter utvikles med muligheter for logging, og verktøy som syslog fører til økte muligheter til å overvåke systemer.

7 Konklusjoner

7.1 Muligheter for logging i industrielle nettverk

Innen industrielle driftskontrollsystemer er det et stort mulighetsrom for logging. For at det skal være praktisk å benytte logger er det vesentlig at komponenter som skal logges har standardiserte funksjoner, som for eksempel syslog for sending av loggmeldinger. Noen av mulighetene for å finne forskjellige loggdata er vist i figur 7-1

[49] Intervju med sikkerhetsorgan

RTU/PLS/IED
Bytte av minnekort Påloggingsforsøk Tilkoblinger Status på porter Innlasting av parametere og fastvare Oppdatering av parametere og fastvare

TCP/IP-baserte protokoller
Pakkestørrelser Funksjonskoder/kommandoer Trafikk på porter

Modem/gateway/fjerntilgangspunkter
Kilde og mål-adresse Handling

Brannmur
Brukt protokoll Port Pakkestørrelse Kilde og mål-adresse

Fieldbus-nettverk
Pakkestørrelser Funksjonskoder/kommandoer Trafikk på porter

Servere/stasjoner/HMI
Applikasjonslogg Sikkerhetslogg Systemlogg

Figur 7-1 Eksempel på loggmuligheter

Hvert enkelt system må kartlegges, og loggingen må implementeres. Under kartleggingen er det vesentlig å avdekke hvilket utstyr som faktisk er en del av nettverket, og hvilke veier som finnes inn til nettverket.

7.2 Logging for økt sikkerhet

I kapittel 5 er det beskrevet strategier for å benytte logger i sikkerhetssammenheng. Her kommer det frem at det er i hovedsak to områder der logger har en funksjon, nemlig å detektere hendelser og å etterforske hendelser.

Det finnes forskjellig loggverktøy, både gratis (f.eks. ELK-stakken) og kommersielle (f.eks. splunk). Ved å benytte loggverktøy er det mulig å både automatisere overvåkning og å gjøre periodiske manuelle analyser for å se etter hendelser som kan indikere uønsket tilgang. Trafikken i industrielle nettverk er til dels statisk, og det er muligheter for å benytte dette til å finne indikatorer på uønsket adgang.. Norske virksomheter i energiforsyningen logger i dag mest av driftshensyn, og det trengs økt fokus på å logging av sikkerhetshensyn. [50]

7.3 Sikring av loggdata

Mengden loggdata kan vokse veldig raskt og kreve mye lagringsplass. Det er allikevel viktig at alle relevante data blir lagret på et sikkert sted, for når relevant data blir lagret, er virksomheten bedre rustet til å kunne gjenopprette systemer etter hendelser, og til å oppdage og etterforske hendelser. Hva som er relevant vil være et resultat av egen kartlegging av systemer. Noen tips til hva som kan være relevant er nevnt i kapittel 5.1. Loggene må være beskyttet mot tilgang fra

[50] Workshop NVE 15/6-2016

uautoriserte brukere, endringer og sletting. En av de første tingene en angriper ofte gjør er å forsøke å få tilgang til loggene og endre/slette disse.[51]

Logger bør lagres så lenge de er relevante. Hva dette innebærer vil variere, men siden det kan gå svært lang tid fra en angriper får tilgang til et system til de blir oppdaget, så vil logger være relevante i sikkerhetssammenheng i minst 2 år om det blir sett på hendelser av samme type som angrepet på energiforsyningen i Ukraina og Stuxnet. Langtidslagring av data kan, når loggene avspeiler menneskelig aktivitet (logger kan logge også applikasjoners aktivitet), ha betydning for personvern. Virksomheten bør derfor også se til regelverket rundt personvern og gjøre en vurdering av hvordan lagringen av forskjellige loggdata kan gå ut over personvernet til brukere av systemene. Datatilsynet[52] tilbyr veiledning til bedrifter om personopplysningsforskriften, slik at ingen enkeltpersoner blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Hvis en komponent har mulighet for å logge hendelser, bør logging være aktivert i den grad det er mulig uten å forstyrre kontrollsystemet.[53] Det bør også tas sikkerhetskopi av loggdata med faste intervaller og sikkerhetskopien bør også sikres mot uautorisert endring og modifikasjon.

