Cyber-sikkerhet i VA-sektoren og bidraget fra STOP-IT-prosjektet

Av Rita Ugarelli, Gema Raspati, Ingrid Selseth, Martin Gilje Jaatun, Jon Røstum, Harald Rishovd og Kjetil Furuberg

Rita Ugarelli (Ph.D) er sjefforsker i SINTEF Community og professor II ved NTNU.
Gema Raspati (Ph.D) er forsker i SINTEF Community.
Ingrid Selseth (B.Sc) er forskningsingenør i SINTEF Community og sekretær for Vannforsk.
Martin Gilje Jaatun (Dr. philos) er seniorforsker i SINTEF Digital og professor II ved UiS.
Jon Røstum (Ph.D) er sjefstrateg i Volue Infrastructure.
Harald Rishovd (M.Sc) er seniorkonsulent i Oslo kommune, Vann- og avløpsetaten.
Kjetil Furuberg (M.Sc) er prosjektleder i Norsk Vann.

Summary

Cybersecurity in water and wastewater sector and the contribution from STOP-IT. This article discusses the current issues related to cyber-security in the water and wastewater sector as a critical infrastructure. It emphasizes the need for rising cyber-physical security awareness, competence, and technological uptake in the sector. Some of the main cybersecurity challenges in the water and wastewater sector are presented and discussed. Furthermore, the article presents state-of-the-art technologies and approaches that can help water utilities to cope with the presented challenges based on the outcomes of the H2020 project STOP-IT.

Sammendrag

Denne artikkelen omhandler aktuelle spørsmål knyttet til cybersikkerhet i vann- og avløpssektoren (VA-sektoren). Vannforsyning er en kritisk infrastruktur, og artikkelen understreker behovet for økende cyber-fysisk sikkerhetsbevissthet, kompetanse og teknologi i sektoren. Noen av de viktigste cybersikkerhetsutfordringene blir presentert og diskutert. Videre presenteres teknologier og tilnærminger fra forskningsfronten som kan hjelpe VA-sektoren med å takle utfordringene, basert på resultatene av H2020-prosjektet STOP-IT.

Cybersikkerhet i VA-sektoren – status

Cybersikkerhet må prioriteres i vann- og avløpssektoren (VA-sektoren). Et cyberangrep kan ha direkte innvirkning på folkehelsen, ikke bare på leveransen til forbrukerne, men også av hensyn til andre kritiske virksomheter som er avhengige av kontinuerlig tilgang på vann.

Nivået på digital modenhet i vannforsyninger varierer mye, fra de som har begrenset bruk av digitale løsninger til de som har omfattende digitale systemer og strategier [1]. Flertallet av vann- og avløpsvirksomhetene er i startgropen for digitalisering sammenlignet med andre sektorer som f.eks. energi og transport. VA-sektoren står overfor flere tekniske, organisatoriske og eksterne utfordringer som er vanskelige å håndtere med tradisjonelle tilnærminger. Derfor trengs det innovasjon som digitalisering

kan gi. Verdien som skapes ved hjelp av digital teknologi er mangfoldig; reduserte driftsutgifter, økt effektivitet, økt kundeengasjement og tilfredshet, og ikke minst, økt kunnskapsbasert beslutningsprosess. Digitalisering kan imidlertid ikke gjøres i blinde; dersom et vannverk investerer stort i sensorer ute på nettet uten at de har en god digital plan, kan det resultere i enorme mengder med data som det ikke nødvendigvis er behov for og som kanskje til og med medfører økt sårbarhet.

De teknologiske fremskrittene kan gi sektoren høyere risiko hvis digitaliseringsprosessen ikke omfatter systematisk styring av risiko med hensyn på både cyber- og fysiske trusler mot konkrete løsninger. VA-sektorens digitalisering må bygge på en klar forretningsstrategi der cybersikkerhet er et avgjørende element. Dette er enda mer presserende enn i andre sektorer, siden vanninfrastrukturen ikke ble designet med cybersikkerhet som hovedanliggende. Et eksempel er kontroll- og styringssystemer (SCADA) som ofte brukes i vannforsyningssystemer og renseanlegg for å sikre bedre integrert drift. Selv med anvendelse av cybersikkerhetsprotokoller kan SCADA-systemer være sårbare for cyberangrep. Jo mer sammenkoblet systemene blir, jo større blir sårbarhetene og konsekvensene. At VA-sektoren også er berørt av cybersikkerhet viser hendelsen i Østre Toten kommune i januar 2021, hvor store deler av kommunens IT-løsninger ble kryptert og ikke lenger var tilgjengelig. I Drammen kommune var det en hendelse med sikkerhetsbrister i driftskontrollsystemet i februar 2021. Fra USA har det nylig vært tilfelle av hacking av et vannverk i Florida hvor en hacker prøvde å øke dosen av natriumhydroksyd (lut) i vannbehandlingsanlegget.

