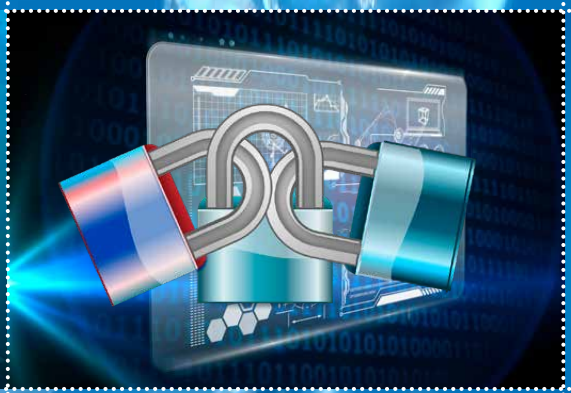
Norsk Vann

Rapport

238 | 2018

Informasjonssikkerhet og skybaserte tjenester for vannbransjen



Norsk Vann

Norsk Vann Rapport

Det utgis tre typer rapporter:

Rapportserie A
Dette er de opprinnelige hovedrapportene.
Dette kan være:

- Rapportering av prosjekter som er gjennomført innenfor organisasjonens eget prosjektsystem
- Rapportering av spleiselagsprosjekter hvor to eller flere andelseiere i Norsk Vann BA samarbeider for å løse felles utfordringer
- Rapportering av prosjekter som er gjennomført av andelseiere eller andre.
  Rapporten vil i slike tilfeller kunne være en ren kopi av originalrapporten
  eller noe bearbeidet

Fortløpende nummer xx-årstall

Rapportserie B
Dette er en serie for «enklere» rapporter, for eksempel forprosjekter, som vil være grunnlag
for videre prosjektvirksomhet mm.

Fortløpende nummer Bxx-årstall

Rapportserie C
Dette er rapporter delfinansiert av Norsk Vann, men som er utgitt av andre.

Fortløpende nummer Cxx-årstall

Norsk Vann

Norsk Vann BA, Vangsvegen 143, 2321 Hamar
Tlf: 62 55 30 30 E-post: post@norskvann.no
www.norskvann.no

Norsk Vann Rapport

Ekstrakt
Digitaliseringen av vannbransjen har ledet til mer effektivitet, men samtidig har digitaliseringen introdusert nye digitale trusler som må håndteres. For VA-virksomheter er beskyttelsen av selve infrastrukturen viktig, men i økende grad også informasjonen om abonnentene og deres personlige data. Rapporten gir en oversikt over nasjonale føringer og eksempler på digitale trusler som er relevante for vannbransjen. Som rammeverk for å analysere informasjonssikkerheten tar rapporten utgangspunkt i et rammeverk utviklet av NSM. Dette inkluderer også et system for verdivurdering av vann- og avløpsinformasjonen. Bruk av skytjenester har stort fokus i Norge og rapporten inneholder en egen sjekkliste som kan brukes av vann- og avløpsvirksomheter som ønsker å bruke skytjenester i forbindelse med drift av sin infrastruktur.

Norsk Vann BA
Adresse: Vangsvegen 143, 2321 Hamar
Telefon: 62 55 30 30
E-post: post@norskvann.no
Internettadresse: norskvann.no

Rapportens tittel
Informasjonssikkerhet og skybaserte tjenester for vannbransjen.

Forfattere
Jon Røstum, Powel
Martin Gilje Jaatun, SINTEF Digital

Rapportnummer: 238/2018

ISBN 978-82-414-0419-1 (trykt utgave)
ISBN 978-82-414-0420-1 (elektronisk utg.)
ISSN 1504-9884 (trykt utgave)
ISSN 1890-9248 (elektronisk utg.)

Emneord, norsk
Skytjenester, informasjonssikkerhet, digitale trusler

Emneord, engelsk
Cloud services, cyber security, digital threats

Forord

Rapporten *Informasjonssikkerhet og skybaserte tjenester for vannbransjen* er en av flere rapporter som Norsk Vann har utarbeidet knyttet til informasjonssikkerhet. Andre rapporter som omhandler tilsvarende problemstillinger er:

- Norsk Vann rapport 229/2018 Veileder for sikring av vannforsyningen mot tilsiktede uønskede hendelser
- Norsk Vann publiserte i 2016 en egen hjemmeside[1)] knyttet til ROS og beredskap, og dette arbeidet inkluderte også hvordan informasjonssikkerhet kan inngå som en del av ROS-analysene
- Norsk Vann rapport 213/2015 Sikkerhetsstyring for Vannbransjen
- Norsk Vann rapport 195/2013 Sikkerhet og sårbarhet i driftskontrollsystemer for VA- anlegg

Jon Røstum i Powel har sammen med Martin Gilje Jaatun i Sintef vært forfattere av rapporten. De har basert sitt arbeid på innspill fra en styringsgruppe som har bestått av følgende personer:

- Broratle Sveen, NRV/NRA IKS
- Geir Krogrud, Hias IKS
- Ali Mekki, Bergen kommune
- Harald Rishovd, Oslo kommune, Vann- og avløpsetaten
- John Larsen/Ørjan Sætre, Trondheim kommune

Styringsgruppen har bidratt aktivt og har levert viktig grunnlagsmateriale til malen for verdivurdering av data og til sjekkliste for planlegging av oppgradering av driftskontrollsystem for VA.

«Styringsgruppen har bidratt aktivt og har levert viktig grunnlagsmateriale til malen for verdivurdering av data og til sjekkliste for planlegging av oppgradering av drifts-kontrollsystem for VA.»

Følgende har gitt innspill på en workshop og gjennom høring av rapporten:

- Kjetil Tveitan, Helse- og omsorgsdepartementet
- Line Ruden, Mattilsynet
- Steven Wang Hole, Ullensaker kommune
- Svein Erik Larsen, Ringsaker kommune
- Tor Håkonsen, Norconsult
- Terje Aarhus, Nasjonal sikkerhetsmyndighet (NSM)

Elin Riise har vært Norsk Vanns prosjektleder i samarbeid med Kjetil Furuberg og Terje Berg.

Norsk Vann vil takke alle som har bidratt til rapporten for konstruktive innspill og for et godt samarbeid.

Hamar, 24. april 2018
Elin Riise, Norsk Vann

1) https://www.norskvann.no/index.php/kompetanse/prosjekter/beredskap

Sammendrag og leseanvisning

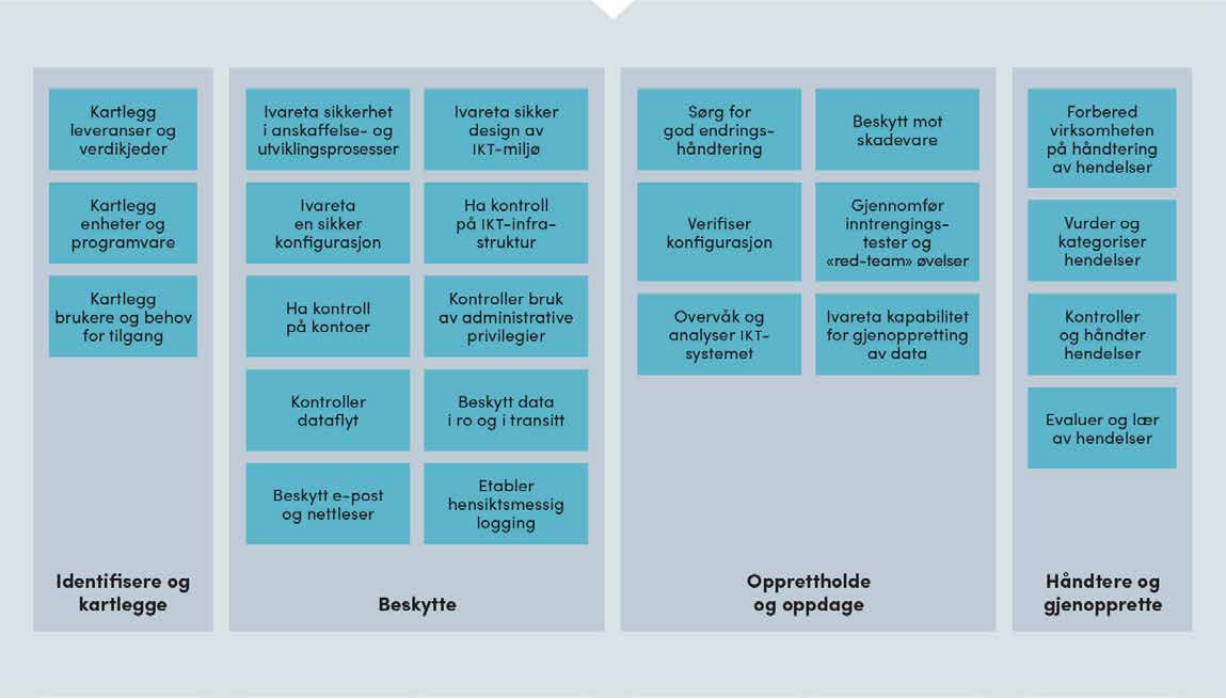
Storsamfunnet forventer at det leveres drikkevann og at avløpsvannet blir håndtert på en sikker måte selv om systemene utsettes for ulike typer trusler og påkjenninger. Dette gjelder også ved utfordringer som oppstår som en følge av digitale sårbarheter. For vann og avløpsverk er *beskyttelsen av selve infrastrukturen viktig,* men i økende grad også informasjonen om kundene og *deres personlige data.* Digitaliseringen av vannbransjen har ledet til mer effektivitet i form av lavere kostnader, raskere responstid, bedre styring og overvåkning, muligheter for bedre kundeservice, men samtidig har digitaliseringen introdusert nye *digitale trusler* som må håndteres.

Rapporten *Informasjonssikkerhet og skybaserte tjenester* for vannbransjen inngår i Norsk Vann sin rapportserie og er i utgangspunktet ment for ansatte i vannbransjen, men kan med fordel deles også med andre etater i kommunen. Dette gjelder særlig IKT-avdelingen i kommunen som ofte er den som beslutter hvilke systemer som skal anskaffes, vedtar sikkerhetsnivåer og til dels har ansvar for drift av systemene. Rapporten bør også leses av andre aktører i verdikjeden til VA-virksomhetene, dvs. leverandører og rådgivere som også leverer tjenester inn mot sektoren.

Hvordan skal rapporten leses?
Rapporten er strukturert i syv ulike kapitler i henhold til figuren under. Kapittel 1 og 2 gir leseren nødvendig bakgrunnsinformasjon til hvorfor det er behov for økt fokus på informasjonssikkerhet i vannbransjen. Kapittel 1 gir en oversikt over nasjonale føringer og initiativ og kapittel 2 gir eksempler på digitale trusler som er relevant for vannbransjen. Samlet sett er målet med kapittel 1 og 2 å motivere for økt fokus på informasjonssikkerhet.

I kapittel 3 er NSM sitt rammeverk for *Grunnprinsipper for IKT-sikkerhet*[2)] beskrevet sett ut i fra vannbransjen sitt ståsted. Rammeverket som er vist i figuren under definerer et sett med grunnprinsipper for å beskytte verdier og *leveranser i en virksomhet. Grunnprinsippene er strukturert i fire kategorier og hvert grunnprinsipp har ulike sikringstiltak som beskriver hva og hvorfor tiltak bør gjennomføres.*

2) https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/introduksjon/



NSMs grunnprinsipper for IKT sikkerhet

1) Identifisering og kartlegging er utgangspunktet for arbeidet med IKT-sikkerhet. En må vite hva en har før en eventuelt vurderer tiltak for beskyttelse. Kartleggingen inkluderer hele VA-verdikjeden fra vannkilde til resipient og inkluderer både de fysiske anleggene, men også de tilhørende informasjonsaktiva som er nærmere beskrevet i kapittel 4 - *Verdivurdering av informasjonen innen VA*. For å utføre verdivurderingen er det utarbeidet et regneark som kan lastes ned fra Norsk Vann sine sider sammen med rapporten. Det må også utføres en kartlegging av de ulike brukere og deres behov for tilgang. Dette inkluderer også eventuelle leverandørbrukere. Krav fra leverandører om å slå av brannmurer eller at brukerne av løsningene må ha superbrukerrettigheter bør ikke forekomme. Kartleggingen som utføres som en del av farekartleggingen iht. drikkevannsforskriften eller ROS-analyser er også en del av dette arbeidet. Kartleggingen må utføres tverrfaglig hvor både VA-kompetanse og IKT-kompetanse bidrar.

2) Beskyttelse av leveranser og verdier må utføres basert på arbeidet med identifisering og kartlegging. For en VA-virksomhet vil det være ulike IKT-systemer, både fagsystemer og administrative systemer som skal beskyttes. Prinsipper som sonedeling og segregering kan benyttes for å beskytte systemene. Dette inkluderer å skille SCADA-systemene fra det administrative nettet. Ivaretakelse av sikkerhet også under anskaffelser er viktig. For eksempel må en være bevisst på hva en legger ut på DOFFIN og hva som legges ut i forbindelse med plansaker. Norsk Vann rapport 195/2013 *Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg* beskriver flere grunnleggende sikkerhetstiltak som fortsatt er aktuelle. Et viktig tiltak er bruk av de siste versjonene av de ulike løsninger i stedet for å vente med oppdateringer. I nye versjoner er ofte eventuelle kjente sårbarheter fjernet.

3) Opprettholde og oppdage. Periodisk bruk av inntrengningstester har vist seg å være svært effektive, ikke minst mht. evnen til deteksjon og sporbarhet. Dette gjelder både inntrengingstester av selve IKT-infrastrukturen, men også av de enkelte løsninger. Det finnes løsninger og verktøy for å kunne overvåke og oppdage uønskede IKT-hendelser, eksempelvis Advanced Threat Analytics og Tiger Eye/Cyber Observer.

4) Håndtere og gjenopprette etter hendelser. For å kunne håndtere IKT-hendelser som måtte oppstå er det viktig at en har tenkt igjennom hva som kan skje før hendelsen oppstår. Dette inkluderer gjennomføring av beredskapsøvelser hvor det er fokus på IKT. Det bør øves både på utfall av systemer og hacker-angrep mot infrastrukturen, hvor både konfidensialitet, integritet og

tilgjengelighet (KIT) testes. Dersom det oppstår hendelser hvor en trenger bistand, bør en selvfølgelig ringe til den Nasjonale vannvakten på telefon 21078888 både for å informere, men også få informasjon om hvor en eventuelt kan få ytterligere hjelp knyttet til IKT-hendelser. VA-virksomhetene bør selv vurdere om det er behov for å etablere avtaler med eksterne parter som KraftCERT, som kan hjelpe til under hendelser. Datalogger må klargjøres så tidlig som mulig for å kartlegge hendelsesforløp og for evaluering i etterkant.

Bruk av skytjenester, er en av de mest betydningsfulle trendene innen digitaliseringen av samfunnet Dette er nærmere beskrevet i kapittel 5. Det er utarbeidet en egen sjekkliste for skytjenester som kan brukes av kommuner og VA-virksomheter som ønsker å bruke skytjenester i forbindelse med drift av vann- og avløpsinfrastrukturen. For å lykkes med arbeidet med informasjonssikkerhet må det etableres en god sikkerhetskultur/cybersikkerhetskultur. Dette er nærmere beskrevet i kapittel 6.

EUs forordning om personvern (GDPR) blir gjort til norsk rett gjennom den nye personopplysningsloven. Dette vil også få konsekvenser for virksomhetene i vannbransjen, blant annet gjennom krav til å kartlegge risiko og personvernkonsekvenser. Ivaretaking av personvernet er ikke bare viktig på grunn av trusselen om store overtredelsesgebyr. Det er også et spørsmål om omdømmet og tilliten til en næring som gjennom digitalisering står foran store muligheter og utfordringer i møtet med innbyggerne. I prosjektet er det utarbeidet et enkelt regneark som hver enkelt VA-virksomhet kan benytte for å kartlegge sin bruk av persondata. Arbeidet med personvern må integreres som en del virksomhetens arbeid med informasjonssikkerhet.

English summary

This report is published in Norwegian by Norwegian Water BA (Norsk Vann BA).

Address: Vangsvegen 143, NO-2321 Hamar, Norway
Phone: + 47 62 55 30 30
E-mail: post@norskvann.no
Website: www.norskvann.no

Report no: 238 – 2018
Report title: Cyber security and cloud services in the water sector
Date of issue: 24. April 2018

Authors: Jon Røstum and Martin Gilje Jaatun

ISBN 978-82-414-0419-1 (printed edition)
ISBN 978-82-414-0420-1 (electronic edition)
ISSN 1504-9884 (printed edition)
ISSN 1890-9248 (electronic edition)

Summary

Whilst the digitalization of the water sector has led to more efficiency, unfortunately digitalization also introduces *digital threats*. For water utilities, the security of the infrastructure and the process itself is critical, but so too is the privacy of the customer. This report identifies cyberthreats relevant for the water industry and describes a framework for cybersecurity which is based on the national framework developed National Security Agency (NSM). The framework includes a system for categorization of data.

Security in the cloud is of great interest in Norway and a cloud security checklist to be used for water utilities has been developed. The checklist should be used by water utilities when purchasing services from software developers using cloud-services.

Innhold

Forkortelser og begreper

CERT. «Computer Emergency Response Team» er en koordinerende enhet for IKT-sikkerhet. Det er flere CERT miljøer i Norge. En del norske vann- og avløpsvirksomheter er medlem av KraftCERT.

CSA. Cloud Security Alliance
- https://cloudsecurityalliance.org/

General Data Protection Regulation (GDPR). Forordning fra EU om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger (personvernforordningen). Inngår ved inkorporasjon i ny personopplysningslov.

Behandlingsansvarlig. Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Behandlingsansvarlig har ansvaret for at opplysninger behandles i tråd med personopplysningslovens krav. Kommunen eller selskapet er typisk behandlingsansvarlig.

En **behandling** av personopplysninger er enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Databehandler. Den som behandler personopplysninger på vegne av den behandlingsansvarlige. Databehandleren har et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet, for å verne personopplysningene som behandles på vegne av behandlingsansvarlige. Databehandleren skal bare behandle personopplysninger i tråd med det som er avtalt med den behandlingsansvarlige. Databehandler kan f.eks. være en IT-leverandør som leverer programvarer til VA-virksomheten. En databehandler vil ha selvstendig ansvar for personopplysninger som behandles på egne vegne, eksempelvis opplysninger om egne ansatte.

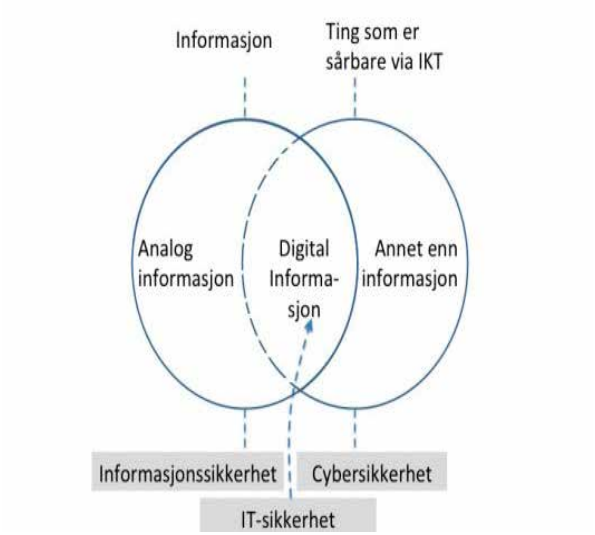
DOFFIN. Den nasjonale kunngjøringsdatabasen for offentlige anskaffelser.

Informasjonssikkerhet. Informasjonssikkerhet har med sikring av informasjon å gjøre, uavhengig av om den er lagret digitalt eller ikke.

IKT-sikkerhet. IKT- sikkerhet har med sikring av informasjons- og kommunikasjonsteknologi å gjøre – altså digital informasjon, maskinvare og programvare. Grunnen til at IKT-sikkerhet og informasjonssikkerhet ofte blir brukt om hverandre, er nok at mye informasjon er lagret og formidlet ved hjelp av IKT. For å beskytte slik informasjon, må man beskytte teknologien den er lagret og formidlet på.

IT-sikkerhet. IT-sikkerhet har med sikring av informasjonsteknologi. I praksis er det ingen forskjell på IKT-sikkerhet og IT-sikkerhet

Cybersikkerhet. Cybersecurity dreier seg om sikring av ting som er sårbare via IKT. NSM har foreslått at begrepet IKT-sikkerhet bør erstattes av cybersikkerhet i politiske og strategiske dokumenter.



Figur 1. *Forskjellen mellom informasjonssikkerhet, IT-sikkerhet og cybersikkerhet (www.ccis.no)*

IoT (Internet of Things). «Tingene internett» vil enkelt si at alt av utstyr, komponenter er koblet opp mot internett og er tilgjengelig via internett.

Malware. (fra engelsk malicious software) eller skadelig programvare er ondartet programvare. Det kan gjerne kalles «skadevare» eller «skadeprogrammer» på norsk

OWASP. Open Web Application Security Project - https://www.owasp.org

SCADA. Supervisory Control and Data Acquisition. Systemer for styring og overvåking (automasjons-, eller kontrollsystemer)

1. Innledning

I NOU 2015-13 «Digital sårbarhet – sikkert samfunn» pekes det på at virksomheter som har en kritisk samfunnsfunksjon, slik som vann og avløp, må planlegge for å opprettholde sine basisleveranser nærmest uavhengig av hvilke påkjenninger de utsettes for. Storsamfunnet forventer at det leveres drikkevann og at avløpsvannet blir håndtert på en sikker måte, selv om systemene utsettes for ulike typer trusler og påkjenninger. Dette gjelder også ved utfordringer som oppstår som følge av digitale sårbarheter. For vann- og avløpsvirksomheter er *beskyttelsen av selve infrastrukturen* viktig, men i økende grad også informasjonen om kundene og *deres personlige data.*

Digitaliseringen av vannbransjen har ledet til mer effektivitet i form av lavere kostnader, raskere responstid, bedre styring og overvåkning, muligheter for bedre kundeservice, men samtidig har digitaliseringen introdusert nye *digitale trusler.* At løsninger som utvikles i vannbransjen er smarte og brukervennlige, har liten betydning om de ikke er til å stole på. God sikkerhet er en av grunnsteinene for å lykkes med digitalisering. Kommunene må ha tillit til løsningene de bruker og innbyggerne må ha tillit til at data som kommunen samler inn om dem blir håndtert på en sikker måte.

I vannbransjen er det fokus både på vannforsyning og håndtering av restproduktet avløpsvann. Svikt i vannforsyningen vil også medføre svikt i avløpshåndteringen. Uten vann til å transportere avløpet i ledningsnettet, vil avløpsnettet raskt bli tilstoppet. Dette vil fort kunne få uakseptable konsekvenser for hygienen.

Det er mange typer hendelser som kan medføre svikt i VA-infrastrukturen, både naturlige hendelser, tekniske hendelser og villede hendelser. Digitale avhengigheter medfører en økt kompleksitet og nye muligheter for alle disse hovedtypene av hendelser. Vannbransjen benytter i dag f.eks. i økende grad IKT-systemer og fjernstyring i alle deler av sin drift. IKT har blitt en integrert del av vannforsyningssystemet, og fremstår som en egen infrastruktur i vanninfrastrukturen. Vannbransjen er i dag kritisk avhengig av stabile, sikre og funksjonelle IKT-systemer for sin systemdrift. Teknologien bak IKT-systemene er i stadig endring, og kompleksiteten i systemene øker. I tillegg foregår det en kontinuerlig teknologiutvikling som ytterligere vil forsterke kompleksiteten. Driftskontrollsystem (DKS) for styring og overvåkning av anleggene er i seg selv et av de mest sårbare punktene i et vannforsyningssystem. Bruken av DKS fra nedbørfelt via vannbehandling og distribusjonsnett, til avløpsnett og videre til avløpsrenseanlegg er nærmere beskrevet i Norsk Vann veiledning 195/2013[3]. Rapporten inneholder en sjekkliste som er basert på beste praksis. Rapporten er riktignok fra 2013, men for de fleste vann- og avløpsvirksomheter vil det fortsatt være mye nyttig kunnskap å kunne hente.

Det er slutt på den tiden hvor IKT-sikkerhet var et teknisk område som var underlagt IT-sjefen, med svak integrasjon til resten av virksomheten. Trusselbildet er stort, mangfoldig og ofte teknisk orientert, noe som understøtter dette synet. I *Global Opportunity Report*[4] pekes det på at mange virksomheter har løftet ansvaret for cyber security opp til toppledelsen. Eksempelvis har den planlagte innføringen av EUs personvernforordning (GDPR) og de tilhørende høye nivåene på overtredelsesgebyrene bevisstgjort ledelsen både i kommuner og selskaper. Viktigheten av å jobbe med informasjonssikkerhet understøttes også av Economic Forum sin rapport *Global Risks Report*[5] *for 2018* hvor cybersikkerhet og tyveri av data trekkes frem særskilt.

3) Jaatun M.G., Røstum J. og Petersen S (2013). Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer. Norsk Vann rapport 195/2013.
4) http://www.globalopportunitynetwork.org/report-2017/
5) https://www.weforum.org/reports/the-global-risks-report-2018

Skyen er på veg til å bli den nye IKT-infrastrukturen. I næringslivet er skytjenester blitt den vanlige måten å levere IT-løsninger på. Stadig flere kommuner og selskaper har allerede valgt å forvalte sine VA-data i en eller annen form for skytjeneste. Samtidig er det mye usikkerhet knyttet til bruk av skytjenester. Dette er både knyttet til sikkerhet, personvern, arkivering og risikovurdering. I denne rapporten gis det veiledning i hva kommuner og VA-virksomheter skal ta hensyn til når de vurderer skytjenester.

1.1. Generelt om informasjonssikkerhet

Når det gjelder sikring av IKT-systemer og den informasjonen som ligger i disse systemene snakker man gjerne om sikring av **K**onfidensialitet, **I**ntegritet og **T**ilgjengelighet som ofte forkortes KIT[6)]:

Konfidensialitet; det å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang. Eksempel på tap av konfidensialitet er at hackere får tilgang til hemmelig informasjon som ligger lagret i driftskontrollsystemet (DKS) eller at ledningsdata (GIS) kommer på avveie.
Integritet; det å sikre at informasjonen og metodene/beregningene er nøyaktige og fullstendige. Dette innebærer at uvedkommende ikke kan endre informasjonen eller systemet som behandler informasjonen. Eksempel på tap av integritet er at hackere logger seg på DKS til et vannbehandlingsanlegg og endrer kjemikaliedoseringen slik at det blir over- eller underdosering. Et annet alternativ er at en endrer styring av pumpestasjoner og overløp. Tap av integritet var tilfellet ved Maroochy Shire hendelsen i Australia i år 2000, hvor en tidligere innleid IT-konsulent som hadde installert DKS som styrte 300 pumpestasjoner for avløp via radiokommunikasjon misbrukte sine tilganger. Konsulenten fikk ikke jobb i vann- og avløpsvirksomheten og hevnet seg ved å manipulere pumpestasjoner og ventiler/luker slik at en million liter ubehandlet avløpsvann rant ut i nærliggende vassdrag[7)].
Tilgjengelighet; det å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov. Eksempel på tap av tilgjengelighet er at driftsoperatørene ikke klarer å logge seg på systemet og endre verdier ved behov. Tilgjengelighet kan også henspille på et vannbehandlingsanleggs evne til å levere rent vann. For eksempel kan et angrep mot en sensors integritet (dvs. feil verdier kommer inn til SCADA-systemer fra sensoren) påvirke vann- og avløpsvirksomhetens evne til å levere rent vann ut på nettet. Et annet eksempel er at ledningsregisteret ikke er tilgjengelig dersom løsningen er avhengig av kommunikasjon med en server.