7.4 Nye teknologier og grensesnitt

Siden det foregår en økende digitalisering av industrielle kontrollsystemer kommer det hele tiden nytt utstyr og nye løsninger på markedet. Det er derfor viktig å holde seg oppdatert på hvilke muligheter det finnes for logging i nye teknologier og ha en plan med implementering i nye og eksisterende systemer. Dette er spesielt viktig med tanke på at i smarte nett, såkalte «smart-grids», har angrepsflaten for eventuelle aktører blitt mye større enn tidligere.

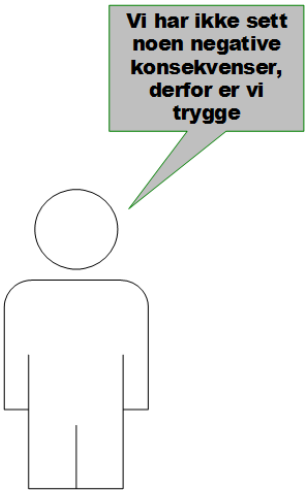
[51] OccupyTheWeb, "How To Cover Your Tracks & Leave No Trace Behind on the Target System", *WonderHowTo* (Juli 2014), URL: http://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/, besøkt 10.08.2016

[52] Datatilsynet URL: http://www.datatilsynet.no

[53] Freling, F.C., "A Common Process Model for Incident Response and Computer Forensics", *University of Mannheim* (September 2007), URL: https://www1.cs.fau.de/filepool/publications/imf2007-common-model.pdf, besøkt 10.08.2016

8 Anbefalinger

8.1 Holdningsarbeid og kompetansebygging



Figur 8-1 Om holdninger

For å sikre seg best mulig er det viktig å skape holdninger hvor sikkerhet er i fokus. Et problem som også Næringslivets sikkerhetsråd har påpekt, er at norske virksomheter ikke logger, eller analyserer loggene, og dermed ikke oppdager sikkerhetsbrudd.[54] En gjenganger i sikkerhetsmiljøet rundt energiforsyningen er at virksomhetene ikke tidligere er truffet av angrep, og dermed føler seg trygge. Denne holdningen kan føre til lite fokus nettopp mot sikkerhet[55]. Ved å alltid ta utgangspunkt i at egen virksomhet og egne industrielle kontrollsystemer et mål for angripere som gjerne opererer «under radaren», er det mulig å forbedre sine sikkerhetsrutiner og systemer betraktelig.

Det er viktig å sikre at virksomheten har personell med tilstrekkelig kompetanse innenfor logging for å kunne utnytte dette verktøyet fullt ut. Det krever at det settes av både tid og penger til kursing og gjennomføring. Beredskapsforskriften[56] § 7-7 sier at «Virksomheten skal ha tilgang til tilstrekkelig personell med nødvendig kompetanse som uten unødig opphold kan håndtere forhold angitt i første ledd», der første ledd er at «Virksomheten skal etablere kontrollordninger for å for å sikre effektiv håndtering av feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemets funksjon.»

8.2 Kjenn dine systemer og følg med på trusselsituasjonen

Det kan være en krevende jobb å kartlegge loggmuligheter i industrielle kontrollsystemer. En viktig del av dette er å ha personell som kjenner hele arkitekturen til systemene, og hva som er normale hendelser i systemene under forskjellige driftsmessige forhold. God kjennskap til

---

[54] Hagen, J, «Mørketallsundersøkelsen, *Næringslivets sikkerhetsråd* (2014), URL: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014.pdf, besøkt 12.08.2016

[55] Intervju med sikkerhetsorgan

[56] Norges Vassdrag og Energidirektorat, «Forskrift om sikkerhet og beredskap i energiforsyningen», *Lovdata* (2013), URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157 , besøkt 10.08.2016

kontrollsystemer vil være en stor fordel når det skal implementeres logging og andre sikkerhetsmekanismer.