Sektoren må jobbe proaktivt for å forhindre, oppdage og redusere nettangrep, ettersom nettangrep vil fortsette å eskalere både med hensyn på hvor avanserte de er og hvor hyppig de opptrer. VA-sektoren har jobbet med styrke informasjonssikkerhet de seinere år. Mattilsynet gjorde i 2016 en undersøkelse om informasjonssikkerhet i norske vannverk, med relativt nedslående resultater. Sommeren 2020 gjorde vi en ny undersøkelse blant et engere utvalg [2] for å se om økt fokus har hatt noen innvirkning på sikkerhetsnivået. Selv om enkelte områder ser marginalt bedre ut, er vårt totalinntrykk at bransjen i større grad innser at den har informasjonssikkerhetsutfordringer; selv om færre enn før svarer at informasjonssikkerhet i driftskontrollsystemer er tilstrekkelig forankret i toppledelsen, betyr ikke det nødvendigvis at toppledelsen er mindre opptatt av temaet enn før, men at man nå er mer klar over hvordan det står til. Vannbransjen, blant annet gjennom Norsk Vann, vil fortsette å arbeide for å styrke oppmerksomheten hos vann- og avløpsetatene om utfordringene, og øke kompetansen på området ved å formidle veiledninger og verktøy som allerede er utarbeidet. Det vil også jobbes aktivt for å styrke de ressursene som kan støtte de enkelte vann- og avløpsavdelingene, spesielt å få forståelse hos IKT-avdelingene i kommunene for de særlige behovene innen vann og avløp.

COVID-19-pandemien har gjort sårbarhetene i sektoren enda tydeligere: vannverk har åpnet sine systemer for eksterne forbindelser til ansatte og leverandører som jobber hjemmefra for å opprettholde virksomheten. Prisen er økt risiko for nettangrep. Selv om mange vannverk har investert store ressurser i cybersikkerhet, er det fortsatt behov for mer for å sikre vanninfrastruktur på strategisk, taktisk og operativt beslutningsnivå. Cybersikkerhet må ses på som en kontinuerlig forbedringsprosess: Angriperne hviler ikke på sine laurbær, det kan heller ikke VA-sektoren gjøre.

Målet med det EU-finansierte STOP-IT-prosjektet (***S**trategic, **T**actical, **O**perational **P**rotection of water **I**nfrastructure against cyber-physical **T**hreats*) som koordineres av SINTEF er å gjøre kritisk infrastruktur i VA-sektoren sikker og motstandsdyktig ('resilient'). Dette gjøres ved å forbedre beredskap, bevissthet og responsevne mot trusler av fysisk eller digital art, og kombinasjoner av disse. STOP-IT-prosjektet avsluttes i 2021. I løpet av fire år har STOP-IT-konsortiet samarbeidet i forskjellige retninger: økning av bevisstheten om cybersikkerhet i VA-sektoren gjennom organisering av dedikerte tematiske

praksisfellesskap, utvikling av risikovurderingsverktøy og utvikling av teknologiske løsninger. Prosjektet har utviklet løsninger som gir vannverk mulighet til systematisk å beskytte sine systemer mot cyber-fysisk angrep ved hjelp av integrerte løsninger som også forbedrer evnen til å takle nye risikoer. STOP-IT har også bidratt til å bygge kompetanse i bransjen gjennom ulike opplæringsaktiviteter.

En annen suksesshistorie er "STOP-IT_N" finansiert av Norges forskningsråd med sikte på å maksimere STOP-IT-effekten i Norge og fremme ytterligere opplæringsaktiviteter for norske studenter og interessenter f.eks. bidrag i 'Ledelse av krise- og beredskapsarbeid i vannbransjen' kurs (Høgskolen i Innlandet), aktiv kommunikasjon med Norske kommuner, og bidrag til et Norsk Vann cyber-sikkerhet seminar i Oktober 2021.

