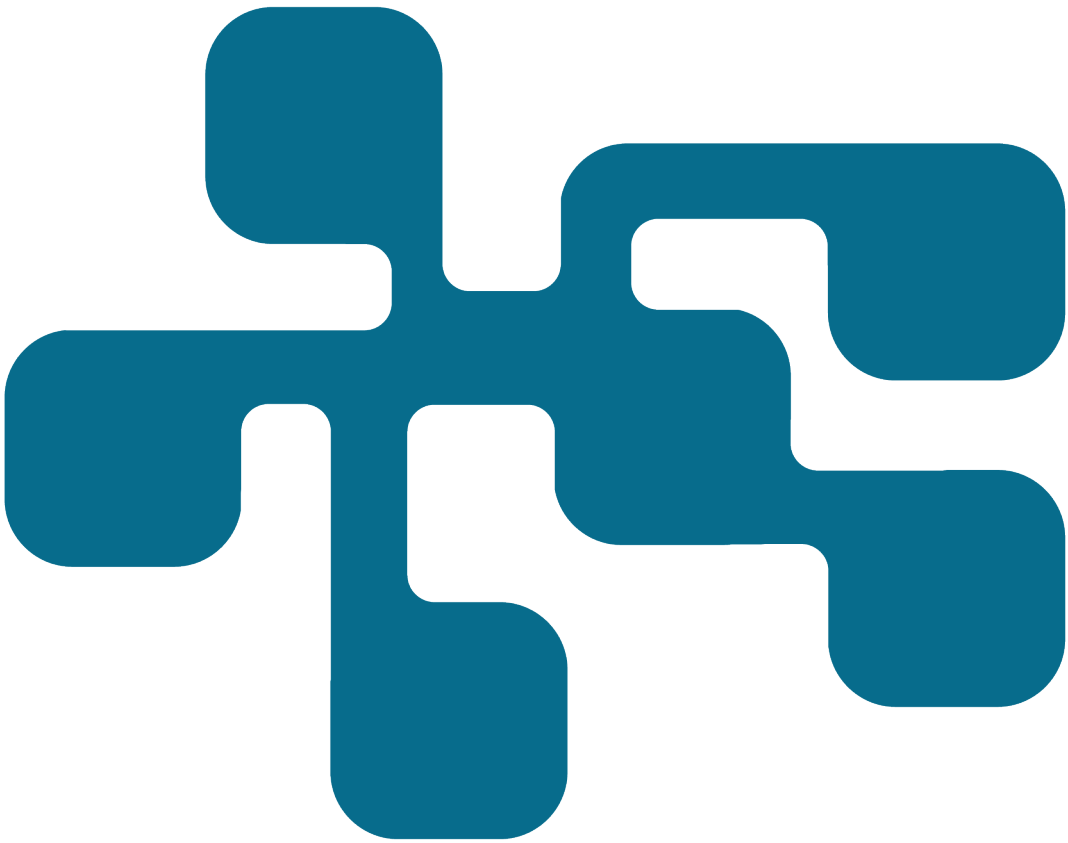
NCS3 – Förstudie om cybersäkerhet i dricksvattenverk

En förstudie om cybersäkerhet, informationsflöden och aktörer inom svenska dricksvattenverk

Hanna Kvist, Minna Severin, David Lindahl

FOI
MSB



FOI-R--5578--SE
MSB 2023-04428
ISSN 1650-1942

Mars 2024

Hanna Kvist, Minna Severin, David Lindahl

FOI-R--5578--SE--SE

NCS3 – Förstudie om cybersäkerhet i dricksvattenverk

En förstudie om cybersäkerhet, informationsflöden och aktörer inom svenska dricksvattenverk.

Titel	NCS3 – Förstudie om cybersäkerhet i dricksvattenverk – En förstudie om cybersäkerhet, informationsflöden och aktörer inom svenska dricksvattenverk.
Engelsk titel	NCS3 – Pilot study on cyber security in water treatment plants
Rapportnr	FOI-R--5578--SE--SE
Månad	3
Utgivningsår	2024
Antal sidor	63
ISSN	1650-1942
Uppdragsgivare	Myndigheten för samhällsskydd och beredskap
Forskningsområde	Informationssäkerhet
FoT-område	-Inget FoT-område-
Projektnr	E380226
Godkänd av	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Sammanfattning

Dricksvattenproduktion är en samhällsviktig verksamhet och dricksvatten brukar kallas vårt viktigaste livsmedel. Dricksvatten har även en betydande roll inom industrin.

Syftet med denna förstudie att skapa en initial övergripande bild av cyberrisker inom vattenproduktionen kopplat till informationsflöden, kritiska cyberfysiska system, säkerhetsarbete och potentiella konsekvenser av framgångsrika cyberangrepp. Förstudien är till för att stödja Myndigheten för samhällsskydd och beredskap (MSB) med underlag för att stärka skyddet av samhällsviktig verksamhet. För att få en övergripande bild har intervjuer genomförts som primär metod, med komplement av rapporter, dokumentation och hemsidor. Totalt genomfördes intervjuer med fem VA-bolag i Sverige, där respondenterna arbetar med, och har ansvar för, säkerhetsfrågor kring IT[1], OT[2] och dricksvattenproduktion. Tillsammans förser de deltagande verksamheterna dricksvatten till cirka 20 % av Sveriges befolkning.

Förstudien visar en övergripande bild av aktörer, informationsflöden och cyberfysiska system inom några VA-bolags vattenverk. Den ger en inblick i hur dessa fem VA-bolag i Sverige ser på informations- och kommunikationsflöden i verksamheten, hur säkerhetsarbetet ser ut, vad de har för utbildningsbehov och vilka hot och utmaningar som finns. Studien visar på att digitaliseringen av verksamheten har skapat nya behov av säkerhetsarbete och utbildning gällande IT/OT-säkerhet[3]. Digitaliseringen har även lett till svårigheter att rekrytera personal som besitter rätt kompetens och kunskap kring både IT och OT till verksamheten. Samtliga verksamheter arbetar med säkerhet, och IT-säkerhet är något som blivit allt viktigare. Säkerhetsfrågan i

[1] Informationsteknik/system: Tekniska system för som hanterar information, till exempel datorprogram, appar, datorer, skrivare, hårddiskar, mobiltelefoner, wifi och vissa delar i styr- och reglersystem (MSB2032, 2023).

[2] OT (från engelskans ”Operational Technology”): industriella informationssystem med huvudsaklig funktion att styra och övervaka en fysisk process (STEMFS 2021:3, 2021).

[3] It-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet (MSB2032, 2023).

vattenverksamheten är komplex då det finns ett stort beroende till andra aktörer, krav från myndigheter samt i att öva på att hantera incidenter.

Förstudien har gett en inblick i hur de deltagande verksamheter arbetar med säkerhet, men underlagets storlek medger inte slutsatser rörande branschen i stort. Det finns flera fördjupningar att göra inom området och studien avslutas med förslag på vidare arbete.

Nyckelord: dricksvatten, cybersäkerhet, informationsflöden, cyberfysiska system, digitalisering, dricksvattensektorn, livsmedelsförsörjning, samhällsviktig verksamhet, industriella styrsystem.

Summary

Drinking water production is part of the critical infrastructure and is important for human health as well as in industries.

The purpose of this pilot study is to create an initial view on cyber risks in water treatment plants connected to information flows, critical cyber physical systems, security work and consequences of a successful cyberattack. The pilot study can support the Swedish Civil Contingencies Agency (MSB) in strengthening the protection for critical infrastructure. The primary data collection took place through interviews with representatives from five organizations in the drinking water sector. This was augmented with data from reports, documents and websites. The five organizations that participated in the study supply drinking water to approximately 20% of the households in Sweden.

The study gives an overview of actors and stakeholders, information flows and cyber-physical systems in the drinking water sector. It gives an insight into how the interviewed companies work with security, their needs for education and training, and what threats and challenges exist. The study shows that the digitalization within the water sector has created new challenges concerning security, and IT-security in particular. The need for competence in both IT and OT have resulted in the organisations having a hard time recruiting enough people with both of these skillsets. Legislative demands, inter- and intraorganizational dependencies, difficulties in training and practice for example sentence practicing cyber incidents, all make cyber security a difficult issue.

The pilot study has provided insight into how the interviewed organizations work on these issues, but due to the small sample of water treatment plants that have been interviewed no firm conclusions about the sector can be drawn. The study concludes with proposals for further work on the subject.

Keywords: drinking water, cyber security, information flows, cyber-physical systems, digitalization, drinking water sector, food supply, industrial control systems.

Innehåll

1 Inledning

Dricksvatten brukar kallas det viktigaste livsmedlet vi har. Vid Sveriges myndigheters krisinformation (Dricksvattenförsörjning, 2023) står det att läsa att

> ”En bra vattenförsörjning är en hörnsten i ett väl fungerande samhälle. […] Som samhällsfunktion karaktäriseras vattenförsörjningen av att den är storskalig och komplex.”

Den ökade digitaliseringen av automationssystem inom dricksvattenproduktion har öppnat upp för en ny sorts säkerhetsrisker: cyberattacker. Cyberattacker har drabbat många delar av samhället de senaste åren, och kan potentiellt ge stor samhällspåverkan om de drabbar kritisk infrastruktur.

Denna förstudie är genomförd inom ramen för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3). NCS3 är ett samarbete mellan Myndigheten för samhällsskydd och beredskap (MSB) och Totalförsvarets forskningsinstitut (FOI) i syfte att stärka säkerheten hos de system som ingår i kritisk infrastruktur. Arbetet inom NCS3 sker på initiativ från MSB.[4]

1.1 Syfte

Syftet med denna förstudie är att skapa en initial och övergripande bild av cyberrisker inom vattenproduktion såsom informationsflöden, kritiska cyberfysiska system, säkerhetsarbete samt potentiella konsekvenser av framgångsrika cyberangrepp.