I en utvidet definisjon av informasjonssikkerhet kan også følgende aspekter inkluderes:
Autentisering; det å få visshet om at en part virkelig er den han/hun utgir seg for å være. Det gjelder både bruker og maskin (jfr. falske minibankautomater). Gode rutiner for brukerautentisering og administrasjon av brukerne og deres tilganger er viktig også for vannbransjen.
Ikke-benekting; det å sikre at de som har sendt meldinger ikke kan benekte eller avvise det i etterkant.
Sporbarhet; enhver endring av informasjon skal kunne spores; hvem som utførte endringen og når dette ble utført. Sporbarhet om hvem som har åpnet eller stengt ventiler og hvorfor dette ble utført er eksempler på dette.
Personvern; sikre at enkeltindividet kan kontrollere informasjon om en selv og hva denne brukes til. Alle har et behov for å være i fred. Ny personvernlovgiving basert på GDPR vektlegger dette ytterligere (mer om dette i kapittel 7).

For drifts- og styringssystemer vil ofte integritet og tilgjengelighet være vel så viktig som konfidensialitet. Man er avhengig av at systemet er tilgjengelig og gjør de oppgavene det er satt til. Dette forutsetter også at systemet har tilgang til riktig informasjon til enhver tid. Men samtidig vil tap av konfidensialitet gjøre det lettere at integriteten og tilgjengeligheten forringes ved en senere anledning.

Tradisjonelt har det vært stort fokus på tap av konfidensialitet, men WannaCry hendelsen våren 2017 viser at tap av tilgjengelighet i form av at data blir tatt som «gissel» er en økende fare som en må være bevisst på. Løsepengevirus krypterer filene på en infisert datamaskin, og en får ikke tilgang til data før man har betalt løsepenger.

6) Definisjonene under er hentet fra NS 7799:2003 Norsk standard for informasjonssikkerhet.

7) J. Slay and M. Miller, "Lessons Learned from the Maroochy Water Breach," in Critical Infrastructure Protection. vol. 253, E. Goetz and S. Shenoi, Eds., ed: Springer Boston, 2007, pp. 73-82.

En sann vannhistorie om informasjonssikkerhet...

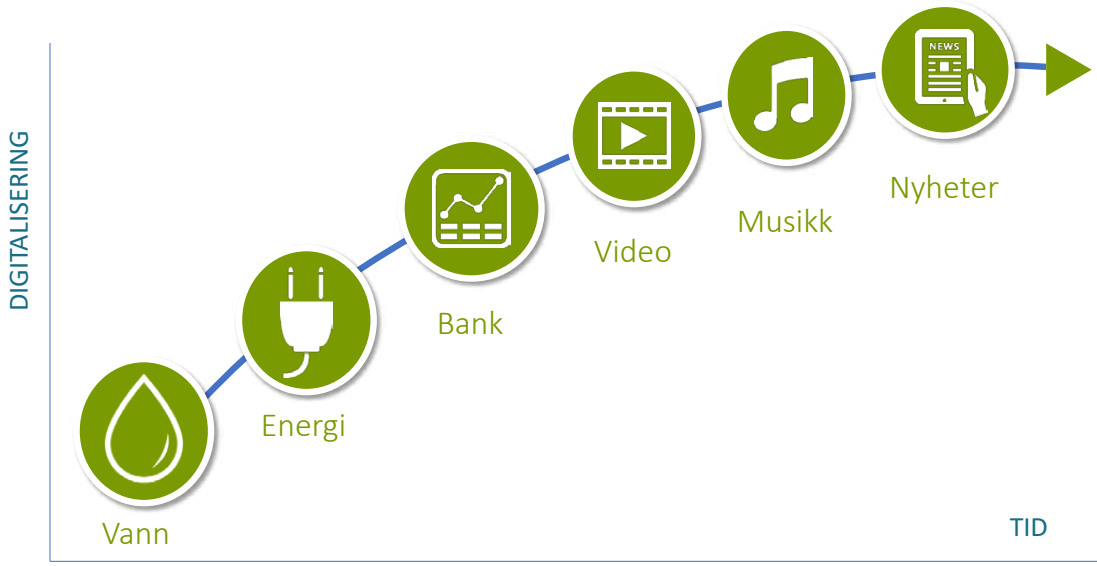
Har du hørt historien om østlendingen som ringte vestlendingen som var på vakt på vannverket?

For noen år siden ble et vannverk på Vestlandet oppringt av en person som spurte vakthavende om han kunne sjekke detaljerte prosessdata for vannverket. Spørsmålene var av typen: «*Stemmer det at vannføringen ut av vannbehandlingsanlegget er 50 l/s?*» og «*stemmer det at UV-dosen er 40 og at verdien er nedadgående?*». Vakthavende kunne bekrefte disse verdiene, hvor på innringer da sa at det var han som styrte anlegget. Innringeren, som må få betegnelsen en «snill» hacker (selv om det som han gjorde også var en ulovlig handling), kunne opplyse at han hadde kommet inn via en åpen bakdør i driftskontrollsystemet som styrte vannverket. I etterkant ble det iverksatt tiltak for å bedre sikkerheten for det aktuelle vannverket, men hendelsen viser at det her var snakk om tap av de fleste aspektene av informasjonssikkerhet; konfidensialitet, integritet og kanskje også tilgjengelighet dersom vannverket i en beredskapssituasjon ikke kunne ha vært driftet manuelt. Eksempelet viser også behovet for prioritering mellom ulike sikkerhetsbehov. I det konkrete tilfellet kan man konkludere med at tilgang til systemet for en leverandør ikke skal prioriteres på bekostning av behovet for integritet.

I denne rapporten skilles det mellom informasjonssikkerhet og IKT-sikkerhet. Informasjonssikkerhet er et bredere begrep og dekker også informasjon som ikke er på en datamaskin. Med IKT-sikkerhet mener vi informasjonssikkerhet med datamaskiner. Cybersecurity dreier seg om sikring av ting som er sårbare via IKT. NSM har foreslått at IKT-sikkerhet bør erstattes av cybersikkerhet som begrep i politiske og strategiske dokumenter.

1.2. Digitalisering av vannbransjen – muligheter

Sammenlignet med andre sektorer, er vannbransjen foreløpig lite digitalisert (figur 2). Vi er vant med streaming av musikk og videoer og at vi alltid kan ha musikken med oss via smarttelefoner. Tilsvarende er vi alltid på nett når det gjelder nyheter og i nettbanken er vi blitt stadig mer selvbetjent. Innen vannbransjen har det også foregått en digitalisering i form av innføring av driftskontrollsystemer, fjernkontrollsystemer, utvikling av digitale kartsystemer, det tas i bruk driftsstøtte løsninger og løsninger for å få bedre kommunikasjon med innbyggerne. Denne utviklingen forventes å øke i årene fremover.

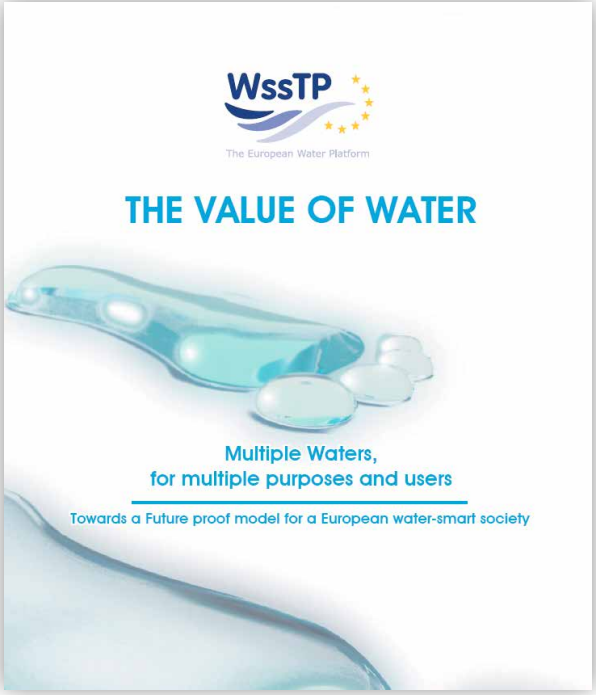


Figur 2. *Illustrasjon av digitaliseringsnivået i vannbransjen sammenlignet med andre sektorer*

Vannteknologiplattformen WssTP (Water Supply and Sanitation Technology Platform) har i sin visjon[8] for vannbransjen for år 2030; *The Value of Water: Towards a Future proof model for a European water-smart society* pekt ut digitalisering av vann (Digital Water) som et viktig element for å nå WssTP sin visjon om et samfunn hvor mennesker, sensorer og prosesser henger sammen via internett. Dette antas å generere store datamengder som kan brukes i mer avanserte analyser for å gi gode beslutninger.

Tilsvarende trend understøttes av FN sin *Global Opportunity Report 2017*[9] hvor bruk av smart vannteknologi (*Smart Water Tech)* og informasjonssikkerhet *(Intelligent Cybersecurity)* pekes ut som de viktigste muliggjørende tiltakene for å løse noen av de store utfordringene i verden. Med smart vannteknologi pekes det på bruk av smarte sensorer, kunstig intelligens, maskinlæring, smarte vannmålere, smarte rørsystemer, bruk av digitale valutaer og blockchain etc.

Bruk av metoder slik som kunstig intelligens i vannbransjen vil også kunne utfordre personvernet. Hvis bruk av kunstig intelligens innebærer en behandling av personopplysninger, utløses det både plikter og rettigheter. Den nye personopplysningsloven krever at de som behandler data vurderer personvernkonsekvensene og bygger inn personvern allerede i utviklingsfasen av et system. Datatilsynet har nylig utarbeidet en veiledning10) om kunstig intelligens og personvern. og det er viktig at denne veilederen leses når man utvikler løsninger for vannbransjen, slik at løsningene får innebygget personvern. Mer om nye regler for personvern i kapittel 7.



Figur 3. *Vannteknologiplattformen WssTP sin visjon for 2030.*

Gartner har identifisert 10 topp strategiske teknologitrender for 2018[11] (Figur 4). Av spesiell interesse for VA-bransjen vil vi trekke fram:

- **AI & personvern:** Kunstig intelligens (Artificial Intelligence - AI) gjør det mulig å behandle stadig større mengder med data (både personopplysninger og andre data), og gjør det mulig å aggregere og korrelere data i langt større grad enn tidligere, noe som medfører at informasjon slik som forbruksmønster på sikt må behandles med enda større forsiktighet enn før.
- **Intelligente ting:** Vi omgir oss med stadig større mengder små og store enheter med varierende grad av intelligens, både privat og i industrien. Der man før snakket om Internet of Things (IoT) snakker man nå om at tingene ikke bare er på internett, men de er også intelligente. VA-bransjen er intet unntak, og kommer til å bruke slike intelligente ting – men da må man ikke glemme at dagens nye teknologi fort kan bli morgendagens sårbarhet, dersom man ikke tenker cybersikkerhet fra starten.

8) http://wsstp.eu/wp-content/uploads/sites/102/2017/11/WssTP-Water-Vision_english_2edition_online.pdf

9) https://www.unglobalcompact.org/docs/publications/Global_Opportunity_Report_2017_SM.pdf

10) https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/rapport-om-ki-og-personvern.pdf

11) https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/

- **Nettsky til kanten:** De smarte tingene kommer til å ha behov for å kommunisere, og stadig flere «ting» kommer til å laste opp sine data direkte til skyen for prosessering og lagring.
- **Adaptiv risiko & tillit:** I et miljø med dynamiske intelligente ting, bruk av kunstig intelligens og nettsky er det klart at sikkerhet ikke kan være en statisk ting. Fremover må man kunne tilpasse sikkerheten til et trusselbilde i kontinuerlig endring. Sånn er det jo allerede, men endringene antas å skje enda raskere enn før og det må også risikoanalysene gjenspeile.

Figur 4. *Gartner topp 10 strategiske teknologier for 2018*

1.3. Mattilsynets tilsynsrapport og funn knyttet til IKT og digitalisering

I 2016 gjennomførte Mattilsynet en omfattende tilsynskampanje knyttet til vannverkenes beredskap[12]. Som en oppfølging også av NOU 2015: 13 og de nedslående resultatene fra Mattilsynets undersøkelse utført i 2015[13] fokuserte Mattilsynet ekstra på digitale sårbarheter. I tilknytning til undersøkelsen i 2015 ble det sendt ut et spørreskjema til omlag 500 vannverk basert på sjekklisten utarbeidet i Norsk Vann rapport 195/2013. I tilsynsrapporten for 2016[14] ble driftskontrollsystem og informasjonssikkerhet vurdert som «ikke tilfredsstillende» hos rundt 20 % av vannverkene. De største vannverkene (forsyner mer enn 100 000 personer) hadde generelt bedre resultater enn de mindre. Mange av avvikene handlet om manglende ROS-analyse knyttet til driftskontroll og IKT-systemer. Mattilsynet pekte særlig på følgende funn:

- DKS og IKT er ikke vurdert i kommunenes ROS-analyser.
- De ansatte har felles passord for pålogging til DKS og det er ingen rutiner for skifte av passord
- Vannverket har ikke redundans av DKS
- Lite fokus på IT-sikkerhet ved vannverket
- Roller og ansvar for DKS og IT-sikkerhet er ikke definert
- Ikke beskrevet rutine for opplæring i IT-sikkerhet
- Personale har ikke opplæring i IT-sikkerhet
- Det foreligger ikke prosedyrer som omhandler svikt og bortfall av DKS- og IKT-system

Når informasjonssikkerhet ikke er inkludert i ROS-analysene vil de heller ikke inngå i vannverkets beredskapsplaner og vil heller ikke være inkludert som et eget tema under beredskapsøvelser. NOU 2015: 13 pekte

12) https://www.mattilsynet.no/mat_og_vann/vann/vannforsyningssystem/rapport_norske_vannverks_beredskap_2017.26356

13) Presentasjon av Mattilsynet på TEKNA sin konferanse "Samfunnssikkerhet og vannbransjen, 21-22 april 2015.

14) https://www.mattilsynet.no/mat_og_vann/vann/vannforsyningssystem/sluttrapport_tilsyn_med_vannverkenes_beredskap_2016.26359/binary/Sluttrapport:%20Tilsyn%20med%20vannnverkenes%20beredskap%202016

Figur 5. *Veiledningsmateriell for ROS og beredskap i vannsektoren (Norsk Vann)*

også på behovet for at vannverkenes ROS-analyser må inkludere sikkerhetsvurderinger knyttet til IKT og informasjonssikkerhet, og at det var behov for å gjennomføre øvelser som inkluderer IKT-hendelser og informasjonssikkerhet.

Norsk Vann publiserte i 2016 en egen hjemmeside[15] knyttet til ROS og beredskap som også inkluderte hvordan informasjonssikkerhet kan inngå som en del av ROS-analysene. Gjennomføring av øvelser som også omfatter bortfall av IKT og DKS anbefales. Kommunene som fikk påpekt mangler knyttet til IKT og ROS bør sjekke disse sidene.

Mattilsynets tilsynsrapport viser at det fortsatt er behov for økt fokus og kunnskapsheving knyttet til informasjonssikkerhet («Vi skjønner fortsatt ikke at vi ikke skjønner!»). Dette gjelder både hos ledelsen og blant de ansatte. Et godt sikkerhetsarbeid er i utgangspunktet et ledelsesansvar, men ledelsen må ha faglig støtte på IKT-sikkerhet, og hver enkelt ansatt må øke sin bevissthet om og sitt fokus på informasjonssikkerhet. Undersøkelsen viser at bruk av felles brukernavn og passord for flere ansatte fortsatt er vanlig i noen vannverk. Dette anbefales ikke. Passord kan komme på avveie og når folk slutter vil passordet være kjent eksternt. Dersom brukeren kan utføre endringer i løsningen, kan en heller ikke i etterkant spore hvem som har utført endringen, også når det har vært en logisk grunn til å utføre endringer. Leverandører av software bør lage løsninger som knytter seg til vann- og avløpsvirksomhetenes løsninger for identitet og tilgangsadministrasjon (f.eks. Microsoft AD eller tilsvarende). Bruk av slike løsninger gjør det lettere og sikrere for kommunen å administrere brukerne med hensyn til tilgang til de enkelte løsningene, og en kan etablere gode passordrutiner. En kan enkelt fjerne tilgangen til folk som slutter, og brukerne vil kunne få en enklere pålogging ved bruk av *single sign on.* Dette gjør at hver enkelt bruker blir unik, og avvikene som Mattilsynet pekte på i sin tilsynskampanje vil kunne lukkes. Kommunene må etterspørre slike løsninger i forbindelse med innkjøp.

Funnene fra undersøkelsen knyttet til mangelfull opplæring, uklare roller/ansvar og manglende rutiner viser at det er behov for å sette arbeidet med informasjonssikkerhet i system i egen organisasjon. Hver enkelt har ansvar, men overordnet ansvar må forankres og løftes frem av ledelsen i organisasjonen. Digitaliseringen av vannbransjen stiller altså høye krav til bevissthet og kompetanse til alle involverte, både ledelsen i VA-verkene, den enkelte bruker og også myndighetene

Selv om Mattilsynet har begynt å fokusere på informasjonssikkerhet under sine tilsyn, peker NSM i sin årlige risikovurdering for 2017 på generell mangelfull IKT-sikkerhetskompetanse hos tilsynsmyndighetene. Dette kan medføre at sårbarheter ikke avdekkes under tilsyn og dermed heller ikke blir utbedret.

NSM har i flere år anbefalt fire effektive tiltak som antas å stoppe opp mot 90 % av alle kjente dataangrep. (NSM, 2017). I følge NSM ville de fleste av hendelsene mot norsk infrastruktur vært forhindret dersom disse tiltakene hadde vært implementert.

Boks 5.1 Slik stopper du 90 prosent av alle angrep[1]

1. Oppgrader program- og maskinvare.
2. Vær rask med installasjon av sikkerhetsoppdateringer, gjør det automatisk hvis mulig.
3. Ikke tildel sluttbrukere administratorrettigheter.
4. Blokker kjøring av ikke-autoriserte programmer.

[1] Nasjonal sikkerhetsmyndighet (2014): *Fire effektive tiltak mot dataangrep.*

15) https://www.norskvann.no/index.php/kompetanse/prosjekter/beredskap

1.4. Nasjonal vannvakt – begrenset fokus på digitale hendelser

Nasjonal vannvakt[16] er en døgnbemannet rådgivningstjeneste for vannverk som trenger råd og støtte ved akutte hendelser som kan påvirke vannforsyningen og medføre helsemessige konsekvenser for befolkningen. Nasjonal vannvakt tilbyr faglig støtte fra personer med erfaring fra vannverksdrift og krisehendelser. Ordningen er organisert under Folkehelseinstituttet. Rådgivningen er rettet mot å vurdere smittepotensial ved mikrobiologisk forurensning og akutt helsefare ved kjemikalieforurensning og har p.t. ikke kompetanse i nettverket knyttet til eventuelle digitale trusler.

I Meld. St 38 (2016-2017) skriver regjeringen at Helse- og omsorgsdepartementet ikke har konkrete planer om å utrede et felles responsmiljø for å håndtere hendelser knyttet til IKT som ivaretar vannbransjen. Det åpnes imidlertid for en eventuell utvidelse av Nasjonal vannvakt til også å inkludere ekspertise innenfor IKT-sikkerhet. Det er opprettet en referansegruppe for ordningen med Nasjonal vannvakt der DSB er med og «sannsynligvis vil en utvidelse til å omfatte IKT-sikkerhet kunne vurderes innen utgangen av 2017». Dette ble ikke gjennomført i løpet av 2017, men dersom det skulle oppstå kritiske hendelser som skyldes digitale sårbarheter, opplyser medlemmer av Nasjonal vannvakt at det vil være naturlig å referere til NSM for eventuelle digitale råd og støtte. Dette vurderes som en grei løsning inntil en eventuelt knytter til seg digital kompetanse i eller utenfor teamet. Så dersom det oppstår digitale hendelser innen ditt vannverk og dere trenger nasjonal hjelp, skal det ringes Nasjonal vannvakt på telefon 2107888.

16) https://www.fhi.no/ml/drikkevann/rad/beredskapsplaner/

NASJONAL VANNVAKT

Det å kunne ringe Nasjonal vannvakt ved en hendelse vil være nyttig, men vel så viktig er arbeidet som en må gjøre i forkant av eventuelle hendelser. Dette inkluderer f.eks. å opprette kontakt med et leverandørfirma med spesialkompetanse på informasjonssikkerhet som kan hjelpe til under hendelser for eksempel ved å analysere datalogger.

En del norske vann- og avløpsvirksomheter, som VAV, Bergen og NRV/NRA har meldt seg inn i KraftCERT[17], som er et myndighetsnøytralt felles responsmiljø opprinnelig tenkt for kraftbransjen, men som nå også bistår vannbransjen og olje&gass- sektoren. KraftCERT bidrar både med forebyggende arbeid og håndtering av IKT-hendelser. Med flere vann- og avløpsvirksomheter som medlemmer, sørger de også for informasjonsdeling av hendelser og trusler som er relevante for svikt i IKT ved virksomhetene. Andre vann- og avløpsvirksomheter bør også vurdere medlemskap i KraftCERT. Hva KraftCERT kan bidra med står nærmere beskrevet i Vannspeilet nr. 2 i 2017[18].

17) https://www.kraftcert.no/om.html

18) https://issuu.com/norsk_vann/docs/vannspeilet_2-2017

1.5. Fysisk sikring – digital sikring – menneskelig påvirkning

Vann og avløpssektoren kjennetegnes av en geografisk spredt infrastruktur. Særlig gjelder dette vann- og avløpsnettet, som har anlegg og utestasjoner lokalisert der behovet for anlegg er (kummer, pumpestasjoner osv.). Tilhørende IKT- infrastruktur må følgelig være tilsvarende geografisk plassert. Dette er enklere for prosessanleggene, hvor alt utstyr er samlet i en eller flere bygninger, noe som gjør fysisk sikring enklere. Fysisk sikring og digital sikring må sees i sammenheng.

I 2017 startet et nytt stort forskningsprosjekt under EUs H2020 program, som omhandler fysisk og digital sikring av vanninfrastruktur. Prosjektet, som heter STOP-IT (Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats), ledes av SINTEF. Oslo VAV og Bergen kommune er med i prosjektet[19]. Prosjektet skal vare i fire år og det vil bli

19) http://stop-it-project.eu/

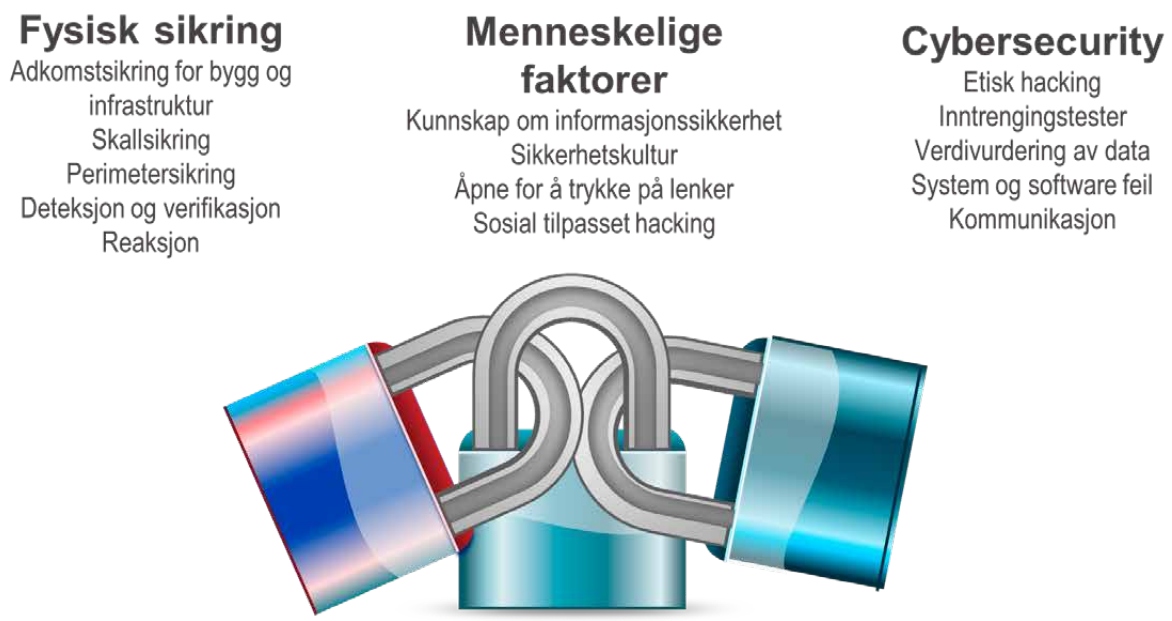
Figur 6. *EU prosjektet STOP-IT som omhandler fysisk og digital sikring av vann infrastruktur. Representanter fra Oslo, SINTEF og Bergen.*

produsert kontinuerlig relevante rapporter for norsk vannbransje, så her er det bare å følge med på leveransene fra prosjektet.

Norsk Vann har nylig utgitt rapport 229/2018 *Sikring av vannforsyning mot tilsiktede uønskede hendelser* med rådgivere fra Forsvarsbygg som forfattere. Veilederen er basert på sikringsprinsippene fra Sikringshåndboka utarbeidet av Forsvarsbygg i 2016. For vannbransjen som har en svært spredt geografisk fordeling av infrastrukturen, er det en utfordring at det kan være lett å få fysisk tilgang til IKT-infrastruktur som er plassert på andre steder enn i virksomhetens hovedbygninger. Dette gjelder for eksempel i vegskap, overløp, pumpestasjoner og målekummer. Svikt i den fysiske sikringen medfører at fremmede får fysisk tilgang til IKT-infrastrukturen. Manglende sikring av IKT-infrastruktur i disse systemene kan medføre at fremmede enkelt får tilgang.

Digitaliseringen medfører endret fokus fra *fysisk sikkerhet til cyber-sikkerhet.* Førstnevnte er fortsatt viktig, men sikkerhetsbevissthet i cyber-sammenheng er kanskje viktigere, ettersom de digitale truslene er mindre synlige for personene som er involvert.

Den menneskelige faktoren spiller en rolle i de fleste hendelsene. De ansatte kan ha mangelfull kunnskap om informasjonssikkerhet og sikkerhetskulturen i organisasjonen kan være svak. Det er mennesker som trykker på lenker og dersom det er lenker som er spesialtilpasset den enkelte (sosial manipulering) vil de fleste kunne trykke på dem. Fysisk sikring, digital sikring og menneskelig påvirkning henger tett sammen, som vist i figuren under. Virksomhetene kan bli sårbare for sosial manipulering gjennom eksternes kartlegging av den enkelte ansatte. Via Facebook og sosiale medier er det lett å få vite mye om en persons interesser. Ettersom den tekniske sikkerheten stadig blir bedre, representerer bruk av sosial manipulering en ny angrepsvektor for de som vil inn i IKT-systemene.