Vannforsyning er en kritisk samfunnsfunksjon

I desember 2020 presenterte EU den nye strategien for cybersikkerhet [3]. Strategien har som mål å styrke Europas motstandsdyktighet mot cyberangrep og vil være en nøkkelkomponent i å forme Europas digitale fremtid, EUs plan for gjenoppbygging av Europa etter Covid-19 og EUs sikkerhetsunion-strategi. Videre la EU fram to forslag for å adressere cyber og fysisk motstandsdyktighet for kritiske virksomheter: et direktiv om cybersikkerhet i hele EU (revidert NIS-direktiv eller 'NIS 2'), og et nytt direktiv på motstandskraften til kritiske enheter [4].

Det foreslåtte direktivet om kritisk motstandsdyktighet (CER) utvider omfanget av direktivet om europeisk kritisk infrastruktur (ECI) som ble vedtatt i 2008, og som bare gjaldt energi- og transportsektoren. Ti sektorer er nå dekket: energi, transport, bankvirksomhet, finansiell infrastruktur, helse, drikkevann, avløpsvann, digital infrastruktur, offentlig forvaltning og romfart. CER synliggjør viktigheten av VA-sektoren som en viktig komponent for samfunnssikkerhet.

Nøkkelaspektet ved CER-direktivet er at medlemsstatene vil være forpliktet til å ha en strategi for å sikre motstandsdyktigheten til kritiske virksomheter, gjennomføre en nasjonal risikovurdering og på dette grunnlag identifisere kritiske virksomheter (art. 10). Videre vil kritiske virksomheter være pålagt å foreta sine egne risikovurderinger, gjøre nødvendige tekniske og organisatoriske tiltak for å øke motstandsdyktigheten og rapportere uønskede hendelser til nasjonale myndigheter (art. 11).

En vellykket innføring av direktivene krever veiledning i bruk hensiktsmessige verktøy og teknikker for å implementere de nødvendige prosessene. Det anbefales å dele kunnskap og erfaring og bygge videre på resultatene fra prosjekter som STOP-IT, for å bygge bro over gapet i cybersikkerhet og for å styrke motstandsdyktigheten i nasjonal og europeisk kritisk infrastruktur.

Utfordringer i cybersikkerheten i VA-sektoren

Forvaltning av urbane vannsystemer utfordres av flere faktorer: Aldrende infrastruktur, store vanntap, og økende press på vannressursene med hensyn til både kvantitet og kvalitet. Disse faktorene vil forverres med tiden på grunn av det globale presset, som demografisk vekst, økt etterspørsel etter vann, byutvikling og urbanisering og klimapåvirkninger. I tillegg kommer økt fokus på kvalitet, sikkerhet og miljø. Disse endringsdriverne presser frem et paradigmeskifte for den tradisjonelle forvaltningen av VA-sektoren som i dag fremstår som konservativ, kompleks og fragmentert av natur.

VA-sektorens natur har ført til en langsommere prosess med digitalisering sammenlignet med andre kritiske infrastruktursektorer. En rekke sikkerhetsutfordringer som begrenser moderniseringen av VA-sektoren presenteres her.

Begrenset integrasjon mellom fysisk og digital sikkerhet

Infrastrukturen i VA-sektoren består av sammenkoblede fysiske og digitale enheter, men likevel forblir fysisk og digital sikkerhet fragmentert. Prosessen med digital transformasjon øker

samspillet og forbindelsen mellom de to lagene (fysisk og digital/cyber), og dermed utvikles vannsystemene til cyber-fysiske systemer der fysiske enheter og tilhørende prosesser er integrert med digitale kontrollsystemer [5].

Sikkerhet har vært høyt prioritert i VA-sektoren i årevis, og cybertrusler medfører en stor bekymring. Det mangler fortsatt tiltak og tilnærminger som tar hensyn til kompleksiteten i sikkerhetsarbeidet, noe som fører til manglende evne til å takle kombinerte cyber-fysiske angrep. Risikoen øker dersom et cyberangrep setter tjenesten som tilbys i fare eller ut av spill, for eksempel forurenset vann, vann som ikke leveres, utslipp av forurensende stoffer osv. Det tilsier at vi må ha en integrert tilnærming for risikostyring hvor vi tar hensyn til alle typer angrep. Videre bør risikostyringen dekke scenarioer som tar hensyn til kombinerte fysiske og cybertrusler i sammenheng med kaskadeangrep ettersom det er de mest komplekse risikohendelsene man må være forberedt på.