Följande aspekter inom produktion av dricksvatten ska mot denna bakgrund studeras:

- Informations- och kommunikationsflöden samt cyberfysiska system av vikt för att produktion av dricksvatten ska fungera.
- Säkerhetsarbete på vattenverken och konsekvenser av en cyberattack.
- Utbildning kring och övning av cyberrelaterade incidenter.

[4] https://www.foi.se/forskning/informationssakerhet/ncs3.html

- Utmaningar med säkerhetsarbete i vattenverken.

1.2 Målgrupp

Målgruppen för NCS3 utgörs av offentlig sektor, NIS-aktörer, andra totalförsvarsaktörer som bedriver samhällsviktig verksamhet, akademi, riksdag och regering samt internationella samarbetspartners. Syftet är också att stärka skyddet för samhällsviktig verksamhet inom staten och dess uppgift att arbeta förebyggande inom cyber- och informationssäkerhet (Informationssäkerhet, cybersäkerhet och säkra kommunikationer, 2023). Föreliggande rapport vänder sig till beslutsfattare och tekniker som arbetar inom eller tillsammans med VA-sektorn samt inom liknande samhällsviktig verksamhet.

1.3 Bakgrund

Enligt FN:s resolution (A/RES/64/292, 2010) är tillgång till rent dricksvatten en mänsklig rättighet. Dricksvattenproduktion ses som en samhällsviktig verksamhet som är komplex i sin karaktär och involverar många olika aktörer samt innehåller cyberfysiska system. I Sverige är det relativt få vattenverk som förser majoriteten av hushåll och människor med dricksvatten. Beroendet av dessa vattenverk innebär en sårbarhet för samhället vid sabotage eller driftavbrott.

Kommunalt dricksvatten är den vanligaste källan för dricksvatten i Sverige, mer än 89 % av befolkningen får sitt dricksvatten från kommunala vattenverk. Det finns drygt 1750 kommunala vattenverk i Sverige varav de flesta tar vattnet från grundvatten (Vattenverk och reningsprocesser, 2023). Det är dock ytvattenverken som producerar störst volymer, där drygt 170 ytvattenverk producerar närmare hälften av allt dricksvatten i landet (Statistiska centralbyrån (SCB), 2022). Den största vattenproducenten förser cirka 1,5 miljoner människor med rent dricksvatten (Detta är Stockholm Vatten och Avfall, u.d.).

1.4 Avgränsningar

För att avgränsa förstudien har omfattningen begränsats till produktionen i vattenverk som tar sitt råvatten från ytvatten. Detta innebär att andra typer av vattenverk, och den fortsatta dricksvattenkedjan såsom distributionen via ledningsnätet inte omfattas av denna studie. Studien

har inte gjort en avgränsning gällande verksamheternas storlek, vare sig för organisationerna eller för vattenverken, utan istället valt att ha med både större och mindre verksamheter.

Det begränsade antalet verksamheter studien behandlar gör att det inte går att dra några sektoromfattande slutsatser. För att kunna dra mer djupgående slutsatser måste en större studie genomföras. Förstudiens resultat ska snarare ses som en initial och övergripande bild av verksamheternas arbete inom cyber- och informationssäkerhet idag.

1.5 Metod

Studien är kvalitativ i sin karaktär och datainsamlingen har primärt skett genom semistrukturerade intervjuer med medarbetare vid fem verksamheter som producerar dricksvatten. Dessa fem organisationer förser sammanlagt ungefär en femtedel av Sveriges befolkning med dricksvatten. De flesta intervjuer genomfördes digitalt på distans. Datainsamlingen har kompletterats med sökning av information via myndigheters och branschorganisationers hemsidor och publika dokument. Resultaten bygger på intervjuer med respondenter med olika typer av säkerhetsansvar vid vattenverken: IT-ansvarig, OT-ansvarig eller verksamhetsansvarig vid vattenverket. Begränsningen i förstudiens omfång har främst att göra med studiens karaktär och syfte. Men det finns också frågor som inte kunde täckas in i denna förstudie på grund av sekretesskäl. En spridning av urvalet av de intervjuade organisationerna gjordes genom att titta på storleken på verksamheterna samt var de geografiskt var belägna i landet. Verksamheterna kontaktades därefter via mail och några valde att medverka medan några få tackade nej till medverkan. Totalt deltog tolv respondenter i studien. Kort information om verksamheterna och intervjuerna visas i tabell 1.

Tabell 1. Information om när intervjuerna skedde samt var organisationerna befinner sig i Sverige.

Verksamhet	**Beskrivning**	**Antal respondenter**	**Datum för intervju**
Verksamhet 1	Kommunalt bolag i Mellansverige	1	17 oktober 2023
Verksamhet 2	Kommunalt bolag i Södra Sverige	3	31 oktober 2023
Verksamhet 3	Kommunalt bolag i Norra Sverige	1	10 november 2023
Verksamhet 4	Kommunalt bolag i Mellansverige	4	10 november 2023
Verksamhet 5	Kommunalt bolag i Mellansverige	3	27 november 2023

Den intervjuguide som användes för intervjuerna kan ses i sin helhet i Bilaga A. Teman för intervjuerna var:

- respondentens ansvarsområde och lokala förutsättningar
- övergripande information om dricksvattenframställningen
- regelverk och policyer
- organisationens arbetssätt
- utbildning och övningar
- hot- och riskbedömningar.

2 Dricksvattenproduktion i Sverige

Våren 2022 fanns det 2555 vattenproduktionsanläggningar registrerade hos Livsmedelsverket. De flesta av dessa försörjer minst 50 abonnenter eller producerar minst 10 000 liter vatten per dygn (Dricksvatten och vattenskydd, 2022). I detta kapitel ges en bakgrund till hur produktionen av dricksvatten i Sverige ser ut. Även relevanta regelverk som påverkar och sätter ramar för verksamheten och som kan påverka cybersäkerhetsarbetet.

2.1 Dricksvattenprocessen

Vattnet till vattenverken tas från naturen (ytvatten eller grundvatten) och renas i vattenverket. Kvaliteten på det inkomna vattnet avgör hur reningsprocessen går till. Nedan beskrivs mycket övergripande vattnets väg från naturen till kranen hos konsumenten:

1. Vatten pumpas från en vattentäkt till vattenverket för att renas.
2. Vattnet *förbehandlas* med hjälp av exempelvis silning för att förhindra att stora partiklar når de mer avancerade reningsstegen.
3. Mindre partiklar avlägsnas med hjälp av en *kemisk rening*.
4. Nästa steg är en sedimentationsbassäng där partiklar sjunker till botten där de fastnar i ett sandlager, detta steg kallas *mekanisk rening*.
5. Därefter kan en finfiltrering ske där vattnet passerar genom filter för att avlägsna små partiklar, bakterier och andra föroreningar. Sand eller kol är exempel på material i filtren.

Olika vattenreningsverk kan använda skilda processer och tekniker för att leva upp till lagstiftning och vattenkvalitetskrav, men stegen är relativt likartade för alla. Ibland används även ytterligare steg:

6. *Biologisk rening* där mikroorganismer tar hand om eventuella oönskade ämnen.
7. *Klor* eller *ultraviolett ljus* kan användas för att döda vissa motståndskraftiga bakterier.
8. *Ljus* kan användas för att döda vissa motståndskraftiga bakterier.

Ytterligare kemikalier kan tillsättas i slutet av processen för att förbättra smak, lukt och färg samt för att binda eventuella kvarvarande föroreningar. Innan vattnet lämnar vattenverket kontrolleras det för att säkerställa att det är rent. Det renade vattnet lagras i vattenreservoarer innan distribution genom ledningsnätet (Reningsprocesser i vattenverk, 2023).

Processen för att tillverka dricksvatten är idag till hög grad automatiserad. Specialiserade datorsystem används för att rena och flytta vattnet. Dessa kallas bland annat *Supervisory Control And Data Acquisition* (SCADA), *Industrial Control Systems* (ICS) eller på svenska industriella styrsystem.[5]

SCADA-systemet består av flera delsystem och det skiljer sig åt mellan olika vattenproducenter huruvida systemet används för:

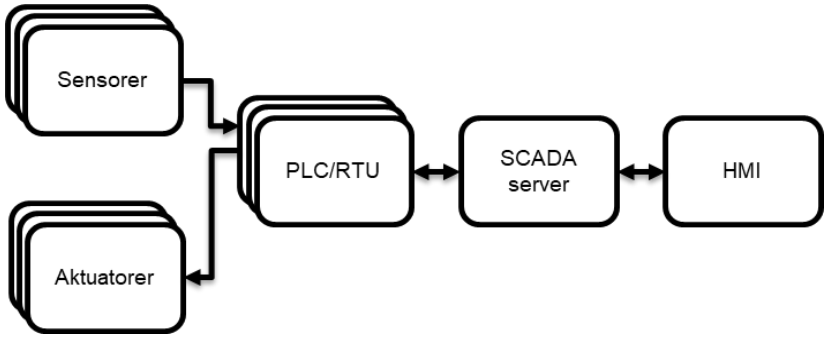
- enbart vattenproduktion
- vattenproduktion och -distribution
- vattenproduktion och andra tjänster som de har i sin verksamhet.

