Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem

Rapport utarbeidet av BDO AS for Norges vassdrags- og energidirektorat

14
2017

RAPPORT

Rapport nr 14-2017

Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør: Jon-Martin Pettersen

Forfattere: BDO AS

Trykk: NVEs hustrykkeri
Opplag: 0
Forsidefoto: Keyboard, DeclanTM via flickr.com
ISBN 978-82-410-1566-3
ISSN 1501-2832

Sammendrag: I denne rapporten beskriver BDO på oppdrag fra NVE en metodikk for hvordan og hva slags informasjon som bør hentes ut av logger etter IKT-hendelser i driftskontrollsystemer. Rapporten drøfter problemstillinger ved bruk av skytjenester til lagring av logger, informasjonsdeling og mulige fremtidige forskriftskrav. Rapporten er en del av underlaget for NVEs interne gjennomgang regel på området IKT-sikkerhet. Prosjektet har pågått i 2016 og 2017, og sluttrapporten som foreslår endringer i reguleringen blir ferdigstilt våren 2017.

Emneord: IKT-sikkerhet, IKT-hendelser, Driftskontroll, Energiforsyning, Sikkerhet, SCADA, IKT, Forskning og utvikling, logging

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

Mars 2017

Forord

Økt digitalisering gjør at IKT-sikkerhet er svært viktig i energisektoren. Digitaliseringen treffer nettselskaper og produsenter, og både administrative systemer og driftskontrollsystemer. Driftskontrollsystemer spiller en vital rolle for å overvåke og styre produksjon og overføring av energi. Dette krever at tilgjengeligheten og integriteten til disse systemene er høy. De må alltid fungere og virke slik som de er tenkt, både i normal-situasjon og i ekstraordinære situasjoner.

IKT-Sikkerhet kan ikke garanteres 100% ved hjelp av forebyggende sikkerhetstiltak. Systemer kan svikte som følge av tilfeldige feil eller målrettede angrep mot systemene. Det vil alltid finnes en restrisiko. Det er derfor viktig at virksomhetene har en god beredskap og klarer å oppdage og håndtere uønskede IKT-hendelser når de oppstår. Da er logger og logganalyse viktig.

NVE har i beredskapsforskriften et krav til logging og logganalyse til driftskontrollsystemer i klasse 2 og 3 (§ 14.c). Gjennom tilsynsarbeidet har NVE sett at det å logge og analysere loggene er krevende for mange selskaper. NVE ser behov for å forbedre kunnskapsgrunnlaget og veiledningen på dette området. NVE har derfor initiert et forskningsprosjekt som omfatter logging og logganalyse i energiforsyningen.

I denne rapporten beskriver BDO på oppdrag fra NVE en metodikk for hvordan og hva slags informasjon som bør hentes ut av logger etter IKT-hendelser i driftskontrollsystemer. Rapporten drøfter også problemstillinger rundt bruk av skytjenester til lagring av logger, informasjonsdeling og mulige fremtidige forskriftskrav til logging og logganalyse. Rapporten er en del av underlaget for NVEs interne gjennomgang av kravene på området IKT-sikkerhet. Prosjektet har pågått i 2016 og 2017, og sluttrapporten som foreslår endringer i reguleringen blir ferdigstilt våren 2017.

Oslo, mars 2017

Ingunn Åsgard Bendiksen

Avdelingsdirektør

Eldri Holo

Seksjonsleder

Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem

Rapport utarbeidet for
Norges vassdrags- og energidirektorat

31.10.2016

BDO

Innholdsfortegnelse

1. Sammendrag og oversikt over anbefalinger

På oppdrag fra Norges vassdrags- og energidirektorat (NVE) har har BDO beskrevet metodikk for hvordan og hva slags informasjon som bør hentes ut av logger etter IKT-sikkerhetshendelser i driftskontrollsystemer. Rapporten har også drøftet og gitt anbefalinger rundt problemstillinger som bruk av skytjenester, informasjonsdeling myndigheter imellom og mulige fremtidige forskriftskrav knyttet til overvåking, logging og analyse av datatrafikk i driftskontrollsystem.

Kraftforsyningen står overfor en betydelig digitalisering. Nettselskapene øker sin avhengighet av IKT i forbindelse med blant annet utrulling av strømmålere med toveiskommunikasjon (AMS), og kraftprodusentene digitaliserer overvåking og styringen av produksjonsanleggene i stadig større grad. Teknologien gir mulighet for mer effektiv styring og drift av kraftinfrastrukturen og raskere feilretting.

Økt kompleksitet betyr samtidig at det blir introdusert nye avhengighetsforhold mellom ulike del- og støttesystemer. Trusselbildet viser også at angrepsmetodene for å komme seg inn i et nettverk eller system nå er så avanserte, at grunnsikring som antivirus og perimeterbeskyttelse i mange tilfeller ikke er tilstrekkelig for å stoppe forsøkene.

For å føre signalene mellom utstyret ute i felten og driftssentralene hos virksomhetene benyttes både kjente og proprietære kommunikasjonsprotokoller[1]. Selv om stadig flere benytter kjente protokoller, som IP, i større grad, benytter mange fremdeles proprietære protokoller. Disse kan være vanskelig å overvåke.

Det mest effektive vil være å benytte kjent nettverksutstyr som benytter kjente protokoller, og bruke disse som sikkerhetssensorer ved å konfigurere de til å avgi logger med informasjon som bidrar til å få et oversiktsbilde over aktiviteten i driftskontrollsystemet.

Eksempler på hva man bør undersøke etter en hendelse er unaturlige påloggingsforsøk, forsøk på innlasting og oppdatering av parametere og fastvare, unaturlig aktivitet rundt tilkoblinger, kontroll av hvilke tilkoblingsporter som er forsøkt brukt til hva og bytte av minnekort.

Å bruke skytjenester til lagring og behandling av logger vil være et svært kosteffektiv alternativ til egne løsninger, og stadig flere virksomheter ønsker å benytte skytjenester i større grad enn i dag. Imidlertid er det stor usikkerhet knyttet til hva det er lov til å benytte skytjenester til hos virksomhetene i kraftforsyningen.

IKT-trusselbildet blir stadig større og uoversiktlig. Det forventes at man vil oppleve hendelser som påvirker flere sektorer, og det vil da være ekstremt viktig at man har etablert rutiner for varsling og samhandlingsrom for deling av informasjon. Dette må sektormyndighetene arbeide tettere sammen om enn i dag.

Det er ikke funnet spesifikke krav til overvåking og logging av driftskontrollsystem i andre Europeiske land. Imidlertid er det et krav i det nye NIS-direktivet om å beskytte samfunnskritiske IKT-system. Samtidig er det arbeid på gang for å gi EU-kommisjonen råd om hvordan og hva slags krav til beskyttelse man bør stille til kritiske informasjonssystem til virksomhetene i den europeiske energiforsyningen.

[1] En **protokoll** i et informasjonssystem er et konvensjonelt eller standardisert sett med regler som bestemmer tilkobling, kommunikasjon og dataoverføring mellom to endepunkter (f.eks. to dataprogrammer på ulike maskiner i et nettverk). Protokoller kan implementeres i maskinvare, programvare, eller en kombinasjon av disse.

Hovedanbefalingene er som følger:

- Mange driftskontrollsystem benytter fremdeles proprietære protokoller. Overvåking og analyse av disse protokollene kan være vanskelig. Det anbefales derfor at det først og fremst konsentreres om å overvåke og logge kjent utsyr som svitsjer, rutere, brannmurer etc som er plassert i driftskontrollsystemet.
- Utvidede krav til overvåking og logging bør sees i sammenheng med virksomhetenes kunnskap og evne til å logge. NVE bør derfor vurdere å gjøre en nærmere kartlegging av virksomhetenes kompetanse på overvåking og logging i driftskontrollsystem før det eventuelt utformes ytterligere og mer spesifikke krav til overvåking, logging og analyse.
- NVE, i samarbeid med virksomheter i kraftforsyningen og andre sakkyndige, bør gjøre en vurdering av bruk av skytjenester til lagring og tilgjengeliggjøring av logger.
- NVE og virksomhetene i kraftforsyningen bør fortsette å forsterke arbeidet med bevisstgjøring, først og fremst av ledere i virksomhetene. Dette er viktig for å gi de forståelse for de digitale truslene mot kraftforsyningen, og hva konsekvensene av disse kan være.
- Aktuelle myndigheter (NVE, NSM, KRIPOS, Nasjonal kommunikasjonsmyndighet med flere) og andre parter bør sammen utarbeide rutiner for varsling, terskler for varsling, hvilke kommunikasjonskanaler det bør varsles gjennom og avklare hvilket mandat de respektive myndighetene har for å sikre at varsling og håndtering av alvorlige IKT-sikkerhetshendelser på tvers av sektorer kan gjøres effektivt og koordinert.
- Krav og retningslinjer for bruk av utenlandske leverandører generelt, og de som kan bistå til å lagre logger og etablere system for logging og overvåking spesielt, bør konkretiseres, da flere virksomheter i kraftforsyningen opplever de eksisterende som uklare.
- Ved hendelser som angår digital spionasje, blir inntrenging ofte ikke avdekket før det er gått uker, måneder eller år etter at trusselaktør først fikk fotfeste i nettverket. Erfaring viser at det er nødvendig å lagre logger i lang tid for å kunne håndtere slike situasjoner. NVE bør vurdere hvorvidt to år med logger kan fungere som et minimum på tvers av bransjen.
- Det er arbeid på gang i europeisk sammenheng for å utvikle forskriftskrav til beskyttelse av kritiske IKT-system i europeisk energiforsyning. NVE bør følge denne prosessen tett og bidra med faglige råd der det er mulig.

2. Innledning

Industrielle prosesskontrollsystemer spiller en vital rolle for å overvåke og styre alle typer kritisk infrastruktur. Dette krever at tilgjengeligheten til disse systemene er svært høy, og at man kan stole på at de fungerer etter sin hensikt.