Deling av informasjon om trusler mot cybersikkerhet

VA-sektoren mangler en felles bevissthet om cybertrusler. Dette kan skyldes at vannverk og tilknyttede IT-tjenesteleverandører ikke systematisk deler informasjon om erfaringer fra hendelser om nettangrep. Delingen kan bidra til å vurdere tilstanden til cybersikkerhet i VA-sektoren, øke beredskapen og muligheten til å beskytte tjenesten. Å være klar over sikkerhetshendelser som har skjedd er veldig viktig for å forstå og forberede seg på situasjoner som kan oppstå.

Deling av informasjon om trusler mot cybersikkerhet og utvikling av prosedyrer for å utveksle god praksis mellom operatører (ikke begrenset til VA-sektoren, men også på tvers av kritiske virksomheter) anses som viktig for raskere reaksjonsevne i tilfelle cybersikkerhetshendelser.

Modenhet av digitale løsninger og cybersikkerhet

Å utvikle riktige strategier for forebygging og respons krever ikke bare implementering av tekniske sikkerhetstiltak, men også etablering av en cybersikkerhetskultur gjennom kompetansebygging, bevisstgjøring og kommunikasjon. Det er for tiden et gap i digital kunnskap generelt, og spesielt i cybersikkerhet i VA-sektoren. Kunnskapshullene er både potensielle kilder til risiko og barrierer for prosessen med digitalisering. De er risikokilder ettersom omtrent 90% av angrepene ser ut til å være forårsaket av menneskelige feil [6]. Begrenset kompetanse kan også medvirke til en nedkjølingseffekt, hvor bekymringer om sikkerhet er demotiverende for økt digitalisering av sektoren. Derfor er det viktig å øke bevisstheten om cybersikkerhet gjennom utdannelse, opplæring og god praksis i VA-sektoren.

STOP-IT løsninger

I det følgende presenterer vi en oversikt over løsninger og anbefalinger fra STOP-IT-prosjektet for å sikre VA-sektorens kritiske komponenter.

STOP-IT plattformen

STOP-IT-plattformen består av ulike "byggesteiner" som kan brukes frittstående eller i kombinasjon med hverandre. Plattformen gir brukerne mulighet til å velge teknologier som er relevante for de spesifikke utfordringene de møter daglig, samtidig som de har mulighet til å utvide med flere "byggesteiner" på et senere tidspunkt. Dette legger til rette for å intensivere beskyttelse mot kombinerte cyber-fysiske trusler og analyse av kaskadeeffekter av fysiske hendelser og cyberhendelser. Plattformen ble testet og bekreftet i et operativt miljø, og alle løsninger demonstreres i reelle miljøer. Dermed har alle løsningene nådd minst TRL (teknologimodenhetsnivå) 7. STOP-IT-plattformen er strukturert i ni moduler som samler teknologiske løsninger og analyseverktøy:

- Strategiske og taktiske verktøy er analyseverktøy utviklet for å støtte ledere og beslutningstakere i arbeidet med å øke beredskapen mot effekten av cyber-fysiske trusler på tjenesten som skal leveres. De genererer tilpassede scenarioer for angrep, vurderer risiko når det gjelder tjeneste-

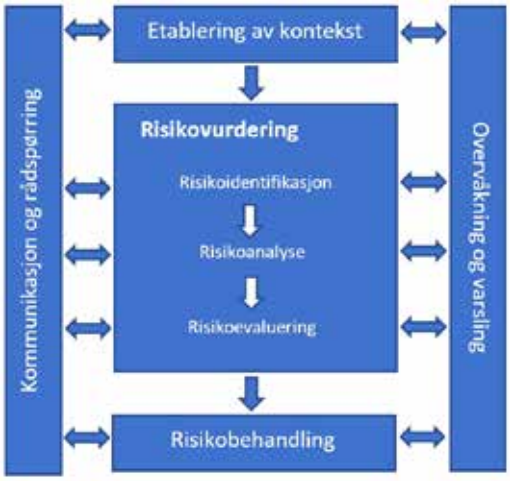
forstyrrelser og beregner effektiviteten av risikoreduserende tiltak for å øke systemets motstandskraft.
- Operasjonelle verktøy støtter sanntidsdrift av det integrerte systemet ved å tilby en omfattende liste over teknologier for å oppdage uregelmessigheter av forskjellig art, for eksempel jamming, IT-angrep, fysisk inntrenging, unormal aktivitet, tap av datatilgjengelighet og integritet.