Figur 7. *Fysisk sikring, cyber security og menneskelig påvirkning*

1.6. NOU 2015-13 Digital sårbarhet- sikkert samfunn, Stortingsmelding 38 og politiske prioriteringer

NOU 2015: 13 *Digital sårbarhet- sikkert samfunn* («Lysneutvalget») ble fulgt opp av Stortingsmelding 38 (2016-2017). I Stortingsmeldingen peker regjeringen på den nye drikkevannsforskriften, Mattilsynets tilsynskampanje 2016 og innføringen av Nasjonal Vannvakt som viktige tiltak.

Lysneutvalget vektlegger øvelser som et viktig virkemiddel for å redusere den digitale sårbarheten. I vannbransjen har det opp gjennom årene vært lite fokus på å inkludere digitale hendelser som en del av beredskapsøvelsene. Norsk Vann prosjektet Beredskap i vannsektoren fra 2016 fokuserte på dette, og på hjemmesiden[20] til Norsk Vann ligger det eksempler på øvelser som også inkluderer digitale sårbarheter. I NOU 2015: 13 peker Lysneutvalget også på samarbeidet mellom vannverket selv og kommunenes egen IKT-avdeling. I mange kommuner er det en egen IKT-avdeling eller et eget interkommunalt IKT-selskap som beslutter hvilke systemer som skal anskaffes, vedtar sikkerhetsnivåer og til dels har ansvar for drift av systemene. IKT-avdelingen i en kommune betjener mange ulike kommunale etater og har ikke nødvendigvis god vannfaglig forståelse.

Tilsvarende har gjerne vannverkets ansatte god vannfaglig kompetanse, men kan ha mindre kompetanse knyttet til IKT og IKT-sikkerhet. Vannverksorganisasjonen vil uansett ha et overordnet sikkerhets- og beredskapsansvar i henhold til drikkevannsforskriften. Det er viktig å avklare hvordan grensesnittet bør være opp mot IKT-avdelingen og IKT-leverandørene, både for anskaffelser og for drift.

Smarte vannmålere var nevnt i NOU 2015:13, hvor sårbarhetsutfordringer med å knytte disse målerne sammen med driftskontrollsystemer ble diskutert. Det ble anbefalt å gjennomføre nødvendige ROS-analyser for å forhindre ukritisk implementering av funksjonalitet ved etablering av smarte vannmålere inn mot driftskontrollsystemer.

Innføring av smarte vannmålere er også nevnt i Stortingsmelding 38 (2016-2017). Fra myndighetenes side er det ikke planlagt noen spesifikke tiltak knyttet til innføring av smarte vannmålere. Dersom vannbransjen selv ønsker å ta i bruk smarte vannmålere, pekes det på vannverkseiers ansvar for å utrede og forsikre seg om at det ikke svekker IKT-sikkerheten. Det følger også av kravet i drikkevannsforskriften § 10.

20) https://www.norskvann.no/index.php/kompetanse/prosjekter/beredskap

Norsk Vann har etablert en egen arbeidsgruppe[21] som skal arbeide med smarte vannmålere. I tillegg til å se på de mulighetene som innføring av smarte vannmålere kan gi, må denne gruppen også se på eventuelle sårbarheter.

I den politiske plattformen for regjeringssamarbeidet[22] 2017-2020 pekes det på at arbeidet med digitalisering av offentlige tjenester skal fortsette og at IKT-sikkerheten må ivaretas og tilpasses et nytt trusselbilde. For å få en brukerorientert, moderne og effektiv offentlig forvaltning, legger Regjeringen opp til å etablere en sentral markedsplass for skytjenester, inspirert av tilsvarende ordning i Storbritannia kalt Digital Marketplace[23]. En slik markedsplass vil kunne gjøre det enklere for kommuner og selskap å finne de rette tjenestene og ta stilling til hvilke leverandører man bør velge. Det planlegges videre å utvikle en strategi for å bidra til tilstrekkelig og oppdatert IKT-kompetanse i forvaltningen, men også styrke den digitale kompetansen i befolkningen generelt.

21) https://www.norskvann.no/index.php/10-nyheter/1770-arbeidsgruppe-for-smarte-vannmalere

22) https://www.venstre.no/assets/v-h-frp-politisk-plattform-2018.pdf

23) https://www.digitalmarketplace.service.gov.uk/g-cloud/services/115545636168897

1.7. Drikkevannsforskriften og informasjonssikkerhet

Den nye drikkevannsforskriften fra 2017 stiller krav til vannverkseierne med hensyn til kvalitet, mengde og leveringssikkerhet for drikkevann. Informasjonssikkerhet er særlig relevant opp mot § 6, 8, 9, 10 og 11.

§ 6. Farekartlegging og farehåndtering
Vannverkseieren skal identifisere farene som må forebygges, fjernes eller reduseres til et akseptabelt nivå for å sikre levering av tilstrekkelige mengder helsemessig trygt drikkevann som er klart og uten fremtredende lukt, smak og farge. Vannverkseieren skal sikre at tiltak som forebygger, fjerner eller reduserer farene til et akseptabelt nivå, identifiseres og gjennomføres. Farekartlegging og farehåndtering skal danne grunnlag for beredskapsforberedelser som er beskrevet i § 11. Vannverkseieren skal sikre at farekartleggingen og farehåndteringen er oppdatert.

Kommentar: Farekartleggingen skal inkludere alle relevante farer som kan oppstå, herunder også farer som skyldes eller påvirkes av IKT og informasjonssikkerhet. Farekartleggingen må oppdateres også som en følge av økt digitalisering av vannbransjen.

§ 8. Kompetanse og opplæring
Vannverkseieren skal sikre at vannforsyningssystemet har, eller gjennom avtale har tilgang til, nødvendig kompetanse. Vannverkseieren skal sikre at alle som deltar i aktiviteter omfattet av denne forskriften, gis opplæring som står i forhold til arbeidsoppgavene.

Kommentar: Vannverket skal sikre nødvendig kompetanse for alle funksjoner. Dette inkluderer også IKT og informasjonssikkerhet dersom vannverket er avhengig av dette. Hva som ansees som nødvendig kompetanse vil være i kontinuerlig endring pga. økt digitalisering av vannbransjen. Kompetanse kan også sikres ved ekstern konsulenthjelp, avtaler med driftsassistanse eller samarbeid med andre kommuner.

§ 9. Leveringssikkerhet
Vannverkseieren skal sikre at vannforsyningssystemet er utstyrt og dimensjonert samt har driftsplaner og beredskapsplaner for å kunne levere tilstrekkelige mengder drikkevann til enhver tid.

Kommentar: Vannverket skal sikre at alt er på plass for alltid å kunne levere nok trygt drikkevann. Dette inkluderer også IKT og informasjonssikkerhet

§ 10. Forebyggende sikkerhet
Vannverkseieren skal sikre at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet er tilstrekkelig fysisk sikret, og at alle styringssystemer er tilstrekkelig sikret mot uautorisert tilgang og bruk.

Kommentar: Sikring av styringssystemene mot dataangrep er spesifikt nevnt i forskriften, og i veilederen er det listet opp eksempler på hva som bør vurderes. I tillegg pekes det i veiledningen på at det må etableres en sikkerhetskultur som sikrer at alle forstår hva som er grunnlaget for sikkerhetskravene, og handler riktig ut fra dette. God sikkerhetskultur er et lederansvar. Det er ledelsen i kommunen som beslutter hvilke sikringstiltak som skal implementeres, og hvilke rutiner som skal være gjeldende på arbeidsplassen.

§ 11. Beredskap
Vannverkseieren skal sikre at det gjennomføres nødvendige beredskapsforberedelser og utarbeides beredskapsplaner i samsvar med helseberedskapsloven og forskrift om krav til beredskapsplanlegging.(...) Vannverkseieren skal sikre at denne planen er oppdatert og følges.

Kommentar: Basert på funn fra farekartlegging og farehåndtering skal det utarbeides en beredskapsplan. Det er viktig å gjennomføre beredskapsøvelser som også inkluderer IKT-hendelser som en del av øvelsesscenariet. Norsk Vann tidligere utarbeidet eksempler på scenarioer (se Figur 5).

For et fåtall vann- og avløpsvirksomheter gjelder også sikkerhetsloven. Denne gjelder for de anlegg som er klassifisert som såkalte skjermingsverdige objekter. Dette kan være vannbehandlingsanlegg, høydebasseng, vannpumpestasjoner etc. som må beskyttes av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Vannforsyningen er viktig for samfunnets funksjonalitet, og er definert som en kritisk infrastruktur. Det er derfor viktig å vurdere eventuelle anskaffelser/teknologiske endringer opp mot §29a i sikkerhetsloven. Sikkerhetsloven beskrives ikke nærmere, men kan være aktuell for flere vannverk enn de som er berørt p.t. En ny sikkerhetslov er på trappene, og flere anlegg forventes å bli vurdert på nytt med tanke på skjermingsbehov.

1.8. NIS-direktivet fra EU

NIS-direktivet (The Directive on security of network and information systems) ble vedtatt i EU 6. juli 2016. Direktivet omhandler tiltak for å sikre et høyt felles nivå for nettverk- og informasjonssikkerhet i EU. Bakgrunnen for direktivet er at EU ikke hadde implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå god nok sikkerhet i nettverk og informasjonssystemer. Gjennom direktivet ønsket EU å forbedre det indre markeds funksjon ved å etablere et høyt felles sikkerhetsnivå i viktige nettverks- og informasjonssystemer.

Justis- og beredskapsdepartementet har hatt NIS-direktivet ute på høring[24] for få belyst konsekvensene av å gjennomføre forslaget i norsk rett. Høringssvarene tyder på at direktivet ansees som relevant og at en i Norge i stor grad allerede har gjennomført de tiltak som kommisjonen foreslår. Direktivet gjelder for virksomheter som er:

a) essensiell for opprettholdelsen av kritiske samfunnsmessige og/eller økonomiske aktiviteter,
b) tjenesteleveransen er avhengig av nettverk og informasjonssystemer, og
c) en hendelse i tjenestens nettverk og informasjonssystemer ville hatt vesentlig forstyrrende virkning på leveransen

Vannforsyning er på generelt grunnlag nevnt som en av de virksomhetene som direktivet gjelder for. Det vil variere fra vannverk til vannverk hvorvidt det enkelte vannverk er essensielt for opprettholdelsen av kritiske og/eller økonomiske aktiviteter (bokstav a). Hvilke vannverk som NIS-direktivet vil gjelde for vil videre være avhengig av hvorvidt bokstav b eller c oppfylles for det enkelte vannverk.

En del større vannbehandlingsanlegg er kompliserte prosessanlegg med mange komponenter, signaler i styringssystemet og prosess- og analyseinstrumenter som forutsetter avansert styring av de ulike integrerte prosessene. Manuell drift av de mest komplekse vannbehandlingsanleggene er ikke mulig, i alle fall ikke over lengre perioder. Dersom et vannverk er så komplekst at det forutsetter automatisk styring og overvåkning for å virke, må en anta at NIS- direktivet vil gjelde for det aktuelle vannverket. For mindre komplekse vannverk hvor anleggene kan driftes manuelt dersom driftskontrollsystemene skulle svikte, vil en følgelig ikke måtte forholde seg til NIS-direktivet. Hvorvidt dette er gjeldende for hvert enkelt vannverk bør følgelig følge direkte av de analyser som vannverkene plikter å utføre iht. drikkevannsforskriftens § 6 *Farekartlegging og farehåndtering og § 11 Beredskap.*

Kravene NIS-direktivet setter til regulering av vannforsyningen er trolig tilstrekkelig ivaretatt gjennom kravene i drikkevannsforskriften til

- farekartlegging (§ 6),
- at alle styringssystemer er tilstrekkelig sikret mot uautorisert tilgang og bruk (§ 10) og
- varslingsplikt (§ 24).

24) https://www.regjeringen.no/no/dokumenter/horing---forslag-til-eu-direktiv-om-sikkerhet-i-nettverk-og-informasjonssystemer/id2506623/

Danmark har lagt seg på en definisjon som tilsier at de vannverk som kan driftes manuelt ikke dekkes av NIS-direktivet.

NIS-direktivet artikkel 9 stiller krav til at det utpekes et sektorvis responsmiljø (CSIRT), også for vannforsyning. I dag ivaretar KraftCERT en frivillig responsfunksjon for energisektoren og en del norske vannverk (frivillig medlemskap). Om vannbransjen skal inngå i f.eks. KraftCERT eller en egen KommuneCERT som nevnt i Lysneutvalget, er ting som må vurderes på nasjonalt nivå. Dette kan også sees i sammenheng med Nasjonal vannvakt og hvorvidt denne funksjonen også skal inkludere IKT.

2. Digitale trusler – trusselbildet

Trusselaktørenes metoder endrer seg hele tiden. Det utfordrer våre evner til å forebygge, oppdage og håndtere hendelser. Det kommer ny teknologi som kan ha innebyggede sårbarheter, og avanserte analysemetoder brukes «på begge sider av banen», både på den gode og på den onde siden. Maskinlæring som metode kan for eksempel også brukes av hackere.

De fleste typer digitale angrep starter som regel med at det brukes ulike varianter av skadevare som distribueres via e-post. Fremgangsmåten for slike angrep blir stadig mer målrettet og tilpasset den enkelte bruker. I følge en undersøkelse fra SSB benyttet 90% av befolkningen e-post i 2016. E-post er følgelig en attraktiv angrepsmåte for trusselaktører, og har potensiale til å ramme mange. I NSM sin risikorapport for 2018[25] (Risiko 2018) refereres det til et «angrep» som NSM har gjort mot en virksomhet i norsk statsforvaltning hvor en prøvde å få de ansatte til å trykke på linker og oppgi påloggingsdetaljer. Ni av ti ansatte lot seg lure til å klikke på den den tilsynelatende legitime lenken og tre av ti oppga sine påloggingsdetaljer. Dette viser at trusselaktører som gjennomfører målrettede og tilpassede e-post angrep har stor sannsynlighet for å lykkes med å lure ansatte til å eksponere sin virksomhets verdier.

Tidsforløpet fra en hacker kommer inn i IT-systemene til det oppdages at noen er inne i systemene varierer mye. Dette kan typisk variere fra automatisk deteksjon (0 dager) til opptil flere år. I gjennomsnitt rapporteres det at det har vært en kraftig reduksjon (forbedring) de senere årene, ned til dagens nivå på 49 dager[26]. I PST sin trusselvurdering for 2018[27], kommer det fram at en «trusselaktør» hadde hatt tilgang til et norsk nettverk i flere år før det ble avdekket. Dersom en hacker har hatt lang tid for seg selv inne i systemene, vil dette også gjøre arbeidet med hendelseshåndtering vanskeligere, da det kan ha gått lang tid fra sårbarheten ble utnyttet til eventuell hendelse oppstår i vannforsyningssystemet. I tillegg vil det være en fare for at en eventuell hacker vil forsøke å komme seg enda dypere inn i systemet, ved å gi seg selv administratorrettigheter i datanettverket.

25) https://nsm.stat.no/aktuelt/risiko-2018/

26) https://www.infosecurity-magazine.com/news/median-dwell-time-for-hackers/

27) https://www.pst.no/trusselvurdering-2018/

2.1. Løsepengevirus

Løsepengevirus (ransomware) krypterer og låser ned den infiserte datamaskinen, og ber eieren om å betale en sum penger i håp om å få den låst opp igjen. Det kommer en jevn strøm av slike virus, eksempler på avanserte kjente virus i 2017 har vært WannaCry[28], NotPetya[29] og Bad Rabbit[30]. WannaCry skal være basert på amerikansk hackingverktøy utviklet hos sikkerhetsorganisasjonen National Security Agency (NSA). Løsepengevirusene inkluderer også betaling ved hjelp av virtuell valuta eller kryptovaluta, slik som Bitcoin. Innbetaling med Bitcoin som betalingsmiddel sikrer anonymitet, noe som øker interessen for løsepengevirus ytterligere.

Viktig tiltak for å redusere risikoen for løsepengevirus er å ha oppdatert programvare, ha rutiner for back-up slik at data kan re-etableres, segmentering av infrastruktur og fokusere ansatte på faren for phishing via ukjente vedlegg.

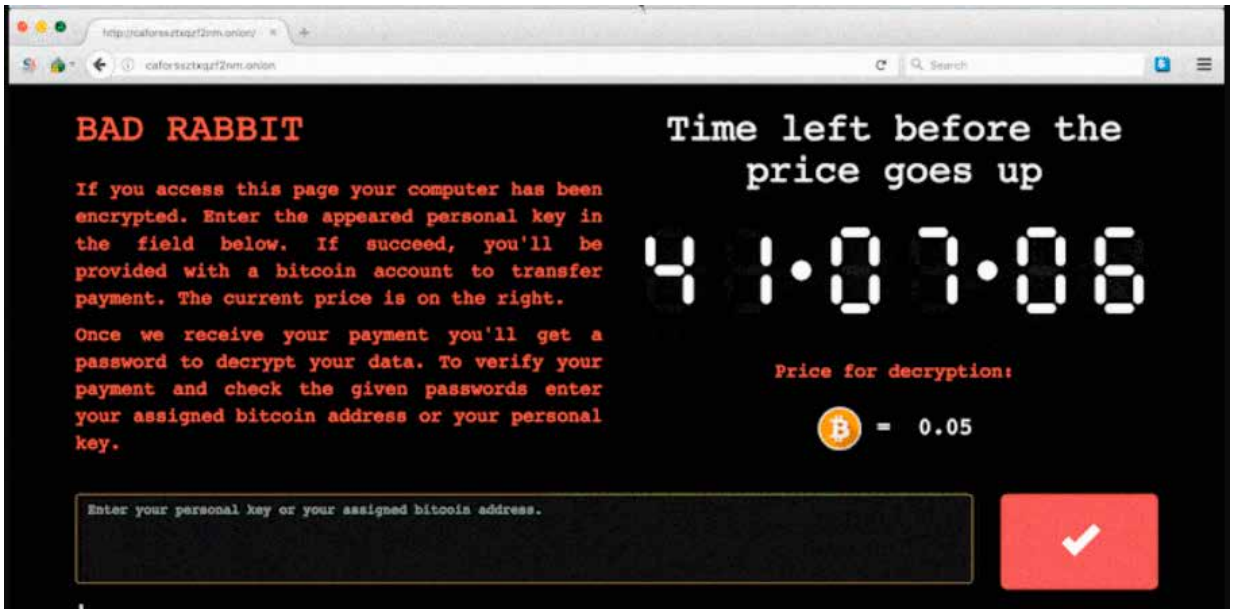
Undersøkelser fra England[31] viser at bare om lag 1/3 av 1400 ledere hadde hørt om løsepengevirus som WannaCry.

28) http://www.zdnet.com/article/wannacry-ransomware-was-the-biggest-challenge-of-the-year-says-cyber-security-centre/

29) https://en.wikipedia.org/wiki/Petya_(malware)

30) https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html

31) https://www.infosecurity-magazine.com/news/just-onethird-execs-heard-wannacry

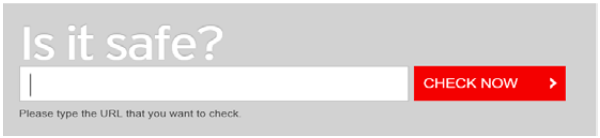


Figur 8. *Skjermbilde for løsepengeviruset Bad Rabbit*

2.2. Sosialt tilpasset skadelig programvare (malware)

Skadelig programvare som er sosialt tilpasset brukerne gjerne også i kombinasjon med løsepengevirus er en mye brukt angrepsvektor. Brukeren blir lurt til å trykke på en lenke eller åpne et vedlegg. Dette kan være under dekke av å installere et program som gir inntrykk av å være legitimt, f.eks. et antivirusprogram. Tiltak for å redusere omfanget er i første rekke god opplæring av de ansatte, ta bort internettilgang fra kritiske PCer og oppdatert antivirusprogrammene.

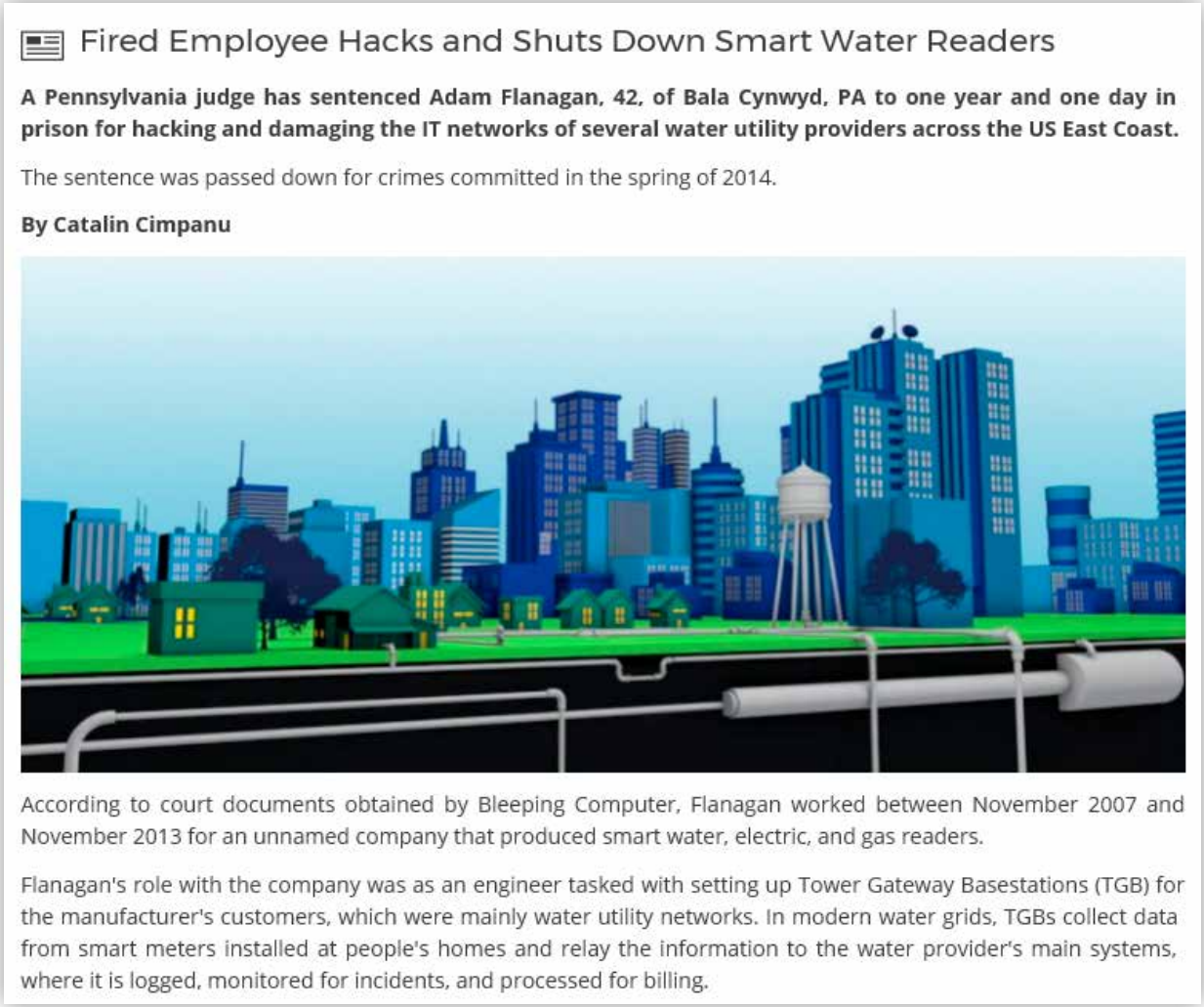
Skadelig programvare videreutvikles stadig, og bruk av avanserte analyseteknikker, slik som maskinlæring, inkluderes også. I dag er vi godt kjent med at maskinlæring brukes av aktører som Netflix, når de anbefaler oss nye filmer som vi mest sannsynlig vil like, basert på de filmene vi allerede har sett. Tilsvarende vil også gjelde for virus. Man bruker maskinlæring til å tilpasse skadelig programvare til den enkelte bruker. E-posten som inneholder lenken som sendes til hver enkelt, vil følgelig være tilpasset hva hver enkelt liker på eksempelvis Facebook. Dette øker sannsynligheten for at brukeren biter på kroken for digital fisking («phishing»). Dersom en ønsker å sjekke om det er trygt klikke på en bestemt lenke, kan en eksempelvis benytte Trend Micros Site Safety Center[32]. En kopierer da inn adressen som skal sjekkes, og den sjekkes så mot kjente sårbarheter.



I 2016 ble en nettstasjon i Ukraina[33] påvirket, noe som resulterte i ca. en time med blackout den 17. desember. Angrepet hadde likhetstrekk med et tilsvarende angrep i 2015, men denne gangen ble det brukt en angrepskode som har fått navnet «Industroyer» som snakker språket til SCADA-systemene og som dermed tok over som kontrollnode i systemet som kommuniserte med de enkelte utestasjonene. Dette medfører en automatisering i forhold til å basere seg på personer som tar over kontrollen for å gjøre manuell endringer.

32) https://global.sitesafety.trendmicro.com/

33) https://www.sintef.no/globalassets/project/nef-tm-2017/rapporter-2017/sesjon-3-3---34---jaatun-nef-tm-2017.pdf



Fired Employee Hacks and Shuts Down Smart Water Readers

A Pennsylvania judge has sentenced Adam Flanagan, 42, of Bala Cynwyd, PA to one year and one day in prison for hacking and damaging the IT networks of several water utility providers across the US East Coast.

The sentence was passed down for crimes committed in the spring of 2014.

By Catalin Cimpanu

According to court documents obtained by Bleeping Computer, Flanagan worked between November 2007 and November 2013 for an unnamed company that produced smart water, electric, and gas readers.

Flanagan's role with the company was as an engineer tasked with setting up Tower Gateway Basestations (TGB) for the manufacturer's customers, which were mainly water utility networks. In modern water grids, TGBs collect data from smart meters installed at people's homes and relay the information to the water provider's main systems, where it is logged, monitored for incidents, and processed for billing.

Figur 9. *Tidligere ansatt som endret passord for kommunikasjonsløsning for smarte vannmålere i USA*

2.3. Ansatte/tidligere ansatte som sikkerhetsrisiko

Ansatte utgjør både en sikkerhetsbarriere, men kan også være en mulig digital sårbarhet. Dette kan både være som en følge av uhell og at de klikker på infiserte vedlegg. De ansatte har tilgang til systemene, så dersom en kommer inn i IT-systemene via en ansatt, vil eventuell hacker være på innsiden av eventuelle sikkerhetsmekanismer. Tidligere ansatte kan også utgjøre en mulig fare, dersom en ikke fjerner tilgangen til systemene når de slutter. Dette var tilfellet i USA i 2014[34], hvor en tidligere ansatt i et firma som leverte smarte vannmålere endret passordet på basestasjonene som samlet inn data fra målerne. I forkant av hendelsen hadde han blitt oppsagt i firmaet og som en siste hilsen til sin tidligere arbeidsgiver endret han passordet for alle basestasjonene til «fu*kyou».