Ett exempel på informationsflödet i ett SCADA-system illustreras i figur 1. Alla SCADA-system har gemensamt att de har lokala industridatorer, *Programmable Logic Controller* (PLC) eller *Remote Terminal Unit* (RTU). PLC:er och RTU:er är små, fysiskt hållbara datorer som kontrollerar en maskin som styr en fysisk process. Genom att inhämta data från *sensorer* kopplade till processen kan PLC:n övervaka vad som sker och om nödvändigt påverka maskinen genom att sända order till *aktuatorer*, vilka utgör kontrolldon av olika slag som ändrar maskinens beteende.

Förutom att övervaka och styra en sådan lokal maskin sänder PLC:n också data om driften av denna till ett övre lager av datorsystem, SCADA-lagret[6]. Detta lager av datorer övervakar många PLC:er och i förlängningen hela industriprocessen.

[5] Alla respondenter använde termen SCADA som en generell term för sina olika styrsystem inom produktionen varför vi följer den standarden i rapporten där de citeras.

[6] Termen ”SCADA-systemet” omfattar i dagligt tal inte enbart SCADA-lagret utan också de övriga lagren ovan som på något sätt relaterar till styrningen av industriprocessen.



Figur 1. Informationsflödet i ett medelstort SCADA-system

SCADA-servrarna aggregerar driftdata från alla delar av processen och sänder dem för att presenteras på ett för människor begripligt sätt i form av ett *Human Machine Interface* (HMI) i ett kontrollrum eller på en datorskärm.

Människan, *operatörerna*, kan via HMI:et sända order till SCADA-servrarna och på sätt ändra produktionskedjan från kontrollrummet och kan därmed övervaka och styra verksamheten utan att behöva vara på samma plats som maskinerna. Flertalet SCADA-lösningar inkluderar även möjligheten att fjärransluta, det vill säga att operatörerna från annan geografisk plats kan ansluta via telekommunikation och styra systemen denna väg.

Större SCADA-system har också en mellannivå med enheter kallade *batch servers* och *historian*. Dessa sparar loggar och data så att systemen utan mänsklig inblandning kan genomföra fler analyser och rutinmässiga förändringar i driften, som till exempel variationer av produktion över dygnet eller samordning av produktion på många produktionsplatser.

2.2 Regelverk och lagar

Ansvaret för dricksvattenprocessen, från uttag i naturen till att konsumenten får vatten i sin kran delas idag mellan olika myndigheter.

Lagen om allmänna Vattentjänster (LAV) (SFS 2006:412, 2006) är den lag som ska säkerställa att vattenförsörjning och avlopp ordnas i samhället om det behövs med hänsyn till människors hälsa eller miljö.

Livsmedelsverket är tillsynsmyndighet (SFS 2018:1174, 2018) för dricksvattenförsörjningen i Sverige och ansvarar för den nationella

vattenkatastrofgruppen VAKA som ger stöd till kommuner och regioner vid akuta kriser. Livsmedelsverget utfärdar föreskrifter om dricksvattentillverkning och genomför tillsyn över drickvattenproducenterna att dessa följs.

Kommunerna i Sverige ansvarar för vattenförsörjningen, eventuellt via ett kommunalt bolag (Ansvar för vatten – vem gör vad?, 2023). Kommunerna ansvarar även för den operativa tillsynen av vattenverken.[7]

Enligt Miljöbalken har varje verksamhetsutövare (enskild verksamhet som bedriver verksamhet, i detta fall dricksvattenverksamhet) ansvar att utöva egenkontroll (Naturvårdsverket, 2001). I detta fall innebär det att de ska kvalitetskontrollera vattenverk och distributionsanläggning för att säkerställa att dricksvattnet är av god kvalitet (Tillsyn av livsmedelsverksamhet, 2023).

Säkerhetsskyddslagen (SFS 2018:585, 2018), Säkerhetsskyddsförordningen (SFS 2021:955, 2021) och Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1, 2022) handlar om att på nationell nivå skydda verksamhet eller information som är av betydelse för Sveriges säkerhet. Enligt 1 kap. 1 § säkerhetsskyddslagen (SFS 2018:585, 2018) gäller lagen för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet. Leverans och försörjning av dricksvatten bedöms som samhällsviktig och säkerhetskänslig verksamhet (Säkerhetspolisen, 2023; Livsmedelsverket, 2023) och faller därmed under denna definition.

Även om säkerhetsskydd omfattar all typ av verksamhet såsom tillträde, sekretessklassning med mera finns det flera delar av lagstiftningen som rör informationssäkerhet. Av särskild relevans för denna studies fokus på cybersäkerhet är att organisationerna som förser samhället med dricksvatten bland annat har skyldigheter med avseende på informationsskydd:

- Enligt lagen (SFS 2018:585, 2018) utreda sitt behov av säkerhetsskydd och vidta de åtgärder som behövs för att uppnå

[7] Operativ tillsyn är sådan tillsyn som utövas direkt gentemot den som bedriver eller har bedrivit en verksamhet eller vidtar eller har vidtagit en åtgärd (Prop. 2019/20:137 , 2020).

skyddet, specifikt för informationssystem ska åtgärderna förebygga att skadlig inverkan drabbar dessa

- Vidta specifika åtgärder (PMFS 2022:1, 2022) för att uppnå tillräcklig informationssäkerhet både vad gäller informationssystem och träning av personal
- Enligt lagen (SFS 2021:955, 2021) har rapporteringsplikt till Säkerhetspolisen rörande IT-incidenter som inträffar, i system för säkerhetskänslig verksamhet om incidenten allvarligt kan påverka säkerheten i systemet.

NIS-regleringen har, till skillnad från säkerhetsskyddslagen, ett snävare fokus på nätverk och informationssystem som är kritiska för att bedriva samhällsviktiga tjänster (Myndigheten för samhällsskydd och beredskap, 2024). NIS-direktivet (Direktiv (EU) 2016/1148, 2016) ställer krav på samhällsviktiga tjänster inom sju sektorer, av vilka leverans och distribution av dricksvatten är ett.[8] Direktivet gäller både privata och offentliga aktörer inom samhällsviktig verksamhet. I Sverige har direktivet implementerats genom lag (SFS 2018:1174, 2018) om informationssäkerhet samt informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1175, 2018), där det i den förra går att läsa att

> ”leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.”

Lagen innehåller undantag för bland annat digitala tjänster och så kallade betrodda företag (SFS 2018:1174, 2018). MSB är nationell kontaktpunkt för Sveriges arbete med NIS (MSB1773, 2021). Enligt MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2021:9, 2021) är det dricksvattenleverantörer som producerar för minst 20 000 personer eller för akutsjukhus som avses i lagen. Direktivet NIS2 (Direktiv (EU) 2022/2555, 2022) som är under utredning kring hur

[8] De övriga är bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, hälso- och sjukvård, och transport (MSB1773, 2021).

implementeringen ska genomföras, kommer att medföra ytterligare krav på kritisk infrastruktur och utökar omfattningen av vem som berörs av NIS. NIS2 ska implementeras senast oktober 2024.

En annat nytt direktiv med fokus på cybersäkerhet är CER-direktivet, direktivet om kritiska entiteters motståndskraft (Direktiv (EU) 2022/2557, 2022) CER handlar om motståndskraften hos kritiska entiteter i viss samhällsviktig verksamhet. Direktivet ställer åtgärdskrav för att stärka motståndskraften. CER- och NIS-direktiven är tänkta att komplettera varandra (EU och arbetet med att stärka motståndskraften i samhällsviktig verksamhet, 2023).En särskild utredare ska under 2024 föreslå de anpassningar av svenskt rätt som behövs enligt NIS2 och CER-direktivet (Dir. 2023:30, 2023).

3 Cyberhot och konsekvenser

Under de senaste tio åren har det runt om i världen inträffat ett antal uppmärksammade cyberangrepp som riktats direkt mot vattenverk, eller som indirekt fått påverkan på deras verksamhet. Sannolikt finns det också ett mörkertal gällande sådana angrepp. I detta kapitel beskrivs kortfattat de konsekvenser som cyberrelaterade incidenter kan resultera i för vattenverk och en generell beskrivning av olika typer av relevanta hotaktörer.

I generella termer kan konsekvenserna av ett cyberangrepp på ett vattenverk delas in i:

- störning eller avbrott i produktionen
- föroreningar i dricksvattnet
- fysisk skada på utrustning
- stöld och/eller förlust av information, tillfällig eller permanent
- monetära förluster
- försämring av varumärke.

3.1 Säkerhetskonsekvenser av SCADA-användning

Den moderna datorstyrningen möjliggör personalbesparingar och ökad produktivitet men introducerar också ett beroende av datorsystemen. En potentiell angripare med möjligheter att ändra informationen i processflödena, databaserna eller i styrprogrammen kan påverka processen på samma sätt som operatörerna i kontrollrummet. Om angriparen lyckas ändra i dataflödet som presenteras av HMI:et kan operatörerna få felmeddelanden som aldrig har sänts från utrustningen. Detta kan leda till att operatörerna luras att tro att problem föreligger och att åtgärder måste vidtas som i verkligheten skadar processens normaltillstånd. Datoriseringen av industriprocessen har således inte enbart inneburit fördelar utan också ökat behovet av IT-säkerhet.

3.1.1 IT och OT

Inom industriell datoranvändning delar man ofta in systemen i IT, informationsteknik, och OT, operativ teknik. IT[9] begränsas i denna subkultur till datorsystem för kontorsanvändning medan OT är datorsystem som används i produktionskedjan för fysiska processer. Anledningen till uppdelningen är att det finns olika kravbild på dessa typer av datorsystem.