For å forstå logginformasjon i en større sammenheng er det også relevant å følge med på trusselbildet. Blant annet gir Nasjonal Sikkerhetsmyndighet[57], Politiets sikkerhetstjeneste[58], Næringslivets sikkerhetsråd[59] og sikkerhetsleverandører ut ugraderte rapporter og oppdateringer om hva som kan være trusselbildet for norske virksomheter.

8.3 Bruk logger, og analyser loggene

Når alle muligheter for logging i kontrollsystemene er kartlagt, bør en gjøre en grundig vurdering av hvilke loggdata som er relevant å ta vare på, og ikke minst hvor lenge dette skal oppbevares. Vurderingen gjøres best ved å korrelere driftsdata med sikkerhetsdata. Virksomheten bør ha kompetent personell som kan analysere disse dataene og sette resultatet inn i en større sammenheng. Det er viktig å understreke at ikke alle uønskede hendelser er forårsaket av målrettede angrep. Feil og uønskede hendelser kan oppstå som følge av programvareoppdateringer og feilkonfigurasjoner, og menneskelige feil. Når det gjelder lagringstiden, er det konkludert i kapittel 7.3 at sikkerhetsloggdata er relevant i minst 2 år, men også her bør det gjøres egne analyser der virksomheten selv vurderer hva som er kritiske hendelser. SANS [60] gir noen råd om hvordan man kan gå fram.

Beredskapsforskriften[61] §7-14c sier at «Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.». En annen formulering kunne vært: «Virksomheten skal ha kartlagt og vurdert alle muligheter for automatisk overvåking i driftskontrollsystemet, og gjennomført tiltak med egnede verktøy for å sikre overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.»

Det kan også være aktuelt å ta dette et steg videre ved å f.eks. stille krav om at virksomheten skal kunne vise til logganalyser og vurderinger under revisjoner.

8.4 Inntrengningstesting

For å sjekke sikkerhetstilstanden kan virksomheten engasjere «red-team» øvelser, der sikkerhetspersonell eller eksterne sikkerhetsleverandører forsøker å trenge inn i systemer med forskjellige metoder for å se hvor sikre systemene er mot tilgang fra uønskede aktører. Gjennomføres slike øvelser, vil en ha mulighet til å se på hvilke loggdata som blir generert som følge av forskjellige angrepsscenarioer, og videre utnytte dette når det skal konfigureres automatisk overvåkningen av logger.

---

[57] Nasjonal sikkerhetsmyndighet blogg: https://www.nsm.stat.no/blogg/
[58] Politiets sikkerhetstjeneste hjemmeside: http://www.pst.no/trusler/
[59] Næringslivets sikkerhetsråd publikasjoner: http://www.nsr-org.no/publikasjoner/
[60] Swift, D, Successful SIEM and Log Management. Strategies for Audit and Compliance. SANS Institute InfoSec Room, November 4, 2010.
[61] Norges Vassdrag og Energidirektorat, «Forskrift om sikkerhet og beredskap i energiforsyningen», *Lovdata* (2013), URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157 , besøkt 10.08.2016

9 Videre arbeid

9.1 Trendlinjer etter forskjellige forhold

Datatrafikkmønsteret i systemene vil variere under ulike driftsforhold. Det kan være nyttig å lage trendlinjer eller profiler på normal aktivitet, som kan være grunnlag for overvåkning av logger og produksjon av alarmer.

9.2 Analysemuligheter

I noen tilfeller kan angripere ha lykkes med å slette sikkerhetslogger under en hendelse. Det bør forskes på og gjøres statistiske analyser av koblingsmuligheter mellom sikkerhetslogger og driftsdata før, under og etter hendelser. Finnes det noe sammenheng mellom sikkerhetslogger og driftslogger? Om det er korrelasjoner kan dette være en stor fordel i etterforskninger i etterkant av hendelser.

