Fylkesmannen i Nordland

Fylkes-ROS, Scenario 14

Svikt i vannforsyning etter cyberangrep

Foto: Pixabay

SCENARIO 14: SVIKT I VANNFORSYNING ETTER CYBERANGREP

11.1 Forutsetninger

Hendelsesforløp

2

I en by i Nordland har kommunen mottatt flere telefoner fra innbyggere som melder om misfarget, illeluktende og usmakelig drikkevann. Undersøkelser viser at uvedkommende kvelden før har vært inne i det kommunale vannverkets kontrollsystem/IKT system. Man finner videre at det har vært en manipulering av systemet samtidig som alarmfunksjoner har sviktet eller bevisst blitt utkoblet. Det fastslås at dette har skjedd som følge av inntrenging i datasystemene

Kommunen befinner seg nå i en situasjon der man ikke kan vite om hovedvannkilden eller ledningsnett/distribusjonsnett er trygt. Det kan være innsug fra forurensede kraner i systemet, rense- og desinfeksjonsprosesser kan være manipulerte, vannet kan være tilsatt skadelige doser av kjemikalier eller andre stoffer. Vannet stenges derfor av umiddelbart. Byen må påregne å være uten vanntilførsel i minst 3 døgn.

Intensjon

Ingen påtar seg ansvaret for angrepet mot vannverkets kontrollsystemer, intensjonen er derfor uklar. Angrep rettet mot IKT systemer i kritiske samfunnsfunksjoner er en økende trend. Målet med angrepet kan være både ren sabotasje, ønske om å ramme kommunen og dens innbyggere, politisk påvirkning, økonomisk tap osv.

Kapasitet

Gjerningsperson er ukjent og dermed er dennes kapasitet heller ikke kjent. Det må antas at vedkommende har tilgang på ressurser som kan utføre lignende angrep rettet mot annen infrastruktur

Lokalisering

By i Nordland

Sammenlignbare hendelser

Bortfall av vann:

- Innbrudd i Hunstadlia høydebasseng i Bodø, februar 2018.
- Langvarig kuldeperiode med frost og tørke, vinteren 2018.
- Potensielt dambrudd ved hovedvannkilde, Sortland, sommeren 2017.
- Rapport utarbeidet for Oslo vannverk viste en lang rekke sikkerhetshull. I rapporten avsløres det at terrorister med en vanlig mobil og det lette passordet kunne overta kontrollen over vannforsyningen i Oslo og fysisk ha kommet seg inn på vannrenseanleggene for å forgifte, stoppe og sabotere drikkevannet til 600.000 mennesker, september 2011[1]

Nettverksangrep mot kritiske samfunnsfunksjoner:

- November 2011: USA, hacking av vannanlegg i Springfield, Illinois. Russiske hackere tok kontroll over pumpe i vannverket og fikk den til å bryte sammen med å slå den av og på gjentatte ganger.[2]
- 2011: USA, ukjent gjerningsmann hacket seg inn på driftskontrollsystemet til vann- og avløpsverket i South Houston, Nevada. Gjorde ingen skade i systemet, men gjorde det kjent at han hadde skaffet seg tilgang
- 2000: Australia, misfornøyd tidligere ansatt manipulerte kontrollsystemer i vannverk som håndterer avløpsvann. 1 million liter kloakk rant ut i nærliggende vassdrag[3]

11.2 Sårbarhetsvurdering

I denne ROS-analysen gjøres det sårbarhetsvurderinger ved å se på hvordan kritiske samfunnsfunksjoner påvirkes av den aktuelle hendelsen. Fargene grønt, gult og rødt brukes for å beskrive hvor sårbar den enkelte kritiske samfunnsfunksjon er. Grønt betyr liten sårbarhet, gult betyr middels sårbarhet og rødt betyr stor sårbarhet.

[1] https://www.nrk.no/ostlandssendingen/drikkevann-ubeskyttet-mot-terror-1.7784850
[2] https://www.dailymail.co.uk/sciencetech/article-2064283/Hackers-control-U-S-public-water-treatment-facilities.html
[3] https://vannforeningen.no/wp-content/uploads/2015/06/2013_875977.pdf

Kritisk samfunnsfunksjon	Sårbarhet
Husly og varme	
Forsyning av mat og medisiner	
Forsyning av drivstoff, olje m.m.	
Strømforsyning	
Elektronisk kommunikasjon (EKOM)	
Fremkommelighet/transport av personer og gods	
Vannforsyning og avløp	
Helse- og omsorgstjenester	
Nød- og redningstjeneste	
Kriseledelse og krisehåndtering	

Nød- og redningstjenesten

Politiet vil spille en viktig rolle i avdekking og etterforskning av en eventuell kriminell handling. Brannvesenet vil utover det vannet de har i sine tankbiler, være avhengige av tilførsel fra naturlige kilder ved brannslukking.