STOP-IT risikostyringsprosess som integrert tilnærming

Den overordnede risikostyringsmetoden som er tatt i bruk av STOP-IT (Figur 1) er inspirert av risikostyringsprosedyren fra NS ISO 31000: 2018 "Risikostyring – Retningslinjer" som består av fem trinn: "Etablering av kontekst", "Risikoidentifikasjon", "Risikoanalyse", "Risikoevaluering" og "Risikobehandling". Kompatibilitet med standarden er nøkkelen for at STOP-IT-rammeverket skal samhandle med eksisterende prosedyrer i VA-sektoren.

"Etablering av kontekst" er en forutsetning for en risikostyringsplan. Den definerer omfanget av risikostyringsprosessen, hovedmålene for verktøyet og setter kriteriene som risikoen skal vurderes etter.

"Risikoidentifikasjon" genererer en omfattende liste over potensielle risikobegivenheter



Figur 1 Overordnet rammeverk for risikostyring i STOP-IT

som kan påvirke et vannforsyningssystem. I STOP-IT har vi en database, RIDB (Risk Identification Database) som dekker typiske risikoer på strategisk, taktisk og operativt plannivå.

STOP-IT RIDB [7] inneholder risikohendelser som gjelder fysiske trusler og cybertrusler. For hver hendelse beskriver RIDB typen risikokilde (f.eks. ekstern angriper, ekstern leverandør, menneskelig feil, gjensidig avhengig kritisk infrastruktur, intern angriper); typen trussel (fysisk og/eller digital) type hendelse (ødeleggelse, avbrudd, manipulering); det spesifikke elementet (fysisk eller digitalt) hvor risikokilden oppstår (f.eks. kontrollsenter, kontrollsystem, doseringssystem); i hvilken del av infrastrukturen risikoen oppstår (f.eks. nedslagsfelt, ledningsnett, drikkevannsbasseng, pumpestasjon); hvilket tap hendelsen medfører (økonomisk, kvalitet, kvantitet, omdømme) og en kort beskrivelse av hendelsen. Hensikten med RIDB er ikke å erstatte den omfattende identifiseringen av risikohendelser for hvert vannverk. I stedet kan eksemplene fra RIDB la brukerne starte en prosess og bli oppmerksomme på noen muligheter som bør undersøkes når lokale forhold som indikerer at en hendelse kan oppstå utvikler seg. Under utviklingen av RIDB ble det avholdt flere møter i hvert vannverk som var involvert i prosjektet. RIDB dekker i dag 81 hendelser som er identifisert som de mest relevante. RIDB skal være en levende database som skal oppdateres og gjennomgås regelmessig.

I RIDB registreres generiske risikohendelser som kan gjelde hele bransjen, så RIDB inneholder ikke sensitiv informasjon. Når risikohendelsene er valgt fra RIDB, kan karakteriseringsprosessen som inkluderer spesifikk og sensitiv informasjon om et gitt vannforsyningssystem starte. Da spesifiseres og detaljeres et potensielt angrepsscenario. "Risikoanalyse og evaluering" og "Risikobehandling" på strategisk og taktisk nivå utføres innenfor et rammeverk for risikovurdering og behandling, Dette rammeverket inneholder:
- En scenarioplanlegger [8] som er designet for å hjelpe brukeren med å velge truslene som skal undersøkes. Den er basert på RIDB

og en oversikt over generiske STOP-IT feiltre. Det gjør det mulig for brukere å bygge scenarioer for interessante angrep som skal undersøkes nærmere og simuleres i stresstestingsplattformen (se under).
- En avansert verktøykasse [8] for analyse og evaluering av risikoer for vannforsyningssystemet. Her simuleres vanndistribusjonssystemet som en cyber-fysisk integrert modell, og virkningen av potensielle hendelser som følge av truslene illustreres. Både vannmengde og vannkvalitetseffekter simuleres.
- En database for risikoreduserende tiltak (RRMD) [9] som har avanserte valgmuligheter som støtte for å lette identifisering og valg av passende risikoreduserende tiltak (RRM). RRMD er koblet til RIDB. Den er implementert for å hjelpe til med valg og vurdering av effektiviteten av RRMer for å øke systemets ytelse under et gitt angrepsscenario.
- En stresstestingsplattform [10-11] som kan simulere både fysiske systemer og cybersystemer (f.eks. fra SCADA til PLS og overvåking). Det er mulig å implementere nettbeskyttelsesløsninger og se hvordan de reagerer på cyberangrep. Plattformen gjør det mulig å analysere for eksempel effekten av å introdusere skadelig programvare til overvåkningssystemet og spore disse effektene til nøkkelindikatorer.