Hvis en virksomhet mistenker at de har blitt utsatt for et angrep fordi loggserver har krasjet og det finnes muligheter for å se på hva som er gjort i systemene, f.eks. i en historikk-server, så er dette noe som kan være av betydning for etterforskningen.

9.3 Standardisering av loggformat

Det finnes mange format som logger lagres i. Standardisering har forenklet arbeidet med logganalyser og overvåkning, og har gjort det enklere for virksomheter å få kompetanse innenfor feltene.

Standardisering generelt av systemkonfigurasjon og -arkitektur kan midlertidig ha en negativ konsekvens: Med oversiktlige nett som benytter samme protokoller, format og lignende, vil det være enklere for en angriper å lære seg systemet og standardisere angrepsmetoder som har gyldighet i flere virksomheter. Samtidig er standardisering en grunnforutsetning for nettverkskommunikasjon og effektiv drift.

9.4 Eksterne sikkerhetsleverandører

En gjenganger i tilbakemeldinger fra intervjuobjekter[62] har vært at å utlevere loggdata til lagring og analyse hos eksterne sikkerhetsleverandører har sine fordeler og ulemper. Dette er veldig sensitive data som tegner et godt bilde av virksomhetens aktivitet over tid. Det har blitt stilt spørsmål om eierskap til loggdata og ulemper dersom bedriften ønsker å benytte andre løsninger i fremtiden. En mulig løsning kan være å definere krav i beredskapsforskriften.

[62] Intervjuer med nettselskaper

9.5 Skytjenester

Bruk av skytjenester for ekstern lagring og prosessering av loggdata kan spare virksomheter for store kostnader og ressurser[63] og i tillegg gi nødvendig fleksibilitet og skalerbarhet. En av utfordringene ved bruk av skytjenester er kravene til beskyttelse av kraftsensitiv informasjon. Beredskapsforskriften[64] §6-2 sier «Kraftsensitiv informasjon er underlagt taushetsplikt etter §9-3 i energiloven[65].». Dersom virksomhetenen velger en skyløsning er det viktig å vurdere om dataene er sensitive etter beredskapsforskriften, og ta med i vurderingen hvor data blir lagret fysisk, og hvilke sikkerhetsmekanismer som er implementert.

Det er ulike modeller for skytjenester, (IaaS – Infrastructure as a Service, PaaS – Platform as a Service, og SaaS – Software as a Service).[66] De ulike modellene fordeler ansvaret på forskjellig vis mellom leverandør og kjøper av skyløsninger.

Skytjenester er ett av temaene NVE ser spesielt på i det videre arbeidet med prosjektet «Regelverksutvikling innen IKT-sikkerhet av betydning for energiforsyningens ivaretakelse av forsyningssikkerhet».

[63] Workshop NVE 15/6-2016
[64] Norges Vassdrag og Energidirektorat, «Forskrift om sikkerhet og beredskap i energiforsyningen», *Lovdata* (2013), URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157 , besøkt 10.08.2016
[65] Olje- og energidepartementet, «Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven), *Lovdata* (2016), URL: https://lovdata.no/dokument/NL/lov/1990-06-29-50, besøkt 10.08.2016
[66] Hagen, J.M., «Teknologiskifte i energiforsyningen», *Norges vassdrag- og energidirektorat* (118:2015)

