Øvelsesplanlegger

Pakke 1 øving 2

«*Cyberhendelse i verdikjede*»

Utgave 1.0

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn og formål

Anlegg og installasjoner i petroleumssektoren skal ha beredskapsplaner for håndtering av uønskede hendelser. Næringen har scenarioer som kan knyttes til IKT-hendelser men Havindustritilsynet (Havtil) har i tilsyn sett at det knapt trenes innen IKT-sikkerhet for de industrielle kontroll- og sikkerhetssystemene. Derfor har Havtil fått utarbeidet et sett med trenings- og øvelsesscenarioer. Dette øvelses-opplegget ble utarbeidet av Proactima med Netsecurity som partner. Opplegget er videre bearbeidet av Havtil.

Aktivitetsforskriften § 23 beskriver 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». Samme formulering finnes også i teknisk og operasjonell forskrift § 52. Det er altså samme krav til trening og øvelser for anleggene på land som det er til innretningene på sokkelen.

Når vi trener, øker vi personlige ferdigheter og kunnskaper. Øvelser tester samhandling og beredskapsevne, avdekke styrker og svakheter, samt forbereder ledelsen på å håndtere ulike kriser.

1.2 Oppbygging av veilederen

Hver enkelt øvelsesplanlegger inneholder ulike scenarioer, og det er foreslått hvilke funksjoner som er aktuelle å inkludere i øvelsen. Scenarioene kan benyttes som trening, table top eller spilløvelse.

Veilederen har i del 3 ekstra informasjon til forberedelse og gjennomføring så som:

- et mulig hendelsesforløp i forkant av startpunkt
- sekvensskjema for hendelsen
- relevant fagstoff

2 Scenario

Scenariet for denne veilederen er et varsel fra KraftCERT om et leverandørkjedeangrep på systemer som benyttes i næringen.

2.1 Oversikt scenarioer

Det er ulike forhold som kan påvirke de industrielle IKT-systemer og her er beskrevet fire steg i en hendelse. Scenariet kan gjerne deles opp i forhold til tilgjengelig tid.
Tabell 1 indikerer hvilke funksjoner/avdelinger som er aktuelle å trene ved bruk av disse scenarioene. For å nedskalere omfanget av øvelsen kan det være aktuelt å spille de rollene som ikke er IKT-faglige.

Tabell 1 - Oversikt over hvem som kan trenes/øves i de ulike modulene

Oppgave	Tittel	SAS/IACS-ansvarlig	Lokal driftsledelse	System-ansvarlig drift	IKT-avdeling
2.2	Innledende forhold - Varsel			x	
2.3	Eskalering - Ny Informasjon		x	x	x
2.4	Virus			x	x
2.5	Oppdatert SW tilgjengelig	x	x	x	

2.2 Innledende forhold – Varsel

KraftCERT sender ut et TLP:AMBER+STRICT[1] varsel om at det er oppdaget et leverandør-kjedeangrep hvor en trusselaktør i flere år har hatt tilgang til utviklingsmiljøet og installert kode med skadevare i programvare fra leverandøren av det sentrale SAS-systemet. Den modifiserte koden inkluderer funksjoner til kontroll og kommunikasjon i industrielle IKT-systemer. Varselet kommer opprinnelig fra et internasjonalt CERT-miljø.

2.2.1 Veiledende spørsmål

Systemansvarlig drift

- Hvordan blir varsler mottatt og håndtert
- Hvordan fastslå om installerte versjoner er påvirket av varselet?
- Hvilke nettverkstilgang har systemene ut mot andre nettverk og enheter?
- Hvordan avdekkes tegn til unormal aktivitet og trafikk?
- Hvem involveres?

2.2.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Verifiser mottak av varsler og kartlegg interne forsinkelser
  - Kartlegg håndtering av varsler både fra aktuell leverandør og fra KraftCERT
- Finner ingen indikasjon på utnyttelse
- Ukjent DNS-trafikk fra systemene
  - Hvordan kan denne kontrolleres og håndteres?

[1] Trafikklysprotokollen (TLP) er en internasjonal standard for å klassifisere og dele ugradert informasjon. Les mer på https://www.nsr-org.no/tlp

2.3 Eskalering – Ny informasjon

Ny informasjon blir publisert av KraftCERT. Det er påvist at aktør gjennom oppdateringer har implementert en bakdør. Det er observert to forskjellige typer bakdører, avhengig av når og hvilke oppdateringer som er utført.