Løsningene som tilbys av STOP-IT på strategisk og taktisk nivå tar sikte på å støtte planleggingsbeslutninger og evalueringer og å øke beredskap gjennom vurdering av systemets ytelser under et (eller flere) potensielle angrepsscenarier. Vurderingen av flere scenarioer hjelper til med å identifisere de kritiske delene og deres betydning for en tjeneste som ikke fungerer.

STOP-IT har også utviklet en organisatorisk stresstestingsplattform som et supplement til den tekniske som beskrevet ovenfor. Gjennom et rollespill stresstestes [10] organisasjonens motstandskraft og evne til å reagere i krisesituasjoner i tilfelle cyber/fysiske angrep. Det gjør det også mulig å dokumentere tilgjengelige prosesser og løsninger for å håndtere stressfaktorer og forbedre disse ved å identifisere hullene og mulige løsninger.

"Risikoidentifikasjon", "Risikoanalyse og evaluering" og "Risikobehandling" på operativt nivå støttes av en analytisk plattform for sanntidsregistrering, analyse og visualisering av cyber- og fysiske sikkerhetshendelser som påvirker vanninfrastrukturen. I tillegg til de strategiske og taktiske verktøyene, er prosjektets innovative bidrag evnen til å kombinere cyber og fysiske sikkerhetshendelser i tillegg til evnen til å oppdage komplekse angrepsscenarioer i sanntid.

Delingsvilje

For å støtte behovet for informasjonsutveksling mellom vannverk og andre kritiske infrastrukturer, har STOP-IT designet og implementert et system for deling av informasjon om nettangrep [12] som samler inn kilder til eksisterende trusler fra relevante kilder, og strukturerer informasjonen ved hjelp av standarder for å lette utveksling av identifiserte sikkerhetstrusler (f. eks. MITRE ATT & CK, STIX og TAXII). Personlige varsler og relevant informasjon kan gis i henhold til abonnementsparametrene som gis av en gitt kritisk infrastruktur. Denne tjenesten hjelper operatører som er berørt av cyberhendelsene med å øke beredskapsnivået ved å kommunisere hendelsesvarsler. Den forbedrer også koordineringen mellom sektorer ved å etablere utvekslingsmetoder for å forhindre, redusere effekten av, og gjenopprette etter hendelser.

Opplæring og bevisstgjøring

Innføringen av nye digitale systemer og enheter for drift av vannforsyningssystemer krever ny type kompetanse. Vannverkene bør investere i sikkerhetsutdanning og opplæring, samt i informasjonssikkerhetskampanjer. STOP-IT-prosjektet har bidratt til opplæring og bevisstgjøring basert på ulike opplæringsaktiviteter og formidling gjennom etablering av praksisfellesskap (CoP).

Opplæring

STOP-IT-prosjektet tar sikte på å forbedre den praktiske kunnskapen om cyber-fysisk beskyttelse av vann- og avløpsinfrastruktur gjennom avanserte, interaktive og modulære opplæringsaktiviteter.

STOP-IT har laget opplæringsmateriell tilpasset tre forskjellige sluttbrukerprofiler som har hver sin rolle i risikostyring for vannforsyninger [13]. Brukergruppene er:

Profil 1: Beslutningstakere

Profilen består av beslutningstakere på høyt nivå, styremedlemmer og ledere av vannverket, og relevante toppledere fra private entreprenører. Bakgrunn og ekspertise til brukerne i denne profilen kan variere betydelig, og tid er ofte en begrensende faktor. Opplæringsmaterialet fokuserer på å gi en generell oversikt over den cyber-fysiske sikkerhetsutfordringen. Bevissthet på dette nivået skaper en kompetansehevende innsats fra toppen som tar sikte på å forbedre vannverkenes generelle beredskap mot cyber-fysiske trusler.