10 Ordliste med forklaring

AMS	Automatiske strømmålere	Smarte strømmålere med to-veis kommunikasjon mellom måler og nettselskap
APT	Advanced Persistant Threat	Et cyber angrep fra en målrettet aktør, som kan pågå over lang tid.
CEF	Common Event Format	Et loggformat
CIM	Common Information Model	Et loggformat
Cyber forencics		Betegnelse for etterforskninger for datakriminalitet
Cyber Kill Chain		Et konsept relatert til strukturen i et cyber-angrep, utviklet av Lockheed-Martin i 2011.
DMZ	Demilititarized zone	Et undernettverk som sitter mellom det interne nettverket og internett for å beskytte mot uønsket trafikk
Ethernet		Den vanligste teknologien brukt i lokalnett
Fastvare	Firmware	Programvare som ligger fast innbygd i elektroniske apparater.
Fieldbus		Samlenavn for alle buss-protokoller som benyttes i industrielle nettverk
Hardware		Maskinvare - Elektroniske komponenter
HMI	Human Machine Interface	Et operatørpanel
IaaS	Infrastructure as a Service	En tredjepart tilbyr maskinvare, programvare, servere, lagring og andre komponenter for styring av systemer.
ICS	Industrial Control System	Industrielle kontrollsystemer.
IDPS	Intrusion Detection and Prevention System	En applikasjon eller komponent som kan overvåke (IDS) eller beskytte (IPS) et nettverk mot uønsket trafikk
IED	Intelligent Electronic Device	Kontrollere som kan kommunisere over nettverk med få funksjoner. Typisk brytere, transformatorer og kondensatorer.
IKT	Informasjons- og kommunikasjonsteknologi	Generell betegnelse for datamaskiner og teknologien rundt dette.
modbus/tcp	Modbus/Transmission Control Protocol	En seriell kommunikasjonsprotokoll som kan kommunisere over tcp/ip-nettverk
PaaS	Platform as a Service	Model der leverandører leverer maskinvare og programvare til en kunde for f.eks. programvareutvikling.
PDF	Portable Document Format	Et digitalt dokumentformat mye benyttet i virksomheter
Phishing	Fisking	En betegnelse på digital snoking etter sensitiv informasjon.
PLS	Programmerbare Logiske Styringer	En kontroller som kan programmeres til forskjellige formål.
Profibus	Process Field Bus	En utbredt feltbuss kommunikasjonsstandard innen Automasjon.
Protokoll		Et konvensjonelt eller standardisert sett med regler som besteller tilkobling, kommunikasjon og dataoverføring mellom to endepunkter
RTU	Remote Terminal Unit	En komponent med mikroprosessor som har grensesnitt mellom fysiske komponenter og industrielle nettverk.
SaaS	Software as a Service	Modell for programvaredistrubisjon der programvare blir gjort tilgjengelig for en kunde gjennom en internettforbindelse.
SCADA	Supervisory Control And Data Acquisition	Mye brukt innen automasjon som en betegnelse for styring og overvåkning.
SIEM	Security Information and Event Management	Programvare som benyttes for å analysere og overvåke meldinger fra fastvare og applikasjoner
Software		Programvare / Applikasjon
Spear-phishing	Spyd-fisking	En selektiv, avansert og sofistikert form for phishing, hvor angriper samler informasjon om målet og bruker dette for å bygge kredibillitet i en epost.
TCP/IP	Transmission Control Protocol/Internet Protocol	en gruppe kommunikasjonsprotokoller som benyttes for å koble sammen datamaskiner i nettverk, blant annet på Internettet.
USB	Universell seriebuss	Industriell standard som bestemmer utstyr og protokoller for kommunikasjon mellom datamaskiner og elektroniske komponenter
VPN	Virtual Private Network	Datateknikk som anvendes for å skape "punkt-til-punkt"- forbindelser, såkalte tuneller gjennom et annet datanett

11 Kilder

Andersen, H., “Scientific Method”, *Stanford* University (November 2015), URL: http://plato.stanford.edu/entries/scientific-method/, besøkt 10.08.2016

ArcSight Inc, “Common Event Format”, *McAfee* (Juli 2010), URL: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/78000/KB78712/en_US/CEF_White_Paper_20100722.pdf, besøkt 10.08.2016

ArcSight Inc, “SecuSphere Configuration Guide”, *Imperva* (April 2009), URL: https://www.imperva.com/docs/SB_Imperva_SecureSphere_CEF_guide.pdf, besøkt 10.08.2016

Assante, M.J., Lee, R.M., “The Industrial Control System Cyber Kill Chain”, *SANS Institute* (2016), URL: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297 , besøkt 10.08.2016

Czanik, P., “The 6 Categories of Critical Log Information”, *SANS Institute* (Versjon 3.01), URL: http://www.sans.edu/research/security-laboratory/article/6toplogs, besøkt 10.08.2016