I kraftforsyningen er industrielle kontrollsystem (kalt driftskontrollsystem) avgjørende for effektiv drift av strømnettet og rask gjenoppretting av strømforsyningen ved utfall. De høye kravene til tilgjengelighet og integritet gjør at driftskontrollsystemene må beskyttes mot både tilsiktede og utilsiktede feil og hendelser.

Kraftforsyningen står overfor en betydelig digitalisering. Nettselskapene øker sin avhengighet av IKT i forbindelse med blant annet utrulling av strømmålere med toveiskommunikasjon (AMS), og kraftprodusentene digitaliserer overvåkingen og styringen av produksjonsanleggene

i stadig større grad. Teknologien gir mulighet for mer effektiv styring og drift av kraftinfrastrukturen og raskere feilretting.

Stadig flere virksomheter utnytter mulighetene et enhetlig kommunikasjonsgrensesnitt gir, ved å integrere driftskontrollsystem med systemer i den administrative delen av virksomheten. Samhandling med andre interne systemer, og utveksling av ny informasjon mellom utstyr og driftssentral, gir nye muligheter i forhold til fjernstyring og optimalisering.

Gjennom skytjenester utvides også mulighetene for forretningsutvikling for nettselskapene. Samtidig gjør integrasjon av systemer og tilgjengeliggjøring via Internett at kompleksiteten i systemene øker.[2] Økt kompleksitet betyr at det blir introdusert nye avhengighetsforhold mellom ulike del- og støttesystemer, og at sårbarheten øker[3]. For å opprettholde kravene til tilgjengelighet og integritet, må virksomhetene ha full oversikt over systemene, ha god risikoforståelse og være i stand til raskt å kunne reagere på feilsituasjoner eller ved mistanke om at uautoriserte forsøker å trenge seg inn i driftskontrollsystemet.

Trusselbildet viser også at angrepsmetodene for å komme seg inn i et nettverk eller system nå er så avanserte, at grunnsikring som antivirus og perimeterbeskyttelse i mange tilfeller ikke er tilstrekkelig for å stoppe forsøkene.

For å øke virksomhetenes evne til å avdekke og håndtere hendelser i driftskontrollsystemene, er det i «Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen» (bfe), som trådte i kraft 1.1.2013, krav om at virksomheter som overvåker og styrer de viktigste delene av kraftforsyningen skal ha etablert systemer som automatisk overvåker, logger, analyserer og varsler ved unormal aktivitet i driftskontrollsystemet.[4]

Når en kritisk hendelse blir avdekket, og spesielt ved et omfattende angrep som kan sette kritisk infrastruktur ut av spill, er det svært viktig at NVE raskt får relevant informasjon, slik at NVE kan kommunisere direkte med de aktuelle virksomhetene, kan vurdere alvorligheten, innhente råd fra andre myndigheter m.fl. og effektivt følge opp situasjonen. Det kan også være aktuelt å utstede straksvedtak.

I tilfeller hvor annen kritisk infrastruktur kan bli berørt, må NVE også kommunisere med andre relevante myndigheter, slik som NSM, Nkom, KRIPOS, Petroleumstilsynet, samt KraftCERT og andre relevante hendelseshåndteringsmiljøer. Denne kommunikasjonen bør skje gjennom etablerte kanaler og rutiner, baseres på ryddighet og skje under forutsetning om at alle involverte er klar over gjeldende ansvarsområder og rapporteringslinjer.

Erfaringsmessig har de ulike myndighetene i Europa forskjellige tilnærminger til hvordan de regulerer sikkerheten til driftskontrollsystemene til virksomhetene som overvåker og styrer strømforsyningen i de respektive landene. Noen land benytter sikkerhetstjenestene til å sette krav, mens andre har sektormyndigheter med spesialdefinerte krav til sikkerhet i driftskontrollsystem.

Med innføringen av det europeiske NIS-direktivet, vil de ulike landene pålegges å innføre enkelte krav til sikkerhet i systemer som inngår i kritisk infrastruktur, samt krav til informasjonsutveksling vedrørende trusler og hendelser mellom myndigheter og land. I tillegg vil det kreves at virksomhetene som inngår i kritisk infrastruktur rapporterer hendelser til

[2] Hagen, J, «Teknologiskifte i energiforsyningen», rapport utarbeidet for NVE, 2015.
[3] Forskningsrådet: «IKT-sikkerhet – det kontinuerlige kappløpet», sluttrapport etter IKT-SoS-programmet, 2008.
[4] Lovdata, Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften), URL: https://lovdata.no/forskrift/2012-12-07-1157/§7-14

respektive myndigheter. Hvordan dette vil slå ut på regelverk for virksomheter med driftskontrollsystemer er fremdeles uklart.

3. Problemstillinger

Denne rapporten belyser følgende spørsmål:

- Hva slags typer logger fra driftskontrollsystemene bør man ta vare på?
- Hvordan bør loggene lagres?
- Hvordan bør det legges til rette for at loggene kan gjøres tilgjengelig for gjennomgang i etterkant av en hendelse?
- Hvordan kan man benytte loggene til proaktiv overvåking?
- Hva er beste praksis i andre land når det gjelder krav til logging og overvåking av driftskontrollsystemer?
- Hva slags informasjon bør rapporteres til NVE ved en hendelse i et driftskontrollsystem?
- Hvordan bør varsling og samhandling på tvers av sektorer foregå dersom en større IKT-hendelse oppstår?
- Er det behov for oppklaring rundt krav til lagring og behandling av logger dersom man ønsker å gjøre dette hos en skytjenesteleverandør?
- Bør NVE vurdere å endre forskriftskravene knyttet til overvåking og logging, sett i lys av dagens teknologiske utvikling og risikobilde?

4. Metode

I dette prosjektet er det innhentet informasjon gjennom:

- Studier av relevant litteratur og rapporter.
- Intervjuer med selskap som har etablert overvåking og logging i sitt driftskontrollsystem.
- Oversikt over beste praksis i andre land, herunder kartlegging av regelverk.

4.1. Intervjuer og informasjonsinnhenting

Til denne rapporten har vi intervjuet følgende selskap:

- Statnett SF
- Statkraft SF
- Østfold Energi AS
- Eidsiva Nett AS

I tillegg har vi benyttet BDOs eget internasjonale nettverk, samt vårt nettverk av samarbeidspartnere innenfor overvåking og hendelseshåndtering for innhenting av informasjon.

4.2. Forbehold

BDOs arbeid er å anse som et utviklings- og rådgivningsoppdrag. Basert på det arbeidet som er gjort gjennom denne rapporten, redegjør og begrunner vi for våre funn, vurderinger og anbefalinger.

Våre analyser er begrenset til den informasjon som vi har fått gjennom samtaler, intervjuer og litteraturstudier, samt prosjektressursenes erfarings- og kompetansebakgrunn.

BDOs arbeid med rapporten har blitt gjort innenfor en begrenset tidsramme, og vi finner det riktig å presisere at vi ikke kan påta oss ansvar for fullstendigheten eller riktigheten i det grunnlagsmaterialet som har vært utgangspunkt for våre vurderinger. Dersom vi har mottatt uriktig eller ufullstendige opplysninger, har vi ikke hatt anledning til å avdekke dette ut over overordnede rimelighetsvurderinger.

5. Generelt om overvåking og logging

Gjennom forskriftsbestemmelsen legges det til grunn at kravet til automatisk overvåking og logging også skal forebygge forsøk på inntrenging, i tillegg til å være viktig for kartlegging og etterforskning av en hendelse i etterkant. Derfor er det viktig at det legges til rette for både proaktiv overvåking, og evne til raskt å kunne hente informasjon fra eldre logger når en hendelse skal gjennomgås.

Det er ikke bare loggene fra utstyret i driftskontrollsystemet, og kommunikasjonen mellom dem, som bør være gjenstand for overvåkning. Mange typer nettverksutstyr kan fungere som sikkerhetssensorer ved å konfigureres til å avgi logger med informasjon som bidrar til å komplettere oversiktsbildet over aktiviteten, f.eks. rutere, svitsjer, brannmurer og klientmaskiner som brukes i et driftskontrollsystem, og tjenester som inngår i tilgjengeliggjøring av systemene.

Riktig logging er ikke ensbetydende med å logge alt. I tillegg til at innsamling, prosessering og lagring av logger medfører kostnader, vil irrelevante data bidra til å redusere verdien av loggene ved at relevante data blir mindre synlige. Denne problemstillingen aktualiseres når stadig flere kontrollsystemer benytter IP til kommunikasjon, hvilket forenkler kommunikasjon og uthenting av logger.

Med dagens verktøy kan analyse av nettverksaktivitet skje i nær sanntid, og avgi umiddelbare varsler ved avvik. Dette setter imidlertid krav til hvordan loggene lagres, organiseres og gjøres tilgjengelig for analyse.

For å sikre god situasjonsforståelse og tidsriktig varsling, er det viktig at myndighetene raskt får nødvendig informasjon. Klare rutiner og gode kommunikasjonskanaler er avgjørende for rask varsling og deling av informasjon.

6. Utfordringer ved overvåking og logging i driftskontrollsystem

Kravene til tilgjengelighet og integritet i driftskontrollsystemer er svært forskjellige fra tradisjonelle IKT-systemer. Driftskontrollsystemer har tidligere vært proprietære systemer som har vært helt adskilt fra andre IKT-systemer[5]. Systemene var selvstendige, uten behov for tilkoblinger utenfor driftskontrollsystemet[6]. I de siste årene har man i stadig større grad

[5] ENISA, «Protecting Industrial Control Systems – recommendations for Europe and Member States», 2011.
[6] NIST, «Guide to Industrial Control Systems (ICS) Security», revision 2, 2015.

integrert driftskontrollsystemer med systemer som befinner seg i den administrative delen av virksomheten. Samhandling med systemer i det administrative nettverket og driftskontrollsystemet har gitt nye muligheter med tanke på fjernstyring og optimalisering.