Profil 2: Risikostyringsledere

Den andre profilen består av nøkkelpersonell for vannverkets risikostyringsprosesser. Et dedikert sett med kursmateriell er designet for denne gruppen for å illustrere hvordan STOP-IT forbedrer risikostyring i et verktøy. Opplæringsmaterialet gir praktisk trening på løsningene utviklet på strategisk og taktisk nivå.

Profil 3: Ansatte som er ansvarlige for sanntidsoperasjoner

Den tredje profilen er personell med ansvar for f. eks. SCADA, vedlikeholdsteam og støttefunksjoner. Ettersom disse personene er ansvarlige for driften av anlegget, er målet å trene på installasjon og drift av teknologier rettet mot operativ risikostyring.

Bevisstgjøring gjennom praksisfellesskap

Praksisfelleskap (Communities of Practice - CoPs) ble etablert med et mål for å øke bevisstheten om cybersikkerhet i sektoren, og for å bidra til utviklingen av verktøyene med et flerinteressent-perspektiv.

STOP-IT CoPs [14] tar sikte på å tilrettelegge og organisere muligheter for kommunikasjon og læring hovedsakelig mellom vannspesialister, men også med nasjonale vannforeninger, beslutningstakere og andre interesserte parter, samt med eksperter fra andre forskningsmiljøer, internasjonale nettverk og initiativer som er relevante for prosjektet. CoPs samler relevante aktører og eksperter for å adressere gitte sikkerhetsproblemer og for å utvikle en felles forståelse av fordelene og ulempene ved ulike muligheter for å takle forskjellige typer trusler. Hovedmålene med STOP-IT CoPs [14] er å:

- fremme en interdisiplinær tilnærming til beskyttelse av vannsystemet ved å stimulere og legge til rette for nettverk og samlæring i henhold til definerte nivåer av kommunikasjonssikkerhet
- koble vannfagfolk med spesifikk kompetanse, interesser, ansvar og/eller problemer for å samhandle med mål om å dele og produsere kunnskap om hvordan man håndterer forskjellige typer trusler mot vanninfrastruktur
- etablere en organisert struktur for kommunikasjon åpen for gjensidig læring
- støtte utviklingen av en bred og varig læringsallianse for god praksis innen beskyttelse av vanninfrastruktur.

STOP-IT håndterer cyber og fysiske trusler mot drikkevannsinfrastruktur. Informasjon om forsyningssystemer og sårbarheter må utveksles mellom flere aktører. Ettersom informasjon og utviklede strategier må beskyttes mot misbruk av uvedkommende, er det opprettet 3 nivå av praksisfellesskap for å håndtere ulike nivåer av konfidensialitet: lokal, prosjekt- og inter-prosjekt CoP:

- Lokalt CoP: opprettet på vannverksnivå for å sikre behandling av tekniske aspekter i et konfidensielt miljø. De involverer utvalgte aktører for hvert vannverk (vannforsyningsoperatører og tilknyttede tekniske leverandører og / eller konsulenter)

- Prosjekt CoP: designet for å etablere et nettverk av forskjellige grupper av interessenter i prosjektet.
- Inter-prosjekt CoP: på tvers av ulike kritiske infrastruktursektorer, involverer internasjonale nettverk og ekspertgrupper og åpent for et bredere publikum.

Opprettelsen av praksisfellesskap i STOP-IT viste seg å være et verdifullt bidrag til prosjektet. I tillegg til den direkte støtten til flere prosjektaktiviteter, muliggjorde CoP-arrangementene også generell bevisstgjøring, kunnskapsutveksling og nettverksbygging mellom viktige interessenter. Spesielt de sistnevnte aspektene har blitt anerkjent som verdifulle av vannverkene som har vært involvert.

Konklusjon

I den kritiske infrastrukturen som VA-sektoren representerer, er digitale og fysiske elementer mer og mer sammenkoblet takket være den pågående prosessen med digital transformasjon. Den økende integrasjonen gir fordeler, men også nye utfordringer, spesielt fra et sikkerhetsperspektiv. For å øke motstandsdyktigheten til vannforsyningstjenesten, er det viktig å bryte siloene som skiller cyber og fysisk sikkerhet, og å innføre et risikostyringsrammeverk som er i stand til å identifisere, analysere og evaluere cyber og fysisk risiko, i kombinasjon og med kaskadeeffekter.