Datatilsynet URL: http://www.datatilsynet.no

Det kongelige olje- og energidepartement, «Kraft til endring – Energipolitikken mot 2030», *Meld. St. 25* (2015 – 2016) URL: https://www.regjeringen.no/contentassets/31249efa2ca6425cab08130b35ebb997/no/pdfs/stm201520160025000dddpdfs.pdf, besøkt 10.08.2016

Eaton, I., “The Ins and Outs of System logging Using Syslog”, *SANS Institute* (2003), URL: https://www.sans.org/reading-room/whitepapers/logging/ins-outs-system-logging-syslog-1168, besøkt 10.08.2016

Escal Institute of Advanced Technologies (SANS), URL: http://www.sans.org

FireEye Inc, “Cyber Threats to the Nordic Region”, *Fireye* (Mai 2015), URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf, besøkt 10.08.2016

Folkerth, L., “Forensic Analysis of Industrial Control Systems, *SANS Institute* (September 2015), URL: https://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-industrial-control-systems-36277, besøkt 10.08.2016

Freling, F.C., “A Common Process Model for Incident Response and Computer Forensics”, *University of Mannheim* (September 2007), URL: https://www1.cs.fau.de/filepool/publications/imf2007-common-model.pdf, besøkt 10.08.2016

Hagen, J, «Mørketallsundersøkelsen, *Næringslivets sikkerhetsråd* (2014), URL: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014.pdf, besøkt 12.08.2016

Hagen, J.M., «Teknologiskifte i energiforsyningen», *Norges vassdrag- og energidirektorat* (118:2015)

Hutchins, E.M., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Lockheed-Martin* (2010), URL: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf , besøkt 10.08.2016

ICS-CERT, "Control System Engineering Workstation", *ICS-CERT* (Juli 2016), URL: https://ics-cert.us-cert.gov/Control_System_Engineering_Workstation-Definition.html, besøkt 10.08.2016

Johansen, P.A., «De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet», *Aftenposten* (Januar 2016), URL: http://www.aftenposten.no/verden/De-sa-det-var-umulig-Na-klarer-russiske-hackere-a-sla-av-stromnettet-13199b.html, besøkt 10.08.2016

Kaspersky, E., "The Man Who Found Stuxnet – Sergey Ulasen in the spotlight", *Nota Bene* (November 2011), URL: https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/, besøkt 10.08.2016

Klein, H., "What is Splunk and How Does it Work?", *Helgeklein.com* (September 2014), URL: https://helgeklein.com/blog/2014/09/splunk-work/, besøkt 10.08.2016

Knapp, E.D., (2011) *Industrial Network Security*, USA: Syngress

Kral, P., "The Incident Handlers Handbook", *SANS Institute* (Desember 2011), URL: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901, besøkt 10.08.2016

Kushner, D., "The Real Story of Stuxnet", *IEEE Spectrum* (Februar 2013), URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, besøkt 10.08.2016

Lee, R.M., "Analysis of the Cyber Attack on the Ukranian Power Grid", *SANS* (Mars 2016), URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, besøkt 10.08.2016

1Leskiw, A., «Understanding Syslog: Servers, Messages & Security», *Network Management Software* (Ukjent dato), URL: http://www.networkmanagementsoftware.com/what-is-syslog/, besøkt 10.08.2016

Microsoft, "Event Logs and Channels in Windows Event Log", *Microsoft* (Juni 2012), URL: https://msdn.microsoft.com/en-us/library/aa385225.aspx, besøkt 10.08.2016

Microsoft, Interpreting the Windows Firewall Log, *Microsoft* (Ukjent dato), URL: https://technet.microsoft.com/en-us/library/cc758040(v=ws.10).aspx, besøkt 10.08.2016

Mitre Corporation, "Common Event Expression", *Mitre* (November 2014), URL: https://cee.mitre.org/, besøkt 10.08.2016

Nasjonal sikkerhetsmyndighet blogg: https://www.nsm.stat.no/blogg/

Nasjonal Sikkerhetsmyndighet, «NSM Helhetlig risikobilde 2015», *Nasjonal Sikkerhetsmyndighet* (August 2015), URL: https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf, besøkt 10.08.2016