En utro tjener blant egne ansatte er også nevnt i Norsk Vann rapport 229/2017 som et av flere trusselscenarioer som norske vannverk kan bli utsatt for. Dette er en hendelse hvor det enten stjeles, distribueres, eller saboteres verdier som vannverkene ønsker å beskytte. NSM har laget en egen veiledning[35] for sikkerhet ved ansettelsesforhold - før, under og ved avvikling av arbeidsforholdet. Veilederen er relevant både for nåværende eller tidligere ansatte, men også overfor innleide leverandører og konsulentselskaper som også sitter på detaljert kunnskap og informasjon. Veilederen anbefaler f.eks. at kommunen ved avslutning av et oppdrag bør ha en avsluttende dialog om hvordan leverandøren eller konsulenten nå skal forholde seg sikkerhetsmessig til informasjonen og kunnskapen vedkommende har tilegnet seg.

34) https://www.bleepingcomputer.com/news/security/fired-employee-hacks-and-shuts-down-smart-water-readers-in-five-us-cities/

35) https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/sikkerhet_ved_ansettelsesforhold_endelig.pdf

2.4. Leverandørverdikjeden som en sårbarhet

Det er svært krevende å holde oversikt over alle sårbarhetene gjennom hele verdikjeden, særlig når «alt henger sammen med alt». Eventuelle sårbarheter og feil hos en underleverandør kan forplante seg og kan få uante konsekvenser. Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester, lavere driftskostnader og bidra til økt fokus på virksomhetens kjernevirksomhet. Det kan imidlertid også føre til økt risiko på grunn av redusert kontroll over stadig mer komplekse verdikjeder. NSM hevder i sin statusrapport for 2017 at trusselaktører har forsøkt å få tilgang til IT- leverandørenes kunder og deres data. Dette er særlig aktuelt dersom leverandøren har svakere sikkerhetsbarriere enn infrastruktureieren, da trusselaktører leter systematisk etter det svakeste ledd. Denne trenden ser en også videreføres i NSM sin risikorapport for 2018[36]. For VA-verk vil følgelig leverandører av ulike IT-løsninger kunne representerer en mulig vei inn egne systemer. Dette var for eksempel tilfellet med Dragonfly viruset i 2014 og Petya viruset i juni 2017. Dragonfly byttet blant annet ut legitime drivere og oppdateringer på nettsidene til leverandører av kontrollsystemer med trojanske versjoner slik at en kom på innsiden av eventuelle brannmurer. I fred og ro kunne så Dragonfly samle inn informasjon om tilstand, verktøy, koblinger og nettverk. Denne inneholdt også en funksjon for fjernoppdatering slik at det var enkelt å oppdatere skadevaren når man måtte ønske for å kunne gjøre mer aktiv skade. Lærdommen fra Dragonfly for norske vann- og avløpsvirksomheter er følgelig å kreve tilstrekkelig sikkerhet hos leverandører av programvare og løsninger, samt at en tester ut at løsningene faktisk er både tilstrekkelige og så gode som leverandøren hevder. Et konkret tips er å kreve signerte utgaver av alle oppdateringer. Mer info om Dragonfly finnes på SINTEF Infosec blogg[37].

Det er eksempler på IT-leverandører innen VA- bransjen som anbefaler usikre metoder. Eksempler på dette er at brannmurer må slås av for at løsningen skal virke eller at bakdører som leverandøren kan benytte til eventuell feilretting står permanent åpne. Tilfellet som er beskrevet tidligere med østlendingen som ringte til vestlendingen og tok over styringen av vannverket er nettopp et eksempel på en bakdør som leverandøren lot stå åpen.

I tillegg deles informasjon med leverandører. Når informasjon deles kan den også mistes. Gode systemer for å sikre informasjonen også hos leverandører er følgelig viktig. Ansvaret for å håndtere data på en sikker måte vil beskrives og reguleres i en databehandleravtale.

Det er følgelig viktig å etablere organisatoriske, tekniske og juridiske sikringstiltak. Verdikjeden som en sårbarhet er også vektlagt av NSM i sin gjennomgang av risikobildet for 2017.

36) https://nsm.stat.no/aktuelt/risiko-2018/

37) https://infosec.sintef.no/informasjonssikkerhet/2017/10/cybersikkerhet-og-stromnettet/

2.5. Bruk av ikke-oppdatert programvare

Bruk av ikke-oppdatert programvare representerer mulige sikkerhetshull. Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner, og de har ofte flere og bedre sikkerhetsfunksjoner. Dette gjelder både program- og maskinvare. Nye sikkerhetsoppdateringer bør installeres så fort som mulig. Kunnskap om nye sårbarheter sprer seg raskt. Derfor bør systemeiere være tilsvarende raske med å oppdatere, før noen bruker sårbarhetene til å bryte seg inn. Viktigheten av oppgradert programvare ble for eksempel dokumentert i Norge under WannaCry angrepet, hvor omfanget av hendelser i Norge var lavt. En viktig grunn til dette var bruk av oppgradert programvare i organisasjonene. Eventuelle produkter som ikke lar seg oppdatere bør unngås.

Aftenposten | Tirsdag 5. desember 2017 NYHETER | 9

For en billig penge kan du betale andre for å utføre dataangrep

Man trenger ikke lenger være ekspert for å utføre et data-angrep. For bare noen tiere kan hvem som helst kjøpe skadevare.

Passordknekkere, løsepenge-virus og annen skadevare er ikke lenger forbeholdt teknisk kompetente hackere.
Man kan nå kjøpe skadevare på en rekke stadig mer bruker-vennlige nettsteder. Aften-postens søk både på det åpne og det mørke nettet viser at prisene er lave.

Det siste året har det i snitt vært 750 tjenestenektangrep i

Figur 10. *CaaS- Kriminalitet levert som en tjeneste.*

2.6. CaaS – Crime as a Service

Man trenger ikke lenger være IT-ekspert for å utføre et dataangrep. Dette kan bestilles på nettet for en billig penge[38]. For eksempel er informasjon om brukere og tilgangsdata til systemer en etterspurt vare kommersielt og til digital krigføring.

38) http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/

2.7. IoT & sikkerhet

Vannbransjen er fortsatt i startgropen når det gjelder innføring av IoT (Internet of Things). «Tingenes internett» vil enkelt si at alt av utstyr/komponenter er koblet opp mot internett. Dermed kan «tingene» også sende informasjon gjennom for eksempel målinger gjort ved hjelp av sensorteknologi. Det utvikles nå IoT-sensorer som både samler data, prosesserer og kommuniserer i 15 år, uten bytte av batteri og uten kabler for kommunikasjon. Dette åpner opp for nye muligheter og representerer en helt ny informasjonskilde. IoT sensorer har typisk enkel installasjon uten bruk av kabling verken for strøm eller kommunikasjon. IoT sensorer muliggjør dermed også å gjøre eksisterende vann og avløpsinfra-

Vet du hva s'en i IoT står for?

struktur smartere. Særlig forventes IoT- sensorer å bli enda mer vanlig innen vannsektoren når kommunikasjonsteknologi basert på narrowband – IoT (nb- IoT) blir gjort tilgjengelig. NB-IoT er designet for å knytte objekter til internett som er på vanskelig tilgjengelige steder slik som tilfellet er for mye av vann- og avløpsinfrastrukturen. Det vil være viktig å fokusere på sikkerhet i forbindelse med utrulling av IoT. Dersom en ikke har tenkt sikkerhet når en designet utstyret, kan IoT- sensorer være en mulig bakveg inn i vannsystemene for

Figur 11. *Oversikt over kommunikasjon fra sensorer, via gateway og videre til database/skyløsning (Figur EL-Watch)*

eventuelle hackere. Viktige problemstillinger er i hvilken grad IoT-sensorer er koblet til SCADA system. Er datakommunikasjonen kryptert fra ende til ende eller kan data manipuleres? Som vist i figuren under bør en ha kryptering helt fra sensor via gateway (hub) og videre til database/skyløsning. Dersom det bare er kryptering fra gateway kan for eksempel et såkalt «menneske-i-midten-angrep» etableres. En hacker kan da komme inn mellom sensor og gateway og rapportere en annen verdi enn hva sensoren måler. Det er derfor viktig med kryptering fra ende til ende.

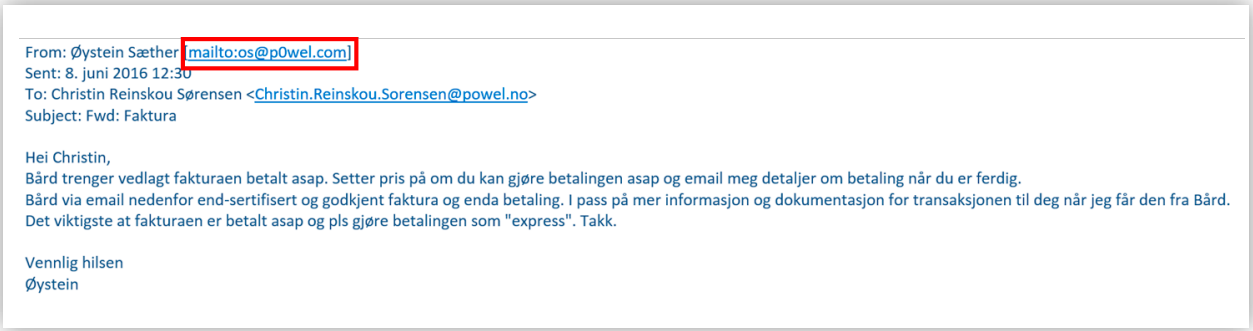
Det er viktig at IoT utstyr som kobles til VA-systemene og til internett er sikkerhetsmessig «herdet» (hacker hardened) og at enhetene som benyttes er designet med tanke på sikkerhet (security by design).

Erfaringer fra det nylig avsluttede EU prosjektet SW4EU, hvor nederlandske og engelske vannselskap testet ut IoT-sensorer for å finne vannlekkasjer, viser at det er behov for robuste, skalerbare og sikre IoT-plattformer for å håndtere de store datamengdene[39].

39) GWI (2017). Water utilities drowning in data ask solution providers for simplicity. I GWI desember 2017. S 46-49.

2.8. Direktørsvindel

Norske bedrifter taper hundrevis av millioner kroner på såkalt direktør-svindel (CEO-svindel), hvor svindlere utgir seg for å være sjefen og lurer typisk økonomiansatte i bedriften til å overføre penger. Som regel haster det med overføringen. E-post adressen er enten svært lik den ekte (Fornavn.Etternavn@Firma.nO), eller sågar identisk. Meldingene er målrettede og gjerne relevant på tema som bedriften arbeider med for tiden. Slike hendelser er kjent både fra leverandørindustrien til vannbransjen, men også hos VA-selskapene. Figuren under viser et forsøk på slik direktørsvindel hvor e-postadressen til avsender er *nesten korrekt.*


From: Øystein Sæther [mailto:os@p0wel.com]
Sent: 8. juni 2016 12:30
To: Christin Reinskou Sørensen <Christin.Reinskou.Sorensen@powel.no>
Subject: Fwd: Faktura

Hei Christin,
Bård trenger vedlagt fakturaen betalt asap. Setter pris på om du kan gjøre betalingen asap og email meg detaljer om betaling når du er ferdig.
Bård via email nedenfor end-sertifisert og godkjent faktura og enda betaling. I pass på mer informasjon og dokumentasjon for transaksjonen til deg når jeg får den fra Bård.
Det viktigste at fakturaen er betalt asap og pls gjøre betalingen som "express". Takk.

Vennlig hilsen
Øystein

Figur 12. *Eksempel på forsøk på direktørsvindel.*

2.9. Nasjonalstater som trusselaktør

Cyberangrep fra ulike nasjonale stater eller statssponsede aktører forekommer. Dette er profesjonelle aktører som har dette som yrke og som har store økonomiske ressurser. Datainnbruddet[40)] hos Helse Sør-Øst i januar 2018 viser at dette også skjer i Norge. I en tidlig fase av etterforskningen spekuleres det i om at hackere har fått administratortilgang til systemene, og om dataangrepet skyldes systematisk hacking etter pasientjournaler, som viser samhandling mellom helsevesenet og forsvaret. Den videre etterforskningen vil kunne vise hvem som stod bak angrepet, hvordan angrepet foregikk, hvilke data de var ute etter og i hvilken grad data kom på avveier.

40) https://www.nrk.no/nyheter/dataangrepet-mot-helse-sor-ost-1.13873606

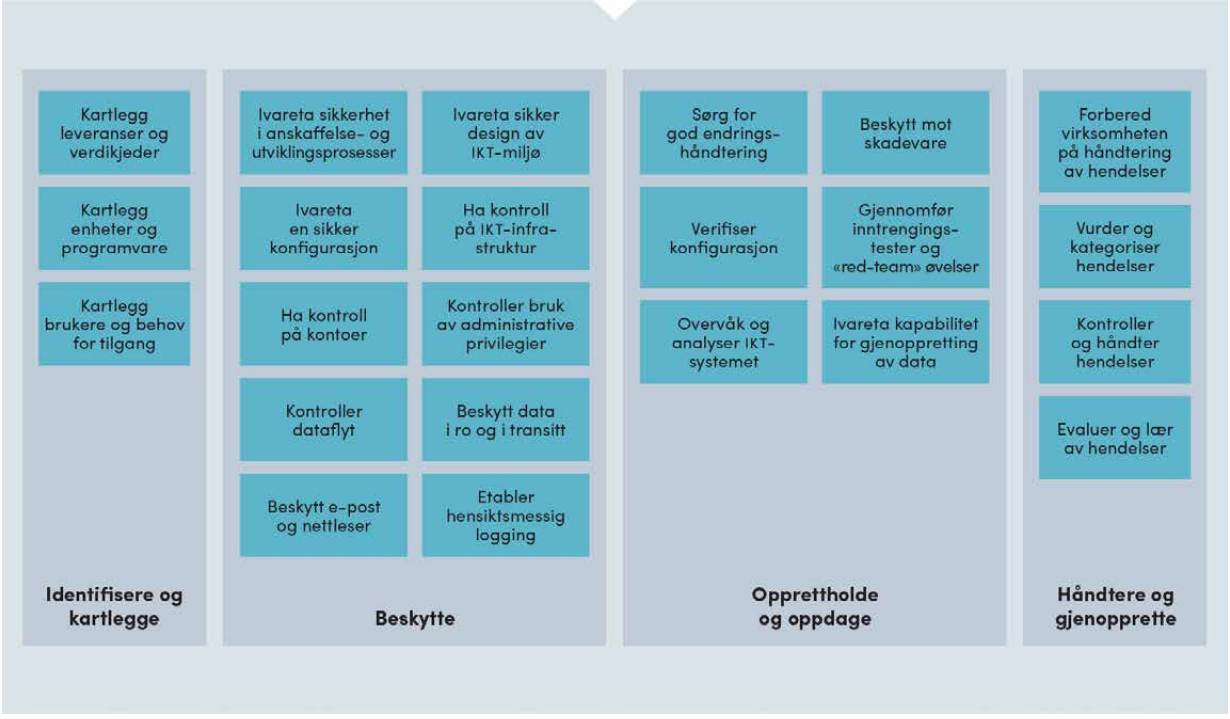
3. Aktuelle grunnprinsipper for IKT-sikkerhet for vann- og avløpsvirksomheter

NSM har utarbeidet et rammeverk for *Grunnprinsipper for IKT-sikkerhet*[41]. Her defineres et sett med grunnprinsipper for å beskytte verdier og leveranser i en virksomhet. Dette kan også være nyttig for vann- og avløpsvirksomheter. Grunnprinsippene er strukturert i fire kategorier, og hvert grunnprinsipp har ulike sikringstiltak som beskriver hva og hvorfor tiltak bør gjennomføres.

1) Identifisering og kartlegging er utgangspunktet for arbeidet med IKT-sikkerhet. En må vite hva en har før en eventuelt vurderer tiltak for beskyttelse. Kartleggingen inkluderer hele VA-verdikjeden fra vannkilde til resipient, og inkluderer både de fysiske anleggene, men også de tilhørende informasjonsaktiva som er nærmere beskrevet i kapittel 4 - *Verdivurdering av informasjonen innen VA*. For å utføre verdivurderingen er det utarbeidet et regneark som kan lastes ned fra Norsk Vann sine sider sammen med rapporten. Det må også utføres en kartlegging av de ulike brukere og deres behov for tilgang. Dette inkluderer også eventuelle leverandører. Krav fra leverandører om å slå av brannmurer eller at brukerne av løsningene må ha superbrukerrettigheter bør ikke forekomme. Kartleggingen som skal utføres som en del av farekartleggingen iht. drikkevannsforskriften og generelle ROS-analyser er også en del av dette arbeidet. Kartleggingen må utføres tverrfaglig hvor både VA-kompetanse og IKT-kompetanse bidrar.

2) Beskyttelse av leveranser og verdier må utføres basert på arbeidet med identifisering og kartlegging. For et VA-virksomhet vil det være ulike IKT systemer, både fagsystemer og administrative systemer som skal beskyttes. Prinsipper som sonedeling og segregering kan benyttes for å beskytte systemene. Dette inkluderer å skille SCADA systemene fra det administrative nettet. Sikkerhet må ivaretas også ved anskaffelser. For eksempel må en være bevisst på hva en legger ut på DOFFIN og hva som legges ut i forbindelse med plansaker. Norsk Vann rapport 195/2013 *Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg* beskriver flere grunnleggende sikkerhetstiltak som fortsatt er aktuelle. Et viktig tiltak er å bruke de siste versjonene av de ulike løsninger i stedet for å vente med oppdateringer. I nye versjoner er ofte eventuelle kjente sårbarheter fjernet.

41) https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/introduksjon/



Figur 13. *NSMs grunnprinsipper for IKT sikkerhet.*

3) Opprettholde og oppdage. Periodisk bruk av inntrengingstester har vist seg å være svært effektive, ikke minst for deteksjon og sporbarhet. Det finnes løsninger og verktøy for å kunne overvåke og oppdage uønskede IKT-hendelser (f.eks. Advanced Threat Analytics).

4) Håndtere og gjenopprette etter hendelser. For å kunne håndtere IKT-hendelser som måtte oppstå er det viktig å ha tenkt igjennom hva som kan skje, før hendelsen oppstår. Dette inkluderer gjennomføring av beredskapsøvelser med fokus på IKT. Det bør øves både på utfall av systemer og hacker-angrep mot infrastrukturen, hvor både konfidensialitet, integritet og tilgjengelighet (KIT) testes. Dersom det oppstår hendelser hvor en trenger bistand bør en selvfølgelig ringe til den Nasjonale vannvakten, både for å informere, men også for å få informasjon om hvor en eventuelt kan få ytterligere hjelp. I tillegg bør det i forkant etableres avtaler med eksterne parter som kan hjelpe til under hendelser (KraftCERT eller tilsvarende). Datalogger må klargjøres så tidlig som mulig for å kartlegge hendelsesforløpet og for evaluering i etterkant.

I det følgende vil vi med utgangspunkt i Figur 13 beskrive nærmere noen utvalgte tiltak som er særlig relevant for vannbransjen.

3.1. Ha kontroll på brukerkontoer og tilhørende tilganger

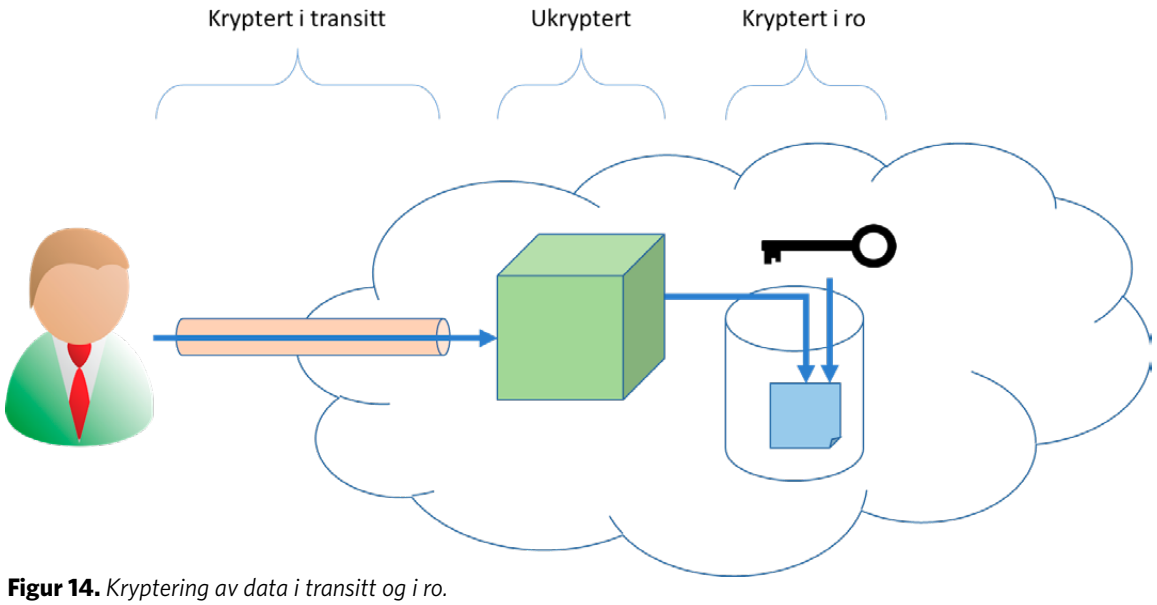
Det er viktig å ha gode systemer for identitets- og tilgangsadministrasjon. Dette ble behørig vist i USA 2014, hvor en tidligere ansatt i et firma som leverte smarte vannmålere endret passordet på basestasjonene som samlet inn data fra smarte husvannmålere (Figur 9). Det er derfor viktig med en brukergodkjennings-tjeneste (f.eks. Azure AD), hvor de ulike brukerne og passord organiseres. En slik brukergodkjenningstjeneste vil medføre sikrere pålogging, men også enklere pålogging for hver enkelt, ved at brukeren slipper å logge seg på flere steder (*single sign on).* Når personer slutter i vann- og avløpsvirksomheten, vil det være nok å fjerne identiteten ett sted (i organisasjonens AD- løsning). På denne måten sikrer en at en tidligere ansatt ikke lenger har tilgang til IT-løsningene. Ved å ha bedre kontroll på brukerkontoer, vil vann- og avløpsvirksomhetene også lukke eventuelle avvik som I sin tilsynskampanje for 2016 fant Mattilsynet flere tilfeller av at ansatte brukte samme brukernavn og passord. Kommunene bør sette krav til at de IT-løsningene som anvendes i vann- og avløpsvirksomhetene skal ha integrerte systemer for identitets- og tilgangsadministrasjon.

3.2. Beskytte data i ro og i transitt

Det er lett å forledes til å tro at sikkerhet i skyen er enkelt; «kan vi ikke bare kryptere dataene?» Det er en kime av sannhet i dette. Samtidig har de aller færreste bruk for en skyløsning som innebærer at dataeier krypterer data på egen infrastruktur, og så laster de krypterte dataene opp i skyen. De alle fleste skyløsninger innebærer at skyleverandøren må ha mulighet til å prosessere dataene, og med dagens teknologi medfører dette at den må ha dataene i klartekst.

Dette betyr at bildet blir litt mer komplisert: Man trenger en løsning for kryptering av dataene mens de overføres mellom kunde og skyen, og en annen løsning som krypterer dataene mens de er lagret i skyen. Leverandøren må så kunne de kryptere dataene når de skal prosesseres, noe som medfører at leverandøren må ha tilgang til krypteringsnøklene. Dette er illustrert i Figur 14.

Kryptering av data i transitt gjøres vanligvis på samme måte som for sikre nettsider, dvs. ved hjelp av Transport Layer Security (TLS) der midlertidige sesjonsnøkler forhandles fram ved hjelp av PKI. For data som lagres kryptert, må leverandøren ha et system for nøkkeladministrasjon som gir tilgang til de relevante krypteringsnøklene ved behov. En slik løsning beskytter mot at en angriper avlytter data mens de lastes opp til skyløsningen, og vil også forhindre en angriper som får tilgang til en (virtuell) disk i skyen fra å lese ut data som ligger på den. Imidlertid vil en angriper som får full kontroll over prosessen som kjører i skyen fortsatt ha tilgang til dataene som finnes i minnet, og kanskje også nøklene som beskytter de krypterte filene.



Figur 14. *Kryptering av data i transitt og i ro.*

3.3. Gjennomføre inntrengingstester for å avdekke sårbarheter i IT-infrastruktur og IT-løsninger

Gjennomføring av såkalte inntrengingstester (penetration test på engelsk) er et effektivt tiltak for å avdekke sårbarheter og teste motstandskraften både i IKT-infrastrukturen (porter, printere, servere etc.), men også av de enkelte software løsningene som VA-virksomheten benytter (SCADA, kartsystem, kundehåndteringsløsning etc.). Inntrengingstester gjøres gjennom målrettet søk og analyse av sårbarheter. Som vist i Figur 15 kartlegges styrken i de innebyggede sikkerhetsbarrierene, og i hvilken grad det finnes bakveier inn i systemene. Inntrengingstester kan utføres både som utsidetester og innsidetester. En utsidetest er en sårbarhetsskanning fra internett, dvs. hackeren er en ekstern bruker uten brukernavn og passord. En innsidetest er en mer omfattende analyse som går ut på å simulere en målrettet trusselaktør med tilgang til administrasjonsnettverket (dvs. at brukernavn og passord er kjent, f.eks. via phishing), hvor målet er å oppnå uautorisert tilgang til virksomhetens systemer.

Kartlegging og forsøk på inntrenging skjer kontinuerlig mot enheter koblet på internett. I Norge ble slike systematiske inntrengingstester for alvor gjort kjent gjennom Dagbladets «Null-CTRL» artikkelserie i 2013/2014[42], hvor en benyttet seg av søkemotoren

42) https://www.dagbladet.no/emne/nullctrl

Figur 15. *Illustrasjon av inntrengingstest for å avdekke sårbarheter i IKT systemene.*

Shodan[43] for å finne IKT-utstyr som var koblet til internett. Det finnes altså fritt tilgjengelige søkemotorer som systematisk kan lete etter sårbarheter i en virksomhets IKT-infrastruktur dersom disse er koblet til internett.

Slike tjenester vil kunne benyttes både av «snille» og «slemme» aktører. På nasjonalt nivå har for eksempel Nasjonal sikkerhetsmyndighet (NSM) laget sin egen kartleggingstjeneste, Allvis NOR (se skjermbilde i Figur 16). Allvis NOR leter gjennom virksomhetens internett-eksponerte IKT-grensesnitt, for å avdekke sårbare eller feil konfigurerte tjenester og utstyr, slik at virksomhetene selv kan redusere sine sårbarheter. Allvis NOR er en tjeneste NSM tilbyr for å bedre sikkerheten i offentlige virksomheter og eiere av kritisk infrastruktur (slik som vann og avløp er), men det presiseres at dette er et lavterskeltilbud som ikke må forveksles med mer omfattende inntrengingstester eller andre helhetlige sikkerhetsevalueringer.

Vann- og avløpsvirksomheter som vurderer at de har behov for slike analyser, kan kontakte NSM på pentest@nsm.stat.no for å gjennomføre analyser ved bruk av Allvis NOR. Dette gjelder også for virksomheter som ikke har skjermingsverdige objekter og således ikke er direkte underlagt sikkerhetsloven. For mer omfattende analyser kan ulike private aktører (f.eks. mnemonic eller tilsvarende) engasjeres for å utføre inntrengingstester. Dette anbefales, da bruk bare av Allvis NOR kan være med å gi vann- og avløpsvirksomhetene en

43) https://www.shodan.io/

Figur 16. *Skjermbilde av NSM sin tjeneste for å skanne etter digitale sårbarheter i IKT-infrastrukturen til en virksomhet (skjermdump: NSM)*

falsk trygghet, da løsningen for eksempel bare skanner tilgjengelig porter og det ikke utføres analyser på innsiden av en eventuell brannmur.