Bakdør 1:

Lytter på TCP/UDP port 1414, hvor man kan oppnå kommandolinje på enheten ved å legge til passordet «ics123» i første forespørsel.

Bakdør 2:

Samme funksjonalitet som Bakdør 1, men har også funksjonalitet som forsøker å oppnå kontakt mot internett (c2). Det er bekreftet at bakdøren forsøker å slå opp mot adressen ics-timedate.com

2.3.1 Veiledende spørsmål

Systemansvarlig drift

- Hvordan fastslå om det er installert programversjoner som kan være påvirket?
- Hvordan avdekke om funksjonen til kontrollsystemene er påvirket?
  - Hvilke tiltak utføres?
- Hvordan avdekke om vi har systemer der bakdøren er installert?
- Hvordan varsle for slike tilfeller?

IKT-avdeling

- Hvordan avdekke tegn til unormal aktivitet og trafikk?
- Hvor finnes relevant log data?

Lokal driftsledelse

- Hvilke drifts- og beredskapsmessige konsekvenser kan dette ha?
- Hvordan påvirkes den daglige risikostyringen?

2.3.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Logger viser oppslag mot ics-timedate.com
- Forsøk på HTTPS-oppkobling mot offentlig IP-adresse

2.4 Skadevare

Ny informasjon om bakdør 2. Bakdøren er integrert i kildekoden til systemet og aktiveres ved oppstart. Det er bekreftet en mulighet for at aktøren gjennom bakdøren kjøre vilkårlige kommandoer (RCE). Dette er bekreftet fra CERT-miljøer og flere brukere av programvaren har rapportert følgende fil (IOC):

Filename: C:\Windows\System32\winhostssvc.exe
Sha256: 2a55d47df5b430bb7c74e7092c8a7f34c7801330ffd5177e3227f3c9ba4fae14

2.4.1 Veiledende spørsmål

Systemansvarlig drift /IKT-avdeling

- Hvordan kan det identifiseres om denne filen er på våre systemer?
- Finnes det tilsvarende filer?
- Har vi overvåkning som lar oss undersøke hva som kan ha blitt kjørt på vegne av systemleverandøren?
- Hva gjør filen som er rapportert?

2.4.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Filen finnes på C:\Windows\System32\
- Tilsvarende sha256sum på en annen fil, c:\Windows\temp\svchost.exe
- Ingen filer som har tilsvarende sha256 hash eller filnavn.

2.5 Oppdatert SW tilgjengelig

Oppdatering tilgjengelig fra leverandøren. Etter installasjon av oppdatering må maskinen startes på nytt for å fjerne bakdøren.

2.5.1 Veiledende spørsmål

SAS/IACS-ansvarlig

- Hvilke korrigerende tiltak må iverksettes før eller under oppdatering?
- Hvordan koordineres oppdatering av scada-noder?
  - Hvem involveres?
  - Hvilke rutiner må følges?

Lokal driftsledelse

- Hvilke korrigerende tiltak må iverksettes før eller under oppdatering?
- Hvilke driftsmessige konsekvenser kan dette ha?

Systemansvarlig drift

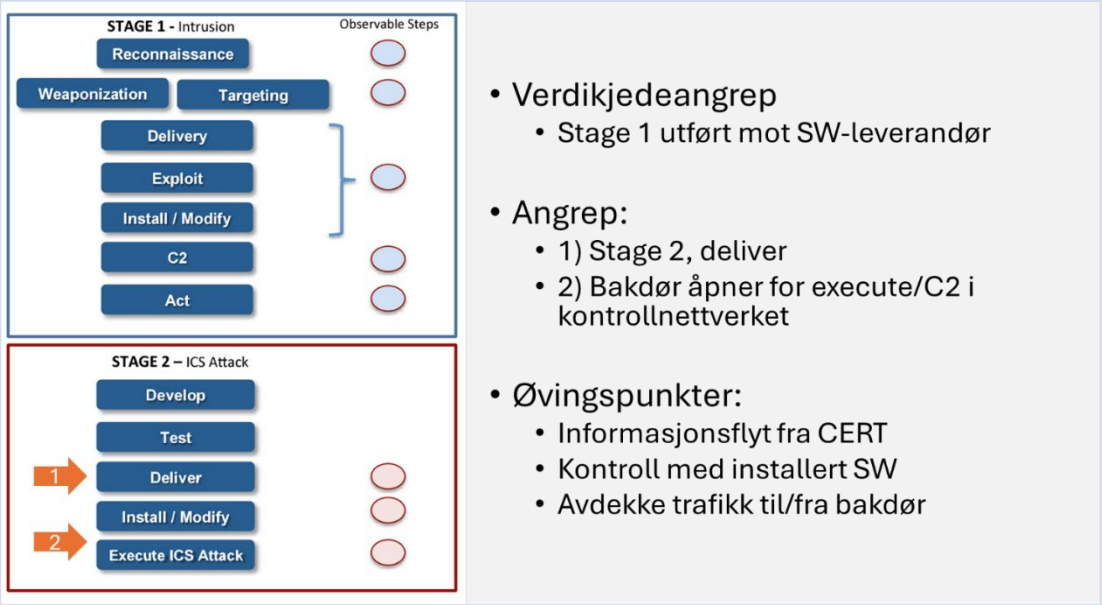
- Hvilken systemer og tjenester blir påvirket av oppdatering og omstart?
- Hvilke rutiner må følges?
- Hvem engasjeres for å gjennomføre arbeidet?
- Hvem påvirkes av oppdateringen?

