Tilsiktede handlinger DKS/IT - dreiebok i vannverk – (Dato for gjennomføring)

I det følgende eksemplet har vi dokumentert en uønsket hendelse ut fra et standardisert oppsett som består av to deler - bakgrunn og faser i håndteringen.
Bakgrunn består av punktene: 1)Beskrivelse av hendelsen, 2)Skadeomfang/ konsekvens, 3) Kritisk materiell, 4)Kritisk personell, 5) Eksterne ressurser, 6)Annet.
Faser i håndteringen: A) Verifisere, B) Varsle, C) Mobilisere, D) Tiltak, E) Normalisere, F) Lære

1 Bakgrunn for scenario/øvelse

Vannforsyningen styres og administreres av et Drifts Kontroll System (DKS) og IT systemer. Disse systemene er ikke så godt sikret som de kunne ha vært, ved at det er felles brukeridentitet og passord som styrer tilgang til DKS-systemene, og ved utskifting av personell skiftes ikke brukeridentitet og passord og man har felles passord som er allment kjent i vannverket. Systemene er gamle og ble laget uten tanke for å håndtere risikoer med mange brukere, internet-tilkopling, virusangrep og sammenkopling av IT systemer og DKS

Denne øvelsen er inspirert av en reell hendelse i 2000 fra et VA-verk i Australia, Maroochy Water services, og er godt beskrevet, se NIST(2000). En av vannverkets innleide teknikere som har installert og kjenner DKS/IT systemene svært godt mister jobben, og gikk deretter til angrep på DKS/IT systemet til vannsekapet. Han slapp bl.a. ut 800,000 liter kloakk i parker, elver og rundt offentlige bygninger. Han logger seg på nettet fra forskjellige steder også tråløst. Han stopper pumper, stopper alarmer og stopper datakommunikasjon mellom pumpestasjoner og sentralt kontrollsenter. Han styrte avløpsstrømmene til de sårbare områdene.

1.1 Beskrivelse av hendelsen – skadeomfang og konsekvenser

En av vannverkets innleide teknikere som har installert og kjenner DKS/IT systemene svært godt har blitt rammet av innskrenkinger og mister jobben. Han har hatt en betrodd stilling og er misfornøyd med den behandlingen han har fått. Han er kjent med felles brukeridentiteter og passord som gir tilgang til DKS og IT systemene. De felles brukeridentiteter og passord skiftes ikke av praktiske grunner, for å forenkle tilgangen til systemene. Han setter i gang målrettede angrep mot vannverket. Han stenger pumper for distribusjon av rent vann, ledningsnettet står i fare for å bli trykkløst i store områder som igjen kan medføre fare for at det kommer forurenset vann inn i ledningsnettet via utettheter. Det blir også sluppet ut kloakk i nærliggende vassdrag via overløp som kan styres. I første omgang blir ikke situasjonen forstått og oppfattet som en beredskapssituasjon.

1.2 Kritisk materiell

Kritisk materiell er utstyr for å varsle (ha dialog med beredskapsteamet) – dvs Internett og telekommunikasjonsutstyr - (dersom det er problemer med infrastruktur regner vi med at nødtelefon er tilgjengelig). Oversikt og kontroll over hvem som har adgang til DKS/IT systemer, Logger fra overvåkning av IT infrastruktur (F.eks. brannmurslogger), Backupløsninger (som er testet/ sertifiserte) og som kan legges inn dersom systemene har blitt endret av angriper/virus.

1.3 Kritisk personell og Eksterne ressurser

Kritisk personell for å håndtere hendelsen er opplærte og utvilte ressurser som Beredskapsleder, tekniske ressurser (Driftsansvarlig datasystemer, driftsansvarlig datanett; Driftsansvarlig strøm -infrastruktur) og Utførende personell i drift. De må ha kompetanse og muligheter for å overvåke signaler, beskjeder og datatrafikk på kontrollnettet for DKS.

En slik hendelse krever også tilgang til rådgivning fra eksterne ressurser som NSM/ NorCert (post@cert.no) og bistand ved informasjonsformidling til forbrukerne (dvs. mediekontakt og tilgang til kommunens kommunikasjonsenhet – som skal oppdatere informasjon til brukerne).