Samtidig må vannverkene overholde nye direktiver om sikkerhet for å utføre risikovurdering og gjøre nødvendige tekniske og organisatoriske tiltak for å øke motstandsdyktigheten.

Å oppnå cybersikkerhet er et bevegelig mål, og forutsetter en kontinuerlig prosess. Dette er en direkte konsekvens av den teknologiske utviklingen og økt hyppighet av stadig mer avanserte cyberangrep. Oppgaven er enda mer utfordrende hvis det eksisterer barrierer som mangel på bevissthet og kompetansegap.

For å nærme seg målet må vannverkene øke sine investeringer i cybersikkerhet og skjæringspunktet med fysisk sikkerhet. Til tross for den økende oppmerksomheten er sektoren fortsatt sårbar for sikkerhetstrusler.

Takk til

STOP-IT har mottatt støtte fra EUs forsknings- og innovasjonsprogram Horizon 2020, prosjektnr. 740610, og STOP-IT_N har mottatt støtte fra NFRs forsterkningsmidler til norske deltakere i Horisont 2020-prosjekter (FORSTERK), prosjektnr. 309334.

Referanser

[1] Sarni, W., C. White, R. Webb, K. Cross, og R. Glotzbach (2019). *Digital Water: Industry Leaders Chart the Transformation Journey.* International Water Association (IWA).

[2] Jaatun, M.G. og J. Røstum (2020) Hvordan er IT-sikkerheten hos norske vannverk? Vannspeilet 4-2020 https://issuu.com/norsk_vann/docs/vannspeilet_4-2020/38

[3] European Council (2020). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE*

Figur 2 Oversikt over tre-nivå CoP-tilnærming (lokalt, prosjekt og inter-prosjekt) innenfor STOP-IT-prosjektet med hensyn til konfidensialitetsnivå [12]

COUNCIL - The EU's Cybersecurity Strategy for the Digital Decade. Council of the European Union. Brussels.

[4] European Council (2020). *Revised Directive on Security of Network and Information Systems (NIS2)*. Council of the European Union. Brussels.

[5] Lee, E. A. (2015). *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models*. Sensors 15(3): 4837-4869. https://doi.org/10.3390/s150304837.

[6] Sanger, D. E. (2016). *Utilities Cautioned About Potential for a Cyberattack*. New York Times. URL: https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyber-attack-after-ukraines.html.

[7] Ostfeld, A., E. Salomons, P. Smeets, C. Makropoulos, E. Bonet, J. Meseguer, H. J. Mälzer, F. Vollmer, og R. Ugarelli (2018). *Risk Identification Database (RIDB)*. STOP-IT Leveranse D3.2. https://doi.org/10.5281/zenodo.3929741.

[8] Makropoulos, C., G. Moraitis, D. Nikolopoulos, G. Karavokiros, A. Lykou, I. Tsoukalas, M. Morley, M.C. Gama, E. Okstad, og J. Vatn. (2019). *Risk Analysis and Evaluation Toolkit*. STOP-IT Leveranse D4.2.

[9] Mälzer, H.J., F. Vollmer, og A. Corchero (2019). *Risk Reduction Measures Database (RRMD) supporting document*. STOP-IT Leveranse D4.3. https://doi.org/10.5281/zenodo.3947951.

[10] Ahmadi, M., R. Ugarelli, T. O. Grøtan, G. Raspati, I. Selseth, C. Makropoulos, D. Nikolopoulos, G. Moraitis, G. Karavokiros, D. Bouziotas, A. Lykou, og I. Tsoukalas (2019). *Cyber – Physical Threats Stress – Testing Platform*. STOP-IT Leveranse D4.4.

[11] Nikolopoulos, D., G. Moraitis, D. Bouziotas, A. Lykou, G. Karavokiros, og C. Makropoulos (2020). *Cyber-physical stress-testing platform for water distribution networks*. Journal of Environmental Engineering 146(7): 04020061. doi:10.1061/(ASCE)EE.1943-7870.0001722.

[12] Expósito, S. og D. Delgado (2019). *Cyber Threat Incident Service*. STOP-IT Leveranse D5.6.

[13] Ahmadi, M., C. Makropoulos, A. Lykou, og L. Zimmermann (2018). *Course design for multiple end-users*. STOP-IT Leveranse D8.1.

[14] Hein, A., J. Koti, J. Frijns, S. Urioc, og S. Damman (2017). *Guidelines for CoP setup and animation*. STOP-IT Leveranse D2.1