Vann- og avløpsvirksomhetene må analysere egen IKT-infrastruktur i tillegg til de ulike fagløsningene som anvendes. I forbindelse med anbud bør det følgelig settes krav til IT-leverandørene at løsningene som tilbys er blitt inntrengingstestet. Dette bør også være i de ulike leverandørers egeninteresse. Dersom det skulle oppstå en hendelse som påvirker konfidensialitet, integritet eller tilgjengelighet, og det viser seg at dette skyldes digitale sårbarheter i løsningene, vil dette kunne være ødeleggende for tilliten til produktet og bedriften som leverer tjenesten. Implementeringen av den nye personvernforordningen (GDPR) gjør dette også svært aktuelt knyttet til persondata.

3.4. Ledningskartverk tilgjengelig på internett

Det har pågått en diskusjon om ledningsdata skal ligge offentlig på internett. Ut fra praktiske hensyn bør ledningskartverket være åpent tilgjengelig for alle og informasjonen gjøres tilgjengelig, men mye taler samtidig for at det ut fra sikkerhetshensyn bør være restriksjoner på hvem som får tilgang. Man kan i et ekstremt tilfelle tenke seg at en ondsinnet aktør ønsker å tilføre ledningsnettet stoffer som forgifter eller forringer drikkevannet. Et slikt målrettet angrep vil kreve god kunnskap om vannforsyningssystemet oppbygging, strømningsretninger, kritiske vannkummer som har enkel adkomst, etc. Dette tilsier at eierne av vannforsyningsanlegget bør ha et bevisst forhold til hvordan ledningskartverket sikres sammenholdt med hvordan anleggene sikres fysisk.

I mangel av myndighetssignaler om informasjonssikkerhet, har styret i Norsk Vann anbefalt at ledningskartverk ikke bør gjøres fritt tilgjengelig på internett[44]. En må videre være klar over at mange vann- og avløpsvirksomheter har lagt ut mye informasjon om f.eks. sine driftskontrollsystem på DOFFIN i forbindelse med anbud. Her er det behov for en kritisk gjennomgang av hvordan offentlige anbud gjennomføres, for å unngå at kritisk informasjon blir liggende åpent på internett.

Innsynssystemene for kart legges stadig oftere over på ulike portalløsninger, hvor data ligger lagret i skybaserte tjenester. I en krisesituasjon uten strøm og ekom, vil det

44) http://norskvann.no/images/pdf/ledningskartverk.pdf

fortsatt være viktig å lokalisere ledninger, kummer etc. En må sikre seg slik at en har tilgang til kartsystemet også i slike situasjoner. Det vil følgelig være behov for off-line modeller, som virker selv om kommunikasjon og nett er nede. Synkronisering og lagring av data under slike krisehendelser er mindre viktig. Det som er viktig er at en har tilgang (tilgjengelighet) til riktig informasjon om VA-infrastrukturen og dette vil kanskje særlig være viktig under en hendelse.

3.5. Entreprenører med tilgang til kartdata – fordeler og ulemper

Mange vann- og avløpsvirksomheter deler ledningsdata digitalt til eksterne aktører, slik som entreprenører og rørleggere som har oppdrag for virksomheten. Vann- og avløpsvirksomheten har for eksempel digitale kartløsninger som er tilgjengelig via nettbrett og som kan brukes i felt. Vann- og avløpsvirksomheten etablerer da en ny bruker i løsningen, som entreprenøren kan benytte i forbindelse med gjennomføringen av prosjektet. Dette gir åpenbare fordeler både for vann- og avløpsvirksomheten og for entreprenøren, men medfører også noen mulige digitale betenkeligheter:

- Vil entreprenøren bare ha tilgang til aktuelt område, eller vil de få tilgang til ledningsdata i hele kommunen?
- Hvordan kan vann- og avløpsvirksomheten sikre seg at data slettes etter at prosjektet er ferdigstilt?

Løsningen kan være at leverandører av kartløsninger gjør det mulig å gjøre bare deler av kartgrunnlaget tilgjengelig. Dette vil også sikre at en har en geografisk oversikt over hvilke data som er utlevert til hvilken entreprenør i løpet av flere prosjekter. Det må også være enkelt å administrere tilgangen til de eksterne, for eksempel når brukeren slettes av kommunen når prosjektet er ferdig.

Kommune		**Entreprenør/rørlegger**	
Fordeler	**Ulemper**	**Fordeler**	**Ulemper**
Enkel overlevering av ledningsdata til entreprenør	Vanskelig å avgrense området som blir tilgjengelig. Data kan komme på avveie.	Enkel og praktisk tilgang til ledningsdata	Informasjonssikkerheten hos entreprenør er en mulig sårbarhet for vann- og avløpsvirksomheten

3.6. Sjekkliste for planleggingshjelp ved oppgradering av driftskontroll VA

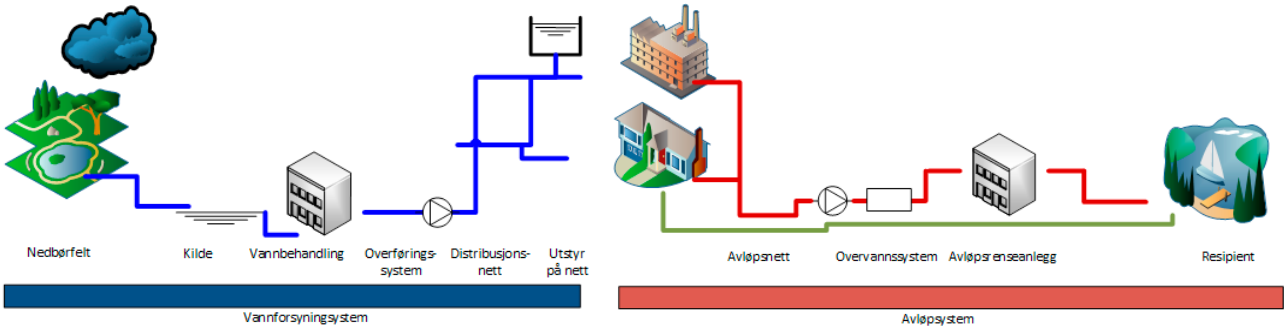
Driftskontrollsystem er en viktig del av IKT-infrastrukturen i vannbransjen. Punktlisten under kan brukes som en sjekkliste for hva en må tenke på i forbindelse med oppgradering driftskontrollsystemet.

- **Risikoanalyse:** Vurdere risiko vedrørende driftsovervåkningen, samt hvilke konskvenser som kan oppstå.
- **Nettverkstruktur:** Planlegge nettverkstopologi der det tas hensyn til sikkerhet, og hvor nettet skal segmenteres i soner med forskjellige tillitsnivåer av hengig av funksjon og sikkerhet. Trafikken mellom sonene filtreres.
- **Program autentisering:** Blokker kjøring av ikke-autoriserte programmer.
- **Administrator-rettigheter:** Begrense tildeling av administrator-rettigheter.
- **Kryptert nettverk:** Eksponerte nettverk må sikres mot dataavlytting ved hjelp av kryptering.
- **Kryptert VPN:** Det skal benyttes kryptert VPN for kommunikasjon utenfor egne nettverk.
- **Nettverksutstyr:** Vurder valg av nettverksutstyr opp mot sikkerhets- og funksjonalitetskravene.
- **Oppdatering:** Etablere rutiner for programvareoppdateringer av operativsystemene og applikasjonene.
- **Tilgang:** Begrense tilgang til nettverket. Unngå at usikre enheter som f.eks usb-enheter, gjeste- eller leverandørmaskiner får tilgang til sikre soner.
- **Antivirusprogram:** Windowsbaserte enheter installeres med antivirusprogram, og det etableres rutine for oppgradering.
- **Brukerautentisering:** Personlig brukerkontoer med brukernavn og passord, samt etablering av flere tilgangsnivåer.
- **Backup:** Etablering av backup-rutiner, samt testing av «recovery».
- **Opplæring:** Informasjon og opplæring til sluttbrukerne for sikker bruk.

Listen er utarbeidet med bistand fra Ørjan Sætre i Trondheim Bydrift.

4. Verdivurdering av informasjonen i vann- og avløpsvirksomheter

Det er mange ulike typer informasjon som må registreres og samles inn for at vann- og avløpssystemene skal virke. Figur 17 viser den urbane vannsyklus med de enkelte elementer som vann og avløpssystemet består av.



Figur 17. *Illustrasjon av de ulike elementer som et vann og avløpssystem består av og som det trengs informasjon om som må klassifiseres og verdivurderes.*

Det er mange ulike arbeidsprosesser og tilhørende datakilder/informasjon som registreres og benyttes gjennom hele verdikjeden, og det viktig å ha oversikt og kontroll på denne informasjonen. De enkelte typer informasjon som finnes, heretter også benevnt informasjonsaktiva, må klassifiseres og verdivurderes. Begrepet verdi defineres som en «ressurs som hvis blir utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen».

Norsk Vann rapport 229/2018 *Veileder for sikring av vannforsyningen mot tilsiktede uønskede hendelser* beskriver kort et generelt rammeverk for verdivurdering av ulike aktiva som finnes innen vannforsyningsvirksomheter, slik som funksjoner, fysiske objekter, nøkkelpersonell og informasjon. Arbeidet er basert på NSM sin generelle rapport om verdivurdering[45)]. I det følgende beskrives et mer detaljert rammeverk for verdivurdering som er mer tilrettelagt for informasjon og data. Arbeidet som beskrives i det følgende er inspirert av Oslo VAV sitt arbeid knyttet til verdivurdering av informasjon, i tillegg til veiledning i klassifisering av informasjon utgitt av Uninett[46)].

Det er eieren av informasjonen som selv må vurdere verdien av sine data. Det vil si at hver enkelt vann- og avløpsvirksomhet må utføre en individuell verdivurdering av sine data basert på den verdi som dataene har for den enkelte virksomhet. De enkelte informasjonsaktiva bør vurderes ut fra en rekke faktorer, slik som om data behandles eksternt og om en eventuell leverandør har tilgang til data. Verdivurdering av informasjon er viktig for å sikre at virksomhetskritisk innhold vil bli tatt vare på, behandlet og avhendet i samsvar med interne og eksterne krav og beste praksis. Det er spesielt viktig å klassifisere dataene før man blottlegger informasjonen, f.eks. ved å lagre informasjon hos skyleverandører, gjøre ledningsdata tilgjengelig for entreprenører eller gjøre data tilgjengelig på mobile enheter som lesebrett og smarttelefoner.

45) https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veiledning-i-verdivurdering-200903.pdf

46) https://www.uninett.no/sites/default/files/ufs136-v2_0.pdf

Eksempler på datakilder som er aktuelle for vann- og avløpsvirksomheter er vist i tabellen under. Tabellen er ikke ment å være komplett, men kan være en inspirasjonskilde som en kan tenke ut i fra og komplettere.

Element	Opplysninger (data/informasjon)
Vannkilde og nedbørfelt	Beskrivelse av vannkilde og vannuttak, sårbarheter, kildekapasitet, etc. Etter drikkevannsforskriften § 17 bokstav f skal vannverkseiere registrere koordinatene til inntakspunkt i alle råvannskildene, inkludert brønner, som inngår i vannforsyningssystemet.
	Grunnvannsbrønner og alarmfunksjoner
	Råvannsinntak og alarmfunksjoner
Vannbehandlingsanlegg	Anleggets utforming (kart, tegninger, koordinater)
	Skallsikring, alarmfunksjoner, adgangskontroll, overvåking
	Styring og overvåkningssystem (SCADA, fjernkontrollsystem)
	Drift og overvåkning (driftsdata, driftsinstruksjoner, rutiner)
Vanndistribusjonssystem (ledninger, høydebasseng, pumpestasjoner, ventilkammer, utstyr, tunneler)	Vital ledningsnettinformasjon (ledningskart, koordinater, rørmateriale etc.)
	Kritiske elementers utforming (høydebasseng, pumpestasjoner, kummer etc.)
	Styring og overvåkning av vannledningsnettet (fjernkontrollsystem)
	Hydraulisk nettmodeller som beskriver funksjonen til ledningsnettet
	Skallsikring, alarmfunksjoner, adgangskontroll, overvåking om kritiske elementer (høydebasseng, pumpestasjoner, viktige vannkummer, felleskulverter)
	Vannforsyningssystemet til særlig sårbare abonnenter (sykehus og andre samfunnskritiske bygninger)
	Kritiske elementers utforming (tunneler, pumpestasjoner, kummer etc.)
	Styring og overvåkning av avløpsnettet (fjernkontrollsystem)
	Hydrauliske nettmodeller som beskriver funksjonen til ledningsnettet
	Skallsikring, alarmfunksjoner, adgangskontroll, overvåking om kritiske elementer (avløpstunneler, pumpestasjoner, viktige kummer, overløp, felleskulvert)
	Rørinspeksjoner
	Stikkledninger
Avløpsrenseanlegg	Anleggets utforming (kart, tegninger, koordinater)
	Skallsikring, alarmfunksjoner, adgangskontroll, overvåking
	Styring og overvåkningssystem (SCADA, fjernkontrollsystem)
	Drift og overvåkning (driftsdata, driftsinstruksjoner, rutiner)
Generell informasjon	Anbudsdokumenter
	Prosjekteringsdata
	ROS-analyser
	Beredskapsplanverk
	Driftsplaner
	FDV dokumentasjon

For hver av de enkelte datatyper/informasjonsaktiva bør følgende registreres slik at vann- og avløpsvirksomheten senere kan rangere og beskytte de ulike dataene tilstrekkelig:

- **Eier.** Hvilken organisatorisk enhet, rolle eller arbeidsprosess eier informasjonen (driftsavdeling, planavdeling, GIS-avdeling etc.)
- **Hjemmel.** Referanse til regulatoriske dokument (lov, regel, forskrift, styrende dokument) hvor oppbevaring og/eller disponering framgår.
- **Lagringssted.** Navnet på systemet og/eller fysiske arkiv der informasjonsobjektet oppbevares (elektronisk journal, saksbehandlingssystem, økonomisystem, ledningsdatabase, osv.).
- **Personopplysninger.** Hvis informasjonen inneholder eller kan inneholde personopplysninger er dette av særlig viktighet å vite. Se også mer om personopplysninger i kapittel 7. Det må angis om det er snakk om personopplysninger eller sensitive personopplysninger.
- **Skylagring.** Det må angis om informasjonen er egnet for skylagring eller ei. Enkelte informasjonstyper kan ikke lagres i skyen på grunn av lovkrav (sikkerhetsloven) eller er ikke egnet for skylagring av andre grunner, slik som lagring utenfor EU/EØS-området. Dette gjelder for eksempel sensitive personopplysninger og virksomhetskritisk informasjon som bør lagres nasjonalt.
- **Lagres hos leverandør.** Det må angis om data kan og skal håndtere og lagres hos en leverandør. Det vil da være aktuelt med en databehandleravtale; dersom det er personopplysninger skal det være en databehandleravtale.
- **KIT** (Konfidensialitet - Integritet - Tilgjengelighet)
    - **Konfidensialitet.** Grad av beskyttelse som kreves for informasjonen.
    - **Integritet.** Hvor viktig det er at ikke informasjonen kan endres av uvedkommende eller ved et uhell? Hvis det er krav til at informasjonen ikke skal endres av uvedkommende eller ved et uhell må den sikres spesielt.
    - **Tilgjengelighet.** Hvor lenge kan man akseptere at informasjonen er utilgjengelig? 1 time, 1 dag, 1 uke eller 1 måned? Noen systemer eller tjenester er kritiske for at VA-virksomheten skal fungere og levere sine tjenester. Fjernkontrollsystemet er for eksempel et slikt eksempel. For en del vann- og avløpsvirksomheter kan man drifte anleggene manuelt, men selv for disse blir det slitsomt å drifte manuelt over lang tid (flere dager).

KIT kriterier for utfylling av profil for informasjonsaktiva

Konfidensialitet nivå:	høy	Informasjon kun åpen for enkelte i vann- og avløpsvirksomheten. Tap av informasjon kan gjøre katastrofal eller alvorlig skade på virksomhetens interesser, samarbeidspartnere, enkeltpersoner eller samfunnet om de kommer uautoriserte i hende.
	medium	Informasjonen må ha en viss beskyttelse og kan være tilgjengelig for både eksterne og interne, med kontrollerte tilgangsrettigheter (entreprenører, rådgivere etc.). Benyttes dersom det vil kunne forårsake en viss skade for vann- og avløpsvirksomheten hvis informasjonen blir kjent for uvedkommende.
	lav	Informasjon åpen for alle uten særskilte tilgangsrettigheter, også eksterne. Liten eller ingen skade.
Integritet nivå:	høy	Svært høye krav til kompletthet, nøyaktighet og gyldighet (regnskap, juridiske dokumenter). Informasjon som direkte påvirker beslutninger og der feil kan føre til betydelig skade, omdømmetap, fatale konsekvenser eller verditap for vann- og avløpsvirksomheten, samarbeidspartnere, enkeltpersoner eller samfunnet.
	medium	Høye krav til kompletthet, nøyaktighet og gyldighet (f.eks. ekstern presentasjon av etaten). Informasjon som i noen grad påvirker vann- og avløpsvirksomhetens beslutningsprosesser.
	lav	Normale krav til kompletthet, nøyaktighet og gyldighet (vanlige dokumenter, e-post, notater). Informasjon der feil i liten eller ubetydelig grad kan påvirke vann- og avløpsvirksomhetens beslutningsprosesser.
Tilgjengelighet nivå:	høy	Informasjon der utilgjengelighet vil føre til store forsinkelser/etterslep, vil føre til kritiske situasjoner eller stans i vesentlige tjenesteleveranser.
	medium	Informasjon der utilgjengelighet kan føre til noe forsinkelse/etterslep og påvirke servicenivå.
	lav	Informasjon der utilgjengelighet har liten eller ingen betydning for vann- og avløpsvirksomheten.

Nivåer innen KIT	**Verdi**
Høy	3
Medium	2
Lav	1

Prosjektet har utarbeidet et regneark som kan brukes som mal for å verdivurdere informasjonsaktiva i vann- og avløpsvirksomheter. Skjermbilde for løsningen er vist i tabell 2 - neste side. Regnearket kan lastes ned sammen med rapporten fra Norsk Vann sine hjemmesider.

Eksempel på klassifisering av data innen vannbransjen (Excel-ark kan lastes ned sammen med rapporten).

Identifisert aktiva	Eier	Hjemmel	Lagrings-sted	Lagres hos leverandør	Sikkerhets-loven?	Person-informasjon
Beredskapsplanverk	Drift	DVF	Lokalt, perm	Nei	Nei	Nei
Dagbok/driftshendelser	Drift		Gemini VA	Ja	Nei	Nei
Drifts- og vedlikeholdsplaner	Drift			Nei	Nei	Nei
Hovedplaner	Plan			Nei	Nei	Nei
Hydrologiske data	Plan		Server	Nei	Nei	Nei
Kommunikasjonsstrategi	Drift			Nei	Nei	Nei
Ledningsnettdatabase	GIS	Arkivlov, Offentlighetslov		Ja	Nei	Nei
osv						
Rammeavtaleliste	Plan	Arkivlov,		Nei	Nei	Nei
ROS-analyser	Plan	DVF	Server	Nei	Nei	Nei
Tegninger høydebasseng	GIS	PBL,		Ja	Nei	Nei
Tegninger overløp	GIS	PBL		Ja	Nei	Nei
Vannkilde	Plan	DVF		Nei	Nei	Nei

+++++

Sensitive personopplysninger	Skylagring	K	I	T	K	I	T	Totalvurdering av kritikalitet
Nei	Nei	lav	medium	høy	1	2	3	6
Nei	Ja	lav	medium	medium	1	2	2	5
Nei		lav	medium	medium	1	2	2	5
Nei	Ja	lav	medium	medium	1	2	2	5
Nei	Ja	lav	medium	medium	1	2	2	5
Nei	Ja	lav	medium	høy	1	2	3	6
Nei	Ja	lav	medium	medium	1	2	2	5
Nei		lav	lav	medium	1	1	2	4
Nei		lav	medium	medium	1	2	2	5
Nei		lav	medium	medium	1	2	2	5
Nei		lav	medium	medium	1	2	2	5
Nei		lav	medium	medium	1	2	2	5

5. Sikkerhet i SKY

Avhengig av hvem du spør, så er nettskyen enten noe som oppstod for en ti års tid siden, eller bare en inkrementell utvikling av måten vi har drevet databehandling på siden 1950-tallet. Det som er klart, er at skyen ikke er i kjelleren din; bruker du nettsky, blir dine data lagret og/eller behandlet på noen andres datamaskin.

På lik linje med enhver annen form for tjenesteutsetting, må behandlingsansvarlig vurdere hvilke data det er forsvarlig å behandle i en nettskyløsning. Et godt sted å starte, vil være Datatilsynets veiledning[47]. NSM har også laget en ny veiledning *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting* (i skrivende stund ennå ikke utgitt, men søk på NSM sine hjemmesider i tiden fremover) hvor det beskrives krav til kompetanse hos virksomheter som vurderer tjenesteutsetting/skytjenester. I det følgende vil vi presentere nødvendig bakgrunn, anbefalinger og en sjekkliste for vann- og avløpsvirksomheter som ønsker å bruke skytjenester.

Offentlige virksomheter, slik som kommuner og kommunalt eide selskap, skal vurdere risiko ved valg av nye IKT-løsninger. Dette inkluderer også bruk av skytjenester. Første steg må alltid være å kontakte kommunens IKT-drift. Sentrale beslutninger rundt valg av skyleverandører kan legge føringer som trumfer mange andre hensyn.

47) https://www.datatilsynet.no/globalassets/global/regelverk-skjema/veiledere/skytjenester-2016.pdf

5.1. Hva er skytjenester?

Skytjenester (cloud computing) er en felles betegnelse på alt fra dataprosessering og datalagring, til programvare som er tilgjengelige fra eksterne serverparker tilknyttet internett. De eksterne serverparkene kan like gjerne være lokalisert i Norge som i andre land.

Skyløsninger oppleves som effektive, på grunn av enkel tilknytning via en nettleser, fleksibilitet, mobilitetsfrihet og stor skalerbarhet for brukeren. Mange leverandører garanterer god sikkerhetskopiering og generelt god fysisk sikring av data, og mange tilbyr ulike former for krypteringstjenester. Løsningene presenteres ofte som rimeligere enn tradisjonelle løsninger. Skyløsninger er godt beskrevet i NOU 2015: 13 Digital sårbarhet – sikkert samfunn, og er også beskrevet i ulike veiledninger fra Datatilsynet.

De viktigste driverne for å ta i bruk skytjenester er:

- **Økonomi.** Fordi en skytjeneste ikke krever lokal infrastruktur, blir både investeringer og kostnader til drift av IKT påvirket. I tillegg vil oppdateringer kunne utføres enklere.
- **Skalering.** Skytjenester tilbyr nærmest ubegrenset kapasitet for databehandling og lagring. Ressursene i nettskyen blir benyttet bare når det er bruk for dem.
- **Sikkerhet.** Bruk av skytjenester kan gi økt teknisk IKT-sikkerhet når leverandøren har bedre kompetanse og ressurser enn kunden. Dette gjelder både fysisk sikring av lokalene hvor servere er plassert og raskere oppdatering av programvarene. Mange kommuner og selskap mangler tilgang på teknisk kompetanse. Backup er vanligvis en del av tjenesteporteføljen når en kjøper skytjenester, inkludert lagring av data på ulike geografiske steder (redundans).
- **Fleksibilitet.** Bruk av skytjenester gjør det i mange tilfeller lettere å legge til rette for at tjenestene (for eksempel et saksbehandlingssystem eller innsynsløsning for kart i en kommune) kan benyttes fra ulike lokasjoner og på ulike klienter (PC, nettbrett, mobil).
- **Tilgjengelighet.** Skytjenester har også påvirkning på tilgjengeligheten til løsningene for innbyggerne i kommunen. Skytjenestene tilbyr f.eks. overvåkning av driften og hjelp til feilsøking. Dette vil bidra til høyere oppetid for løsningene.

Markedet for skytjenester domineres av store globale selskaper (Google, Microsoft og Amazon). Norske IT-selskaper bygger gjerne sine egne løsninger inn i løsningene til de globale aktørene.

I 2017 anbefalte Kommunal og moderniseringsdepartementet alle statlige virksomheter å ta i bruk skytjenester når det ikke foreligger spesielle hindringer for det, for eksempel særskilte krav til sikkerhet iht. sikkerhetsloven. I Nasjonal strategi for bruk av skytjenester slår Kommunal- og moderniseringsdepartementet fast at offentlige virksomheter skal (og private virksomheter

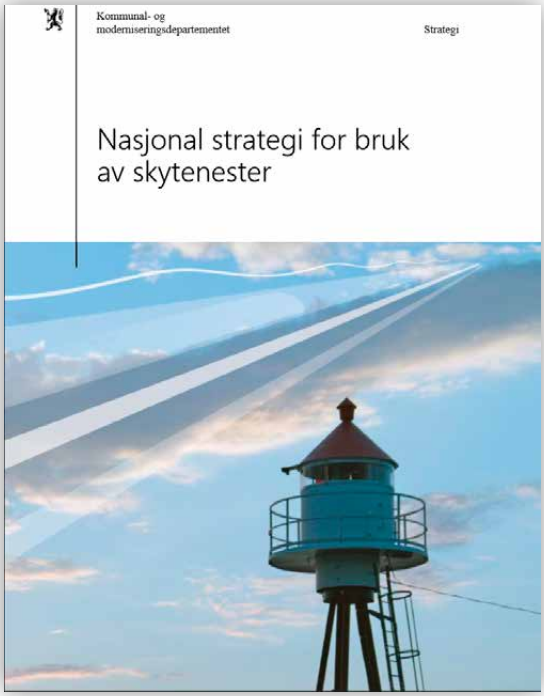
Figur 18. *Bilde fra datasenteret til stor skyleverandør (foto: Google)*

bør) gjennomføre risikovurderinger ved større endringer som ved etablering av nye digitale tjenester.