Kriseledelse og krisehåndtering

Nasjonal
Hendelsen vil være en alvorlig nasjonal hendelse, hvor regjeringen raskt vil bli involvert. Justis- og beredskapsdepartementet (JD), vil normalt ha ansvaret for å koordinere den sentrale krisehåndteringen, Justisdepartementet vil være involvert i krisehåndtering gjennom sine underlagte direktorater, POD, NSM og DSB. I tillegg vil mediehåndtering og koordinering av informasjon fra sentrale myndigheter til befolkning og underliggende etater være viktig. De mest berørte fagdepartementene vil være Helse- og omsorgsdepartementet. Forsvarsdepartementet vil også kunne bli involvert. Folkehelseinstituttet har døgnåpen vannvakt, som kan bistå i situasjoner som går ut over det vannverket normalt kan håndtere.

Regional
Fylkesmannen (FM) vil iverksette krisehåndtering som regional samordningsmyndighet. Det betyr at FM tar kontakt med berørt kommune. Fylkesmannen vil få mange oppgaver på helseområdet hvis sykehuset i byen må stenge ned og pasienter overflyttes til andre sykehus og til andre kommuner. Ved

behov vil FM støtte opp om og samordne lokalt hjelpebehov. Samordning av informasjon og rapportering til sentrale myndigheter vil også være en viktig oppgave for FM. Hele eller deler av fylkesberedskapsrådet vil også bli innkalt for ei felles oppdatering om situasjonen og for å diskutere behovet for samordning og oppfølging. Spesielt sivilforsvaret, politiet, mattilsynet og Helse Nord vil bli sentrale samordningsaktører.

Lokal
God håndtering av hendelsen forutsetter et nært samarbeid mellom politiet, mattilsynet og kommunen som er rammet. For den kommunale kriseledelsen vil lokal samordning, formidlinga av informasjon og mediehåndtering være en krevende oppgave. Teknisk avdeling i kommunen vil få stort press på seg for å klarere vannsystemet som sikkert igjen. Helse- og omsorgssektoren vil få utfordringer med drift av sykehjem og andre institusjoner. Oppvekstsektoren vil måtte vurdere om skoler og barnehager skal holde åpne. En nedstenging av denne sektoren vil få ringvirkninger for de andre sektorene med at folk må være hjemme med barna sine. Kommunen må håndtere distribusjon av nødvann.

Helse- og omsorgstjenester

Mangel på vann vil utfordre all drift av institusjoner. I tillegg vil hjemmetjenesten bli utfordret med at brukerne må ha hjelp til å få alternative løsninger. Institusjonskjøkkener vil ikke kunne driftes slik at matlaging til eldre vil bli utfordrende.

Hvis sykehuset må overføre pasienter til kommunene vil også nabokommuner bli berørt av hendelsen.

Smittefaren vil øke hvis det oppstår avløpsproblemer. Dette vil igjen legge beslag på legevakt og fastleger.

Ved stenging av skoler og barnehager, samt økt sykefravær vil helse- og omsorgssektoren utfordres på personellsiden.

Fremkommelighet/transport av personer og gods

I utgangspunktet forventes transport av personer og gods å gå som normalt med unntak av flytrafikken. Mangel på vann til brannslukking vil kunne gi utfordringer for flytrafikk.

Vannforsyning og avløp

Vannforsyning er helt borte i 3 døgn. Gjennomsnittlig vannforbruk i husholdningene var i 2014 på 206 liter per døgn[4] Bortfall av vann vil derfor umiddelbart skape utfordringer for husholdningene.

All industri som benytter vann i produksjon vil bli økonomisk rammet.

Det vil raskt oppstå problematikk knyttet til avløp også.

Ved åpning av vannforsyning vil denne sannsynligvis være redusert til kun sanitærvann (avløp) i en periode. Dette skyldes at stenging med påfølgende åpning av system vil kunne føre til lekkasjer og andre skader. Disse må utbedres før vannforsyningen er fullverdig og kan brukes til både drikkevann og hygieneformål.

[4] https://www.ssb.no/natur-og-miljo/statistikker/vann_kostra/aar/2015-06-16

11.3 Risikovurdering

Tabellen gir en skjematisk presentasjon (oppsummering) av resultatene fra risikovurderingene.

Sannsynlighetsvurdering

	Svært lav	Lav	Middels	Høy	Svært høy	Forklaring
Sannsynligheten for at hendelsen skal inntreffe						Dagens trusselbilde tilsier at sannsynligheten er lav.