Ett kontorssystem kan normalt startas om eller hantera driftstörningar utan större konsekvenser, medan ett industrisystems fysiska process på några sekunder kan drabbas av allvarliga konsekvenser om styrningen störs. För kontors-IT är konfidentialitet viktigast, systemen är relativt billiga, har kort livslängd och byts ut ofta, och säkerhetsaspekterna byggs in allt eftersom. I OT-miljön är i stället tillgänglighet viktigast, systemen är dyra, och har lång livstid (20-50 år i många fall) vilket gör att de sällan byts ut. Moderna IT-säkerhetslösningar finns därför inte nödvändigtvis tillgängliga för OT. Av detta följer att säkerheten i styrsystem hanteras av andra krav och förhållanden än kontorsmiljöer och kräver utökad kompetens i tillägg till den ”normala” IT-säkerheten.

3.1.2 Vad blir konsekvenserna av ett angrepp

Vilka konsekvenser ett angrepp får på systemen är beroende av flera faktorer. Den första faktorn är processens egenskaper. En instabil kemisk reaktion kan leda till explosioner eller utsläpp av hälsofarliga ämnen medan ventilationsstyrningen i ett varuhus på sin höjd kan orsaka kvavt klimat i lokalerna.

Den andra faktorn är systemets arkitektur, det vill säga om anläggningen har byggts på ett sådant sätt att avsteg från normalläget får minimala konsekvenser. Ett exempel är säkringar i elsystem eller när man bygger in explosionsluckor i kvarnar.

Den tredje faktorn är säkerhetsmekanismerna i informationssystemen. Genom att utforma styrsystemen så att de innehåller olika typer av intrångsdetektionssystem, brandväggar, ändringsskydd med flera åtgärder kan man göra det svårare för en angripare att komma åt systemen via

[9] Vi använder kontors-IT för att förtydliga betydelsen.

datorintrång och samtidigt förbättra möjligheten att upptäcka och åtgärda intrånget.

Den fjärde faktorn avser kontinuitetsplanering och incidenthantering. Om personalen till exempel tränats i att hantera cyberangrepp och vet hur de ska agera eller om de enbart tränats i driftskötsel och måste improvisera under en kris.

Alla dessa faktorer samverkar vid ett angrepp och skapar förutsättningar för att i första hand förhindra angreppet, i andra hand minimera konsekvenserna och slutligen snabbt återställa systemen till normalläge.

Även om ett angrepp stoppas utan skador på systemen kommer det att medföra kostnader i form av exempelvis arbetstid, förlust av produktion, höjda försäkringspremier och/eller ersättning till kunder som inte har fått den tjänst som de har betalat för.

Beroende på hur ett angrepp hanteras kan även organisationens rykte påverkas allvarligt. Generellt gäller att organisationen måste kontrollera hur omgivningen uppfattar situationen och agera proaktivt. Ledning och medieansvariga måste aktivt presentera den bild de vill förmedla.

3.2 Störning eller avbrott i produktionen.

Störning eller avbrott i produktionen innebär att en angripare, genom cyberangrepp mot informationssystemen, i någon mån hindrar produktionen av dricksvatten. Detta kan åstadkommas genom att till exempel påverka styrningen av maskiner, kryptera informationen i datorsystemen eller lura operatörerna att vidta felaktiga åtgärder genom att sända falsk information till HMI:et.

Ett exempel på en cyberattack som drabbade vattenproduktion var i Riviera Beach, USA 2019 (Hassanzadeh, o.a., 2020) Det startade med att en polis öppnade ett e-postmeddelande med *ransomware*[10], skadlig kod som spred sig i polisens datorsystem, krypterade register och stängde ner tjänster.

[10] En autonom programvara som försöker sprida sig till alla datorer den kan och kryptera all data den hittar.

Men polisens datorsystem var sammankopplat med Riviera Beach stads datornätverk och eftersom att denna koppling inte var gjord på ett säkert sätt spred sig koden vidare. Då staden hade kopplat samman nästan alla sina organisationer med detta nätverk var de alla sårbara för självspridande kod när en av dem blivit drabbad (Doris, 2019).[11]

Inom några minuter hade i princip alla stadens IT-tjänster gjorts otillgängliga. Biblioteket, televäxlarna, stadskontoret och vattenverket blev alla infekterade. Den skadliga koden tog sig in i vattenverkets administrativa system och sedan vidare ned i system vid pumpstationerna samt system som testar vattenkvalitet. Angreppet ledde till att vattenproduktionen måste styras manuellt.

Effekten av denna typ av cyberangrepp kan innebära allt från minskad mängd producerat vatten till en total avstängning av processen under en längre tid. Hur allvarligt angreppet blir beror på hur snabbt situationen kan avhjälpas. I ett initialt skede kan det vatten som redan finns i reservoarer och vattentorn fungera som en buffert. En snabb återställning av produktionen gör då att konsumenterna inte märker av händelsen.

I det fall ett produktionsbortfall blir så allvarligt att vattenbrist i näten uppstår kan samhällspåverkan bli stor. Under vissa omständigheter är det möjligt att koppla förbi reningen av det inkommande råvattnet så att konsumenterna kan använda toaletter, tvätta sig och kanske koka dricksvatten. Det förutsätter dock att vattnet är tillräckligt tjänligt och att angreppet inte har påverkat pumpsystemen. Notera även att ett längre tryckfall i ledningsnätet, även om produktionen inte helt avstannar, kan leda till att mikroorganismer kommer in i ledningsnätet från markvatten, vilket i sin tur kan leda till fara för infektioner för konsumenterna och ta lång tid att skölja bort.

Även industrier som är beroende av vatten behöver agera vid ett produktionsbortfall i vattenproduktionen när de inte kan få de mängder vatten de normalt behöver. Om de inte kan upprätthålla sin produktion

[11] Vilken bäst beskrivs av att den tillfällige IT-chefen informerat stadens fullmäktige att stadens servrars säkerhetssystem var så gammalt att tillverkaren inte längre tillhandahöll service.

kan det leda till en förvärrad situation när deras kunder i sin tur inte får de tjänster eller resurser de behöver.

3.3 Föroreningar i dricksvattnet

Utöver tillgänglighet till vatten utgör föroreningar i dricksvattnet en fara för liv och hälsa. En angripare skulle, genom att anfalla de delar av systemen som sköter reningen av vattnet, kunna orsaka att organismer eller hälsofarliga ämnen kommer in i dricksvattennätet.

Flera exempel illustrerar hur angripare har försökt att förorena dricksvattenproduktion, ofta genom att ändra proportionerna av lut, fluor eller klor i processen (Greenberg, 2021; Chawaga, 2022; Aslam, Tufail, Kim, Apong, & Raza, 2023).

Till exempel drabbades ett dricksvattenverk i Israel 2020 av en incident som enligt Yigal Unna ('Cyber winter is coming,' warns Israel cyber chief after attack on water systems, 2020), chef för Israels cyberdirektorat hade kunnat få mycket allvarliga följder:

> ”If the bad guys had succeeded in their plot we would now be facing, in the middle of the Corona crisis, very big damage to the civilian population and a lack of water and even worse than that”

Exakt vad som skedde har inte officiellt kommenterats men enligt Unna kunde klor ha blandats in i råvattnet i felaktiga proportioner vilket skulle ha kunnat resultera i ”skadlig eller katastrofal utgång”.

Men trots att ett antal angrepp har försökt orsaka skada på detta sätt har de faktiska effekterna hittills varit små. Generellt har vattenverk separata system för att övervaka föroreningar. Dessa har hittills inte varit uppkopplade till internet och har larmat innan tillräckligt mycket förorenat vatten hunnit produceras. Det krävs ganska stora mängder föroreningar för att det ska kunna påverka konsumenterna i och med att vattnet späds ut i reservoarer, ledningsnätet och vattentorn.

År 2010 fick mikroorganismen Cryptosporidium spridning i Östersunds ledningsnät när det befintliga reningssystemet inte stoppade det. Utbrottet var i detta fall inte resultatet av en angripares åtgärder utan berodde på att den invasiva organismen var ny i ekosystemet och skydd

mot den därmed inte hade behövts tidigare. Incidenten utgör dock ett exempel på hur biologisk spridning skulle kunna ske om delar av reningen sätts ur spel (Sjukdomsinformation om cryptosporidiuminfektion, 2019).

Ett kombinationsangrepp där en större mängd skadliga ämnen externt tillförs systemet (genom till exempel intaget vid en dricksvattentäkt) samtidigt som reningssystemet deaktiveras skulle kunna åstadkomma allvarlig skada. Inget sådant angrepp har dock observerats hittills.

En slutsats som går att dra av detta är att det inte verkar sannolikt att kunna åstadkomma större akuta skador med de befintliga kemikalier som används i processen om det finns personal som kan ingripa i tid vid larm. Detta kan dock behöva undersökas ytterligare i samarbete med VA-organisationerna.

3.4 Fysisk skada på utrustning

Det finns demonstrationer av cyberangrepp där industriell utrustning har blivit fysiskt förstörd (Gjendemsjø, 2013) och det har även skett skarpa angrepp (Lee, Assante, & Conway, 2014) vilka har orsakat stor ödeläggelse. Dessa är dock relativt sällsynta då industrisystem byggs för att fungera under svåra förhållanden, vilket innebär att en angripare både behöver övervinna de spärrar som maskinen själv besitter och de passiva system som omger den (exempelvis säkringar eller överflödesventiler) innan skada kan sprida sig från maskinen till omgivningen.