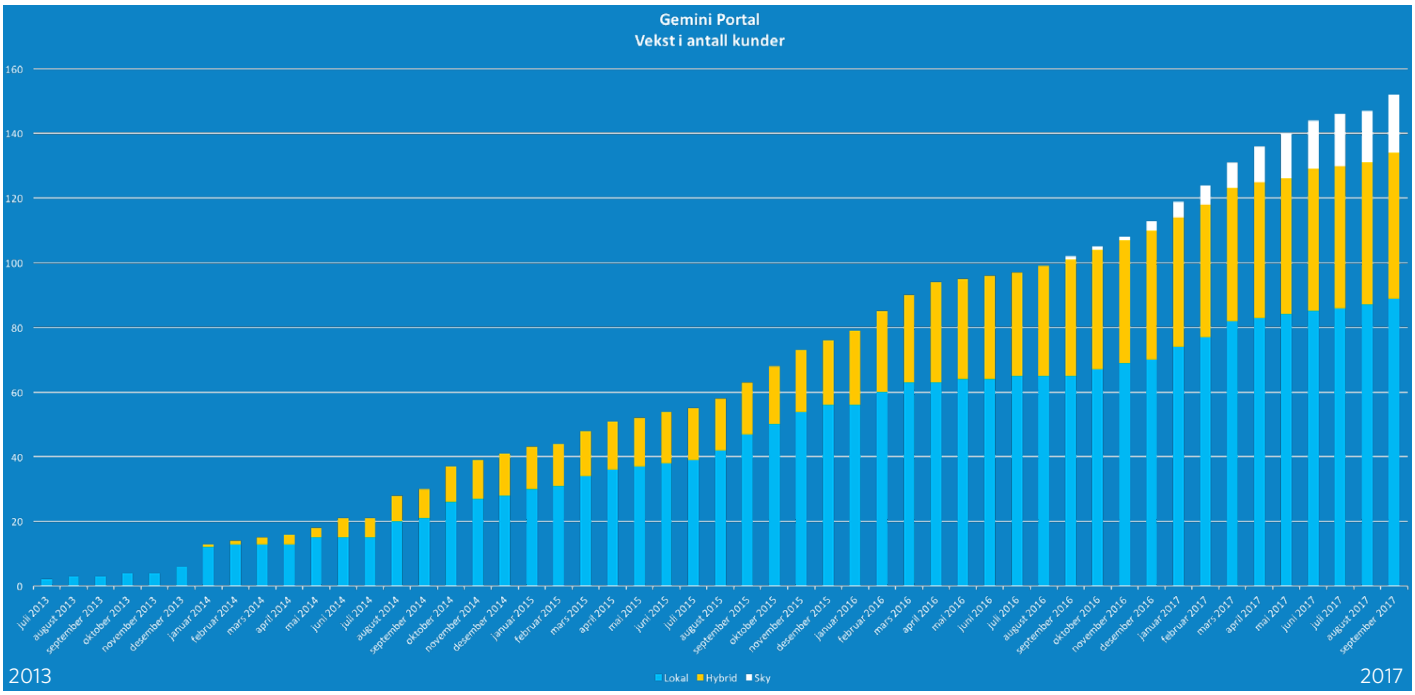
Skytjenestene kan leveres på ulike måter, avhengig av hva vann- og avløpsvirksomheten har bruk for. Det er vanlig å skille mellom programvare som tjeneste (Software as a Service, SaaS), plattform som tjeneste (Platform as a Service, PaaS) og infrastruktur som tjeneste (Infrastructure as a Service, IaaS):

- Programvare som en tjeneste (SaaS) innebærer at kunden i utgangspunktet ikke har kontroll over verken applikasjoner, nettverk, servere, operativsystemer eller lagringsmuligheter, dette er det leverandøren som har ansvaret for. For eksempel leverer Powel mange av sine nye løsninger som en SaaS. I en SaaS vil tjenesteleverandøren typisk tilby mer programvare og tjenester enn dersom man «kun» leverer en IaaS.
- Plattform som tjeneste (platform as a service - PaaS), inkluderer alt som trengs for å støtte bygging og levering av digitale tjenester. En plattform kan være en database eller et utviklingsmiljø eller testmiljø som blir kjørt hos skyleverandøren. Kunden har kontroll over egne applikasjoner, men har ikke kontroll over nettverk, servere, operativsystemer eller lagringsmuligheter.
- Infrastruktur som tjeneste (infrastructure as a service - IaaS), som gjelder levering av datainfrastruktur som en tjeneste over et nettverk. Kunden har kontroll over relevante applikasjoner, servere, operativsystemer og lagringsmuligheter, samt i noen tilfeller visse elementer i nettverket (for eksempel på brannmursiden).

Skytjenester kan leveres på mange ulike måter:



- En *offentlig tilgjengelig sky* (Public Cloud) er skytjenester som blir solgt på det åpne markedet, dvs. som standardiserte løsninger som stort sett er like for alle kunder. De største og mest kjente leverandørene er Google, Amazon og Microsoft. Den offentlige skyen kan også være en del av arkitekturen til



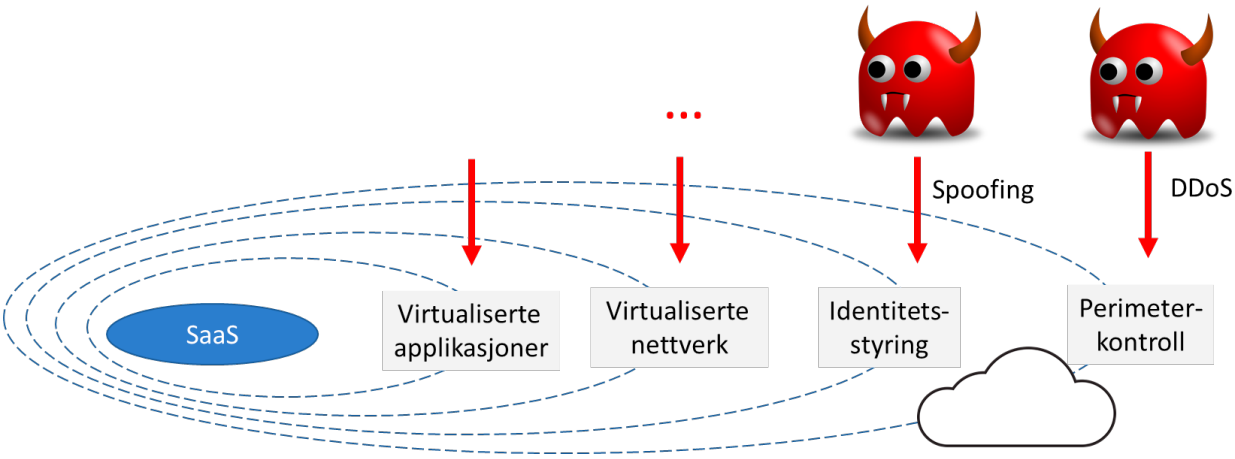
Figur 19. *Eksempel på utvikling av skytjenester innen vannbransjen.* *Lokal* *Hybrid* *Sky*

programvareleverandører som tilbyr sine løsninger levert over internett.
- En *privat tilgjengelig sky* (Private cloud) som benyttes innenfor en bedrift eller et konsern, dvs. et eget datasenter for bedriften.
- En *hybrid sky* (Hybrid Cloud) er en kombinasjon av de to alternativene. En virksomhet som bruker en kombinasjon av den offentlige skyen og et tradisjonelt lokalt driftet IKT-system (en privat sky), kaller vi det hybrid sky.

Figur 19 viser utviklingen av innsynsløsningen Gemini Portal, hvor en ser en historisk utvikling der en har gått fra ren lokal installasjon, til hybrid løsning, og nå flere og flere kommuner som velger rene skyløsninger.

Mange vann- og avløpsvirksomheter vil kunne ha informasjon som de av ulike årsaker synes er vanskelig å plassere i en offentlig sky. Det kan for eksempel være informasjon som er kritisk for virksomheten, skjermingsverdige objekter eller at en i tjenesten ikke vil være avhengig av forsinket behandling/svikt i kommunikasjon med utlandet. Samtidig kan offentlige skytjenester være et godt alternativ når en trenger ekstra kapasitet, som en sikker plass for backup eller for informasjon som er kritisk eller inneholder informasjon som må lagres lokalt. En arkitektur med en hybrid sky gjør at vann- og avløpsvirksomheten både kan utnytte fordelene med den offentlige skyen, og samtidig holde kritiske komponenter under egen kontroll. Risikoanalysen som kommunene skal gjennomføre skal avdekke hva som egner seg for hvilke typer data.

Figur 20 viser hvordan en tjenestetilbyder som utvikler SaaS- løsninger er beskyttet av et digitalt forsvar i dybden når tjenestene kjøres som en skytjeneste.

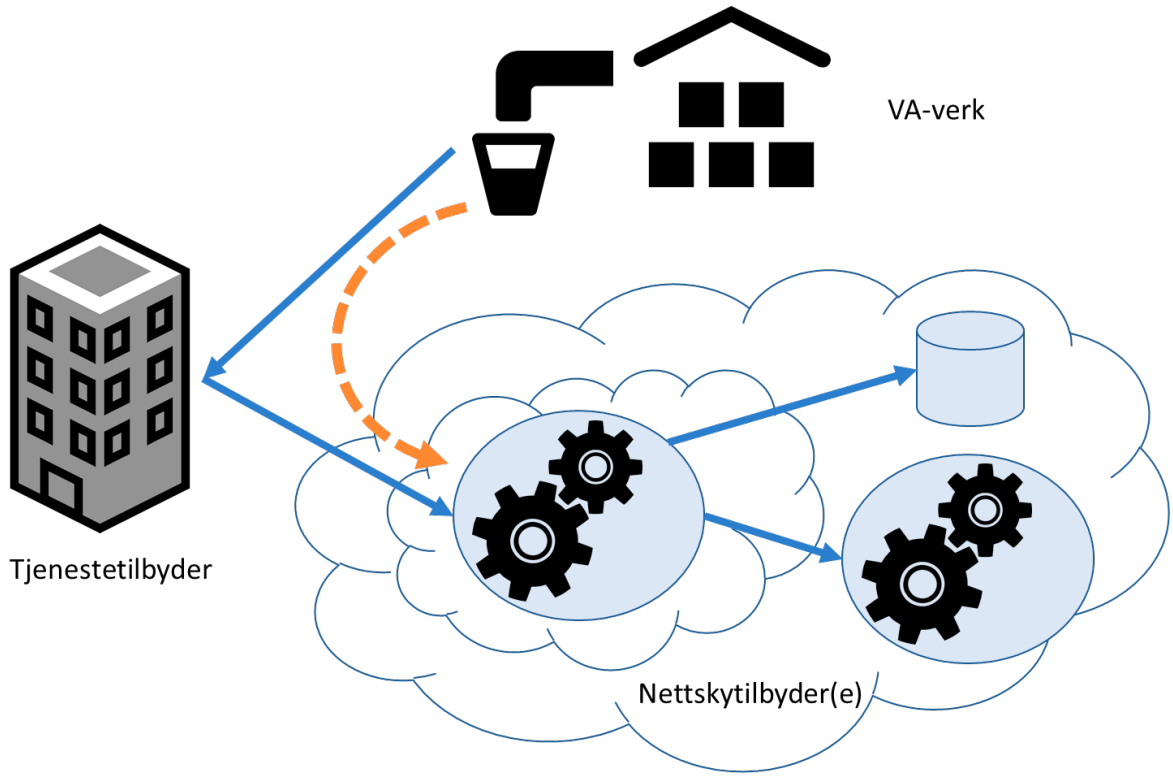


Figur 20. *Illustrasjon av forsvar i dybden når en bruker skytjenester.*

5.2. Sjekkliste for skytjenester

I det følgende beskrives en sjekkliste for skytjenester og hva vann- og avløpsvirksomheter må tenke på. Sjekklisten er generell, og de store skyleverandørene vil typisk kunne oppfylle kravene, men bestiller i kommunen må ofte spesifisere hva behovene er. Dette setter krav til bestillerkompetanse.

I figur 21 illustreres virkeligheten for mange vann- og avløpsvirksomheter: Kommunen har en avtale med en tjenestetilbyder rundt drift, overvåkning, etc. av en løsning. Tjenesten som tilbys er i realiteten en skytjeneste som kjører i datasenteret til en (stor) kommersiell nettskyleverandør (typisk: Azure, AWS, Google). Denne kan bruke andre nettskyressurser (lagring eller andre tjenester) hos samme eller andre nettskyleverandører. Det trenger ikke være åpenbart at tjenesten som tilbys er en nettskytjeneste. Tilgangen vil typisk skje gjennom en nettadresse som tilhører tjenestetilbyderen, f.eks. www.WeakCoal.no.



Figur 21: *Forholdet mellom vann- og avløpsvirksomheter, tilbydere, og nettskytjenester.*

I det følgende beskrives en rekke krav som vann- og avløpsvirksomheter bør stille til en skytjeneste ved inngåelse av en avtale. Enkelte krav vil kunne være komplementære. Kravene er hentet fra SINTEF-rapporten *Cloud Security Requirements*[48], med tilpasninger for vann- og avløpsvirksomheter. Som nevnt, er det imidlertid viktig at valg av skytjeneste gjøres i samråd med kommunens IKT-avdeling, ettersom eventuelle tidligere sentrale beslutninger kan legge føringer for valgmulighetene.

Krav til lagring av data

Kategori	Beskrivelse	Sikkerhetskrav
Kryptering	Sørge for at data ikke lagres i klartekst når de ikke er i bruk	
		Alle data er kryptert når de er lagret. Det vil være tilstrekkelig å kryptere disken (også virtuell disk)
		Hver vann- og avløpsvirksomhets data krypteres med en egen nøkkel
Fysisk plassering	Sørge for at data lagres i en spesifikk geografisk lokasjon	
		Man bør velge nettskytjenester som tilby lagring innenfor EU
		Iht. arkivloven skal alle arkivverdige data (inkl. sikkerhetskopi) fysisk lagres i Norge. Dersom nettskytjenesten ikke er basert i Norge, kan dette løses ved å ha en løpende kopi av data i Norge, samt at en sikkerhetskopi også lagres i Norge.
Isolasjon	Sørge for at alle data isoleres fra andre kunders data	
		Informasjon skal segmenteres slik at alle data fra en gitt kunde segregeres fra andre data tilhørende andre kunder hos leverandøren. Dette betyr at data fra vann- og avløpsvirksomhet X ikke vil være synlige/tilgjengelige for vann- og avløpsvirksomhet Y selv om de bruker samme nettskyleverandør.
Eierskap	Sørge for at kunden beholder eierskap til egne data	
		Alle data som kunden lagrer i skyløsningen forblir kundens eiendom
		Det skal utarbeides en databehandleravtale med leverandøren. Dette kan både være med en leverandør som utvikler egne løsninger ved bruk av skyleverandøren, men også direkte med skyleverandør dersom det er aktuelt.
		Leverandøren kan ikke bruke data for egne formål
		Kunden beholder eierskap til egne data også etter tjenestekontraktens utløp.
Portabilitet	Sørge for portabilitet av kundedata	
		Data må ikke "låses" inne av skyløsningen, men skal kunne eksporteres til et nærmere bestemt format når kunden ønsker det
Integritet	Sørge for riktighet og konsistens i kundens data	
		Dataintegritet opprettholdes for alle data som lagres i skyløsningen
Sletting	Sørge for forskriftsmessig sletting av kundens data	
		Alle replikerte data skal slettes innen nærmere angitt tid når det kreves. For personverndata er dette nærmere beskrevet i ny personopplysningslov (GDPR)
Back-up	Sørge for at backup gjøres på en ordentlig måte	
		Det skal utføres backup av data i skyløsningen minst daglig.

48) https://infosec.sintef.no/wp-content/uploads/2015/08/Cloud-Security-Requirements-v2.0.pdf

		Det skal ukentlig tas en lokal backup av dataene i skyen (read only). Denne skal kunne brukes også når skyløsningen ikke er tilgjengelig Hvis ROS-analyse er gjennomført og oppetid hos leverandør etc. er vurdert til å være tilstrekkelig, kan evt. rest-risiko aksepteres og krav om lokal speiling frafalles
		Oppbevaring av sikkerhetskopier Daglig: Hver daglig sikkerhetskopi bør oppbevares i 21 dager Ukentlig: Hver sikkerhetskopi fra fredager bør oppbevares i 12 uker. Dette gjelder også lokal speiling for de som har dette. Månedlig: Hver sikkerhetskopi fra siste fredag i måneden bør oppbevares i seks måneder Kvartalsvis: Hver sikkerhetskopi fra siste fredag i januar, april, juli og oktober bør oppbevares i to år
		Sikkerhetskopier lagret i skyen skal sjekkes ved gjenoppretting til skyggesystem minst en gang i måneden. ROS-analyse kan medføre krav om hyppigere frekvens. Det må avklares med leverandør om hvordan dette kan dokumenteres
		Lokal backup (speiling) sjekkes ukentlig (når den lages)
		Leverandøren skal oppgi garantert tid for gjenoppretting av sikkerhetskopi. Lokal speiling er tilgjengelig når den er laget Sky backup hvis ikke lokal backup
		Sikkerhetskopier skal oppbevares geo-redundant et annet sted i tillegg til hvor dataene oppbevares til vanlig.
		Sikkerhetskopiering: Daglig backup i skyen Avhengig av risikoanalyse: Ukentlig backup til lokal/nasjonal "speiling" – for beredskap dersom skyen er nede (tilfredsstiller arkivloven)

Dataprosesseringskrav

Kategori	Beskrivelse	Sikkerhetskrav
Isolasjon	Sørge for at alle data isoleres fra andre kunders data	
		All kundedata i minnet (RAM) skal isoleres fra andre kunders data
		Tilbyderen skal implementere mekanismer som sikrer at forskjellige virtuelle maskiner ikke påvirker hverandre.
		Data som sendes til tjenesten i forbindelse med en spesifikk forespørsel er ikke synlig for noen andre brukere av tjenesten
Monitorering	Sørge for at brudd på avtaler om aksepterbar bruk vil bli detektert	
		Oppførselen til kjørende Virtuelle Maskiner (VM) vil monitoreres kontinuerlig.
Fysisk plassering	Sørge for at data prosesseres på et nærmere bestemt sted	
		Alle data bør prosesseres i et datasenter innenfor EU/EØS-området
Migrering	Sørge for en sikker overføring av VMer mellom forskjellige fysiske datamaskiner	
		Alle VM-data er kryptert under VM-migrering

Dataoverføringskrav

Kategori	Beskrivelse	Sikkerhetskrav
Kryptering	Sørge for at data aldri overføres i klartekst	
		Opp- og nedlasting av kundedata er kryptert
		Alle kommunikasjonssteg bør krypteres
		Ende-til-ende-kryptering anbefales der det er mulig (se figur 11)
Integritet	Sørge for nøyaktighet og konsistens av kundedata	
		Alle kundedata skal være integritetsbeskyttet i forbindelse med opp- og nedlasting
Isolering	Sørge for at alle data isoleres fra andre kunders data	
		Nettskytilbyderen tilbyr nettverksisolasjon mellom kunder. Dette betyr bl.a. at trafikk fra en vann- og avløpsvirksomhet ikke kan avlyttes av en annen vann- og avløpsvirksomhet.

Aksesskontrollkrav

Kategori	Beskrivelse	Sikkerhetskrav
Aksesskontroll for administrasjon	Sørge for sikker tilgang til skyens administrasjonsgrensesnitt (dashboard)	
		Tilbyderen bruker en anerkjent passordpolitikk, fokusert på lengde og kompleksitet av passord. Tidligere har anbefalingene vært å skifte passord hver 3. måned (NV 2013). Dette har man nå gått bort fra og anbefaler istedenfor lenger passord (https://www.nsm.stat.no/blogg/passordrad/)
		Tilbyderen støtter multi-faktor autentisering
		Tilbyderen støtter tredjeparts autentiseringsløsninger for enkel pålogging (SAML/OpenID). Dette kan f.eks. være bruk av Azure AD (Active Directory) system for brukerhåndtering
Aksess-kontroll for brukere	Sørge for sikker tilgang for nettskybrukere	
		Det finnes et system for å opprette, oppdatere, sette på vent (suspend) og slette brukerkonti, for å fjerne ansattes tilgang når de forlater virksomheten, og nullstille glemte, tapte eller stjålne akkreditiver (f.eks. passord)
		Alle nettskybrukere skal ha egen brukerkonto med tilhørende passord (eller tilsvarende). Fellesbrukere med felles passord skal ikke benyttes.
		Tilgang til skytjenester bør være rollebasert
		Ved behov skal det være mulighet for å skille ut data som ikke skal vises på bestemte plattformer (bærbare enheter, etc.). F.eks. for skjermingsverdige objekter
Fysisk adkomstsikring	Sørge for at datasentre er sikret på en betryggende måte	Det er stor forskjell fra skyleverandør til skyleverandør. Store leverandører har typisk god fysisk sikring, så disse punktene er mest aktuelle for eventuelle mindre skyleverandører.
		Datasentrene er beskyttet med fysiske sikkerhetsperimetre (gjerder/vakter/overvåkning/låser)
		Sikrede områder overvåkes, og tilgang er begrenset til autorisert personell
		Tilbyderens personell som har tilgang til kundedata har vært gjenstand for bakgrunnssjekk (f.eks. klarering)
		Tilgang til applikasjon, program eller kildekode er begrenset til autoriserte ansatte med tjenstlig behov

Krav til sikkerhetsprosedyre

Kategori	Beskrivelse	Sikkerhetskrav
Revisjon	Sørge for at nettsky-tjenester kan revideres	Det er stor forskjell fra skyleverandør til skyleverandør. Store leverandører kan forventes å ha jevnlige eksterne revisjoner. Små leverandører må kanskje utføre på forespørsel
		Kunden skal kunne få tilgang til en uavhengig revisjonsrapport som dokumenterer sikkerheten til nettskytjenesten
		Revisjonen bør omfatte fysiske, tekniske og organisasjonsmessige sikkerhetstiltak, og dokumentere hvorvidt disse er hensiktsmessige for den aktuelle nettskytjenesten.
		I tilfelle av sammensatte nettskytjenester, bør vurderingen omfatte forsikringer om at sikkerheten til hvert ledd av leverandørkjeden som kan antas å være involvert i behandling av kundens data tilfredsstiller sikkerhetskravene
Klassifisering	Sørge for at nettsky-tjenesten tilfredsstiller en bestemt klassifisering	
		Nettskytilbyderen skal jevnlig gjennomføre sikkerhetsrevisjon av bruk av nettsky-tjenesten
Mottiltak	Sørge for at nettsky-tjenesten implementerer forsvarsmekanismer	Dette er viktig for å sikre oppetiden til systemet.
		Brannmurer er installert og konfigurert
		Mekanismer for å beskytte mot eller minske effekten av DoS/DDoS er installert og konfigurert
		Mekanismer for datatapsbeskyttelse er implementert
		All programvare er oppdatert med seneste sikkerhetsoppdateringer. Viktig å avklare ansvarsforhold
		Tjenesten er satt opp med en redundant konfigurasjon
Testing	Sørge for at sikkerheten til en nettskytjeneste kan testes.	
		Tilbyderen bør foreta jevnlige sårbarhetsskanninger.
Deteksjon	Sørger for at angrep og inntrengninger vil bli detektert	
		Et inntrengningsdeteksjonssystem (IDS) har blitt installert og konfigurert korrekt
		Disker, minne og nettverk skannes jevnlig for skadevare
		Det er etablert prosedyrer for overvåkning og jevnlig gjennomgang av logger. Det finnes løsninger som overvåker logger jevnlig f.eks. Tiger Eye/Cyber Observer.
Varsling	Sørge for at kunder får informasjon om sikker-hetsrelaterte endringer	
		Leverandør må informere sine kunder om eventuelle sårbarheter som oppdages. Bør inkluderes i avtaler. Tidsfrister for varsling kan inngå i avtalen.
		Tilbyderen kan framskaffe informasjon om sikkerhetsoppdateringer og kontroll-mekanismer som er på plass
		Når en har varslet om en sårbarhet må en i etterkant informere om hvilke oppdateringer som er utført.
		Endringer i geolokasjon (hvor server til skytjenesten er lokalisert) må oppgis til kunde.

Gjenoppretting	Sørge for at nettsky-tjenesten kan gjenopp-rettes etter et angrep	
		Tilbyderen vedlikeholder periodiske sjekkpunkter av tilstanden til virtuelle maskiner
		Tilbyderen garanterer at dersom systemet kompromitteres, vil tjenesten kunne re-etableres på en sikker måte innen et bestemt tidsintervall.
		Tilbyderen foretar jevnlig (minst en gang per måned) tester av gjenopprettelse av sikkerhetskopier
Nøkkelhåndtering	Sørge for sikker hånd-tering av kryptografiske nøkler	
		Leverandøren skal på forespørsel kunne dokumentere en sikker måte for nøkkel-håndtering
Transparens	Sørge for transparens til nettskytjenesten og dens sikkerhetsmekanismer	
		Leverandøren skal på forespørsel kunne fremlegge (men ikke nødvendigvis utlevere) dokumentasjon på arkitektur, design av løsningen og sikkerhetsmekanismer.

Hendelseshåndteringskrav

Kategori	Beskrivelse	Sikkerhetskrav
Respons	Sørge for at det er et system på plass for å respondere på sikkerhets-hendelser	
		Tilbyderen bør utarbeide periodiske sammenstillinger som viser omfang av hendelser (f.eks. antall DoS angrep siste periode)
		Hendelser bør kategoriseres etter et veldefinert mønster
		SLA bør inneholde krav til tidsfrister for når tilbyder skal senest respondere for en gitt kategori hendelser
		Leverandøren skal ha et bevisst forhold til håndtering av sikkerhetshendelser, gjerne basert på en anerkjent standard eller retningslinje.
Logging	Sørge for at tilbyderen logger sikkerhets-hendelser	
		Tilbyderen skal oppbevare revisjonslogger med registrert aktivitet for privilegerte brukere, autoriserte og u-autoriserte aksessforsøk, system-avvik, og informasjons-sikkerhetshendelser
		Leverandøren skal på forespørsel kunne fremlegge logg for hendelser relevant for den enkelte kunde
Rapportering	Sørge for at tilbyderen rapporterer sikkerhets-hendelser til kundene	
		SLA bør inneholde frister for når sikkerhetshendelser skal rapporteres til kunde
		Varsler bør gis i henhold til en forhåndsdefinert varlingsprosedyre og kommunika-sjonskanal
		Ved hendelser må leverandør estimere reparasjonstid. Ved store avvik må ny infor-masjon gis.
Etterforskning	Sørge for at tilbyderen kan tilby nødvendig støtte til etterforskning	
		Leverandøren bør ha retningslinjer for hvordan bevismateriale kan samles inn og overleveres til relevante myndigheter i forbindelse med sikkerhetshendelser knyttet til lovbrudd eller andre juridiske forhold.

Krav til sammensatte tjenester

Kategori	Beskrivelse	Sikkerhetskrav
Tjenesteutsetting	Krav til tredjeparts tjeneste-tilbydere	
		Tilbyder vil kun sette ut tjenester eller deler av tjenester til leverandører som behandler data i EU/EØS
Overvåkbarhet	Sørge for kundens evne til å inspisere hvordan tjenesten er satt sammen	
		Kunden bør ha mulighet for å inspisere hvilke komponenter tjenesten er satt sammen av
		Ved endringer må leverandør informere om endringer i de sammensatte tjenestene (f.eks. ny underleverandør)

Andre kilder til ytterligere informasjon

Det finnes mange gode kilder til mer informasjon om sikkerhet i nettskyen. Organisasjonen Cloud Security Alliance (CSA) har laget arbeidsgruppen *Top Threats to Cloud Computing*[49], hvor de dokumenterer de 12 viktigste truslene i nettskyen. Dette er et pågående prosjekt, hvor den siste rapporten fra 2016 identifiserer følgende trusler:

1) Brudd og tap av sensitive opplysninger
2) Utilstrekkelig identitets- og tilgangskontroll
3) Usikre grensesnitt og API
4) Systemsårbarheter
5) Kapring av brukerkonti
6) Ondsinnede innsidere
7) Avanserte persistente trusler
8) Tap av data
9) Utilstrekkelig forarbeid
10) Misbruk og ondsinnet bruk av skytjenester
11) Tjenestenekting
12) Utfordringer med delt teknologi

CSA har også laget en oversikt over sikkerhetsmekanismer som adresserer disse og andre trusler[50]. Open Web Application Security Project (OWASP) har et eget prosjekt som også har laget et utkast til en topp-10 liste[51], denne avviker noe fra CSA sin, men slike lister vil uansett oppleve en naturlig variasjon fra år til år.