7

Konsekvensvurdering

Verdi	Konsekvenstype	Svært små	Små	Middels	Store	Svært store	Forklaring
Liv og helse	**Dødsfall**						Dødsfall kan ikke utelukkes ved sykehus.
	Skader og sykdom						Mulighet for utbrudd av magevirussykdommer.
Stabilitet	**Sosiale og psykologiske påkjenninger**						Hendelsen vil føre til uro i befolkingen både knyttet til vannmangel men også cybervirksomhet.
	Påkjenninger i hverdagen						Hele samfunnet vil bli rammet.
Natur og kultur	**Skader på naturmiljø**						Forurensing i forbindelse med at avløpssystemer ikke fungerer.
	Skader på kulturminner og -miljø						Ikke relevant.
Økonomi	**Materielle skader**						Over 100 millioner kr.
Samlet vurdering av konsekvenser							Totalt sett svært store konsekvenser

Usikkerhet **Liten** **Moderat** **Stor**

Sannsynlighet

Økt bruk og avhengighet til IKT-baserte systemer gir økt sårbarhet. Vi har ikke kunnskap om spesifikke aktører med intensjon om å gjennomføre et angrep av denne typen mot norske vannverk. At det finnes aktører med kapasitet er derimot bekreftet. PST trusselvurdering for 2019 peker blant annet på virksomheter innen kritisk infrastruktur som potensielle mål for nettverksoperasjoner[5]. I tillegg kan man

[5] https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

anta at personer med kjennskap til spesifikk teknologi og kontrollsystemer kan utnytte svakheter i disse om det skulle oppstå et ønske, slik som i hendelsen fra Australia i 2011. Sannsynligheten for at den skisserte hendelsen skal inntreffe i Nordland er å anse som lav så lenge det ikke finnes aktører med en kjent intensjon. Scenarioet er likevel ikke utenkelig og inkluderes derfor i det regionale risikobildet.

Liv og helse

8

Hendelsen har middels konsekvenser for liv og helse. I utgangspunktet anses det ikke som noen fare for dødsfall med mindre kjemiske/bakteriologiske stoffer er fysisk sluppet i vannet. Ved nedstenging av sykehus må pasienter overføres til andre sykehus. Påkjenninger her kan føre til dødsfall.

Scenarioet kan føre til utbrudd av magevirussykdommer. Dette vil medføre middels konsekvenser for samfunnet.

Stabilitet

Denne hendelsen inneholder fire av de seks definerte kjennetegnene som kan indikere «sosiale og psykologiske reaksjoner» for innbyggerne. Konkret gjelder dette at krisen er «ukjent» i en initial fase, en «tilsiktet hendelse», «den rammer sårbare grupper», og kan medfører «forventningsbrudd til myndighetene»:

Avhengige av hvem som står bak cyberangrepet og deres intensjon vil angrepet kunne defineres som en hybrid hendelse. Denne hendelsen vil dermed ha en sikkerhetspolitisk dimensjon og må sees i sammenheng med scenario 12 sikkerhetspolitisk krise i Nord.

Materielle verdier

Økonomiske tap vil i første rekke dreie seg om tap for næringsdrivende som er avhengige av vann. Tapet vil avhenge av næringsstruktur i rammet bykommune. Også kommunen må påregne økonomiske tap som følge av hendelsen.

11.4 Usikkerhet

Kunnskapsgrunnlaget	Merknad
Tilgang på relevante data og erfaringer	Cyberangrep mot både vann og annen kritisk infrastruktur er kjent i utlandet.
Forståelse av hendelsen som analyseres (hvor kjent og utforsket er fenomenet)	Hendelsen er lite beskrevet.
Enighet i arbeidsgruppen	Ingen stor uenighet.
Samlet vurdering av usikkerhet	Usikkerheten knyttet til anslagene for sannsynlighet og konsekvenser vurderes som stor til moderat.

11.5 Overførbarhet

Scenarioet bygger på at vannet må stenges grunnet et cyberangrep. Vel så viktig er å håndtere hendelsen bortfall av vann uavhengig av årsak. Årsakene kan være et stort brudd på hovedvannledning. Hendelse på vannverk (brann, innbrudd etc.) Fysisk terror mot vannledning. Bortfall av vann kan være en følgehendelse etter naturulykker som beskrevet i scenario 1 langvarig strømbrudd, scenario 2 kvikkleireskred, eller en tilsiktet hendelse som beskrevet i scenario 10, terrorhandling.

11.6 Oppfølging

- Følge opp kommunenes planverk, spesielt der det er skjæringspunkter mot andre aktører. For eksempel nødvann til sykehus
- Oppfølging av Cyberproblematikk som en del av utviklingen av totalforsvaret.