Som en konsekvens av dette - og for å effektivisere, redusere kostnader og standardisere -, har virksomhetene i stadig større grad gått over til IP-kommunikasjon også i driftskontrollsystemer. I dag brukes IP i stor grad kun frem til anleggene. Videre inn i anleggene, og ut til feltutstyret, benyttes fremdeles proprietære protokoller i stor grad.

Det er likevel en rekke proprietære protokoller i bruk, og kompetanse om disse protokollene er begrenset, spesielt knyttet til hvordan man skal gjøre overvåking og logging av disse. At kunnskapen om protokollene er begrenset, betyr også at kapasiteten til trafikkanalyse er begrenset. Dette er en utfordring for effektiv hendelseshåndtering.

Ønsker man å etablere overvåking av aktiviteten helt ut i anleggene, kreves det at virksomhetene må bruke tid og ressurser på lære seg trafikkmønster og lage en såkalt «baseline» for hva som er legitim trafikk[7]. Dette innebærer at man over tid må studere trafikken, og tilpasse overvåkingsverktøyene, slik at analytikerne lærer seg å forstå hva som er legitim trafikk. Dette krever igjen at selskapet har kompetent personell som har inngående kunnskap om sitt driftskontrollsystem og protokollene, men også verktøyet som skal tolke aktiviteten.

7. Oppsummering av intervjuene

Et av hovedmålene med intervjuene var å kartlegge hvordan et utvalg virksomheter strukturerer og henter ut logger fra sine driftskontrollsystemer. Videre var det ønskelig å kartlegge om virksomhetene kunne gjøre rede for en intern, fungerende sikkerhetsorganisasjon[8] som har kapasitet og kompetanse til å håndtere IKT-sikkerhetshendelser av varierende størrelse og alvorlighet.

7.1. Sikkerhetsorganisasjoner i virksomhetene i kraftforsyningen

Samtlige virksomheter som ble intervjuet har opprettet rutiner for varsling og beredskap ved IKT-hendelser, men på ulikt nivå. En del av virksomhetene benytter seg av eksterne sikkerhetsleverandører ved håndtering av IKT-sikkerhetshendelser, enten som bistand eller som fullstendig responsmiljø.

De virksomhetene som ble intervjuet hadde i varierende grad etablert en egen sikkerhetsorganisasjon. Noen har etablert operative sikkerhetsorganisasjoner med både kapasitet og kompetanse til å håndtere IKT-sikkerhetshendelser og loggmengden fra driftskontrollsystemene. Noen har beredskapsordninger hvor ansatte blir varslet ved hendelser, men hvor oppgavebekrivelsene til disse personene ikke fullt ut er konkretisert. Flere viste til at det er vanskelig å få forståelse for å bruke ressurser på å investere i verktøy og kompetanse, utover det å oppfylle forskriftens krav knyttet til å oppdage og håndtere hendelser.

[7] Mnemonic, «Sikkerhetsmonitorering av driftskontrollsystem», notat utarbeidet for NVE, 2013.
[8] Vi bruker begrepet sikkerhetsorganisasjon i denne rapporten som et samlebegrep for den delen av virksomheten som har ansvaret for å sikre driftskontrollsystemet, oppdage unormal aktivitet og håndtere sikkerhetshendelser. Begrepet er hentet fra NSMs veileder til sikkerhetsadministrasjon. URL: https://nsm.stat.no/globalassets/dokumenter/veiledninger/veiledning-i-sikkerhetsadministrasjon-v1.0.pdf

En tidligere kartlegging har vist, at en stor andel av nettselskapene i Norge ikke tror at truslene mot driftskontrollsystemer kan ramme dem. Dette er med på å forklare hvorfor mange selskaper i liten grad har brukt ressurser på etablering av funksjoner for håndtering av IKT-sikkerhetshendelser, både i det administrative nettverket og i driftskontrollsystemet[9].

7.2. Strukturering av systemer og nettverk

Virksomhetene har forskjellige tilnærminger for strukturering av systemer og nettverk. De fleste har forståelse for segmenterte nettverk og sikre soner, og har satt opp nettverkene etter regulatoriske krav.

Driftskontrollsystemene ble beskrevet som adskilte systemer i sikre soner hvor tilgangen er svært begrenset, og drift blir gjort av virksomhetene selv. Ingen brukere eller leverandører har enkel tilgang til de sikre sonene fra kontornettverkene, og det er få muligheter for fjerntilgang fra andre nettverk. De fleste virksomhetene har en ordning der fjerntilgang er nøye regulert, f.eks. gjennom bruk av flere autentiseringsfaktorer og manuell godkjenning av hver enkelt innlogging.

7.3. Protokollbruk

Alle virksomhetene som ble intervjuet benytter flere ulike protokoller i sine driftskontrollsystem. Kommunikasjon mellom komponenter og kontrollere i et driftskontrollsystem har i lang tid kun bestått av seriell kommunikasjon med tilhørende protokoller (Modbus/Profibus) i et fieldbusnettverk. I senere tid har IP blitt mer utbredt, også langt inn i driftskontrollsystemene. Bruk av IP vil øke mulighetene for å etablere enkel og hensiktsmessig logging. Logginnsamlingsmetoder som allerede benyttes i vanlige kontornettverk vil kunne benyttes i nettverk med driftskontrollsystemer.

I dag benyttes i stor grad proprietære protokoller fra kontrollrommet ute i anleggene og til feltutstyret som er tilknyttet de ulike anleggene, som generatorer, spennings- og effektbrytere, spenningstransformatorer, kondensatorer og vern. Dette kan by på utfordringer. Utbredte protokoller som benyttes til kommunikasjon og transport av informasjon i et driftskontrollsystem er DNP3, IEC 60870-5-101, IEC 60870-5-104, IEC 61850, og ICCP/TASE.2.

7.4. Leverandørspesifikke protokoller

Gjennom informasjonsinnhentingen har det kommet fram at det finnes en stor mengde leverandørspesifikke protokoller som benyttes i forskjellige driftskontrollsystemer. Under lister vi opp et utvalg protokoller som benyttes i leverandørers driftskontrollsystemer. Vi har valgt å fokusere på ABB og Siemens som er to av de største leverandørene av utstyr og system til driftskontrollsystemene i kraftforsyningen. Leverandørene benytter seg ofte av åpne standarder også, for eksempel Modbus og IEC 60870 og IEC 68150.

[9] Bartnes, Line, "Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations", Journal of Critical Infrastructure Protection, Volume 12, March 2016.

- Siemens[10]
    - Profibus DP (åpen standard, styring av sensorer via en kontroller)
    - Profinet (åpen standard)
    - Sinec H1
    - Siemens 3964R (åpen, brukes til seriellkommunikasjon mellom «master» og «slave»)
- ABB[11]
    - MasterBus 300 (kommunikasjon mellom ABB-kontrollere og ABB-mastere)
    - DriveBus (kommunikasjon mellom ABB-kontrollere og ABB-disker)
    - AF 100 (kommunikasjon mellom ABB-kontrollere og Advant-produkter)
    - MOD5-to-MOD5 (kommunikasjon mellom ABB-kontrollere og MOD5 prosesskontrollsystemer)

8. Logger og annen informasjon for kartlegging av hendelsesforløp

Logging er generelt svært viktig, og vil i de fleste tilfeller fungere som bevis i etterkant av alvorlige IKT-sikkerhetshendelser. I logger vil en kunne finne informasjon som kan hjelpe til å forkorte deteksjonstiden ved fremtidige hendelser. Videre i dette kapitlet beskriver vi logger og annen informasjon som kan være nyttig og aktuelt å ta vare på i en hendelsessituasjon.

8.1. Logguthenting fra driftskontrollsystem

Logguthenting fra driftskontrollsystemer i adskilte nettverk kan være mer utfordrende enn å hente ut logger fra normale kontornettverk. Nettverkene som driftskontrollsystemene er plassert i, er i hovedsak delt opp i flere sikre soner. Dette gjøre det utfordrende å samle inn logger til et sentralisert system, samtidig som sikkerheten for driftskontrollsystemene skal ivaretas.

En stor utfordring ved å hente ut logger fra driftskontrollsystem, er at det fremdeles benyttes proprietære protokoller i lokalkontrollanleggene. Utfordringen kan være[12]:

- Feltutstyret (aktuatorer, måleinstrumenter, sensorer, vern etc.) har som oftest ikke innebygget mulighet for å logge signalene som mottas og sendes fra utstyret.
- For det utstyret som kan avgi logger, så er dette som regel avslått, da leverandørene ikke forventer at trafikken skal logges.

[10] Siemens, URL: http://w3.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/simatic-pcs-7-system-components/communication/PROFINET_%20PROFIBUS/Pages/PROFINET_PROFIBUS.aspx?tabcardname=profinet

[11] ABB, Communication Protocols, URL: https://library.e.abb.com/public/ff6ab6766689f2a7c1257b40001b8b28/3BSE035982-511_en_AC_800M_5.1_Feature_Pack_Communication_Protocols.pdf

[12] Homeland Security: Recommended Practice: Creating Cyber Forensics Plans for Control Systems, 2008.

- Feltutstyret har svært begrenset prosesserings- og lagringskapasitet til å behandle og lagre loggene. Derfor må det legges til rette for at disse sendes til en ekstern lagringsenhet.
- Det er en rekke proprietære protokoller i bruk, og kompetanse om disse protokollene innen IKT-sikkerhetsfaget er begrenset. Kapasiteten til trafikkanalyse er begrenset. Dette er en utfordring for effektiv hendelseshåndtering.

Det viktigste ved innhenting av logger fra driftskontrollsystemer i forskjellige sikre soner, er at transport og oppbevaring av data gjøres på en sikker måte, og at dette er dokumentert i sikkerhetspolicyer.

Transport og lagring bør helst krypteres med sterke krypteringsalgoritmer for å forhindre uautorisert innsyn. Lagringen bør skje utenfor hver av de sikre sonene, og tilgang bør reguleres og sikres med to-faktor-autentisering.