Exakt vad som kan åstadkommas är helt beroende av hur det lokala systemet är byggt och vilken process det sköter. Ett exempel är det järnverk som angreps i Tyskland 2014 (Federal Office for Information Security (BSI), 2014). I och med att industriprocessen var beroende av ständig kylning räckte det med att angriparen lyckades stänga av kylvattnet för att ugnarna skulle överhettas till den grad att anläggningen måste evakueras och sedan påvisade omfattande skador. Andra typer av processer kanske inte kan skadas fysiskt genom datorstyrning. Även om den här typen av angrepp hittills är ovanliga är det vitalt att OT-system byggs på ett sådant sätt att man planerar för möjlig felaktig styrning av en cyberangripare på samma sätt som man planerar för operatörsmisstag i den fysiska miljön.

3.5 Förlust av information - tillfälligt eller permanent

En angripare som vill skaffa sig information, till exempel för industrispionage, kan använda cyberangrepp för att få tillträde i stället för att göra fysiska inbrott. Denna typ av angrepp riktar sig sällan mot styrsystemen i sig då proprietär information normalt lagras i kontorsnäten, men i praktiken är de moderna styrsystemen inte fysiskt åtskilda från kontorsnäten då datadelning från driftövervakning och andra tjänster behövs av rent ekonomiska skäl. Ett misstag i säkerhetsarbetet kan leda till att det från kontorens ändpunkter (se beskrivning i kapitel 4.3.1) oavsiktligt går att nå OT-sidans utrustning. Dessa kommunikationsvägar blir angreppsvektorer[12] via vilka skadlig kod skulle kunna påverka OT-sidan.

Angrepp där information exfiltreras[13] eller krypteras för att hållas som gisslan kan få stor påverkan. Dessa sker nästan alltid med automatiserad programvara, så kallad ransomware. Konsekvenserna av ett sådant angrepp är direkt beroende av graden av förberedelser såsom säkerhetskopior, segmentering[14] av nätverken, möjlighet till återställning och så vidare. Ett dåligt utfört förarbete kan leda till enorma kostnader och permanent förlust av data.

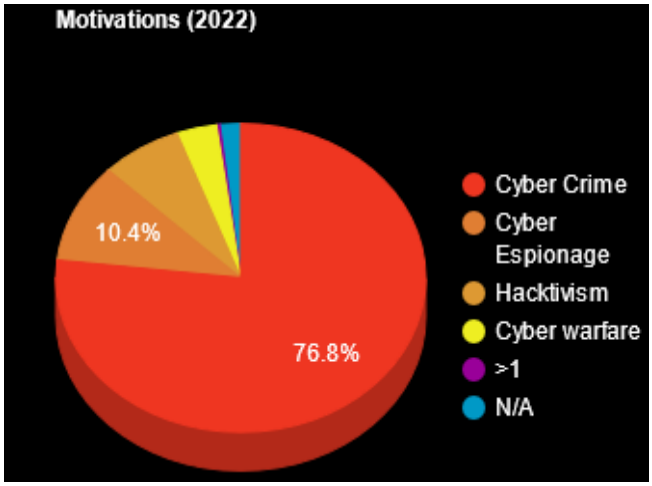
3.6 Hotaktörer

Med hotaktörer menas här de angripare som aktivt försöker försätta systemen i osäkra eller farliga lägen. Hotaktörer delas normalt in i olika kategorier baserat på vilken teknisk och ekonomisk förmåga de har, samt vad som motiverar dem. En fördelning av de vanligaste hotaktörerna för 2022 kan ses i figur 2.

[12] Angreppsvektor är en potentiell väg eller metod för en angripare att nå systemen.

[13] Exfiltration är olovlig kopiering av data till lagringsplatser utanför organisationen.

[14] Segmentering är en uppdelning av datornätverken med spärrar mellan delnät i form av brandväggar eller andra säkerhetsåtgärder. Målet är att isolera ett angrepp till en liten del av systemen för att minska konsekvenserna.



Figur 2. Illustration av fördelning av cyberangreppstyper under 2022, sammanställd av Paolo Passeri (2022 Cyber Attacks Statistics, 2023).

3.6.1 Kriminella

I första hand utgörs angripare av kriminella med monetär vinning som mål. Dessa utgör en överväldigande majoritet av angreppen på internet. Under 2022 utgjorde de enligt forskaren Paolo Passeri (2022 Cyber Attacks Statistics, 2023) mer än 75 % av alla angrepp (se figur 2 ovan). Dessa angripare har en mycket stor spännvidd i sin kompetens. Det handlar om allt från amatörer som köpt eller laddat ner sina angreppsverktyg från internet, till välutbildade och organiserade grupper som i princip fungerar som internationella mjukvaruföretag med kriminalitet som affärsverksamhet.

Alla dessa aktörer kan tänkas vara intresserade av dricksvattensektorn som helhet för att kunna utpressa dessa organisationer på pengar. Det kan ske antingen genom att använda ransomware-angrepp med krav på betalning för att återställa informationen de krypterar eller genom att orsaka störningar av driften och kräva pengar för att upphöra med angreppen.

Det finns också ett intresse bland kriminella av att använda organisationers datorsystem för bedrägerier. Sådana kan avse att skapa falska fakturor och betala ut pengar, eller att stjäla personlig information som banklösenord eller persondata för identitetsstöld eller andra bedrägerier.

3.6.2 Hacktivister

Aktörer som använder cyberangrepp som vapen, primärt drivna av en politisk motivation, brukar kallas hacktivister. Exempel från senare år är Anonymous Sudan, en grupp som anfallit svenska webbplatser med överbelastningsangrepp[15] efter att en politiker brände en Koran i Sverige.

Bland hacktivister finns en mycket stor spridning i kompetens även om det stora flertalet organisationer oftast använder tekniskt enkla metoder. Dessa metoder kan vara tillräckliga för att nå ett mål som exempelvis kan avse publicitet för en politisk fråga eller trakasserier av politiska meningsmotståndare.

Hotet från hacktivistangrepp gäller inte bara för politiska aktörer, utan för alla de organisationer där ett angrepp kan leda till publicitet eller politisk effekt. Det kan innebära att även ett vattenverk kan bli angripet enbart som ett verktyg för att hacktivister ska kunna påverka en annan part.

3.6.3 Främmande makt

Det finns ett antal statliga aktörer som är aktiva på cyberarenan mot Sverige eller svenska intressen (Säkerhetspolisen, 2023). Det kan i sammanhanget rimligen antas att vattenverk är högintressanta mål för att påverka Sverige i händelse av en konflikt.

Efter att USA officiellt startade U.S. Cyber Command[16] 2010 har många andra länder offentliggjort förekomsten av liknande enheter. Dessa agerar tillsammans med underrättelsetjänster för att kartlägga andra staters personal, resurser och infrastruktur i fred. Syftet är att i händelse av en konflikt kunna utföra olika typer av operationer för psykologisk påverkan, ekonomisk påverkan och understöd till konventionella truppers agerande genom cyberoperationer.

Det finns relativt lite stöldbegärlig information i vattenverk eftersom programvaran för styrsystemen nästan alltid är känd och kan köpas på den öppna marknaden. Vidare är de data som lagras sällan hemliga i någon större utsträckning. Det innebär sammantaget att

[15] Överbelastningsangrepp sker genom att man sänder ett stort antal anrop till en webbplats, vilket orsakar att legitima användare inte får tillgång till webbplatsen.

[16] U.S. Cyber Command är ett amerikanskt militärkommando som ansvarar för cyberkrigsföring.

underrättelseinhämtning från vattenverk sannolikt inte är särskilt intressant.

Däremot är dricksvatten en av våra absolut viktigaste resurser så det som ligger nära till hands för vattenverk är hotet om sabotage av driften. Exempelvis som en del av en påverkansoperation då driftstoppet kan utnyttjas för att åstadkomma en politisk eller psykologisk effekt alternativt för att orsaka logistikproblem när distributionen påverkas så pass mycket att konsumenten märker av det.

Cybermiliser är en annan term som myntats för att referera till hacktivistorganisationer som egentligen är statskontrollerade. Genom att använda en front som trovärdigt kan förnekas kan stater agera utan att ställas till svars. I händelse av en konflikt skulle stater kunna vilja slå mot vattenverk på samma sätt som en normal hacktivistgrupp men för att egentligen uppnå andra mål.

3.6.4 Insiders

Insiders är angripare som tillhör den egna organisationen. Denna aktörskategori skiljer sig från de andra i den meningen att angripare som är insiders också normalt kan klassas i en annan grupp, än till exempel kriminella eller aktivister beroende på bakomliggande motiv.

Insiders utgör en stor fara mot organisationen i och med att de redan har tillgång till lokaler och system. De har dessutom information som utomstående inte har om hur systemen är uppbyggda och ofta någon form av etablerad identitet i systemen. Till skillnad från andra angripare har de därmed rättigheter i systemen genom normal inloggning och kan passera många av de säkerhetsåtgärder som skyddar nätverken.

Dessutom har de som medlemmar i organisationen normalt ett mycket större förtroendekapital än en främling och kan använda detta för att manipulera andra anställda att ovetandes utföra åtgärder som främjar angrepp.[17]

Insidern är därmed den angripare som kan orsaka större skada i förhållande till sina resurser och kompetens än andra kategorier.

[17] Denna verksamhet kallas ofta för social ingenjörskonst.

4 Sammanställning av intervjuerna

I kapitlet presenteras resultaten från gjorda intervjuer med medarbetare från de fem dricksvattenproducenter som deltog i studien. Syftet är att översiktligt redovisa hur respondenterna ser på informations- och kommunikationsflöden i verksamheten, säkerhetsarbete som utförs, utbildningsbehov samt vilka hot och utmaningar som föreligger och hur dessa hanteras i verksamheten.

