PETROLEUMSTILSYNET

«MOTTAKERNAVN»
«ADRESSE»
«UTLANDSADRESSE»
«POSTNR» «POSTSTED»

Ved: «KONTAKT»

Vår saksbehandler
Asbjørn Ueland

Deres ref.	Vår ref. (bes oppgitt ved svar)	Dato
«REF»	Ptil 2019/1176/AU	18.9.2019

Informasjon om håndtering av IKT-sikkerhetshendelser

Bakgrunn

I januar 2019 ble Nasjonal strategi for digital sikkerhet presentert. Et av delmålene i denne strategien er at Nasjonal sikkerhetsmyndighet (NSM) videreutvikler Rammeverket for håndtering av IKT-sikkerhetshendelser. Vi vil med dette brevet informere næringen om hvordan større IKT-sikkerhetshendelser planlegges håndtert på nasjonalt nivå.

Målgruppe

Vi ber om at sikkerhetsansvarlige for kontroll- og sikkerhetssystemer så vel som ansvarlige for IKT-systemene samt vernetjenesten blir gjort kjent med innholdet i dette brevet.

Rammeverk for håndtering av IKT-sikkerhetshendelser

Målgruppen for dette rammeverket er blant annet offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner og sektorvise responsmiljøer (SRM). Det er ikke avklart i hvilken grad petroleumsvirksomheten inngår i kritisk infrastruktur og/eller kritiske samfunnsfunksjoner, men vi vurderer at det vil være tjenlig at virksomhetene i sektoren er kjent med dette rammeverket.

Formålet med rammeverket er blant annet:

- å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon
- å effektivt håndtere alvorlige IKT-sikkerhetshendelser fra virksomhetsnivå til politisk nivå.

Samarbeid mellom NSM/NorCERT, sektorvise responsmiljøer og den enkelte virksomhet som er rammet, er vesentlig for å sikre effektiv håndtering og koordinering. Rammeverket forutsetter at den enkelte virksomhet utarbeider egne detaljerte planer for håndtering av alvorlige IKT-sikkerhetshendelser som henger sammen med øvrig beredskapsplanverk.

Rammeverket er tilgjengelig på NSM sine hjemmesider:
https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

Kunnskap IKT-sikkerhet og CERT (responsmiljø)

Sintef har gjennomført et kunnskapsprosjekt om IKT-sikkerhet for å bidra til økt kunnskap og innsats rundt IKT-sikkerhet blant personell i petroleumsnæringen. Oppgaven ble gjennomført våren 2018. Rapporten er basert på intervju og gjennomgang av relevant litteratur og dokumenter, samt SINTEFs generelle kompetanse og erfaring innenfor IKT-sikkerhet.

Rapporten diskuterer CERT-kapasitet i næringen. Det synes å være større interesse for medlemskap i ulike nettverk for informasjonsdeling enn i CERT. Det er lite fokus, spesielt blant de mindre aktørene, på å systematisk dele informasjon og erfaringer om IKT-sikkerhetshendelser med hverandre.

Rapporten gir et øyeblikksbilde med bakgrunn i datagrunnlaget som ble samlet inn våren 2018, og informasjonen har blitt anonymisert. Rapporten er tilgjengelig på våre nettsider:
https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter-2019/industrielle-kontroll--og-sikkerhetssystemer-i-petroleumsvirksomheten/

Digital sårbarhet – sikkert samfunn

I 2015 leverte Lysneutvalget utredningen NOU 2015:13 Digital sårbarhet – sikkert samfunn. Denne rapporten belyser utfordringer knyttet til IKT-sikkerhet for mange sektorer i samfunnet og i kapittel 14 diskuteres petroleumssektoren. Blant annet gis det en vurdering av tilknytningen til responsmiljø (s.158):

> Sektoren mangler et felles responsmiljø. Bransjen er internasjonal og består av utenlandske og norske selskaper. De utenlandske selskapene kan være del av større internasjonale konsern og ha sikkerhetssamarbeid via sitt moderselskap eller eget responsmiljø innad i virksomheten. Bare noen få aktører i bransjen er tilknyttet NSM Nor-CERT. De små selskapene, som ikke er en del av et CSIRT-samarbeid, faller utenfor. Det er ikke etablert noe felles kontaktpunkt for sektoren som myndighetene eksempelvis kan benytte til varsling om nettbaserte angrep. Det er også få formelle fora der sektoren kan utveksle erfaringer.

Utvalget anbefaler derfor at «virksomhetene i sektoren enten inngår et samarbeid med KraftCERT eller finner andre løsninger for operativt samarbeid.»

Vi ser at næringen kun i begrenset grad har tatt tak i denne anbefalingen. Nyhetsoppslaget i e24.no 21. juni i år bekrefter at noe gjøres. https://e24.no/boers-og-finans/aker-bp/aker-bp-tar-cybergrep-allierer-seg-med-kraftbransjen/24644448.