8.2. Identifisere enheter og loggmuligheter

For å kunne gjennomføre hensiktsmessig overvåking og innhenting av logger fra driftskontrollsystemer, er det nødvendig å identifisere hvilke enheter og komponenter som er plassert i samme nettverk. Videre må det kartlegges hvilke av disse som har mulighet til å logge og hvilke det vil være hensiktsmessig å hente inn logger fra. Blant komponentene som må kartlegges er «Master Terminal Units» (MTU), «Remote Terminal Units» (RTU), «Programmable Logic Controllers» (PLC), «Intelligent Electronic Devices» (IED) og «Human-Machine Interfaces» (HMI).

Enhetslister er nyttig for å kunne fange opp og reagere med en gang en ukjent enhet dukker opp i nettverket.

Følgende informasjon kan det være nyttig å logge fra RTU/PLC/IED-komponenter i et driftskontrollsystem[13] [14].

- Innlasting og oppdatering av parametere og fastvare
- Påloggingsforsøk
- Tilkoblinger
- Status på hvilke tilkoblingsporter som brukes
- Bytte av minnekort

Samtidig vil det være fornuftig å logge følgende informasjon fra MTU- og HMI-komponenter:

- Applikasjonslogg
- Sikkerhetslogg
- Systemlogg

8.3. Applikasjonslogger

Applikasjonslogger sendes ut fra enheter som har en eller flere applikasjoner kjørende. Loggene kan vise på hvilket tidspunkt en applikasjon blir åpnet eller kjørt, hvilken bruker som

[13] Hovland, K, «Logging og logganalyse», studentrapport utarbeidet for NVE i 2016.
[14] Homeland Security: Recommended Practice: Creating Cyber Forensics Plans for Control Systems, 2008.

bruker applikasjonen, og hvilke handlinger som blir gjort av brukeren. Et eksempel er å hente logger fra et Windows-system som kjører HMI.

8.4. Sikkerhetslogger

Sikkerhetslogger fra sikkerhets- og infrastrukturprodukter bør alle virksomheter være i stand til å hente ut. Disse loggene sendes fra brannmurer, rutere, svitsjer, IDS-/IPS-systemer og antivirusprogrammer, ofte til et sentralt innsamlingspunkt. Sikkerhetslogger kan blant annet vise hendelser basert på regler satt på de ulike komponentene i nettverket.

IDS (Intrusion Detection System) er en løsning laget for å detektere og varsle mistenkelig aktivitet i et nettverk. IPS (Intrusion Prevention System) fungerer som en IDS, men har mulighet til å blokkere trafikk som ikke samsvarer med reglene som er satt i IPS-systemet. Begge systemene avgir logger som kan være svært nyttige i hendelsessituasjoner. De fleste leverandører av SCADA-system anbefaler ikke bruk av IPS i selve driftskontrollsystemet, da dette kan forhindre legitim trafikk, og redusere tilgjengeligheten for systemene. I tillegg krever dette igjen spesialkompetanse, både på IPS-verktøyet, nettverket i driftskontrollsystemet og protokollene som brukes i driftskontrollsystemet[15].

8.5. Systemlogger

Systemlogger kan blant annet vise informasjon om systemets driftsstatus. Dette innebærer informasjon om prosesser og feilmeldinger, men også autentisering og kjøring av filer med forhøyede rettigheter. Systemlogger kan bidra til kontinuerlig driftsovervåking for å sikre stabil og sikker drift.

8.6. NetFlow/IPFIX

NetFlow/IPFIX viser trafikkflyt i et nettverk. Disse loggene inneholder kun metadata, som vil gi informasjon om hvor trafikk stammer fra og hvor den går (IP-adresser), hvilke porter trafikken går på, hvor mye trafikk som går (antall pakker og pakkestørrelse) og ikke minst tidsrommet dette skjer i. Logger som viser trafikkflyt er viktige for å kunne spore mistenkelig aktivitet i en hendelse tilbake til den opprinnelige kilden.

8.7. Autentiseringslogger og tilgangslister

Autentiseringslogger gir en oversikt over hvilke brukere som har fått tilgang til hvilke tjenester. Loggene kan benyttes til å kartlegge mistenkelige innlogginger og oppdage avvik fra normal aktivitet. Avvik kan for eksempel være et stort antall feilede innlogginger fra en eller flere brukere, eller innlogginger fra forskjellige steder i verden.

Det er nødvendig å ha gode rutiner for hvordan brukere og tilganger settes opp, endres og slettes i et nettverk. I en hendelse vil angripere ofte forsøke å bruke legitime brukeres tilganger. Det kan også forekomme at angripere forsøker å opprette nye brukere med svært brede tilganger. Derfor er det viktig å ha oppdaterte og verifiserte bruker- og tilgangslister tilgjengelig, for å avdekke uautoriserte brukere.

[15] Horkan, Michael: «Challenges for IPS/IDS deployment in Industrial Control Systems, 2015. URL: https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127

8.8. Konfigurasjonsendringer

Det er svært viktig å overvåke konfigurasjonsendringer kontinuerlig, og ikke minst hente ut dette i en hendelsessituasjon. Oppdages uautoriserte konfigurasjonsendringer bør dette absolutt følges opp. Logger over konfigurasjonsendringer kan benyttes sammen med bruker- og tilgangslister for å avdekke brudd på policyer og sikkerhet. Revisjon av disse loggene i etterkant av hendelser kan også være nyttig for å avdekke rutinesvikt.

8.9. Tabelloversikt: Loggtyper og informasjon

Tabellen under viser loggtypene nevnt tidligere i rapporten, og hvilken informasjon som kan være nyttig å hente ut under, eller etter en hendelse.

Tabell 1: Oversikt over logger og hva slags informasjon disse kan avgi.

Loggtype	**Informasjon**	**Begrunnelse**
Applikasjonslogg	Dato og tid Applikasjonsnavn / ID Bruker Brukers handlinger	Kan i en hendelsessituasjon vise hvilke applikasjoner som har blitt kjørt av uautoriserte brukere eller legitime brukere som har blitt kompromittert.
Sikkerhetslogg fra brannmur	Dato og tid Kilde- og destinasjonsadresse Porter Protokoll Blokkert / ikke blokkert	Informasjonen kan vise hvilken innkommende og utgående nettverkstrafikk som er blokkert og hvilken som har blitt godtatt. Protokolltype og port kan videre brukes til å kartlegge hvilke tjenester som har blitt forsøkt aksessert.
Sikkerhetslogg fra IDS	Dato og tid Kilde- og destinasjonsadresse Porter Protokoll Alarminformasjon	Loggene viser alarmer fra IDS-løsning, typisk mistenkelig aktivitet. I en hendelsessituasjon vil dette trolig kunne brukes til å knytte aktivitet opp mot kjente angripere eller kampanjer, basert på trafikkmønsteret i alarmen(e).
Systemlogger	Dato og tid Komponent / System / ID Prosessoversikt Feilmeldinger	Viser om et system har hatt uventede feil eller om det har blitt startet nye, mistenkelige prosesser på hendelsestidspunkt.

Netflow/IPFIX (Trafikkflyt)	Dato og tid Kilde- og destinasjonsadresse Porter Pakkeantall Trafikkstørrelse	Viser nettverkstrafikk mellom to endepunkter og kan hjelpe til med å spore mistenkelig aktivitet tilbake til en maskin. Informasjonen kan gi en indikator på om det har blitt sendt mye data inn og ut fra berørt virksomhet.
Autentiseringslogger	Dato og tid Tjeneste Kilde Bruker Blokkert / ikke blokkert	Informasjonen vil bidra til å kartlegge uautoriserte innloggingsforsøk til ulike tjenester. Uautoriserte innloggingsforsøk kan være en angriper.
Tilgangslister	Dato og tid for opprettelse Bruker Tilganger	Uthenting av informasjonen vil kartlegge om det har blitt opprettet uønskede brukere på hendelsestidspunkt, og eventuelt med hvilke tilganger.
Konfigurasjonsendringer	Dato og tid Konfigurasjon / ID Konfigurasjon endret av	Uautoriserte konfigurasjonsendringer kan sees i sammenheng med virksomhetens tilgangslister for å se om en potensiell angriper har endret kritiske konfigurasjoner.

9. Lagring og håndtering av logger fra driftskontrollsystemer

9.1. Lagring

Lagring av logger som hentes ut fra driftskontrollsystemer kan være komplisert og ressurskrevende. Svært mange driftskontrollsystemer er omfattende, med mye utstyr som kan avgi logger. Antallet loggkilder vil øke jevnt etter hvert som ny teknologi innføres. Hvor mye lagringsplass loggene krever, avhenger av hvor langt tilbake i tid loggene skal oppbevares og hvor mye informasjon loggene inneholder.

Samtlige virksomheter som deltok i intervjurunden lagret logger og informasjon i sin egen infrastruktur, men hadde ulike løsninger. En løsning gikk ut på å benytte «varme» og «kalde» lagre. De varme lagrene inneholdt virksomhetens nyeste logger, som var indeksert, noe som gjorde søketiden i loggene kort. De «kalde» lagrene inneholdt logger lengre tilbake i tid. De «kalde» loggene er som regel ikke indeksert, slik at det tar betydelig lenger tid å søke i dem.

En annen løsning gikk ut på å lagre logger direkte på enhetene. Med komplekse systemer og mange komponenter vil uthenting av logger kreve mye manuelt arbeid, og anbefales ikke. Et oppsett med et sentralt punkt for lagring og håndtering av logger vil alltid være beste praksis. Håndteringen vil da være mer effektivt og øke virksomhetens operative evne.

Det sentrale punktet for lagring og håndtering av logger bør være redundant og godt sikret, slik at risikoen for tap av data, er liten. Loggene må kun være tilgjengelige for brukere som har tjenstlig behov, da disse i noen tilfeller kan inneholde kraftsensitiv informasjon. Slik informasjon på avveie kan i verste fall tipse potensielle angripere om sårbarheter i driftskontrollsystemer.