Deltagarna har ibland använt IT som term för kontorssystem och ibland för övergripande informationssystem samt för delar av OT-system. I kapitlet nedan används IT/OT för att benämna datorsystem, delar av datorsystem och det ensamma IT eller OT endast när respondenterna poängterade denna tillhörighet.

4.1 Bakgrund

Här beskrivs i korthet de vattenverksamheter som är representerade i studien samt vilka roller och funktioner som respondenterna företräder.

4.1.1 De studerade verksamheterna och dess företrädare

De organisationer som representeras i studien är alla organiserade som kommunala bolag. Antalet anställda varierar från 100 till 1000 och ansvaret avser allt från några få till cirka tjugo vattenverk med olika produktionskapacitet. Bolagen skiljer sig också åt vad gäller kundantal och kundkrets samt avseende IT-verksamhetens utformning. Med hänsyn till IT-avdelningens placering kan den till exempel vara intern eller extern. En ytterligare skillnad mellan organisationerna är den geografiska utbredningen. En stor utspridning av verksamheten påverkar säkerhetsarbetet i fråga om bevakning, responstider, bemanning och behov av fjärrstyrning. Noterbart är också att alla organisationer, utöver vattenproduktion, även har ansvar för andra verksamhetsområden såsom vattendistribution, avlopp eller energiproduktion. För flera av bolagen är det vanligt att det är samma datornät, styrsystem och PLC:er som sköter vattenproduktionen och de övriga verksamhetsområdena.

I studien ingår organisationer som har bolagsintern IT-avdelning, som nyttjar kommunens IT-avdelning och sådana som har externt

upphandlade IT-tjänster. Kompetens gällande OT finns oftast inom den egna organisationen. De respondenter som finns representerade i studien har olika roller och funktioner. På ett övergripande plan kan dessa roller och funktioner delas in i fyra kategorier: *säkerhetsansvarig, IT-ansvarig, OT-ansvarig* och *verksamhetsansvarig vatten*. De intervjuade har olika kompetenser som kopplar till säkerhetsområdet, såsom fysisk säkerhet och IT-/OT-säkerhet. OT-säkerheten är i samtliga fall kopplad till driften medan IT-säkerheten har olika lösningar som både kan vara kopplade till drift och kontors-IT.

4.1.2 Samverkande organisationer

Vid intervjuerna framfördes behovet av samverkan med andra aktörer kopplat till bland annat infrastruktur och kompetens. Denna samverkan beskrivs närmare i de följande avsnitten.

Tillsynsmyndigheten

Samtliga respondenter arbetar i en verksamhet som faller under NIS-direktivet, utifrån vilket Livsmedelsverket utför tillsynen på vattenverken. De intervjuade gav uttryck för en positiv inställning till den tillsyn som Livsmedelsverket utför. Bland annat utgör den dels ett kvitto på det utförda arbetet, dels ett stöd för framtagande av riktlinjer för verksamheten.

Alla respondenter lyfte NIS2 och att arbetet med att hantera det nya direktivet redan påbörjats. Även om direktivet innebär stora arbetsinsatser ses direktivet också som en möjlighet till mer konkret information om vilka åtgärder som ska genomföras. Det anses vidare medföra att ansvaret för informationssäkerhet tydliggörs för ledning och styrelse med förhoppningen att frågorna prioriteras i högre grad.

Vid intervjuerna framgick att NIS2 och CER i framtiden kommer att innebära nya förhållningsregler. Respondenterna framhöll i sammanhanget ett behov av att tillsynsmyndigheten och andra myndigheter på ett konkret sätt ska förtydliga hur vattenverksamheterna ska arbeta för att praktiskt uppfylla sina juridiska skyldigheter.

Kommuner

Samverkan är omfattande mellan bolagen och kommunerna, framförallt i de mindre organisationerna där det saknas en egen IT-avdelning och man

använder kommunens IT-resurser. I flera fall har det framkommit att verksamheterna har sina produktionsnät och förvaltning av dessa inom kommunens infrastruktur. Nätverken är då segmenterade från resterande IT-miljö. Krav på nätdelning och segmentering specificeras i NIS-direktivet. Det är också något som samtliga verksamheter framhåller som viktigt i den meningen att man delar upp datornätverken i olika segment så datatrafik inte kan flöda fritt mellan dessa.

De verksamheter som använder kommunens IT-avdelning är naturligtvis beroende av kommunens kompetens och dess resurser såsom nätverkstekniker och systemtekniker.

Privata aktörer

De verksamheter som använder eller anlitar en extern IT-avdelning är beroende av denna kompetens och dessa resurser. För en av organisationerna i studien gäller att det är den externa parten som förvaltar servrar och databaser.

Samtliga verksamheter använder sig av privata aktörer som konsulter och leverantörer, men i olika omfattning. I vilken mån verksamheten förlitar sig på dessa varierar. Till exempel är beroendet av leverantörer för styrsystem stort hos samtliga verksamheter till följd av den expertkompetens leverantörerna besitter, bland annat gällande underhåll och uppdateringar. En ambition hos flera är dock att minska detta beroende.

4.1.3 Regleringar och standarder

Alla verksamheter arbetar med riktlinjer, strategier och riskanalyser. Gällande IT-säkerhet nämnde samtliga organisationer ISO 27000 standarderna som styrande för verksamheten. Dessa innehåller konkreta åtgärder för dataskydd samt cyber- och informationssäkerhet. Främst nämndes ISO 27001 som beskriver vilka krav som finns (ISO/IEC 27001:2022, 2022) och ISO 27002 som innehåller riktlinjer för åtgärder (ISO/IEC 27002:2022, 2022).

4.2 Informations- och kommunikationsflöden samt systemunderhåll

Den ökade digitaliseringen av branschen medför nya risker gällande IT/OT-säkerhet. Dessa risker ställer nya krav på informations- och kommunikationssäkerhet, bland annat i form av säkerhetskopior och rutiner för systemimplementering. Användning av molntjänster är ett exempel på en sådan teknisk utveckling som också kan ha bäring på dricksvattenproduktionen. På frågan om vilket system som är viktigast för dricksvattenproduktionen, svarade majoriteten att SCADA-systemet är det allra viktigaste.

4.2.1 Kommunikationstjänster

För att dricksvattenverksamheten ska fungera behövs kommunikationstjänster och i samband med detta pekade respondenterna ut teleoperatörer som en avgörande aktör. Detta kopplades till att vattenverksamheten och produktionen i många fall är spridd över en geografiskt stor yta. Fiber och fjärranslutning lyftes fram som centrala i sammanhanget som nödvändiga för att kommunicera över den geografiskt spridda verksamheten.

Fiber

Fiber framstår som organisationernas förstahandsval. Flera av verksamheterna har egen fiber, så kallad svartfiber, som är avsedda för den egna verksamheten och som kan kompletteras med andra fibernätverk.

Fiber finns inte alltid tillgängligt, vilket gör att det kan finnas flera olika kommunikationsmetoder inom samma produktionsanläggning, till exempel där det finns flera vattenverk utspridda över större geografisk yta. I dessa fall används även 4G och radio, där radio främst fungerar som en reservlösning vid problem.

Fjärranslutning

För att kunna fjärransluta till produktionsanläggningarna krävs behörigheter och anslutningen sker via VPN[18]. Kommunikationen är

[18] Virtuellt privat nätverk

krypterad och går via en jumphost[19] för att ta sig förbi brandväggar som finns. För att komma åt anläggningen och SCADA-systemen behöver det aktuella kontot ha korrekt behörighet. Behörighetskontroll sker via multifaktorautentisering med bland annat lösenord och BankID, samt i vissa fall dedikerad hårdvara.

Externa användare, till exempel konsulter, omfattas ibland av ytterligare begränsningar gällande behörighet såsom tidsbegränsningar. Respondenterna nämnde även rutiner för att hantera behörigheter för ordinarie personal, exempelvis rensning av behörigheter när någon har slutat. Det framkom i några intervjuer att det saknades rutiner för hantering av behörigheter vid interna rollbyten.

Molntjänster

Samtliga respondenter var eniga om att molnlösningar inte är en bra lösning i en dricksvattenanläggning. När det gäller OT så ska inga molntjänster användas utan allt ska vara on-premises[20], alltså i anläggningen. På kontorsmiljöns IT-sida används en del molntjänster för kringtjänster och administrativa system. Vissa verksamheter beskriver att de använder molntjänster eller SMS för att ta emot larm men att det inte är en kritisk del av verksamheten.

Vid intervjuerna framkommer en oro kring att det i dagens läge finns andra aktörer eller medarbetare inom samma organisation som tycker molntjänster är en bra lösning. Det efterfrågas fler och bra argument för dem att nyttja och föra vidare som påvisar de negativa sidorna med molntjänster. En organisation nämnde att det finns andra som arbetar med SCADA-as-a-service[21], och det finns en farhåga att man då är extremt beroende av externa tjänster för att hålla igång produktionen, vilket man behöver vara medveten om. Det framkommer en tydlig oro för att andra i branschen överväger molntjänster av denna typ men de respondenter vi talat med skulle aldrig överväga att använda sådana lösningar.

[19] Hoppserver. Används för att på ett säkert sätt ta sig mellan delar i ett nätverk.