Det blir rapportert at det er økt aktivitet rettet mot både vår næring generelt men også mot de industrielle kontroll- og sikkerhetssystemene. Dragos, et av de ledende selskapene innen IKT-sikkerhet for industrielle systemer, skriver i sin rapport for august 2019:

> The oil and gas industry is a valuable target for adversaries seeking to exploit industrial control systems (ICS) environments. As the number of attacks against ICS overall is increasing, adversaries with specific interest in oil and gas companies remain active and are evolving their behaviors. This report provides a snapshot of the threat landscape as of August 2019 and is expected to change in the near future as adversaries and their behaviors evolve. https://dragos.com/resource/dragos-oil-and-gas-threat-perspective-summary/

Næringen må være forberedt til å håndtere disse utfordringene. Et samlet og sterkt responsmiljø for bransjen vil kunne bidra til økt robusthet i forhold til å bedre kunne håndtere et komplekst og tiltakende trusselbilde rettet eksplisitt mot industrielle kontroll- og sikkerhetssystemer.

Regelverk

HMS-regelverket har en del paragrafer som er relevante i vurderingen av IKT-sikkerhet for industrielle kontroll- og sikkerhetssystemer. Tabellen presenterer disse og vår forståelse av hvordan de kan komme til anvendelse:

Styringsforskriften § 4 Risikoreduksjon: den ansvarlige [skal] velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.	Dette innebærer at det velges løsninger for IKT-sikkerhet som reduserer sannsynligheten for IKT-angrep som forårsaker skade, feil eller faresituasjoner.
Styringsforskriften § 8 Interne krav: Den ansvarlige skal sette interne krav som konkretiserer krav i regelverket, og som bidrar til å nå målene for helse, miljø og sikkerhet	Det må settes krav til hvordan IKT-sikkerhet håndteres, både teknisk, operasjonelt og organisatorisk.

Innretningsforskriften §§ 32-34 Sikkerhetssystemer: Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer. Veiledning: systemet kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket som følge av systemsvikt, feil eller enkelthendelser i disse systemene.	Kravet om at grensesnitt mot andre systemer ikke skal påvirke negativt innebærer at heller ikke IKT-angrep skal hindre at systemene kan utføre tiltenkte funksjoner.
Innretningsforskriften §§ 34a Kontroll- og overvåkingssystem: Veiledning: I tillegg bør Norsk olje og gass retningslinje nr. 104 legges til grunn for beskyttelse mot IKT-relaterte farer.	Veiledningen viser til anerkjent retningslinje, men også andre standarder kan benyttes.
Aktivitetsforskriften § 21 Kompetanse: Den ansvarlige skal sikre at personellet til enhver tid har den kompetansen som er nødvendig for å kunne utføre aktivitetene i henhold til helse-, miljø- og sikkerhetslovgivningen. I tillegg skal personellet kunne håndtere fare- og ulykkessituasjoner.	Kravet om kompetanse er også relevant for de som skal håndtere faresituasjoner i forhold til IKT-hendelse med de industrielle kontroll- og sikkerhetssystemene
Aktivitetsforskriften § 21 Trening og øvelser: Den ansvarlige skal sikre at det utføres nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner på en effektiv måte	Kravet om trening og øvelser er også relevant for de som skal håndtere faresituasjoner i forhold til IKT-hendelse med de industrielle kontroll- og sikkerhetssystemene og samhandle med responsmiljøer
Aktivitetsforskriften § 45 Vedlikehold: Den ansvarlige skal sikre at innretninger eller deler av disse holdes ved like, slik at de er i stand til å utføre sine krevde funksjoner i alle faser av levetiden.	Oppdatering og patching av programvare når det oppdages sikkerhetssvakheter er å forstå som vedlikehold
Aktivitetsforskriften § 48 Planlegging og prioritering: Det skal utarbeides en samlet plan for utføring av vedlikeholdsprogram og korrigerende vedlikeholdsaktiviteter	Kravet om planlegging innebærer en systematikk for hvordan selskapet har kontroll på hvilke oppdateringer som er relevante og hvilke utstyrskomponenter som må ha vedlikeholdsprogram

Styringsforskriften § 29 Varsling og melding: Veiledning: situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse).	Melding om IKT-hendelse slik det framkommer i veiledningen er en informasjon til oss om situasjonen. Dersom det er knyttet sensitiv informasjon til hendelsen, må teksten merkes slik at denne delen kan unntas for innsyn. NSM sitt rammeverk som er omtalt ovenfor beskriver hvordan hendelser i kritisk infrastruktur / kritiske samfunnsfunksjoner skal håndteres.

Innretningsforskriften og Aktivitetsforskriften gjelder for virksomheten offshore. Teknisk og operasjonell forskrift som gjelder for landanlegg har tilsvarende paragrafer.

Med hilsen

Torleif Husebø e.f.
Fagleder

Asbjørn Ueland
sjefingeniør

Dette brevet er godkjent elektronisk i Petroleumstilsynet og har derfor ingen signatur