Nasjonal Sikkerhetsmyndighet, «Systemovervåking ved bruk av ELK-stakken», *Nasjonal Sikkerhetsmyndighet* (April 2016), URL: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-11_systemovervaking_ved_bruk_av_elk-stakken.pdf, besøkt 10.08.2016

Netgear, "How do i view the activity logs of my Nighhawk router?", *Netgear* (Februar 2016), URL: http://kb.netgear.com/app/answers/detail/a_id/24224/~/how-do-i-view-the-activity-logs-of-my-%20nighthawk-router%3F?cid=wmt_netgear_organic, besøkt 10.08.2016

Norges Vassdrag og Energidirektorat, «Veiledning til forskrift om sikkerhet og beredskap i energiforsyningen», *Norges vassdrag og energidirektorat* (2013) URL: http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf , besøkt 10.08.2016

Norges Vassdrag og Energidirektorat, «Forskrift om sikkerhet og beredskap i energiforsyningen», *Lovdata* (2013), URL: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157 , besøkt 10.08.2016

Næringslivets sikkerhetsråd publikasjoner: http://www.nsr-org.no/publikasjoner/

OccupyTheWeb, "How To Cover Your Tracks & Leave No Trace Behind on the Target System", *WonderHowTo* (Juli 2014), URL: http://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/, besøkt 10.08.2016

Olje- og energidepartementet, «Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven), *Lovdata* (2016), URL: https://lovdata.no/dokument/NL/lov/1990-06-29-50, besøkt 10.08.2016

OpenSecurityArchitechture, "SP-023: Industrial Control Systems", *OSA* (Ukjent dato), URL: http://www.opensecurityarchitecture.org/cms/library/patternlandscape/293-sp-023-industrial-control-systems, besøkt 10.08.2016

Politiets sikkerhetstjeneste hjemmeside: http://www.pst.no/trusler/

Rafter, M.V., "New Security Risks from USB Flash Drives", *Norton (Ukjent dato)*, URL: http://us.norton.com/yoursecurityresource/detail.jsp?aid=usbdrives, besøkt 10.08.2016

Samani, R., "Updated BlackEnergy Trojan Grows More Powerful", *McAfee* (Januar 2016), URL: https://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/, besøkt 10.08.2016

Scarfone, K., "Guide to Intrusion Detection and Prevention Systems (IDPS)", *National Institute of Standards and Technology* (Februar 2007), URL: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, besøkt 10.08.2016

Schneider, B., "The Story Behind The Stuxnet Virus", *Forbes* (Juli 2010), URL: http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html, besøkt 10.08.2016

1Splunk, «Splunk 4.3 Demo» (Video), *Splunk* (Januar 2012), URL: http://www.splunk.com/view/SP-CAAAGNB, besøkt 10.08.2016

Stouffer, K., "Guide to Industrial Control Systems (ICS) Security", *National Institute of Standards and Technology* (Juni 2011), URL: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, besøkt 10.08.2016

Swift, D., “A Practical Application of SIM/SEM/SIEM Automating Threat Identification”, *SANS Institute* (Desember 2006), URL: http://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781, besøkt 10.08.2016

Swift, D, “Successful SIEM and Log Management. Strategies for Audit and Compliance”, *SANS Institute*, (November 4), https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528, besøkt 30.08.2016.

Vergun, D., “Critical Infrastructure Vulnerable to Attack, NSA Leader Says”, *Army News Service* (April, 2016), URL: http://www.defense.gov/News/Article/Article/740177/critical-infrastructure-vulnerable-to-attack-nsa-leader-says, besøkt 10.08.2016.

Zetter, K., “Everything we know about Ukraine’s power plant hack”, *Wired* (Januar 2016), URL: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/, besøkt 10.08.2016

Zetter, K., “Hacker Lexicon: What are phishing and spear phishing?”, *Wired* (Juli 2015), URL: https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/ , besøkt 10.08.2016

Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no