[20] Ha mjukvara och hårdvara lokalt

[21] Använda SCADA som en molntjänst

4.2.2 Leverantörstjänster

Det är inte ovanligt att man har sina styr- och mätsystem i drift länge - en organisation nämnde att man haft ett tidigare styrsystem i 30 år. Leverantörerna av systemen är i detta fall experterna på just sitt system och kommer ibland in till verket för att göra förbättringar, felsökningar och uppdateringar. En verksamhet nämner att det ändå är viktigt att kunskapen också finns inne i den egna verksamheten. Det bör finnas redundans och att verksamheten själv ska ha koll på sina system. Vissa av respondenterna beskriver att det ibland kan bli missförstånd då leverantören är expert på sitt system men kanske inte alltid har den fulla förståelsen för processen i ett vattenverk som kan behövas. Det kan även gälla vilka säkerhetskrav som finns i verksamheten som leverantören inte är insatt i.

Upphandlingar av leverantörssystem av dessa slag innebär en lång process och antalet leverantörer är begränsat. Respondenterna berättar att organisationerna har en hög tilltro till leverantörerna men att de fortfarande har säkerhetsåtgärder för fjärranslutningar som leverantörerna använder.

Det framkommer i intervjuerna att det varierar i vilken grad personal vid dessa anläggningar har möjlighet att påverka och arbeta i systemen. Vissa har ingen åtkomst alls för att göra förändringar, vilket skapar ett beroende av leverantören vid uppdateringar eller systemunderhåll. Respondenterna ser det som problematiskt att de har ett högt leverantörsberoende, delvis för att de behöver förlita sig på leverantörens säkerhetsarbete och menar att säkerhetsansvaret och den tekniska kompetensen och kunskapen borde ligga på respondenternas organisationer. Detta anses vara viktigt för att kunna förebygga och åtgärda problem.

4.2.3 Implementering av nya system

Vissa organisationer nämner inte hur processen ser ut för att koppla in nya enheter på de olika nätverken. En respondent berättar att det inte finns en nedskriven process för det, men att de installerar om, lägger på antivirus, krypterar förbindelser, härdar systemen och segmenterar. En annan organisation säger att de på IT-sidan har agenter som håller koll på alla enheter som kopplas in i på nätverken och att det är svårt för icke godkänd utrustning att kopplas in på dessa nät. Enligt respondenterna är

denna typ av lösningar svårare att implementera på OT-sidan men det är också mindre sannolikt att det inträffar sådana incidenter på de näten.

En verksamhet tar upp att det finns regler gällande att koppla in enheter i nätverken, och att de till exempel inte får förflytta och koppla in datorer mellan OT-näten och andra nät. I dessa fall har de dubbla enheter för att hålla näten och kopplingen mellan dem helt separerade. Respondenterna påpekar att utbildning därför är viktigt så att inte en anställd av misstag kopplar upp enheter på nätverk där de inte ska vara.

4.3 Säkerhetsarbete

Respondenterna upplever att säkerhetsarbetet trappats upp de senaste fem till tio åren. Uppfattningen de redogjorde för är att det skett en förflyttning av fokus från fysisk säkerhet och informationssäkerhet till IT-säkerhet. I sammanhanget framhölls att det var lättare att arbeta med, och få förståelse för, den fysiska säkerheten, än för arbetet med IT-säkerhet. Ansvaret för IT-relaterade frågor som rör OT-miljöerna kan falla på de som arbetar på vattenverken. Det finns ingen komplett separation mellan IT- och OT-nät i dagsläget, men det finns bryggor mellan dessa. Hur dessa bryggor ser ut och vilka säkerhetsåtgärder som finns för att hindra obehöriga att röra sig mellan dessa miljöer ser olika ut på de olika verksamheterna. Hos samtliga är dessa bryggor krypterade och kräver multifaktorautentisering, och i vissa fall krävs dedikerad utrustning för att få tillgång till OT-näten. Nedan presenteras hur respondenterna arbetar med säkerhetsarbete och vilka konsekvenser en cyberattack skulle kunna få på verksamheten.

4.3.1 Ändpunkter

Datorer, mobiler, klienter, servrar och andra system kallas för en organisations nätverksändpunkter. Skulle någon obehörig få åtkomst till ändpunkter finns risk att man via dessa kan ta sig till andra system. Enligt respondenterna har ett antal säkerhetsåtgärder implementerats för att förhindra den sortens intrång.

Samtliga respondenter har högt förtroende för implementerade säkerhetslösningar. De menar att kombinationen av lösningar med allt från multifaktorautentisering och användning av dedikerad hårdvara som krypterade, härdade datorer med avancerade antivirusprogram bidrar till

den höga säkerhetsnivån. Vidare är kommunikationen mellan systemen krypterad och det finns rutiner på plats för förvaltning och säkring av systemen.

En utmaning som lyfts vid intervjuerna är att vissa organisationer inte har tillräcklig egen förmåga utan är beroende av kommunens IT-kompetens för att kunna göra riskanalyser och klassning av system och information. De framhåller även att det kan vara svårt att göra dessa riskanalyser eftersom systemet och information som systemet ska hantera anses ha olika klassningar.

4.3.2 Säkerhetskontroller av personal

Fyra av fem verksamheter anser att säkerhetskontroller av personal är en viktig förebyggande åtgärd inom säkerhetsarbete. De påtalar att dricksvattenproduktion kan vara en säkerhetskänslig verksamhet och där så är fallet säkerhetsprövas och säkerhetsklassas ny personal på vattenverket. Beroende på roll och funktion i verksamheten görs ibland istället egna interna säkerhetskontroller på ny personal. En av organisationerna gjorde ingen säkerhetsklassning av personalen. De har låg personalomsättning och beskriver att det alltid är någon som känner den nya medarbetaren som anställs.

Kommuner gör ibland säkerhetsklassningar på sin personal. Vad gäller säkerhetskontroller av externa aktörer, såsom leverantörer av cyberfysiska system, tecknas särskilda säkerhetsavtal.

Några av de intervjuade nämner att det finns problem kring att man inte får göra kontroller av redan anställd personal samt gråzoner kring när man klassas som ingående i samhällsviktig verksamhet, och om verksamheten då faller under säkerhetsskyddslagen eller ej.

4.3.3 Hot- och riskbedömningar

Majoriteten av respondenterna anser att verksamheten är utsatt för hot och att angreppsrisken har ökat drastiskt de senaste åren. De förväntar sig därför att cyberangrepp kan riktas mot verksamheten. En del i säkerhetsarbetet handlar om att göra hot- och riskbedömningar vilket görs regelbundet. Bedömningarna initieras och genomförs på olika sätt. Flera av de tillfrågade använder Säkerhetspolisens årsrapporter för att få en generell uppfattning om hotbilder, samtidigt som de genomför egen

omvärldsbevakning. CERT-SE[22] är en viktig källa för att hålla sig uppdaterad. De verksamheter som har egen IT-personal är de som verkar vara mest uppdaterade kring aktuella cyberangrepp i världen.

Säkerhetsanalyser

Alla studerade vattenverksamheter gör olika typer av säkerhetsanalyser där hot, risker, sårbarheter samt åtgärder beaktas. Ett sätt att genomföra analyserna är att följa vattnets väg och samtidigt göra en inventering. Det innebär att följa vattnets väg från intag till färdigt livsmedel och analysera teknik och risker vid delstationerna. Resultatet från säkerhetsanalyserna resulterar i en åtgärdslista. I flertalet fall belyser dessa analyser vanliga problem relaterade till grundläggande IT-hygien som är relativt lätta att åtgärda, vilket bidrar till att öka säkerheten i sin helhet. Dessa bedömningar innehåller inte endast IT-relaterade hot utan kan också gälla andra typer av hot. Arbetet med dessa analyser inkluderar personal med olika kompetenser och kan göras tillsammans med till exempel kommunens IT-verksamhet. Respondenterna nämner även ett antal forum vid olika myndigheter och branschorganisationer som de använder sig av vid hot- och riskanalyser. De framhåller vidare vikten av samarbete kring dessa frågor för att Sverige ska upprätthålla tillräckligt bra kunskap och förutsättningar på nationell nivå.

Hotaktörer

Vid diskussioner om hot var det två aktörer som respondenterna såg som relevanta: kriminella aktörer och insiders. Enligt en verksamhets säkerhetsanalys är kriminella aktörer det största hotet medan statliga aktörer inte ses som ett stort hot. Analysen hade gjorts med avseende på att verksamheten utgör ett mindre bolag och att större vattenproducenter troligen hade en större hotbild från statliga aktörer. De flesta respondenter nämnde insiders som det största hotet och påtalade samtidigt att det kanske var det svåraste hotet att skydda sig mot. Anställda med tillgång till systemen har stora möjligheter att skada verksamheten, avsiktligt och oavsiktligt. För att minska risken har en av verksamheterna prioriterat arbetet med att löpande utbilda personal. Några respondenter ansåg att tydliga regler för vilka personer som ska ha

[22] CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team).

tillgång till vilka funktioner, ett arbete enligt principen ”least privilege”[23], minskar risken för mänskliga misstag. Det framkom vidare att gruppkonton för att logga in på vissa system är en sedan länge tillämpad metod som dock används i allt mindre utsträckning, bland annat för att åstadkomma spårbarhet kring vem som varit inloggad när.

4.3.4 Kontinuitetsplanering

Kontinuitetshantering handlar om att hålla igång verksamhet på en tolerabel nivå, oavsett vad organisationen har påverkats av (MSB1501, 2020). Verksamheten ska kunna klara av olika typer av störningar, vilken kan innefatta strömavbrott såväl som cyberangrepp.