2.5.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Oppdateringen fungerer som den skal og systemene kommer opp i løpet av kort tid.
- Det er en feil som blir oppdaget under oppdateringen, «missing dependencies».
  - Er ikke i stand til å komme i kontakt med leverandør.
  - Får tilbud om bistand fra leverandør.
  - Krever omfattende oppdateringer av systemet (dependencies).

3 Ekstra informasjon til forberedelse og gjennomføring

Dette kapittelet inneholder bakgrunns-informasjon om hvordan en trusselaktør kan infiltrere industrielle IKT-systemer. Digitale angrep følger ofte faste mønster, på engelsk kalt kill chain. Verdikjedeangrep følger også dette mønsteret, men er mer utfordrende siden steg 1 skjer i en annen organisasjon. Figuren viser hvilke steg som er med i denne øvelsen og hvilke øvingspunkter som er innarbeidet.



3.1 Innledning til hendelse

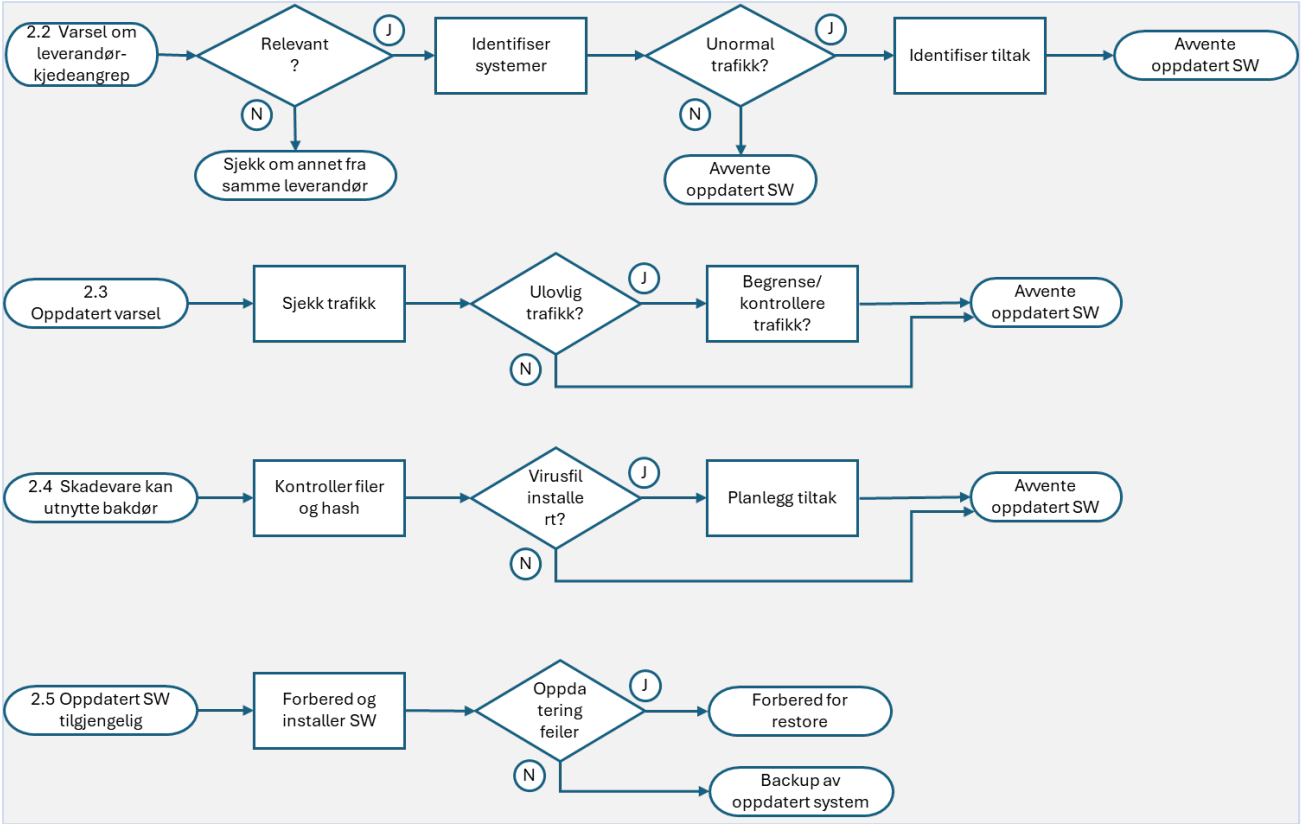
Trusselaktørene går ikke alltid direkte mot det egentlige målet. Virksomheter som vet at de kan være attraktive, har ofte gode rutiner og robuste løsninger som kan være vanskelige å trenge gjennom. Det er ikke alltid underleverandører har sammen nivå av sikkerhet.