9.2. Logghåndtering

Sentralisert logging betyr at logger fra enheter i et nettverk sendes til et sentralt punkt for lagring og håndtering. Dette har vært en økende trend i mange sektorer, og med sentralisert logging følger forskjellige logghåndteringsverktøy. Logghåndteringsverktøy sikrer enkel og effektiv korrelering og analyse av logger fra flere loggkilder. For større virksomheter med mange loggkilder vil slike verktøy sørge for mest effektiv håndtering av logger.

Det finnes flere verktøy for effektiv logghåndtering. Formålet med å benytte et logghåndteringsverktøy er å behandle data fra forskjellige loggkilder og presentere disse i et felles loggformat for enkel korrelering, kategorisering, analysering og søk. Logghåndteringsverktøyene indekserer loggdata, noe som muliggjør raske søk gjennom store mengder data.

Kommersielle logghåndteringsverktøy er ofte kostbare og dermed mindre aktuelt for små virksomheter med få loggkilder.

10. Kraftsensitiv informasjon og bruk av skytjenester

Bruk av skytjenester har økt betydelig den siste tiden, og stadig flere selskap i alle sektorer har tatt i bruk skytjenester både til fillagring og kjøring av applikasjoner.

Regjeringen ønsker at også statlige myndigheter, så langt det er mulig, benytter skytjenester for sine digitale tjenester[16]. Regjeringen har i den forbindelse utarbeidet en nasjonal strategi for bruk av skytjenester i statsforvaltningen. Hovedbegrunnelsen er at dette vil spare staten for store drifts- og investeringsutgifter på IKT-siden.

Å benytte skytjenester til lagring, behandling og tilgjengeliggjøring av logger kan være svært kostnadseffektivt, spesielt for mindre selskaper.

Kraftsensitiv informasjon er definert som spesifikke opplysninger som kan brukes til å skade fysiske kraftanlegg eller påvirke kritiske produksjonsfunksjoner. Hovedenheter som sender styringskommandoer og informasjon i driftskontrollsystemet vil anses som viktige, og dermed karakteriseres som kraftsensitive.

Logger fra andre komponenter som ikke benyttes til styring, men som allikevel er en del av driftskontrollsystemene, bør kunne lagres i en skytjeneste uten at dette skal gå utover integriteten og konfidensialiteten til systemene.

Det anbefales derfor at det gjøres en kartlegging av hvilke skytjenester som finnes, og hvilke som er aktuelle for kraftbransjen[17]. Leverandørene må ha nødvendige sikkerhetsmekanismer og dokumentasjon på plass slik at kraftbransjens verdier sikres tilstrekkelig. En vurdering av

[16] https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/sec1

[17] USA og Storbrittannia har etablert hvert sitt program for standardisering av krav til skytjenesteleverandører, og har utarbeidet lister over leverandører som oppfyller standardiseringskravene. USA: www.fedramp:gov, Storbritannia: https://www.digitalmarketplace.service.gov.uk/

skytjenester bør ideelt sett gjøres på tvers av sektorer og i regi av myndigheter. Det anbefales at NVE spesielt ser på følgende problemstillinger hva gjelder kraftsensitiv data og skytjenester:

- Hvilke komponenter i et driftskontrollsystem produserer kraftsensitiv data?
- Vil metadata fra driftskontrollsystemene karakteriseres som kraftsensitivt på lik linje med innholdsdata?
- Kan logger som inneholder for eksempel seks måneder gamle data karakteriseres som kraftsensitivt?
- Kan eldre data lagres og behandles i en skytjeneste?

Dersom loggene fra driftskontrollsystemene ikke anses som kraftsensitiv informasjon, eller lagringen og behandlingen anses som sikker nok, bør logger kunne lagres og behandles av eksterne tjenesteleverandører eller skytjenester. De økonomiske og operative fordelene ved slik tjenesteutsetting er mange, særlig for mindre selskaper. Vi anbefaler at NVE tydeliggjør problemstillingen og mulighetsrommet overfor virksomhetene i kraftforsyningen.

11. Andre myndigheters behov for informasjon

Norske myndigheter, mer spesifikt Nasjonal sikkerhetsmyndighet (NSM) og Politiet, kobles ofte inn når det oppstår alvorlige IKT-sikkerhetshendelser mot kritisk infrastruktur. Både NSM og Politiet har responsmiljøer innen IKT-sikkerhet og har mulighet til å bistå virksomheter med håndtering av alvorlige hendelser.

11.1. Rapporteringsplikt i andre sektorer

Det er flere myndigheter som har innført rapporteringsplikt i sin sektor. Dette gjelder for eksempel Nasjonal kommunikasjonsmyndighet (Nkom) og Finanstilsynet. Petroleumstilsynet har ingen direkte rapporteringsplikt knyttet til digitale trusler mot olje- og gassnæringen[18], men selskapene har krav på seg på grunnlag av risikoanalyser, å ha beredskap for å håndtere IKT-trusler og IKT-hendelser. Dette er utdypet i vedlagt brev av 1.12.2014 som svar på spørsmål fra Lysneutvalget på innspill til utvalgets arbeid.

Tilbydere av ekomtjenester er pålagt å varsle Nkom om alvorlig IKT-hendelser som kan redusere, eller har redusert, tilgjengeligheten til elektroniske kommunikasjonstjenester[19]. Det kreves også oppdatert varsling dersom det er vesentlige endringer underveis i hendelsen og når hendelsen er normalisert[20].

Virksomheter i finanssektoren er pålagt å varsle Finanstilsynet dersom det oppdages hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet i IKT-systemer og/eller data[21]. Dette er virksomhetene pålagt i «Forskrift om bruk av informasjons- og kommunikasjonsteknologi» (IKT-forskriften)[22].

[18] Regeringen.no: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/5.pdf, vedlegg til NOU:2015:13 «Digital sårbarhet – sikkert samfunn»
[19] http://www.nkom.no/teknisk/sikkerhet-og-beredskap/kriseh%C3%A5ndtering/varsling-og-rapportering-av-hendelser-i-ekomnett
[20] https://lovdata.no/forskrift/2004-02-16-401/§8-5
[21] http://www.finanstilsynet.no/no/Artikkelarkiv/Rundskriv/2009/4-kvartal/Rapportering-av-IKT-hendelser-til-Kredittilsynet/
[22] https://lovdata.no/forskrift/2003-05-21-630/§9

11.2. Beskrivelse av andre myndigheters responsmiljø

11.2.1. Nasjonal sikkerhetsmyndighet, NorCERT

NSM NorCERT kan bistå virksomheter i håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur. Enheten har etablert samarbeid med norske og utenlandske myndigheter, responsmiljøer for IKT-sikkerhet i norske virksomheter, og KraftCERT.

NSM NorCERT har publisert flere artikler og hefter som omhandler håndtering av IKT-sikkerhetshendelser, og hva som er viktig informasjon for enheten i håndteringssituasjoner:

- Oppsummering og tidslinje for hendelsen
- Vurdering av hendelsens alvorlighet
- Virksomhetens rolle i samfunnet
- Aktuelle logger, avhengig av hvilken type hendelse og omfang
- Oversikt over virksomhetens undersøkelser
- Oversikt over mulig berørte maskiner
- Eventuell delingstillatelse for videre deling til sikkerhetsmiljøet

11.2.2. Politiet (KRIPOS)

KRIPOS er den nasjonale enheten for bekjempelse av organisert og annen alvorlig kriminalitet og har følgende roller[23]:

- Nasjonalt kompetansesenter for norsk politi
- Nasjonalt kriminalteknisk laboratorium
- Nasjonalt kontaktpunkt for internasjonalt politisamarbeid
- Behandlingsansvarlig for sentrale registre i politiet
- En aktør for forebygging og samfunnssikkerhet

Dette omfatter bekjempelse av datakriminalitet, herunder alvorlige IKT-sikkerhetshendelse. Basert på erfaring, samsvarer ofte informasjonsbehovet til KRIPOS med informasjonsbehovet til NSM NorCERT.

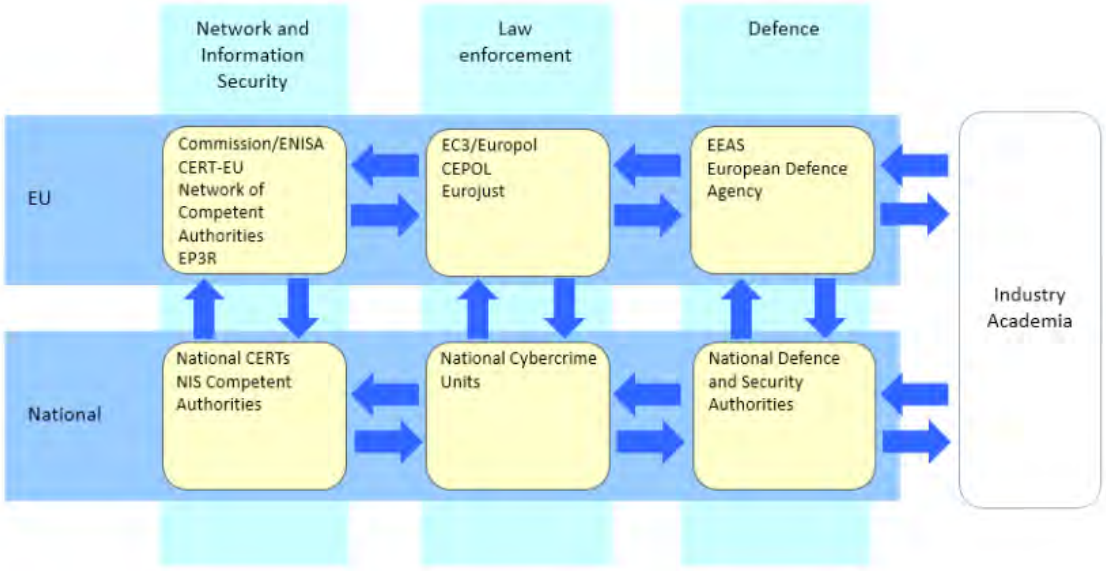
12. Internasjonalt regelverk

12.1. Overblikk

I EU varierer det i hvilken grad sektormyndigheter har regulert sikkerhet i driftskontrollsystem og krav til logging, analyse og informasjonsdeling.[24] På tross av at det er et økende antall land i EU som arbeider med å utarbeide lov- og forskriftskrav knyttet til SCADA-sikkerhet og informasjonsdeling ved hendelser, er det først og fremst de frivillige og selvpålagte kravene, ved for eksempel å følge etablerte standarder og beste praksis, blant virksomhetene i de ulike landene som er fremtredende. NIS-direktivet (se pkt 9.2) er et forsøk på å implementere et felles rammeverk for informasjonsdeling, spesielt blant nasjonale og sektorvise CERT/CSIRT-miljøer på tvers av EU-landene ved store IKT-hendelser.