2 Faser i håndteringen

I det følgende beskrives de forskjellige fasene i håndteringen, hvor det forutsettes at beredskapslederen er den som sitter som ansvarlig for å følge opp aktivitetene.

2.1 Verifisere, Varsle og Mobilisere

Det kommer inn mange telefoner fra forbrukerne om at de ikke får vann, vannet har dårlig trykk og kvaliteten på vannet er svært dårlig. Det er i første omgang uklart hva som skjer, men det gjennomføres løpende datateknisk loggføring av hendelsene. Det avdekkes at pumper har blitt stengt bevisst. Det kommer inn mange tekniske meldinger fra nettet som gjør at det blir etablert en beredskapssituasjon, beredskapsleder blir varslet og tar ansvaret og mobiliserer drift.

2.2 Tiltak

I første omgang orienteres helsemyndighetene om at vannet er forurenset. Informasjon om hendelsen legges ut på hjemmesiden. Samtidig oppdateres Facebook og det sendes ut Twitter meldinger om at det er problemer med vannforsyningen og at vannet må kokes. Det kommer inn rykter via Facebook og Twitter om at det er bakterier i vannet – informasjon må derfor løpende oppdateres på WEB, Facebook og Twitter om hva som er korrekt.

Beredskapsansvarlig sender ut driftspersonell for å sjekke pumper og basseng, for å få oversikt over hva som har skjedd. Pumpene står fordi de har blitt slått av med via fjernstyring. En må fysisk dra til pumpestasjonen for å starte pumpene manuelt. Det er logg i driftssentralen som viser hva som har skjedd. Det oppdages at flere pumper har blitt stengt via nettet. Det tar en del tid før det avklares at problemene skyldes et bevisst angrep, siden man har lite erfaring og kjennskap til både sårbarheter og tidligere hendelser.

Det tas kontakt med NorCert og DKS/IT ekspertise for å få hjelp til å håndtere hendelsen. Ved å gå gjennom loggene for DKS og IT systemene ser det ut som om det er en tidligere ansatt hos en leverandør som har gjennomført et angrep. Vedkommende har fått tilgang dels via en gammel brukeridentitet som ikke er slettet ved fratrede, ellers er det lagt inn standard brukeridentitet og standard passord fra leverandøren som gir minimalt med sikkerhet i systemet. De kjente passordene er benyttet for å få tilgang. Det har ikke vært etablert avtaler knyttet til sikkerhet og sikring med underleverandøren.

Vannledningsnettet blir trykkløst i store områder og det er fare for at det kommer inn forurenset i ledningsnettet. Det er sannsynlig at vannet har blitt forurenset og at det er behov for omfattende, spyling av ledningsnettet og det er behov for at vannet må kokes i de første dagene. Driftsansvarlig på stedet nullstiller pumpene, tvangsstyrer pumpene manuelt, og setter i gang pumpene ut fra etablerte manuelle prosedyrer. Brukeridentitet og passord for tilgang til DKS/IT systemet skiftes slik at bare autoriserte ansatte har tilgang til systemene.

2.3 Normalisere og Lære

Etter at det er skiftet passord, etableres normal driftssituasjon i vannverket og det sendes ut beskjed til kundene om tidsplanen for dette.

Vi har i det følgende beskrevet mulige gode lærdommer knyttet til angrep av DKS/IT systemene: Forskjellige type hendelser kan skje, direkte angrep er ikke ofte forekommende, men det kan skje og da er

det viktig at en har etablert rutiner for å vite om risikobildet, unngå hendelser eller oppdage og håndtere slike hendelser så raskt som mulig.

Risikobildet: I USA har en samlet inn hendelser og angrep på IT og industrielle styringssystemer i en egen kommersiell database, www.risidata.com . De har samlet inn data fra 2001, kalt "Industrial Security Incidents Database (ISID)". Erfaringen fra innsamlede hendelser er følgende:

- **20% bevisste angrep** fra eksterne hackere (9.4%) eller fra innsida -ansatte, konsulenter. – (10.6%)
- **80% ubevisste hendelser** som skyldes feil i komponenter eller programvare (38.4%), "Generell Malware" (30.4%), Menneskelige feilhandlinger (11.2%).