49) https://cloudsecurityalliance.org/group/top-threats

50) https://cloudsecurityalliance.org/group/cloud-controls-matrix/

51) https://www.owasp.org/images/3/3f/OWASP_Cloud_Top_10.pdf

Nyttige lenker til nettsider om skytjenester:

Difi: https://www.difi.no/artikkel/2017/03/anskaffelse-av-skytjenester

NorSIS: Veiledning for IT-outsourcing https://nettvett.no/veiledning-for-it-outsourcing/

Datatilsynet: Skytjenester – en veiledning https://www.datatilsynet.no/Teknologi/Skytjenester---Cloud-Computing/

NSM: Sikkerhetsfaglige anbefalinger ved tjenesteutsetting (veiledning under utarbeidelse som vil bli tilgjengelig via NSM sine nettsider)

6. Sikkerhetskultur

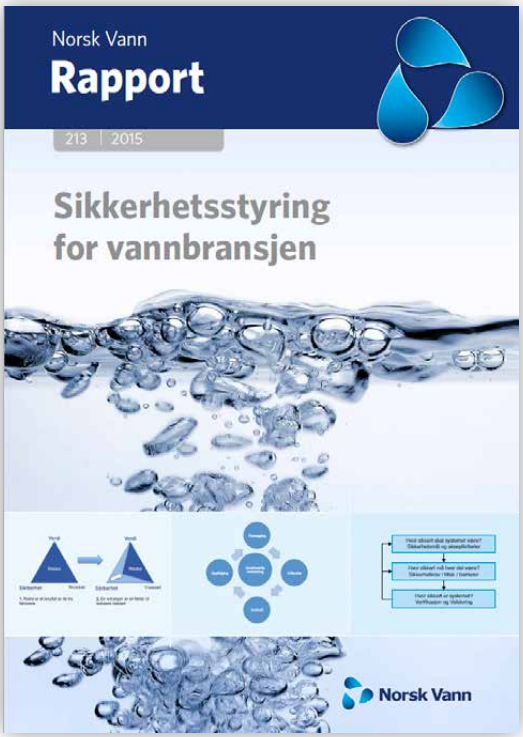
For å lykkes med arbeidet med informasjonssikkerhet i en organisasjon må det etableres en god sikkerhetskultur. Alle organisasjoner har en sikkerhetskultur, spørsmålet er om den er god eller dårlig. Sikkerhetskultur handler om adferd knyttet til sikkerhet, for eksempel med tanke på informasjon eller objekter. NSM definerer sikkerhetskultur som summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.

For vann- og avløpsvirksomheter setter for eksempel drikkevannsforskriften krav til nødvendig sikkerhetskultur i organisasjonen i § 10 som omhandler «forebyggende sikring». I sin veiledning til bestemmelsen har Mattilsynet skrevet følgende:

«Skal de forebyggende tiltakene for sikring få effekt, må alle som gjør oppgaver for vannforsyningssystemet, få opplæring. En forutsetning for å skape den nødvendige sikkerhetskulturen er at alle forstår hva som er grunnlaget for sikkerhetskravene, og handler riktig ut fra dette.»

Det foreligger allerede minst to Norsk Vann rapporter som i ulike grad omhandler sikkerhetskultur. Norsk Vann rapport 213/2015[52] *Sikkerhetsstyring for vannbransjen* gir en oversikt over ulike sjekkpunkter som bør passeres på veien til etableringen av en sikkerhetsstrategi for den lokale vann- og avløpsvirksomheten, og peker også på hvordan sikkerhetskulturen kan måles. Norsk Vann rapport 229/2018 Veileder for sikring av vannforsyningen mot tilsiktede uønskede hendelser beskriver viktigheten av å ha en god sikkerhetskultur ut i fra målet om å sikre vann- og avløpsinfrastrukturen fysisk. Om ansatte omgår sikkerhetsrutiner og slipper inn ukjente gjennom en fysisk dør uten å sjekke hvem vedkommende er, eller om de ansatte slipper inn ukjente gjennom digitale dører eller bakdører (ved å trykke på lenker etc.) beror i begge tilfeller på mangler ved sikkerhetskulturen.

Det viser seg at medarbeideres feil og manglende kompetanse er en viktig faktor for at sikkerhetshendelser oppstår i virksomheter. Mørketallsundersøkelsen fra



2016[53] peker også på brukeren/ansatte som den viktigste bakenforliggende årsaken til de fleste uønskede hendelser knyttet til informasjonssikkerhet. Det er dermed viktig at medarbeidere kjenner virksomhetens sikkerhetsrutiner og forstår hvorfor rutinene må følges. Medarbeideres sikkerhetsbevissthet må økes for eksempel ved hjelp av opplæringspakker. Mange virksomheter bruker Nasjonal sikkerhetsmåned som arrangeres i oktober hvert år til å gi medarbeidere innsikt i trusselbildet og hvordan de ved å følge virksomhetens sikkerhetsprosesser kan minske faren for uønskede hendelser. Videre bør de ansatte få opptrening i hvordan sosial manipulering virker.

52) www.norskvann.no/kompetanse/va-bokhandelen/rapporter/product/507-r213-sikkerhetsstyring-for-vannbransjen

53) https://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen_2016.pdf

6.1. Etablere en cybersikkerhetskultur

En god cybersikkerhetskultur må etableres. Eksempelvis har SINTEF utarbeidet en egen opplæringspakke[54] kalt «OJ!», som fokuserer på informasjonssikkerhet. Målrettede kampanjer av typen «Tenk før du klikker!», «Gi aldri fra deg passord!», «Kan e-posten være lureri?» og «Husk å låse PCen før du forlater den!», gir de ansatte enkle råd og sikrer kontinuerlig fokus på arbeidet med informasjonssikkerhet.

I arbeidet med innføring av ny personopplysningslov vektlegges viktigheten av å inkludere arbeidet med personvern som en integrert del av virksomhetens kontinuerlige arbeid med informasjonssikkerhet. Når de nye rutinene er på plass vil det være viktig at alle ansatte følger rutinene slik at personvernet sikres. En god sikkerhetskultur er en forutsetning for at også arbeidet med personvern lykkes.

Hva kjennetegner så en vann- og avløpsvirksomhet som har en god sikkerhetskultur/ organisasjonskultur med hensyn på informasjonssikkerhet?

Det finnes flere rammeverk og metoder for å bygge kultur for informasjonssikkerhet. Et eksempel er Security Culture Framework (SCF)[55], som opererer med fire komponenter:

- Metrikker
- Organisasjon,
- Tema
- Planlegger

I henhold til SCF må man først definere mål, og så måle nåtilstanden. Deretter må man involvere de rette folkene og bruke kjennskap til målgruppen for å bygge tillit. Videre må man velge ut hvilke konkrete aktiviteter man skal innføre, og til slutt planlegge og utføre aktivitetene, med jevnlige målinger for å kunne dokumentere forbedring.

SCF opererer med to forskjellige typer mål; resultatmål og læringsmål. Resultatmål fokuserer på konkrete hendelser (som man typisk ønsker færre av), f.eks. at antall kryptovirustilfeller skal reduseres med 90%. Læringsmål fokuserer på læringsaktiviteter, f.eks. om viktigheten av å ikke klikke på linker i e-post og alternative måter å dele informasjon på.
Aktivitetene det henvises til her kan være opplæringstiltak som illustrert i Figur 22. SCF har mange eksempler på typer av aktiviteter, fra nanolæring, større kurs,

54) https://infosec.sintef.no/wp-content/uploads/2015/09/OJ---En-smak-av-sikkerhetskultur.pdf

55) https://securityculturefra mework.net/

Figur 22. *Eksempel på opplæringspakke for ansatte i informasjonssikkerhet for å bedre sikkerhetskulturen*

videoer, reklamemateriell, til forskjellige former for kunnskapstester.

Den amerikanske organisasjonen SANS har også mange nyttige tips og maler innenfor sikkerhetskultur, med et fokus på sikkerhetsbevissthet[56]. SANS dekker områder som å sørge for støtte fra interessenter, fokusere på sikkerhetsbrudd og tap av sensitive opplysninger, krav for etterlevelse av lover og regler, hvordan få sikkerhetsbevisstheten til å sitte, identifisering og prioritering av risiko, metrikker for måling av effekten av bevissthetsprogrammet, og metrikker for å måle menneskelig oppførsel. SANS tilbyr også en rekke kurs innen dette området.

56) https://www.sans.org/security-awareness-training/resources/security-awareness-planning-toolkit

6.2. Organisatoriske forhold

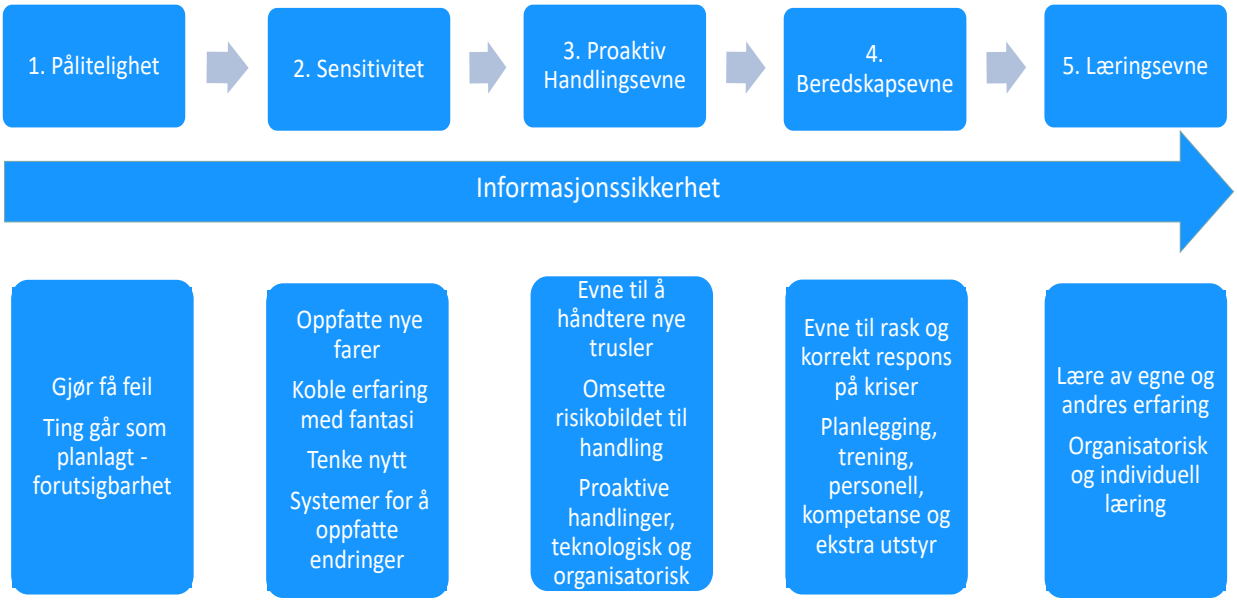
Et rammeverk for hvordan for eksempel en vann- og avløpsvirksomhet kan analysere organisatoriske forhold med tanke på økt robusthet, er beskrevet i rapporten etter 22. juli kommisjonen[57]. I det følgende har vi tilpasset denne modellen til også å gjelde informasjonssikkerhet i vann- og avløpsvirksomheter.

I følge modellen må en organisasjon som skal operere sikkert over tid, utvikle fem ulike sett av organisatoriske egenskaper (se figur 23):

- Organisasjonen må være **pålitelig.** Det vil si at virksomheten er godt planlagt og styrt, med gode rutiner og tydelige ansvars- og myndighetsforhold fra øverst til nederst i organisasjonen. Informasjonssikkerhet er altså forankret hos den øverste ledelsen i vann- og avløpsvirksomheten, og ledelsen har klart å formidle dette også nedover i organisasjonen. Medarbeiderne har IKT-kompetanse nok til å håndtere arbeidsoppgavene, og kompetansen utvikles etter behov, gjennom opplæring og trening. Vann- og avløpsvirksomheter som er pålitelige kjennetegnes av at det normalt gjøres få feil. En god grunnsikring av vann- og avløpsvirksomheten vil være viktig for å oppnå få feil i daglig drift. Med en god grunnsikring vil mindre endringer i trusselbildet ikke utgjøre noen vesentlig fare for anlegget.
- Organisasjonen må være **sensitiv.** Det vil si at en har prosedyrer, rutiner, praksis og kultur som gjør at en oppdager og forstår mulige faresignaler innenfor eller utenfor virksomheten, også når dette forutsetter at en kombinerer informasjon på nye og ikke-planlagte måter. Eventuelle nye sårbarheter og trusler knyttet til informasjonssikkerhet fanges opp både eksternt og internt i organisasjonen. Trender i data, slik som økning i antall ikke-autoriserte påloggingsforsøk til driftskontrollsystemer, må registreres slik at en tidlig kan fange opp at noe er under utvikling. I tillegg må de ansatte være sensitive selv for å se etter eventuelle ting som er unormalt og som kan representere en mulig trussel.
- Organisasjonen må utvikle **proaktiv handlingsdyktighet.** Det vil si at en har kompetanse, rutiner og reaksjonsevne, slik at tilløp stoppes før de utvikles til mer omfattende og alvorlige hendelser. I mange situasjoner innebærer det at organisasjonen må ha evne til improvisasjon, fordi det kan oppstå situasjoner som en ikke har forestilt seg eller har forberedt seg på. Med proaktiv handlingsdyktighet inkluderes planlegging og iverksetting av forebyggende tiltak, og nødvendig organisering for å kunne håndtere ekstraordinære situasjoner.
- Organisasjonen må ha reaktiv **handlingsdyktighet/beredskapsevne.** Det vil si at en må være i stand til å håndtere de uønskede hendelser og ulykker som måtte inntreffe, slik som tekniske sammenbrudd, brann, eller terrorhandlinger. Dette inkluderer også evne til å gjenopprette funksjoner slik at DKS raskt kommer opp og går igjen etter en hendelse. For å få god beredskapsevne mot IKT-sikkerhetshendelser, må det trenes. Sammenlignet med vanlige øvelser i vann- og avløpsvirksomhetene, kjennetegnes IKT-sikkerhetshendelser av at en gjerne må knytte hendelser som inntreffer med lengre tids mellomrom til hverandre. For eksempel kan en forstyrrelse som oppstår en dag ha en sammenheng med tap av en bærbar PC som inneholdt ledningskartverket som ble mistet tre måneder tidligere.
- Organisasjonen må ha **evne til læring.** Det vil si at en må være i stand til å registrere og analysere ulykker og hendelser og bruke dette som grunnlag for både formell og uformell erfaringsoverføring og læring. Det er også viktig å trekke lærdom ut av det som går som det skal, og å lære fra egne og andres erfaringer knyttet til svikt av IKT-systemer via egne systemer for hendelseshåndtering[58]. Medlemskap i organisasjoner slik som KraftCERT vil kunne være nyttig ut i fra flere av disse aspektene som nevnt over.

57) P. M. Schiefloe, «En modell for samfunnssikkerhet,» NTNU Samfunnsforskning AS, 2012. Vedlegg til 22. juli kommisjonen sin rapport.

58) http://infosec.sintef.no/informasjonssikkerhet/2014/06/god-praksis-for-hendelseshandtering/



Figur 23. *Modell for organisatorisk informasjonssikkerhet (basert på Schifloe, 2012)*

Et sentralt poeng her er at de ulike kapabilitetene/ evnene forutsetter ulike organisatoriske egenskaper, og det er ikke nødvendigvis noen sammenheng mellom disse. En veldrevet vann- og avløpsvirksomhet kan operere pålitelig og «uten feil», men likevel være dårlig rustet til å oppdage tilløp som ikke er definert inn som noens bestemte ansvarsområde. Særlig kan dette være aktuelt for IKT-systemer siden informasjonssikkerhet og IKT tradisjonelt sett ikke inngår i kjernevirksomheten til en vann- og avløpsvirksomhet. En tilsynelatende robust organisasjon kan også vise seg å være ute av stand til å håndtere uventede hendelser dersom organisasjonen mangler evne til improvisasjon. Rammeverket som beskrives i figur 23 bør også sees i sammenheng med NSM sine grunnprinsipper for IKT-sikring (Figur 13). Det er i praksis snakk om de samme fasene som skal håndteres, men ut i fra henholdsvis et teknisk og organisatorisk perspektiv.

7. Ny personopplysningslov og relevans for vannbransjen

EUs forordning om personvern[59] (General Data Protection Regulation (GDPR)), som skal gjøres til norsk rett gjennom en ny personopplysningslov, trer i kraft 25. mai 2018. Det nye regelverket gir virksomheter nye plikter og enkeltpersoner nye rettigheter. Justis- og beredskapsdepartementet har utarbeidet et nytt forslag til personopplysningslov som gjør EUs forordning direkte gjeldende som norsk rett, men med en del nasjonale tillegg som forordningen åpner opp for[60]. I Norge har gjeldende personopplysningslov dekket mange av de aspekter som den nye personvern-forordningen legger opp til. Virksomheter som i dag følger gjeldende personopplysningslov, vil oppleve små endringer.

Bakgrunnen for EUs personvernforordning var blant annet behovet for harmonisering av regelverket i EU og et ønske om å gjenetablere tilliten til personvernet for digitale tjenester. Digitaliseringen av samfunnet er også en av driverne bak forordningen. Bruk av persondata er det «nye økonomiske gullet», som dersom en sammenstiller det kan gi verdifull informasjon. Det har tidligere vært krav om med konsesjon fra Datatilsynet for å kunne registrere persondata, men dette vil ikke lenger være nødvendig. Nå vil virksomhetene selv få et større ansvar. Det settes krav til virksomhetenes behandling av personopplysninger, og til varsling ved eventuelle brudd på sikringen av personopplysningene. I tillegg vil størrelsen på overtredelsesgebyrene øke kraftig.

Alle virksomheter som samler inn eller bruker personopplysninger plikter, både etter gammel og ny personopplysningslov, å ha oversikt over hvilke personopplysninger det er snakk om, hvor de kommer fra og det rettslige grunnlaget for behandlingen.

Personvern og IKT-sikkerhet følger hverandre. Et godt personvern fordrer gode sikkerhetsmekanismer. Ivaretakelsen av personvernet er en forutsetning for en vellykket digitalisering i samfunnet, og dette inkluderer også personverndata innen vannbransjen. Godt personvern er nøkkelen til at brukerne skal ha tillit til digitale løsninger. NOU 2009: 1 Individ og integritet – Personvern i det digitale samfunnet (Personvernkommisjonen) definerer personvern:

Personopplysningsvern dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold.

Det skilles mellom *personopplysninger og sensitive personopplysninger.* Datatilsynet skriver at *personopplysning* er en opplysning eller vurdering som kan knyttes til deg som enkeltperson, slik som navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) og fødselsnummer (både fødselsdato og personnummer). Opplysninger om adferdsmønstre er også regnet som personopplysninger. Opplysninger om hva du handler, hvilke butikker du går i, hvilke tv-serier du ser på, hvor du beveger deg i løpet av en dag og hva du søker etter på nettet er alt sammen personopplysninger. *Sensitive personopplysninger* er opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger.

Ansvaret for å behandle personopplysninger ligger alltid hos den enkelte juridiske enhet, det vil si den enkelte vann- og avløpsvirksomhet. I praksis betyr det at det

59) https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf

60) https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/?utm_source=www.regjeringen.no&utm_medium=epost&utm_campaign=Høringer-06.07.2017

skal utnevnes en person (en såkalt personvernrådgiver) som har det daglige ansvar for persondata og som til enhver tid kan dokumentere at kravene overholdes, dvs.:

- Vi vet hvilke data vi samler inn og kan begrunne behovet for dette
- Vi har en holdning og opplyser om denne
- Vi gjør hva vi sier og kan dokumentere dette

Selv om en medarbeider er utpekt som personvernrådgiver, så ligger det juridiske ansvaret hos ledelsen i kommunen/selskapet.

Databehandler

En databehandler er en virksomhet (f.eks. Powel) som behandler data på vegne av en annen virksomhet, den såkalte behandlingsansvarlige (kommune/selskap). Etter den nye personopplysningsloven følger databehandleres plikter av en databehandleravtale mellom den behandlingsansvarlige og databehandleren. Loven pålegger dem å ha en slik avtale. Den nye forordningen vil inneholde selvstendige plikter også for databehandlerne, som kommer i tillegg til de plikter som avtales i databehandleravtalen. Dette gjelder særlig knyttet til:

- Sørge for informasjonssikkerhet (artikkel 32)
- Umiddelbart varsle den behandlingsansvarlige ved avvik (artikkel 33)

Databehandleravtale

For å ivareta krav til informasjonssikkerhet hos eksterne IT-leverandører som behandler opplysninger på vegne av vann- og avløpsvirksomheten, skal det foreligge en databehandleravtale. Dersom tjenesten behandler personopplysninger, må en ha en databehandleravtale med skytjenesteleverandøren. Datatilsynet har laget en mal[61] for databehandleravtaler, som er et godt utgangspunkt.

Det er ikke nødvendig å inngå databehandleravtale med en leverandør som bare selger en lisens eller et abonnement som er installert lokalt hos vann- og avløpsvirksomheten, hvis produktet ikke har tilgang til personopplysninger (f.eks. Office-pakken). Men dersom leverandøren kan få tilgang til systemene via fjernsupport, bør det inngås en databehandleravtale. En del vann- og avløpsvirksomheter benytter gratis fildelingstjenester, slik som Dropbox. Det er lite sannsynlig at vann- og avløpsvirksomheten får Dropbox til å underskrive en databehandleravtale, da Dropbox bare vil henvise til standardbetingelsene. Slike tjenester bør ikke benyttes for lagring av personopplysninger.

Underleverandør

Et viktig spørsmål knyttet til databehandler er også bruken av eventuelle underleverandører. En underleverandør er en virksomhet som behandler personopplysninger på vegne av en databehandler. Forordningen setter krav til at dataansvarlig skal godkjenne alle underleverandører skriftlig. Dvs. om en IT-leverandør bruker Microsoft eller Amazon sine skytjenester som en del av sin leveranse, skal dette i forkant godkjennes skriftlig av vann- og avløpsvirksomheten. Dersom underleverandøren ikke følger reglene, er det databehandleren som er ansvarlig ovenfor den behandlingsansvarlige.

Overtredelsesgebyr

Dersom pliktene i den nye personopplysningsloven ikke overholdes, kan det ilegges et maksimalt gebyr på 20 millioner euro eller 4% av årsomsetningen, dersom denne er høyere. Datatilsynet skal i den enkelte sak sikre at overtredelsesgebyret er virkningsfult, står i forhold til overtredelsen, og virker avskrekkende. Overtredelsesgebyret vil også gjelde for offentlige virksomheter, slik som kommuner og kommualt eide selskap. I høring til ny lov er det foreslått at offentlige virksomheter skal kunne ilegges overtredelsesgebyr med faste summer (ikke %).

Trusselen om høye gebyrer har gjort at den nye personvernforordningen har fått stor oppmerksomhet, men respekten for den enkeltes personvern bør i seg selv være en god nok grunn til å jobbe systematisk med personvern.

Datatilsynets anbefalinger

På Datatilsynets hjemmeside[62] er det samlet mye stoff om de nye personvernreglene. Datatilsynet har laget en kortversjon av hva de nye personvernreglene vil bety og hva som må gjøres for å forberede seg til at loven trer i kraft. I det følgende er det gitt en del kommentarer knyttet til relevansen for vannbransjen.

1. Alle norske virksomheter får nye plikter. Alle virksomheter (dvs. både kommuner og kommunalt eide selskap) må sette seg inn i den nye lovgivningen og finne ut hvilke nye plikter som gjelder dem. Ledelsen må få på plass rutiner for å overholde de nye pliktene. Alle ansatte må følge de nye rutinene når reglene trer i kraft. Selv om andre deler av kommunen (f.eks. skole, helse) vil ha større utfordringer med personvernforordningen enn vann- og avløpsvirksomhetene, vil man også innen vann og avløp måtte ha fokus på temaet.

61) https://www.datatilsynet.no/regelverk-og-skjema/veiledere/databehandleravtale/

62) https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/

2. Alle skal ha en forståelig personvernerklæring. Informasjon om hvordan din virksomhet behandler personopplysninger skal være lett tilgjengelig og skrevet på en forståelig måte. Det nye lovverket stiller strengere krav til informasjonens form og innhold enn dagens lovgivning. Alle skal gi god informasjon om hvordan de behandler personopplysninger. Kravene til hva slags informasjon man må gi er litt ulike hvis man samler inn opplysningene fra den registrerte selv, eller om dere henter dem fra noen andre. Det må komme klart frem hva som er formålet med behandlingen av personopplysninger, hva slags personopplysninger som behandles, og med hvilken rett en samler inn persondata (behandlingsgrunnlaget). Dersom behandlingsgrunnlaget er samtykke, skal det informeres om retten til å trekke samtykket tilbake. Dette betyr at dersom en innbygger har meldt inn en hendelse om vann i kjelleren via kommunen sin løsning og senere ønsker å slette disse dataene, skal dette la seg gjøre både teknisk og praktisk.
3. Alle skal vurdere risiko og personvernkonsekvenser. Dersom et tiltak utgjør en stor risiko for personvernet, må virksomheten også utrede hvilke personvernkonsekvenser tiltaket kan ha. Datatilsynet har laget en veileder for konsekvensvurdering63). Innsamling og avanserte analyser av data fra smarte vannmålere kan være et eksempel på et slikt tiltak. Hvis utredningen viser at risikoen er stor og vann- og avløpsvirksomheten ikke selv kan redusere den, skal Datatilsynet involveres i forhåndsdrøftelser.
4. Alle skal bygge personvern inn i nye løsninger. De nye reglene stiller krav til at nye tiltak og systemer skal utarbeides på en mest mulig personvernvennlig måte. Dette kalles innebygd personvern/«privacy by design». Eksisterende løsninger må også oppdateres, slik at persondata sikres. Den mest personvernvennlige innstillingen skal være standard i alle systemer. Sørg for å ha gode systemer for å ivareta de registrertes rettigheter, slik som retten til informasjon, rett til innsyn og rett til sletting. Systemene må også legge til rette for samtykkehåndtering, inkludert tilbaketrekking av samtykke. Dette må gjelde både for eksisterende og nye løsninger. Dette vil f.eks. gjelde for meldingstjenester som benyttes i mange kommuner i dag, hvor innbyggerne melder inn til kommunen om lavt trykk, brunt vann, vann i kjeller etc. via web, SMS eller telefon. Man må få aksept av personen, før eventuelt navn og telefonnummer registreres til hver enkelt melding. Uten et slikt aktivt samtykke, skal navn og nummer ikke knyttes til meldingen.
5. Mange virksomheter må utpeke en personvernrådgiver. Dette gjelder alle offentlige og mange private virksomheter. En personvernrådgiver er virksomhetens personvernekspert, og et bindeledd mellom ledelsen, de registrerte og Datatilsynet. Denne rådgiveren kan være en ansatt eller en profesjonell tredjepart/innleid.
6. Virksomheter som holder til utenfor Europa må også følge forordningen, dersom de tilbyr varer eller tjenester til borgere i et EU eller EØS land. Dette gjelder også om de ikke direkte tilbyr tjenester, men kartlegger adferden til europeiske borgere på nett. De som er etablert i flere land i Europa, skal bare trenge å snakke med personvernmyndighetene i det landet der de har sitt europeiske hovedkvarter.
7. Alle databehandlere får nye plikter. Databehandlere er virksomheter som behandler personopplysninger på oppdrag fra den ansvarlige virksomheten, f.eks. kommunen. Ofte er det snakk om leverandører av IT tjenester (Powel, Norkart etc.). De nye reglene pålegger databehandlere å ha rutiner for innsamling og bruk av personopplysninger. Databehandlere skal også si fra til oppdragsgiveren sin hvis de får instrukser som er i strid med loven. Oppdragsgiver skal godkjenne databehandlerens underleverandører. Databehandlere kan bli holdt økonomisk ansvarlig sammen med oppdragsgiveren. Datatilsynet har utarbeidet en mal for databehandleravtale som er oppdatert iht. ny personvernforordning.
8. Alle bør samarbeide i egne nettverk og følge bransjenormer. De nye reglene oppmuntrer til sektorvis utforming av retningslinjer og bransjenormer. Datatilsynet skal godkjenne bransjenormene, men slike detaljerte retningslinjer er ennå ikke utarbeidet for vann- og avløpsvirksomhetene, utover denne rapporten.
9. Alle får nye krav til avvikshåndtering. Reglene for håndtering av sikkerhetsbrudd blir strengere. Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles. Kort sagt skal man si fra raskere og oftere enn man gjør i dag, ved at avvik skal meldes innen 72 timer til berørte personer. De berørte personene skal varsles med et klart og tydelig språk.
10. Alle må kunne oppfylle borgernes nye rettigheter. Den enkeltes rett til å kreve sine personopplysninger slettet blir styrket. Dette kalles «retten til å bli glemt». Norske og europeiske borgere vil blant annet kunne kreve å ta med seg personopplysningene sine fra en leverandør til en annen i et vanlig brukt filformat. Dette kalles «dataportabilitet». De kan også motsette seg profilering. Alle henvendelser fra borgere skal besvares innen en måned.