[23] Kripos, «Om Kripos», URL: https://www.politi.no/kripos/om_kripos/Tema_71.xhtml
[24] ENISA, «Cyber Security Information sharing: An Overview of Regulatory and Non-Regulatory Approaches, 2015. URL: https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

I 2013 ble det utarbeidet en europeisk IKT-sikkerhetsstrategi som baseres på pilarene «nettverks- og informasjonssikkerhet», «håndhevelse av lov» og «forsvar og nasjonal sikkerhet». Figuren under viser prinsippene i strategien:



Figur 1: Prinsippene for EUs IKT-sikkerhetsstrategi. Kilde: «Cyber Security Information sharing: An Overview of Regulatory and Non-Regulatory Approaches", ENISA, 2015

I 2013 vedtok EU EPCIP-direktivet (EU's Programme for European Critical Infrastructure Protection),

I EPCIP-programmet inngår identifisering og utpeking av europeisk kritisk infrastruktur og vurdering av behovet for å beskytte den bedre, et Critical Infrastructure Warning Information Network (CIWIN) og det finansielle programmet «Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks». Innenfor programmet ligger opprettelse av ekspertgrupper, utveksling av «best practice» og identifisering og analyse av gjensidige avhengigheter mellom ulike infrastrukturer.

I Norge ble EPCIP-direktivet innlemmet gjennom en endring av sivilbeskyttelsesloven[25]. Lovendringen medførte at det er sektordepartementene som er ansvarlige for at EPCIP-direktivets krav blir oppfylt innen deres ansvarsområde, og da særlig identifiserings- og utpekingsprosessen.[26]

Som et av tiltakene under EPCIP-paraplyen, ble det etablert et prosjekt kalt «DENSEK[27]» (Distributed ENergy SEcurity Knowledge) som har som mål å etablere en felles, europeisk tjeneste (ISAC) for deling av trusler og analyser som berører europeisk energisektor.

Når det gjelder konkrete krav til sikkerhet i SCADA[28]-system, så har enkelte land som Polen, Tyskland, Frankrike, Spania og Ungarn en viss form for regulering knyttet til SCADA-system for styring av kritisk infrastruktur[29]. Ingen har imidlertid spesifikke krav til SCADA-system i

[25] https://lovdata.no/dokument/LTI/lov/2012-12-14-90
[26] https://www.regjeringen.no/no/dokumenter/prop-129-l-20112012/id685449/sec1
[27] http://www.densek.eu
[28] Vi benytter begrepet SCADA i stedet for driftskontroll i denne konteksten, da man ellers i Europa benytter begrepet «SCADA-systems» for spesifikke system innen spesifikke sektorer eller «Critical infrastructure» når det gjelder kritisk infrastruktur generelt.
[29] ENISA: «Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors», 2015. URL: https://www.enisa.europa.eu/publications/maturity-levels

kraftforsyningen, men ser på sikkerhet i SCADA-system i et bredere perspektiv knyttet til beskyttelse av kritisk infrastruktur. Beskyttelse av SCADA-system blir da ikke regulert spesielt, men kravene til sikkerhet blir på samme nivå som krav til beskyttelse av kritisk infrastruktur generelt. Da er det gjerne virksomhetene selv som må sette egne krav til beskyttelse av SCADA-system som harmoniserer med de generelle kravene til beskyttelse av kritisk infrastruktur.

12.2. NIS-direktivet

6. juli 2016 vedtok EU-kommisjonen NIS-direktivet (Directive on Security of Network and Information systems).

Direktivet pålegger medlemsstatene å sørge for et visst nivå for landets IKT-sikkerhet ved å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) som blant annet skal samarbeide med andre lands CSIRT-er, og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser[30].

Direktivet legger opp til at "operatører av essensielle tjenester" og "tilbydere av digitale tjenester" skal omfattes av direktivet. Direktivet er ikke et såkalt fullharmoniseringsdirektiv, jf. artikkel 3 i direktivet. Dette betyr at norske myndigheter i teorien kan bestemme at direktivet kan gjelde for flere enn det direktiver legger opp til, gjennom en norsk lov om informasjonssikkerhet.

"Operatører av essensielle tjenester" omhandler virksomheter som har ansvar for informasjonssystem som er viktige eller kritiske for opprettholdelse av viktige samfunnsmessige funksjoner. Som en retningslinje anbefales det at alle virksomheter som har en vesentlig rolle i leveranse av strøm, drivstoff, elektronisk kommunikasjon, samferdselstjenester, vann og avløp samt annen infrastruktur bør omfattes av direktivet. Både kraftforsyning, vannforsyning og petroleumsvirksomheten kan omfattes av kravene i direktivet[31]. Unntaket kan være i de tilfellene virksomheten er pålagt like strenge eller strengere krav til IKT-sikkerhet enn det direktivet krever.

Direktivet pålegger medlemsstatene (herunder også EØS-landene) å sørge for at operatører av essensielle tjenester iverksetter flere sikkerhetstiltak. Dette inkluderer blant annet risikostyring og varslingsplikt om hendelser som kan få vesentlig betydning for opprettholdelse av kritiske samfunnsfunksjoner, og der bortfall kan få alvorlige negative konsekvenser for samfunnssikkerheten og økonomiske og samfunnsmessige aktiviteter.

Dette vil kreve at operatørene også er i stand til å oppdage og håndtere hendelser som kan påvirke IKT-systemene som styrer de samfunnskritiske funksjonene.

12.3. Australia

I samsvar med oppstartsmøtet for prosjektet, har prosjektet kontaktet BDO Australia for å kartlegge om Australia har et fungerende regelverk hva gjelder logging og overvåking i driftskontrollsystemer.

[30] Regjeringen, «NIS-direktivet», URL: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/
[31] Føyen Torkildsen, URL: https://foyentorkildsen.no/artikler-og-publikasjoner/network-and-information-security-direktivet-betyr-norske-virksomheter/

Australske virksomheter som styrer kritisk infrastruktur, har ingen konkrete krav på seg gjennom lov eller forskrifter å beskytte SCADA-system som overvåker og styrer kritisk infrastrukur. Australske myndigheter anbefaler på generell basis å bruke National Institute of Standards and Technology (NIST) sin retningslinje for å sikre driftskontrollsystemer[32].

12.4. Pågående arbeid i EU – norsk engasjement

I november 2015 ble det nedsatt en ekspertgruppe under programmet Energy Expert Cyber Security Platform (EECSP). Gruppen har som oppgave å komme med anbefalinger til EU-kommisjonen om i hvilken grad det skal fastsettes krav til sikkerhet i informasjonssystem i energisektoren, herunder system som er kritisk for forsyningssikkerheten, IKT-system i Smart-Grid-løsninger og system som styrer atomkraftverk.[33]

NVE bør følge denne prosessen tett da det antas at nye direktiver eller forordninger på dette området også vil være EØS-relevant. Norge er blant de landene som har kommet lengst i å spesifisere krav til beskyttelse av driftskontrollsystem, og bør kunne være med på å påvirke regelverksutviklingen i EU.

13. Aktiviteter etter inntruffet hendelse

I dette kapittelet gis det en oversikt over viktige aktiviteter som bør gjennomføres underveis og i etterkant av alvorlige IKT-sikkerhetshendelser. Aktivitetene går ut på å lære av hendelser som oppstår hos virksomhetene og dele informasjon med aktuelle myndigheter og andre aktuelle parter.

13.1. Aktivitet: Uthenting av logger, korrelering og analyse

13.1.1. Formålet med aktiviteten

Formålet med aktiviteten er å sørge for hensiktsmessig uthenting og korrelering av logger underveis, eller i etterkant av en IKT-sikkerhetshendelse. Logger som normalt vil bli analysert ved hendelser i tradisjonelle kontornettverk (e-postlogger, aksesslogger, webtrafikklogger og DNS-logger) er her ikke nevnt, da aktiviteten i hovedsak skal beskrive analyse av logger fra industrielle prosesskontrollnettverk.

13.1.2. Aktuelle logger

Alle logger som kan belyse hendelsen er aktuelle logger. Først og fremst vil det være nyttig å hente ut logger fra sikkerhets- og infrastrukturprodukter, for eksempel:

- Brannmurlogger
- Logger fra IDS-løsninger
- Autentiseringslogger
- Flow-logger
- Oversikt over brukere og tilganger

[32] NIST, «Guide to Industrial Control Systems (ICS) Security", URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf
[33] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341

Innhenting og analyse av disse loggene vil danne grunnlaget for videre logguthenting. Loggene nevnt over kan i beste fall føre til identifisering av kompromitterte systemer. Dermed blir det videre aktuelt å hente ut følgende logger fra disse systemene:

- Systemlogger
- Applikasjonslogger
- Konfigurasjonsendringer

13.1.3. Korrelering og analyse

Når aktuelle logger har blitt hentet ut fra komponenter i nettverket er det hensiktsmessig å korrelere og analysere disse. Dette gjøres mest effektivt ved hjelp av et sentralt logghåndteringsverktøy. Dersom en ikke har tilgang på et logghåndteringsverktøy, er man nødt til å korrelere og bygge en tidslinje for hendelsen manuelt.