En annen tilnærming kan være å gå mot virksomheter som leverer løsninger til mange. To slike forhold er referert i kapittel 3.4.

I denne hendelsen er det en produsent av kontrollsystemer som blir utnyttet ved at programvareoppdateringer inneholder skadevare.

3.2 Hendelse

I utarbeidelsen av øvingen er det tatt utgangspunkt i følgende forløp:



Dette hendelsesforløpet viser en mulig fremgangsmåte for hvordan industrielle IKT-systemer kan infiltreres. Trusselaktøren «APT29» går ofte mot bransjer som energi og telekom, i tillegg til militær og statlig virksomhet. Det antas også at de har en nær relasjon til den russiske utenlandsetterretningstjenesten (SVR).[2]

På siste side i denne øvingsveilederen kan du finne en figur fra den globale kunnskapsdatabasen MITRE ATT&CK®[3]. Den viser et utdrag av taktikker og teknikker basert på innrapporterte observasjoner. MITRE ATT&CK® inneholder også informasjon om hvilke taktikker og teknikker som er typiske for de ulike gruppene av trusselaktører.

[2] https://attack.mitre.org/groups/G0016/
[3] https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json

3.3 Læring

Gjennomgang av rutiner, avklaring av ansvarsforhold og forbedring av systemer.

- Hvordan involveres deltakerne i sluttrapporten fra øvelsen?

Systemansvarlig drift

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?

SAS/IACS-ansvarlig

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?
- Hvordan sikrer en læring til alle skift?

Lokal driftsledelse

- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Hvordan sikrer en læring til alle skift?

3.4 Aktuell litteratur om verdikjedeangrep

Verdikjedeangrep er ikke bare en tenkt hendelse. Her er to eksempler:

I desember 2020 ble det avdekket at den russiske utenlandsetterretningstjenesten SVR hadde etablert tilgang til de interne nettverkene hos SolarWind. Dette ble utnyttet slik at skadevare ble distribuert som en del av ordinær programkode. Amerikanske myndigheter har utarbeidet en beskrivelse av bl.a. denne hendelsen i dokumentet «SolarWinds and Related Supply Chain Compromise».[4]

I april 2024 kunne vi i *Securityweek.com* lese at en aktør fra Nord-Korea i minst fem år har utnyttet en sårbarhet i oppdateringen av antivirus-programmet eScan. Denne sårbarheten har muliggjort et 'man-in-the-middle'-angrep der ondsinnet kode er blitt koblet sammen med de ordinære oppdateringene.[5]

[4] https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds%20and%20Related%20Supply%20Chain%20Compromise%20White%20Paper.pdf

[5] https://www.securityweek.com/north-korean-hackers-hijack-antivirus-updates-for-malware-delivery/?is=152b81581ed4086dca174884e2d1b3dd849835878ef11af1c750fefad5244aa6

Utdrag av taktikk og teknikker som benyttes mot industrielle IKT-systemer. «MITRE ATT&CK®», https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json