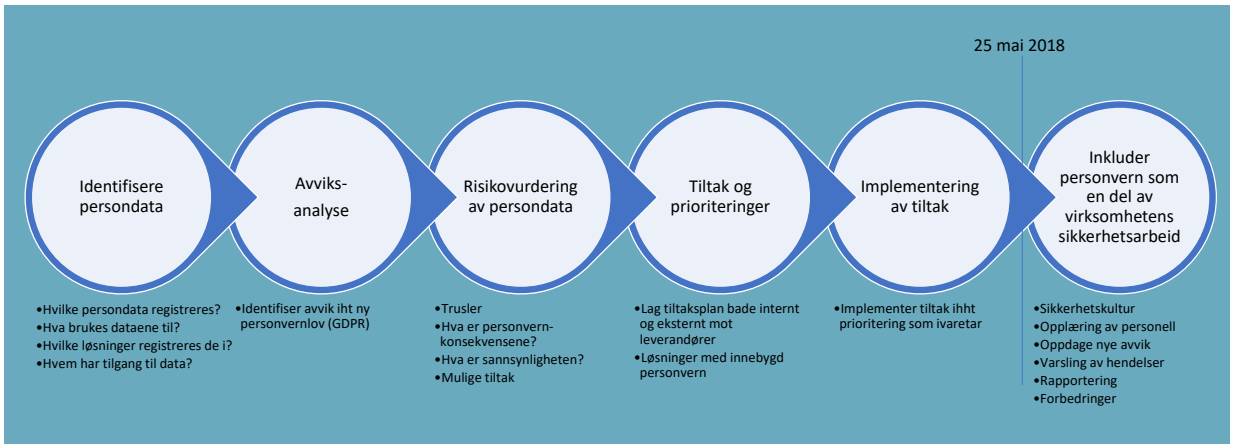
63) https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hvordan-vurdere-personvernkonsekvenser-pia/sporsmal-til-bruk-ved-kartlegging-av-konsekvenser-for-personvernet/

7.1. Kort og langsiktig plan for hva kommuner og selskap må gjøre for å forberede seg på ny personlov

Hva bør virksomhetene gjøre så raskt som mulig (helst før 25. mai 2018)?
Vann- og avløpsvirksomhetene bør ha en oversikt over hvilke personopplysninger en behandler. De som samler inn eller bruker personopplysninger skal ha oversikt over hvilke personopplysninger det er snakk om, hvor de kommer fra og hva som er det rettslige grunnlaget for behandlingen. Hvordan dette arbeidet kan utføres er det vist eksempel på i figur 24.

Hva bør virksomhetene gjøre etter 25. mai 2018?
Implementere arbeidet med personopplysningsloven som en integrert del av virksomhetens arbeid med informasjonssikkerhet. Dette inkluderer å revidere/utarbeide rutiner for behandling av personopplysninger. Er systemene som benyttes bygget for å ivareta kravet om innebygget personvern og dataportabilitet og personvern som standardinnstilling? Etablering av nye rutiner er et ledelsesansvar. Når de nye rutinene er på plass, vil det være viktig at alle ansatte følger rutinene slik at personvernet sikres.

Figuren under sammenstiller hva vann- og avløpsvirksomhetene må gjøre frem til 25. mai 2018 og i perioden etterpå.



Figur 24. *Plan for arbeidet med personvernsdata før og etter 25. mai 2018.*

7.2. Identifisering av personopplysninger som behandles av kommunen/selskapet

Vann- og avløpsvirksomhetene samler inn forskjellige typer data, både om ansatte og om abonnentene. Det er viktig å få oversikt over (dersom en ikke allerede har det) hvilke opplysninger som en samler inn i dag som er omfattet av personvernreglene. Data registreres i ulike løsninger og for hver løsning i virksomheten skal det vurderes om en registrerer persondata/sensitive persondata eller ikke. Dette gjelder både data som registres om abonnentene som en del av de ulike fagløsningene, men også persondata som registreres i ulike administrative støttesystemer, slik som e-post. I tillegg må virksomhetene ha oversikt over interne persondata for egne ansatte. Dette gjelder både typiske HR-data, som lønnsdata, men kan også registrering i de enkelte fagløsninger knyttet til driftsoppgaver utført av egne ansatte.

Listen under viser eksempler på løsninger som benyttes i norske vann- og avløpsvirksomheter og hvilke data som er relevant mht. persondata:

- **Ledningsdatabase/kartverk**
  Mulighet for å registrere initialene til den enkelte driftsoperatør som registrerer de enkelte driftshendelser (spyling etc.). Data fra matrikkelen[64]) benyttes også for å foreta oppslag om bygninger, boliger, hjemmelshaver og adresser. Dette er data

64) https://www.kartverket.no/eiendom/eiendomsinformasjon/matrikkelen/

som er tilgjengelig i løsningen og som må sikres på en god måte, siden dette også er persondata. Statens Kartverk har ansvaret for matrikkelen.

- **Oppfølgingsverktøy**
  Søknader om tiltak, pålegg om utbedringer. Abonnent/søker.
- **VA forvaltning**
  - **Slamavskillere og andre avløpsløsninger**
    Eiere eller kontaktperson
  - **Olje- og fettutskillere** Eiere
  - **Vannmålere** Abonnenter
  - **Meldinger** Alle kan legge inn navn, telefonnummer og e-post i forbindelse med registrering av en melding. Inneholder logg og tilbakemelding.
    Enkeltpersoner med navn, mobil, mail.
  - **Gebyr** Informasjon om vann/avløpsgebyrer på eiendommer/bygninger. Abonnenter.
  - **Rørleggerarkiv** med skannede rørleggermeldinger. Dokumenter og skannede tegninger kan inneholde persondata.
  - **Publikumsvarsling** (Varsling24, Powel Varsling etc.). SMS/mail og fasttelefon varsling. Logg over hvem som er varslet. Enkeltpersoner og firma.
  - **Administrative systemer,** som e-post, saksarkiv, økonomisystem, HR-system og timeregistreringssystem.

For de ulike IT-verktøy som benyttes må det registreres hvilke persondata som registreres i hver enkelt løsning. Det er utarbeidet et regneark/tabell[65] (regneark som kan brukes som mal kan lastes ned sammen med Norsk Vann rapporten) som kan brukes som mal for å identifisere persondata (se Figur 25). Følgende data registreres for hver løsning som er aktuell:

- Beskrivelse (Hvilken løsning registreres data i?)
- Behandlingsformål (Hva skal opplysningene brukes til?)
- Typer av personopplysninger (Hvilke persondata er det snakk om?)
- Sensitive personopplysninger (Noen persondata er mer sensitive enn andre slik som opplysninger om rase, politisk, religion, straffedømt, helse, seksuelle forhold, fagforening)
- Dataeier (Hvem i kommunen/selskapet eier dataene?)
- Tilgang (Hvem har tilgang til data?)
- Innsamlingsmetode (Hvordan samles data inn?)
- Overførselsmetode (Hvordan overføres data?)
- Oppbevaringsmetode (Hvor ligger data lagret? Sky, lokal server, hybrid løsning etc.)
- Metode til videresendelse (Hvordan eksporteres data?)
- Ekstern adgang (Har eksterne tilgang til data? Leverandører etc.)
- Krypteringsmetode (Er data kryptert under lagring og transitt?)
- Backupmetode (Hvordan sikres det backup?)
- Databehandler (Er det en databehandler som behandler data på vegne av kommune/selskap?)
- Tredjepartsmottakere (Er det noen eksterne som har tilgang til data utover databehandler?)
- Overførsler til annet land/ internasjonal org.

Informasjon om vannforbruket i en husstand anses ifølge Datatilsynet som en personopplysning[66]. Dette gjelder både om en har en gammel type vannmåler som bare avleses manuelt en gang i året og om en har en smart vannmåler som registrerer vannforbruket kontinuerlig. Omfanget av registreringen av persondata vil selvfølgelig variere, avhengig av målertype. Dette vil påvirke risikovurderingen. Ved å koble vannmålerdata for en husstand til matrikkeldata, kan en se hvem som bor i huset og hvor mye vann de bruker. Ved fjernavlesning med fin tidsoppløsning, kan f.eks. kommunen få tilgang til hvor mye vann som brukes hjemme hos en person på et gitt tidspunkt.

Opplysninger fra fjernavleste vannmålere kan brukes til mange nyttige ting, for eksempel vil opplysningene kunne brukes til raskere å finne vannledningsbrudd på offentlig nett, og huseiere kan varsles dersom det oppstår lekkasjer innomhus. Men opplysningene kan også misbrukes, dersom de kommer i gale hender. Detaljerte vannforbruksdata kan gi en eventuell innbruddstyv indikasjon på om en forbruker er på ferie, slik at en lettere kan foreta et innbrudd i huset. Ved fin tidsoppløsning på vannmålerne er det mulig ved hjelp av dataanalyse å gjenkjenne hvilket vannforbrukende utstyr (vaskemaskin, dusj etc.) som virker til enhver tid. Det gir mening å forebygge at slike data kommer på avveie, ikke bare for å unngå eventuelle store overtredelsesgebyr, men også fordi alternativet vil medføre at innbyggernes tillit til kommunen svekkes.

Opplysningene som samles inn må beskyttes slik som personopplysninger skal. Innbyggerne må også gis tilstrekkelig informasjon om hva det innebærer å ha en slik automatisk avlesning. Samtidig vil økt overvåkning via vannmålerdata gi kommunen mye informasjon om den enkelte abonnenten. Det blir da også et spørsmål om hvordan denne informasjonen benyttes.

65) Inspirert av maler fra Danske Vandverk: https://danskevv.dk/viden-om/cybersikkerhed/

66) Datatilsynet (2017). Personopplysninger og personvern. Innlegg av Hallstein Husand på TEKNA sin VA-jus konferanse 2017.

Figur 25. *Eksempel på utfylling av mal for identifisering av persondata (regneark kan lastes ned sammen med rapporten via Norsk Vann sine nedlastingssider).*

Verktøy som inneholder persondata mot kunder/innbyggere

Beskrivelse	Behandlings-formål	Typer av personopplysninger	Sensitive personopplysninger	Dataeier	Innsamlings-metode	Overførsels-metode
Gemini Portal	Nettinformasjonssystem	Matrikkel data, bruker initialer	Nei	GIS	Manuelt	Internett
Gemini Melding	Kundehenvendelser	Navn, Adresse, Telefon, Email, Målernumre, Forbrugernummer (kundenummer),	Nei	Drift	Automatisk	Internett
Vannmåler	Måleravlesning	Forbruksdata (evnt også Smarte vannmålere)	Nei	Myndighet	Manuelt	SMS, internett
Osv						

Persondata internt i virksomheten

Beskrivelse	Behandlings-formål	Typer av personopplysninger	Sensitive personopplysninger	Dataeier	Innsamlings-metode	Overførsels-metode
HR persondata	Allminnerlige HR aktiviteter	HR data (alle former for personopplysninger)	Ja	HR sjef	Manuelt	Ingen
Lønnssystem (Agresso)	Lønnssystem	HR data (alle former for personopplysninger)	Ja	Regnskap	Manuelt	Via lønnsystem
osv						

Støttesystemer

Beskrivelse	Behandlings-formål	Typer av personopplysninger	Sensitive personopplysninger	Dataeier	Innsamlings-metode	Overførsels-metode
E-post	Kommunikasjon med med forbrukere	Navn, Adresse, Telefon, Email, målernummer,	Nei	Driftssjef	Manuelt	Internet
osv						

Oppbevaringsmetode	Metode til videresendelse	Eksterne adgang	Krypterings-metode	Backupmetode	Databe-handler	Databehandler avtale	Tredjeparts-modtagere2	Overførsler til annet land/ international org.
Sky Azure	Internett	Ingen	Kryptert kommunikasjon	Sky + lokalt	Powel	Ja	Nei	Data lagres i Nord Europa
Lokalt på server	Internett	Ingen	Ingen	Ekstern backup service	Powel	Ja	Nei	Nei
Lokalt på server	Internett	Ingen	Ingen	Ekstern backup service	Powel	Ja	Nei	Nei

Oppbevaringsmetode	Metode til videresendelse	Eksterne adgang	Krypterings-metode	Backupmetode	Databe-handler	Databehandler avtale	Tredjeparts-modtagere2	Overførsler til annet land/ international org.2
Egen server	Ingen	Ingen	Ingen	Ekstern backup service	Nei	Nei	Nei	Nei
Hos Agresso	Krypteret via internet	Ingen	Utføres av Agresso	Utføres av databehandler	Agresso	Nei	Nei	Nei

Oppbevaringsmetode	Metode til videresendelse	Eksterne adgang	Krypterings-metode	Backupmetode	Databe-handler	Databehandler avtale	Tredjeparts-modtagere2	Overførsler til annet land/ international org.2
Sky Microsoft	Internett	Internett	Både ukrypteret og krypteret	Utføres av databehandler	Microsoft	Nei	Nei	Nei

TIDLIGERE UTGITTE RAPPORTER

2017
- 229 Sikring av vannforsyning mot tilsiktede uønskede hendelser
- 228 Tilførsel av industrielt avløpsvann
- 227 Beregning av forurensningsutslipp fra avløpsanlegg
- 226 Tømming av slam
- 225 Trykkavløp i spredtbygde og urbane strøk
- 224 Eierskap til stikkledninger

2016
- 223 Finansieringsbehov i vannbransjen 2016–2040
- 222 Dokumentasjon av utslipp fra avløpsnettet
- 221 Smart ledningsfornyelse – bruk av NoDig-metoder
- B21 Utvikling av studietilbud i bachelor i vann- og miljøteknikk
- B20 Norske tall for vannforbruk med fokus på husholdningsforbruk
- 220 Kritiske ledninger for vann og avløp – klassifisering og tiltaksvurdering
- 219 Eksempler på implementering av bærekraft i vannbransjen
- 218 Vann til brannslokking og sprinkleranlegg
- 217 Videreutvikling av beregningsmetodikk for gjenanskaffelsesverdi og investeringsbehov

2015
- 215 Tilbakestrømssikring – veiledning til vannverkseiere
- 214 Forslag til ny sektorlov for vanntjenester
- 213 Sikkerhetsstyring for vannbransjen
- 212 Veiledning for dimensjonering av vannbehandlingsanlegg
- 211 Erfaringer med ozon-biofiltrering for behandling av drikkevann
- 210 Veiledning for praktisering av selvkost

2014
- 209 Veiledning i mikrobiell barriere analyse
- 208 Sikring av kvalitet på ledningsanlegg
- 207 Stikkledninger – ansvar og teknisk utforming
- 206 Biostabilitet i drikkevannsnett
- 205 Bærekraftig forvaltning av VA-tjenestene
- 204 Åpne flomveger i bebygde områder
- 203 Fra driftsassistanser til regionale vannassistanser
- 202 Microbial barrier analysis (MBA) – a guideline
- 201 Anskaffelser i vannbransjen
- 200 Håndtering av overvann fra urbane veger

2013
- 199 Etablering av gode VA-løsninger i spredt bebyggelse
- 198 Organiske miljøgifter i norsk avløpsslam – Resultater fra undersøkelsen i 2012/13
- 197 Avløpsanlegg Vurdering av risiko for ytre miljø
- 196 Veiledning i tilstandskartlegging og fornyelse av VA-transportsystemer
- 195 Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg
- B19 Varmepumper i drikkevannsforsyningssystem
- B18 Kranvannets kokebok for kommunikasjon
- B17 Investeringsbehov i vann- og avløpssektoren

2012
- 194 Energiriktig design og prosjektering av avløpsrenseanlegg
- 193 Veiledning i dimensjonering og utforming av VA-transportsystem
- 192 Veiledning for valg av riktige sensorer og måleutstyr i VA-teknikken
- 191 Rettigheter til uttak av vann til allmenn vannforsyning
- 190 Klimatilpasningstiltak innen vann og avløp i kommunale planer
- 188 Veiledning for drift av koaguleringsanlegg
- C8 Omdømmeplattform og -strategi

2011
- 187 Kommunal overtakelse av vannverk organisert som andelslag eller samvirkeforetak
- 186 Veiledning i omorganisering av andelsvannverk til samvirkeforetak
- 185 Fett i avløpsnett. Kartlegging og tiltaksforslag
- 184 Tilsyn med utslipp fra avløpsanlegg innen kommunens myndighetsområde
- 183 Veiledning om regulering av VA-tjenester til næringsmiddelindustri
- 182 Prøvetaking av avløpsvann og slam
- 181 Veiledning i bygging og drift av drikkevanns-basseng
- 180 Fjernavlesning av vannmålere
- 179 Veiledning i utarbeidelse av kommunale gebyrforskrifter for vann og avløp
- B16 Veiledning for kartlegging av energibruk i VA-sektoren
- B15 Vannforskriftens økonomiske konsekvenser for kommunesektoren og avløpsanleggene
- C7 Forvaltningspraksis ved norsk damsikkerhet

2010
- 178 Grunnundersøkelser for infiltrasjon – mindre avløpsanlegg
- 177 Drikkevannskvalitet og kommende utfordringer - problemoversikt og status
- 176 Statlige gebyrer og avgifter på de kommunale VAR-tjenestene
- 175 Vann og avløp for nye i bransjen – læreplan. E-læring og samlinger
- 174 Hygienisering av avløpsslam. Langtidslagring og enkel rankekompostering. Resultater fra 3 års valideringstesting
- 173 Veiledning for bruk av støpejernsrør
- B14 Klimatilpasningstiltak i VA-sektoren – forprosjekt
- B13 Silslam – mengder, behandlingsløsninger og bruksområder. Forprosjekt.

2009
- 172 Trykktap i avløpsnett
- 171 Erfaringer med lekkasjekontroll
- 170 Veileder til god desinfeksjonspraksis
- 169 Optimal desinfeksjonspraksis fase 2
- 168 Veiledning for dimensjonering av avløps-renseanlegg
- 167 Veiledning for kjøp av VA-kjemikalier
- 166 Tiltak for å bedre fosforfjerningen på kjemiske renseanlegg
- 165 Innsamlingsverktøy for vedlikeholdsdata
- B12 Drikkevatn i media

2008
- 164 Veiledning for UV-desinfeksjon av drikkevann
- 163 Veiledning for innhenting og evaluering av tilbud på analyseoppdrag
- 162 Veiledning i klimatilpasset overvannshåndtering
- 161 Helsemessig sikkert vannledningsnett
- 160 Driftserfaringer med membranfiltrering
- 159 Håndbok i kildesporing i avløpssystemet
- 158 Termoplastrør i Norge – før og nå
- B11 Økonomiske forhold i interkommunalt VA-samarbeid – praksis og kjøreregler
- B10 Vannkilden som hygienisk barriere
- B9 Utvikling av et system for spørreundersøkelser blant VA-kundene
- C6 I veien for hverandre – Samordning av rør og kabler i veigrunnen

2007
- 157 Organiske miljøgifter i norsk avløpsslam. Resultater fra undersøkelsen i 2006/07
- 156 Veiledning for oljeutskilleranlegg
- 155 Norm for merking og FDV-dokumentasjon i VA-sektoren
- 154 Norm for tagkoding i VA-anlegg
- 153 Norm for symboler i driftskontrollsystemer for VA-sektoren
- 152 Veiledning for anskaffelse av driftskontroll-systemer i VA-sektoren
- 151 Veiledning for vedlikeholdssystemer (FDV)
- 150 Dataflyt – Klassifisering av avløpsledninger
- B8 Forprosjekt energinettverk i VA-sektoren
- B7 Sandnesmodellen. Eksempel på system for kommunikasjon og virksomhetsstyring

2006
- 149 Tilførsel av industrielt avløpsvann til kommunalt nett. Veiledning
- 148 Veiledning i utarbeidelse av prøvetakings-programmer for drikkevann
- 147 Optimal desinfeksjonspraksis for drikkevann
- 146 Bærekraftig vedlikehold. Betraktninger av utvalgte problemstillinger knyttet til langsiktig forvaltning av vannledningsnett
- B6 Kommunikasjonsstrategi for NORVAR og norske vann og avløpsverk
- B5 Utslipp fra bilvaskehaller
- B4 Vannkvalitet i ledningsnett – Problemoversikt og statur. Forprosjekt.
- B3 Kvalitetsheving av nye VA-ledningsanlegg. Kartlegging og tiltaksforslag
- C5 Økt sikkerhet og beredskap i vannforsyningen – veiledning
- C4 Effekter av bruk av matavfallskverner på ledningsnett, renseanlegg og avfallsbehandling

2005
- 145 Inspeksjonsmanual for avløpssystemer. Del 1 – Ledninger
- 144 Veiledning i overvannshåndtering (Erstattet av 162/08)
- 143 Kartlegging av mulig helserisiko for abonnenter berørt av trykkløs vannledning ved arbeid på ledningsnettet
- 142 NORVARs benchmarkingsprosjekt 2004 Presentasjon av målesystem og resultater for 2003 ed analyse av datamaterialet
- B2 PressurePuls for deteksjon av lekkasje på vannledninger.
- C3 Samarbeid om økt bruk av avløpsslam på grøntarealer

2004
- 141 Trenger Norge en VA-lov? Drøfting av behovet for en egen sektorlov for vann og avløp
- 140 NORVARs videre arbeid med slam. Strategisk plan for prosjektvirksomhet, informasjon og kommunikasjon. Forprosjekt
- 139 Erfaringar med klorering og UV-stråling av drikkevatn
- 138 Veiledning for kontrahering av rådgivnings- og prosjekteringstjenester innen VAR-teknikk. Revidert utgave
- 137 Veiledning i bygging og drift av drikkevanns-basseng (Erstattet av 181/2011)
- 136 Hygienisk barrierer og kritiske punkter i vannforsyningen: Hva har gått galt?
- 135 Vannledningsrør i Norge. Historisk utvikling. 26 dimensjonstabeller
- 134 VA-JUS. Etablering og drift av vann- og avløpsverk sett fra juridisk synsvinkel (Erstattet av boken Vann- og avløpsrett (2010) og nettportalen va-jus.no)
- B1 Effektive VA-organisasjoner og tilfredse brukere. Forprosjekt
- C2 Stoff for stoff – kilde for kilde. Kvikksølv i avløpsnettet

2003
- 133 IT-strategi for VA-sektoren. Veiledning
- 132 Forslag til nytt system for prosjektvirksomheten i NORVAR
- 131 Effektivisering av avløpssektoren
- 130 Gjenanskaffelseskostnadene for norske VA-anlegg
- 129 Rørinspeksjon med videokamera. Veiledning/ rapportering hovedledninger
- C1 Sårbarhet i vannforsyningen

2002
- 128 Bruk av resultatindikatorer og benchmarking i effektivitetsmåling av kommunale VA-virksom-heter. Erfaringer og anbefalinger fra et prøveprosjekt
- 127 Vassdragsforbund for Mjøsa og tilløpselvene – en samarbeidsmodell
- 126 Organisering og effektivisering av VA-sektoren. En mulighetsstudie
- 125 Mal for forenklet VA-norm
- 124 Nødvendig kompetanse for legging av VA-ledninger. Læreplan for ADK 1
- 123 Utslipp fra mindre avløpsanlegg. Veiledning for utarbeidelse av lokale forskrifter (Utgått)
- 122 Prosessen ved utarbeidelse av miljømål for vannforekomster. Erfaringer og råd fra noen kommuner
- 121 Kjøkkenavfallskverner for håndtering av matavfall. Erfaringer og vurderinger
- 120 Strategi for norske vann- og avløpsverk. Rapport fra strategiprosess 2000/2001

2001
- 119 Omstruktureringer i VA-sektoren i Norge En kartlegging og sammenstilling
- 118 Veiledning for kontrahering av rådgivnings- og prosjekteringstjenester innen VAR- teknikk (Erstattet av 138/04)
- 117 VA-juss. Etablering og drift av vann- og avløpsverk sett fra juridisk synsvinkel (Erstattet av 134/03)
- 116 Scenarier for VA-sektoren år 2010
- 115 Pumping av avløpsslam. Pumpetyper, erfaringer og tips
- 114 Nødvendig kompetanse for drift av vannbehand-lingsanlegg. Læreplan for driftsoperatør vann
- 113 Nødvendig kompetanse for drift av avløpsrense-anlegg. Læreplan for driftsoperatør avløp
- 112 Erfaringer med nye renseløsninger for mindre utslipp

2000
- 111 Eksempel på driftsinstruks for silanlegg. Cap Clara i Molde kommune
- 110 Veileder i konkurranseutsetting. Avtaler for drift og vedlikehold av VA-anlegg
- 109 Resultatindikatorer som styringsverktøy for VA-ledelsen
- 108 Data for dokumentasjon av VA-sektorens infrastruktur og resultater
- 107 Utslipp fra mindre avløpsanlegg. Teknisk veiledning. Foreløpig utgave
- 106 Effektiv bruk av driftsinformasjon på rense-anlegg/mal for rapportering
- 105 Sjekkliste plan- og byggeprosess for silanlegg
- 104 Nordisk konferanse om nitrogenfjerning og biologisk fosforfjerning 1999
- 103 Returstrømmer i renseanlegg. Karakterisering og håndtering

Norsk Vann BA, Vangsvegen 143, 2321 Hamar
Tlf: 62 55 30 30 E-post: post@norskvann.no
www.norskvann.no