Loggmengden vil i de aller fleste tilfeller bli stor, og det kan derfor være nyttig å gjøre følgende under korrelering og analyse:

- Strukturere loggdata. Sørge for at alle loggtypene har samme tegnsetting og tilnærmet samme format.
- Sørge for at alle logger bruker samme tidssone, og har samme tidsstempelformat. Ved bruk av et sentralt logghåndteringsverktøy, vil dette i de fleste tilfeller allerede være gjort før hendelsen avdekkes.
- Dele opp loggmengden i flere filer/kataloger/indekser. Avhengig av loggmengden kan det være hensiktsmessig å dele opp loggmengden for dag, uke, måned eller år. Ved ekstreme loggmengder må en kanskje dele opp time for time. Dette er også noe et sentralt logghåndteringsverktøy har som oppgave.
- Bruke identifisert mistenkelig aktivitet som vippepunkter for å gå videre i analysen. Det er viktig å arbeide med utfylling av tidslinjen både før og etter denne aktiviteten.
- Loggfunn bør dokumenteres underveis, for eksempel i en wiki, slik at man er sikker på at alle spor blir fulgt opp. Det er nyttig å utpeke en «Information Manager» som samler inn resultater fra alle som håndterer hendelsen, og sørger for at oversikten er komplett. Oversikten er viktig for å etterse at man er på riktig spor og bruker ressursene på en hensiktsmessig måte.
- Loggfunn kan sammenliknes og knyttes opp mot trusler omtalt i åpne informasjonskilder, eventuelt lukkede informasjonskilder. Ved å knytte funn opp mot kjente trusler vil en trolig ende opp med ny informasjon som kan benyttes videre i nye loggundersøkelser.

13.2. Aktivitet: Læringspunkter

13.2.1. Formålet med aktiviteten

Virksomheten vil, ved hjelp av denne aktiviteten, tilegne seg en oversikt over hvilke steg i håndteringen som fungerte og hvilke som ikke fungerte. Virksomheten skal evaluere tiltakene som har blitt iverksatt, ressurs- og verktøybruk og samarbeid med andre involverte virksomheter. Etter gjennomført evaluering vil virksomheten ha et bedre grunnlag for håndtering av fremtidige hendelser.

13.2.2. Punkter til evaluering

1. Hvordan ble hendelsen oppdaget?

2. Hvordan vurderte virksomheten hendelsen? Ble vurderingen endret på et senere tidspunkt?
3. Hvordan ble omfanget av hendelsen kartlagt?
    a. Hvilke systemer/nettverk?
    b. Vurderes som målrettet?
4. Hvilke andre parter ble koblet inn i håndteringen?
    a. Når ble disse partene koblet inn?
5. Hvordan fungerte kommunikasjonen med andre involverte parter?
6. Hva ble gjort bra underveis i håndteringen?
7. Hvilke hindringer møtte virksomheten på?
8. Hva kunne blitt gjort bedre underveis i håndteringen?
9. Hvilke verktøy ble benyttet til håndtering av hendelsen?
10. Hadde virksomheten tilstrekkelig med ressurser?
11. Hvor kjapt ble normaltilstand gjenopprettet?
12. Hvilke sårbarheter ble identifisert?
    a. Hvilke risikoreduserende tiltak ble iverksatt for å fjerne eller minske sårbarheten(e)?
13. Hvilke tiltak har blitt gjort hos virksomheten i etterkant av hendelsen?
    a. Personellendringer?
        i. Dedikert personell?
    b. Maskinvare- og programvareendringer?
    c. Fysisk sikring?
        i. Dørlås?
        ii. Videoovervåking?
        iii. Vakt?
    d. Systemtilganger?
    e. Forbedret sporbarhet?
        i. Utvidet logging?
        ii. Endring i virksomhetens infrastruktur?
14. Har virksomheten sammenstilt all teknisk informasjon i et dokument som kan deles?
15. Hvilke økonomiske konsekvenser hadde hendelsen for virksomheten?
    a. Personellkostnader
    b. Innkjøp av utstyr og tekniske verktøy
    c. Bistand fra eksterne
    d. Produksjonsstans
    e. Annet
16. Hva er de viktigste læringspunktene virksomheten tar med seg videre?

13.3. Aktivitet: Informasjonsdeling

13.3.1. Formålet med aktiviteten

Alle virksomheter i kraftforsyningen plikter å varsle NVE ved sikkerhetstruende hendelser i driftskontrollsystemet[34]. Det forutsettes videre at kriminelle handlinger anmeldes til politiet,

NVE er beredskapsmyndighet, og vil vurdere hvorvidt det er nødvendig å varsle andre relevante myndigheter eller samarbeidsorganer om hendelsen.

Hendelser som NVE bør vurdere å varsle videre om, er for eksempel om én eller flere selskaper har fått kompromittert driftskontrollsystemet, eller at det oppdages at noen forsøker å innhente informasjon om driftskontrollsystemet.

NVE kan også få informasjon fra andre myndigheter eller samarbeidsorganer om sikkerhetstruende hendelser som kan berøre kraftforsyningen.

Ved hendelser som kan påvirke flere sektorer, er det viktig at sektormyndighetene på forhånd har opprettet rapporteringsrutiner, slik at varsling kan skje raskt, målrettet og sikkert.

Det er da viktig å få på plass følgende:

- En beskrivelse av hvilke hendelser som bør varsles videre, blant annet.
    - Datainnbrudd eller forsøk på datainnbrudd hos flere selskap samtidig/med kort tids mellomrom.
    - Kompromittering av driftskontrollsystem, eller at det oppdages at noen forsøker å innhente informasjon om driftskontrollsystemet.
    - Funksjonssvikt i driftskontrollsystem i flere selskap.
    - Angrep eller forsøk på angrep mot administrasjonsnettverket til flere selskap.
- En oversikt over hvilke myndigheter og samarbeidsparter som bør varsles ved ulike hendelser. Oversikten anbefales lagt inn i en beredskapsplan.
- En oversikt over personer eller funksjoner som kan kontaktes hos de respektive sektormyndighetene. Dette bør også være listet opp i en beredskapsplan.

Siden KraftCERT er en del av kraftforsyningen[35] vil de fungere som en støtte og viktig samarbeidspartner under en større hendelse. KraftCERT har en bred kontaktflate i sikkerhetsmiljøene i inn- og utland, og kan bistå NVE i å innhente informasjon ved større hendelser.

Informasjonen som bør deles må være så presis og konkret som mulig, særlig hvis det dreier seg om teknisk informasjon. NVE kan da ta utgangspunkt i varslingsskjemaet for deling av informasjon.

Hvis hendelsen karakteriseres som sensitiv, må kommunikasjonen mellom myndighetene skje på en sikker måte - enten via fysiske møter eller ved at informasjonen oversendes over sikrede kommunikasjonskanaler. Dette bør også omtales i en beredskapsplan.

Rutinene bør være samordnet mellom de aktuelle myndighetene. Det anbefales at man i samarbeid utarbeider detaljene for selve varslingsrutinene, samt tersklene for varsling.

13.3.2. Aktuelle mottakere av informasjon

[34] https://lovdata.no/forskrift/2012-12-07-1157/§2-6
[35] KraftCERT ble innlemmet i KBO etter vedtak av NVE datert 22.12.2014.

For NVE vil det være aktuelt og relevant å varsle en rekke myndigheter og samarbeidsparter ved større hendelser, ut over Kraft-CERT og eventuell direkte varsling til virksomhetene i kraftforsyningen. Dette omfatter *blant annet*:

- Nasjonal sikkerhetsmyndighet NorCERT (NSM)
- Politiet (KRIPOS)
- Nasjonal kommunikasjonsmyndighet
- Petroleumstilsynet
- Direktoratet for samfunnssikkerhet og beredskap

13.3.3. Informasjon til deling

1. Teknisk informasjon og analyser
    a. Indikatorer som kan benyttes til søk i andre virksomheters systemer og nettverk (IP-adresser, domenenavn, URL-er etc.)
    b. Angripers operasjoner (hvis avdekket)
    c. Eventuelle analyser
        i. Nettverksanalyse
        ii. Digital etterforskning (analyse av kompromitterte maskiner)
        iii. Skadevareanalyse
    d. Hendelsesrapport
2. Overordnet informasjon om hendelsen
    a. Hvordan hendelsen ble oppdaget
    b. Hendelsens omfang (berørte systemer og nettverk)
    c. Eventuell driftsstans
3. Håndtering og tiltak
    a. Virksomhetens håndtering av hendelsen
    b. Tiltak iverksatt underveis og i etterkant av hendelsen
    c. Anbefalinger fra berørt virksomhet
4. Fullstendig hendelsesrapport med analyser og teknisk informasjon
    a. Hvis mulig bør hendelsesrapport deles

14. Rapporteringsskjema: IKT-sikkerhetshendelser

14.1. Beskrivelse

Nedenfor gir vi en anbefaling til rapporteringsskjema som bør fylles ut av virksomhetene i kraftforsyningen som blir utsatt for IKT-sikkerhetshendelser. Skjemaet skal sørge for at NVE får en oversikt over omfanget hendelsen har, som et grunnlag for videre myndighetsoppfølging. Opplysningene det blir bedt om, vil være sensitive, og – når ferdig utfylt – bør oversendes på sikker måte.

14.2. Minstekrav

Det er viktig at rapporterende virksomhet gir så mye og nøyaktig informasjon som mulig. Rapporteringen bør minimum inneholde en kort beskrivelse av hendelsen, berørte systemer og nettverk, samt status for hendelsen på rapporteringstidspunkt.

14.3. NVEs behandling av rapporteringsskjemaet

Ved mottak av skjema, bør NVE raskt gjøre en vurdering av om hendelsen som rapporteres er av en slik karakter at den bør varsles til andre samarbeidspartnere og virksomheter innenfor kraftbransjen.