Hendelsesbildet er sammensatt, vi ser i det følgende på mulige gode lærdommer for å unngå, oppdage og håndtere slike hendelser:

A1. **Kunnskap – om at bevisste angrep kan skje – trening og policy**, og en bør ha lært opp ansatte og underleverandører), tenkt igjennom hva som kan gå galt, og hvordan en kan forsvare seg mot både bevisste angrep og ubevisste/tilfeldige hendelser. Det bør gjennomføres kurs som forteller om sikring og sikkerhet for DKS og IT systemer, hvordan oppdages angrep, hvordan skal angrep håndteres (beredskapsplaner) og hvordan skal man ta seg i akt. Det vises i denne sammenheng til ROS analysene for DKS/IT og sjekklistene fra NSM. Det bør være laget en kort policy for sikring og sikkerhet av DKS og IT systemer.

A2. **Formaliserte avtaler med leverandører.** Det bør finnes formelle avtaler med underleverandører som evt. brukes for vedlikehold av DKS/IT systemer slik at de følger sikkerhetsprosedyrer og etablert policy for sikring og sikkerhet av DKS og IT systemer.

A3. **Samarbeid med eksperter.** Ved å gjennomføre slike øvelser vil en kunnen styrke kjennskapen til faglige nettverk som bør kunne benyttes ved slike angrep – f.eks. NorCert.

A4. **Det bør være unike brukeridentiteter** og unike (vanskelige) passord for de forskjellige brukerne og de forskjellige oppgavene de har. Brukeridentitet bør skiftes periodisk og ikke deles f.eks. via gule lapper på skjermene – en bør unngå enkle passord som "100". Når en ansatt slutter/funksjonen opphører – bør bruker og passord slettes. Det bør være svært begrenset hvem som har administrator-rettigheter til det som kan være kritiske funksjoner i DKS/IT.

A5. **Det bør finnes logger** som dokumenterer hva som har skjedd i systemet, f.eks. pålogging via tråløs nett eller via internett, eller når alarmer slås av, slik at en kan dokumentere hva som har skjedd. Det bør være noen som har ansvaret for å gå gjennom logger f.eks. for brannmurer.

A6. **Manuelle muligheter og robusthet**. Dersom systemet blir utsatt for angrep bør det være muligheter for å ta over kontrollen manuelt, eller legge inn tidligere (sertifiserte) versjoner og systemer som er sikre slik at systemet kan startes opp med en sikker feilfri versjon. Robusthet av systemet er knyttet til at systemet bør kunne håndtere overaskende uhell, og likevel kunne gjenvinne viktige deler av sin funksjonalitet. Det bør være forsvar i bredde og dybde, slik at de kritiske komponentene i DKS/IT system er skjermet bak flere barrierer som egne nett/brannmurer.

A7. **Improvisasjon.** Det bør være ansatte/eksperter som har god kjennskap til systemet, slik at en kan avdekke hva som har skjedd, og sette i verk tiltak som gjør at en kan gjenvinne driften av systemet på en tilfredsstillende måte.

A8. **Sikre at god praksis benyttes.** NSM har foreslått rutiner og sjekklister som beskriver god praksis for å unngå slike hendelser, eller for å redusere konsekvensen av slike hendelser. Gjennomgang av slike sjekklister og råd, samt trening på å håndtere dette kan gi gode mulighet for å verifisere at sikkerheten følger beste praksis innen område.

3 Referanser

Norsk Vann (2015) *ROS analyser av DKS/IT for vannverk*.

NIST (2008) National Institute of Technology and Standards -Computer Security Resource Center (CSRC) *"Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia"* http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

NSM (2014) *Ti viktige tiltak mot dataangrep* (Oppdater versjon via www.nsm.stat.no)

- Noe mer detaljert: The Center for Internet Security(2015) "*Critical Security Controls*" via www.counciloncybersecurity.org/critical-controls/
- NERC (2007) *Top 10 Vulnerabilities Of Control Systems And Their Associated Mitigations* – 2007, North American Electric Reliability Council, Control Systems Security Working Group, U.S. Department of Energy, National SCADA Test Bed Program, at energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC_2007_Top_10.pdf

Scenario 1 – Tilsikted handling – Angrep på DKS/IT

Pumper slås av og vannledningsnettet i områder med dårlig rentvannskapasitet vil snart bli tomt for vann, det blir varslet at det er lite vann.
På grunn av lite vann i ledningsnettet blir det forurensninger i vann-nettet.