14.4. Skjema

Rapporterende virksomhet		*Virksomhet X …*
Kontaktperson	**Navn**	*Person X …*
	Rolle	*Rolle X …*
	Telefon	*Telefonnummer X …*
	E-post	*E-postadresse X …*
Andre eksterne involverte		*Sikkerhetsleverandør X …*
Andre involverte myndigheter		*Myndighet X …*
Tidsperiode for hendelse		*YYYY-MM-DD – YYYY-MM-DD*
Dato for rapportering		*YYYY-MM-DD*
Rapport vedlagt (Ja/Nei)		*Ja/Nei …*

Beskrivelse

Kort sammendrag av hendelsen og oppdatert hendelsesforløp.

Status

Hva er status på rapporteringstidspunkt?

Er normaltilstand gjenopprettet?

Skadeomfang

Beskrivelse av hendelsens omfang, herunder berørte nettverk og systemer.

Har hendelsen ført til nedetid i kritiske driftskontrollsystemer?

Har det blitt gjennomført vurdering av skaden som har skjedd?

Undersøkelser og tiltak *Beskrivelse av virksomhetens undersøkelser og tiltak.* *Hvilke strakstiltak ble iverksatt av virksomheten?* *Hvilke tiltak har blitt iverksatt/skal iverksettes i etterkant av hendelsen?*
Tilgjengelig teknisk informasjon *Hvilke tekniske data er tilgjengelig for analyse ved behov?* *Hvor langt tilbake har rapporterende virksomhet logger?*
Tilleggsinformasjon *Tilleggsinformasjon til rapporteringen.*

15. Konklusjoner og anbefalinger

15.1. Hvor gjennomførbart er logging i driftskontrollsystem?

Rapporten har listet opp en rekke logger og informasjon som kan være aktuelt å hente ut fra et eller flere driftskontrollsystemer, inkludert informasjon fra enkeltkomponenter. Problemstillingen er å finne ut hva som er sannsynlig og gjennomførbart for de aller fleste virksomheter i kraftbransjen.

Svært mange driftskontrollsystem benytter fremdeles proprietære protokoller. Trafikken fra disse kan være vanskelig å kartlegge og tolke, og krever i mange tilfeller spesialkompetanse. I og med at stadig flere er i ferd med å gå over til standard IP-protokoller, bidrar det til å lette overvåking og analyse av datatrafikken.

Vi anbefaler at virksomhetene først og fremst benytter logger fra sikkerhetsmekanismer og infrastrukturprodukter innført i nettverkene. Dette er logger alle virksomheter er i stand til å hente ut. Loggene kan komme fra svitsjer, brannmurer, IDS-løsninger og autentiseringsløsninger. Korrelering og analyse av disse loggene vil danne grunnlaget for videre håndtering av hendelsen og eventuell uthenting av andre logger virksomheten har tilgjengelig.

I en hendelsessituasjon vil det være hensiktsmessig å ha logger en god stund tilbake i tid, erfaringsmessig to år eller lenger. En angriper kan ha vært på innsiden i lang tid uten at dette har blitt oppdaget, og derfor er det viktig å kunne søke i logger langt tilbake i tid for å kartlegge hendelsesforløpet.

15.2. Krav og kompetanse

Når det gjelder krav til overvåking, logging og analyse bør formelle krav sees i sammenheng med virksomhetenes kunnskap og evne til å logge.

Det vil være naturlig å vurdere utvidede krav til større virksomheter (klasse 2 og 3), blant annet ved at det kan spesifiseres nærmere krav til systemlogger, konfigurasjonsendringer og applikasjonslogger fra sentrale komponenter i driftskontrollsystemene. Dette begrunnes med at disse virksomhetene har demonstrert god kompetanse på nettverk og nettverksutstyr som svitsjer, rutere, brannmurer og liknende.

Uthenting av logger fra standard nettverksutstyr er noe alle selskap bør ha kunnskap om, i hvert fall om man benytter eksterne leverandører av nettverkstjenester til kontornettverk. Et eventuelt krav om overvåking og logging bør være gjennomførbart, men det anbefales at det i forkant gjøres noen mer detaljerte undersøkelser om hva som kan være realistisk å kreve av disse virksomhetene.

15.3. Bevisstgjøring

Vår erfaring er at det er et forbedringspotensial hva gjelder forståelse for hvilke trusler som truer kraftbransjen. Med så mange kritiske systemer er det viktig at det fokuseres på bevisstgjøring av ledere, brukere og IT-/sikkerhetspersonell internt hos virksomhetene, slik at forståelsen for truslene mot kraftforsyningen er tilstede. Proaktiv overvåking og deteksjon

Ved å samle inn logger fra mange loggkilder har en mulighet til å se aktivitet i driftskontrollsystemer over lengre tid. Dette vil hjelpe til med å kartlegge hva som er normal nettverkstrafikk og hva som er mistenkelig.

Analysering av logger kan føre til proaktiv overvåking, ved at en utformer signaturer basert på observert trafikk, som så skal detektere ondsinnet trafikk på senere tidspunkter. Signaturene som utformes benyttes i IDS-løsninger og alarmerer hvis nettverkstrafikk samsvarer med signaturen.

15.4. Fremtidsmuligheter

Digitalisering medfører enklere tilgang på data, men også flere mål for potensielle angripere. Det er av stor betydning at NVE og aktuelle samarbeidspartnere holder seg oppdatert på ny teknologi og sikkerhetsløsninger. Nye komponenter og løsninger i driftskontrollsystemene vil mest sannsynlig bety flere loggmuligheter, og kravene for logging bør dermed endres i tråd med utviklingen.

NVE bør også ta stilling til i hvilken grad NVE skal tillate bruk av skytjenester for lagring og behandling av logger fra driftskontrollsystem, som nevnt tidligere i rapporten. Det finnes en stor mengde leverandører som kan være aktuelle. Derfor er det nyttig at NVE, i samarbeid med andre myndigheter og sakkyndige, kartlegger leverandørene og anbefaler et utvalg av disse på tvers av sektorer.

15.5. Deling av informasjon

Deling av informasjon underveis og i etterkant av hendelser er svært viktig for den nasjonale situasjonsforståelsen. Dette gjelder både internt i den enkelte sektor, og på tvers av sektorene.

Det er viktig at NVE og virksomheten(e) samarbeider om kontakt med NSM og eventuelt Politiet (KRIPOS) ved hendelser. KraftCERT er en naturlig samarbeidspartner for NVE, både for kontinuerlig kontakt, men også i en hendelsessituasjon.

Ut over kraftforsyningen, bør deling av informasjon gjøres av NVE i samarbeid med berørte virksomheter for å nå de mest aktuelle sektorene raskest mulig.

Aktuelle myndigheter (NVE, NSM, KRIPOS, Nasjonal kommunikasjonsmyndighet med flere) og andre parter bør sammen utarbeide rutiner for varsling, terskler for varsling, hvilke kommunikasjonskanaler det bør varsles gjennom og avklare hvilket mandat de respektive myndighetene har for å sikre at varsling og håndtering av alvorlige IKT-sikkerhetshendelser på tvers av sektorer kan gjøres effektivt og koordinert.

15.6. Bevisstgjøring av leverandører til kraftforsyningen

Det finnes en rekke leverandører av utstyr og løsninger innenfor kraftforsyningen. En av virksomhetene som ble intervjuet opplever i stor grad at mange av leverandørene har manglende sikkerhetsfokus. Et eksempel på dette er at leverandørene forsøker å sette opp egne løsninger for fjerntilgang til komponenter i driftskontrollsystemene. Dette er utfordrende for virksomheter som forsøker å ha et godt sikkerhetsfokus.

Det hadde vært nyttig om NVE, gjerne i samarbeid med utvalgte virksomheter, tok en gjennomgang av hvilke krav som bør settes for de ulike leverandørene.

15.7. Kilder

- Hagen, J, «Teknologiskifte i energiforsyningen», rapport utarbeidet for NVE, 2015.
- Forskningsrådet: «IKT-sikkerhet – det kontinuerlige kappløpet», sluttrapport etter IKT-SoS-programmet, 2008.
- NSM, «Risiko 2016», URL: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf
- Lovdata, Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften), URL: https://lovdata.no/forskrift/2012-12-07-1157/§7-14
- ENISA, «Protecting Industrial Control Systems – recommendations for Europe and Menber States», 2011.
- NIST, «Guide to Industrial Control Systems (ICS) Security», revision 2, 2015, URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf
- Homeland Security: Recommended Practice: Creating Cyber Forensics Plans for Control Systems, 2008.
- Mnemonic, «Sikkerhetsmonitorering av driftskontrollsystem», notat utarbeidet for NVE, 2013.
- Bartnes, Line, "Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations", Journal of Critical Infrastructure Protection, Volume 12, March 2016.
- Siemens, URL: http://w3.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/simatic-pcs-7-system-

components/communication/PROFINET_%20PROFIBUS/Pages/PROFINET_PROFIBUS.aspx?tabcardname=profinet

- ABB, Communication Protocols, URL: https://library.e.abb.com/public/ff6ab6766689f2a7c1257b40001b8b28/3BSE035982-511_en_AC_800M_5.1_Feature_Pack_Communication_Protocols.pdf
- Hovland, Kristoffer, «Logging og logganalyse», studentrapport utarbeidet for NVE i 2016.
- Splunk, URL: https://www.splunk.com/
- Elastic Stack, URL: https://www.elastic.co/
- NSM, «Håndtering av digital spionasje», URL: https://nsm.stat.no/globalassets/dokumenter/norcert/apt_2015_web.pdf
- Kripos, «Om Kripos», URL: https://www.politi.no/kripos/om_kripos/Tema_71.xhtml
- Regjeringen, «NIS-direktivet», URL: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/
- Føyen Torkildsen, «NIS-direktivet», URL: https://foyentorkildsen.no/artikler-og-publikasjoner/network-and-information-security-direktivet-betyr-norske-virksomheter/
- Knapp, Eric D. & Langill, Joel, «Industrial Network Security, Second Edition», Syngress 2015
- Intervjuer med utvalgte virksomheter innen norsk kraftbransje

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no