Arbete med kontinuitetsplan

Samtliga intervjupersoner angav att deras organisationer arbetar med kontinuitetsplanering. Att ta fram planer för hanteringen av en incident är en av flera aktiviteter som ingår i kontinuitetshanteringen. En av respondenterna nämner att de har kontinuitetsplaner för alla funktioner inom vattenverket, men att det i övrig verksamhet pågår ett förbättringsarbete kring detta. Det nämns att kontinuitetsplanen för snabb hantering måste finnas fysiskt tillgänglig på vattenverken i samband med en störning. Detta är viktigt att beakta, inte minst mot bakgrund av den pågående digitaliseringen av branschen. På vattenverken har man till exempel prioriterat att ha fysiska kopior av olika instruktionsmanualer tillgängliga så att man alltid ska kunna hålla produktionen igång utan tillgång till IT-system.

Respondenter beskriver att kontinuitetsplanens roll kan illustreras med ett exempel från en nyligen inträffad incident. Planen kunde bistå med avgörande information i form av en karta över ledningar och vem som hade tillgång till dem.

Det kan finnas utmaningar relaterat till digitalisering vid nya, stora vattenverk där skalan och komplexiteten hos de interagerande systemen gör det svårt att ta fram en kontinuitetsplan. Vid de små vattenverken, med få system och pumpar, är det relativt enkelt att hålla driften igång, men i större anläggningar kan det vara mer komplicerat. Det kan

[23] ”Least privilege” innebär att man inte ska erhålla mer behörighet än vad man behöver för sitt arbete.

dessutom vara ett problem när nyanställd personal, som saknar erfarenhet, ska hantera störningar. Det finns också en risk att nya anläggningar inte är utformade för att hantera manuell styrning i en större skala.

Öva på kontinuitetsplanen

Kontinuitetsplanerna testas ofta, bland annat genom övergång till manuell drift. De innehåller inte enbart cyberrelaterade problem utan även andra typer av störningar. Ibland får de testas skarpt, exempelvis vid blixtnedslag. Kontinuitetsplaneringen inkluderar även scenarion som att det kommer in oönskade kemikalier, problem med eltillförseln, cyberattacker och personalbrist.

En verksamhet vi intervjuar går igenom sin kontinuitetsplanering med jämna mellanrum, dock inte kontinuerligt enligt given tidsperiod. En annan verksamhet uppdaterar och testar sin plan minst vart fjärde år. Det faktum att den testas är en del av kontinuitetsplanen i sig.

En av verksamheterna har skaffat ett extra system för att kunna öva samt har redundans om det blir problem med det primära systemet. De har även köpt in servrar för att testa att återställa systemen vilket de anser är viktigt att öva på. De menar att de inte ska vara naiva och tro att de kan göra all återställning och ha redundanta system som fungerar fullt ut, utan de övar så att de kan säga att de vet att de kan göra det. En av respondenterna säger att de behöver uppdatera och öva på sin kontinuitetsplan för att veta att den fungerar, och det viktigaste är att alltid kunna återställa både IT- och OT-system.

Synen på kontinuitetsarbetet

Generellt rörande kontinuitetshanteringen anser respondenterna att *orsaken* till problemet inte är lika viktigt som *resultatet* av problemet. Det medför att hanteringen sällan är direkt inriktad på IT-attacker som orsak till problemen. Planen innehåller istället exempel på hur verksamheten ska hantera att en viss tillgång är borta (till exempel en databas). I första läget är inte fokus på att ta reda på varför tillgången försvann, utan det kan bero på cyberangrepp eller något helt annat som gör att man inte kommer åt tillgången.

Säkerhetskopia och säkerställande av system

Verksamheterna arbetar med tre olika typer av säkerhetskopior: en man kan återställa omedelbart, en off-line och en off-site. Vissa har redundanta SCADA-system som är på två parallella servrar, som det också görs säkerhetskopior av. Några nämner att de har säkerhetskopior på allt, och att de har säkerhetskopior både on-site och off-site, och att dessa förvaras på ett säkert ställe. Virtuella maskiner används ibland, där man använder ett snapshot (en ögonblicksbild), vilket gör det lätt att återställa dessa.

En respondent nämner att trots att de har säkerhetskopior på sitt SCADA-system, är det inte så enkelt att bara stoppa in en hårddisk och sedan att få allt att fungera igen. Det krävs en del arbete för att sätta upp systemet och ställa in alla parametrar. Just de personerna vi pratat med i denna verksamhet vet inte om de har säkerhetskopior på olika ställen, det är information de säger att de borde ha men de vet inte.

De olika systemen säkerhetskopieras kontinuerligt, system off-site lite mer sällan än system som är on-site, men alla enligt en given tidsram. Det sparas också några versioner tillbaka för att säkerhetsställa att man har en säkerhetskopia som fungerar och som inte är kontaminerad.

4.3.5 Förväntade konsekvenser av cyberattacker

Hur organisationerna skulle hantera en cyberattack beror på vilken sorts attack det skulle vara. En organisation tar upp att det skulle kunna få stora konsekvenser om någon skulle förfalska information eller styra anläggningen men uttrycker samtidigt att det är just det som de skyddar sig bra emot.

Flera uttrycker att om något misstänkt hittas i deras nät så kopplar de bort segmenten från varandra, och isolerar systemen i en ”ö”, samt går över till manuell drift (ö-drift) om nödvändigt. Samtliga är övertygade att de kan hålla produktionen igång samtidigt som de noterar att det kommer krävas mer personal och rondering. Kommer det in något från kontorsnätet, som en e-post som krypterar data, så ska det inte kunna komma in i OT-näten. Olovlig kommunikation mellan dessa nät ska inte kunna ske, men vid misstanke om intrång kopplas kablar ur som en ytterligare säkerhetsåtgärd så att det fysiskt inte finns någon koppling alls. En av respondenterna säger att ett användarkonto med rätt behörigheter,

som någon kan missbruka, är den största svagheten. Det belyser återigen det faktum att mänskliga misstag och en eventuell insider skulle vara det största hotet.

Vid en eventuell cyberattack som skulle vara förstörande för systemen och den information som finns i dem, så skulle de behöva använda sina säkerhetskopior för att återställa miljön. Det skulle krävas en del arbete för att ta reda på hur långt tillbaka man ska återställa - man vill ha en så aktuell version som möjligt men inte en version som redan var infekterad. En respondent menar att vid en eventuell attack är det viktigt att stoppa attacken, stänga ute de som eventuellt fått tillgång till systemet, påbörja arbetet för att säkerhetsställa vad som hänt och återställa plattformen och alla system.

Samtliga respondenter har en bild av att de skulle kunna hantera en attack som kommer utifrån bra. De har många säkerhetslösningar som är på plats för att förhindra att det ska gå att röra sig lateralt mellan system. Det finns även planer för hur de ska isolera och gå till manuell drift vid behov. Säkerhetskopior för systemen finns, och endast mer personal skulle behövas. En av anledningarna till att de skulle klara det bra är för att dricksvattenproduktionen hos flera av organisationerna inte är tidskritisk, eftersom det finns reservreservoarer och vattentorn. Konsumenterna skulle inte bli utan vatten från den minut som vattenverket står still, och målet är att konsumenterna inte ska märka någon skillnad vid kortare driftstörningar. De nämner att de har i kontinuitetsplanen att återställa säkerhetskopiorna för SCADA på ett dygn, och på ett av de större vattenverken finns reservvatten för att hantera att vattenverket skulle stå still under samma tid.

Gällande dagens krav på rapportering till tillsynsmyndigheten påtalade nästan alla att de skulle ha svårigheter att göra relevant rapportering till tillsynsmyndigheten om de skulle behöva gå över till manuell drift under en längre tid. Detta beror bland annat på att det kommer att vara svårt att få tillgång till tillräckligt bra mätdata kring hur mycket dricksvatten som produceras.

4.4 Säkerhetsutbildning och övningar

Utbildning av personal är något samtliga verksamheter arbetade med, framförallt grundläggande säkerhetsutbildningar inom både informations- och cybersäkerhet.

4.4.1 Utbildning

Oftast sker de flesta utbildningar vid en nyanställning men ofta får de som har en säkerhetsklassning en årlig utbildning kopplat till dennes klassning. De flesta verksamheter som studerades nämnde olika former av nano-utbildningar, det vill säga små, korta, webbaserade utbildningar som sker löpande under året och som är tillgängliga för samtliga medarbetare. Dessa utbildningar upplevs som ett smidigt sätt att kunna lära sig i sitt dagliga arbete utan att verksamheten påverkas.

Relaterat till IT får personalen utbildning i systemens handhavande och grundläggande nätverksutbildning. Även nano-utbildningarna täcker IT-relaterat innehåll. Det verkar vara personal som direkt arbetar med IT som får mer konkret IT-utbildning. Den personalen är då inte alltid i den egna organisationen utan har roller vid kommunen eller extern leverantör.

Utbildningarna kan hållas av egen IT-ansvarig personal, leverantörer för system, Försvarshögskolan, myndigheter såsom MSB och FOI eller en annan extern leverantör av utbildningar. En respondent nämner att de arbetar med personliga utvecklingsprogram, och försöker hitta utbildningar för vad den individen behöver. Det påpekas att det finns en viss svårighet att få gehör och höja medvetenheten och kunskapen om IT-säkerhet och IT-hot generellt inom branschen, och att det delvis kan bero på att det är få personer som arbetar inom dessa områden med en kritisk roll i verksamheten. Den person som har en kritisk roll i verksamheten är ofta den som skulle gynnas mest av en mer fördjupande specialistutbildning. Ett problem är ofta att den personen inte har möjlighet att åka på utbildning som pågår i flera dagar, då det får för stor inverkan på verksamheten.

Respondenterna säger att det finns stor vikt av att öka kunskapen inom IT-säkerhet och IT-relaterade hot för hela branschen, något som branchorganisationen Svenskt Vatten arbetar med att genomföra via bland annat utbildningar.

Samtliga verksamheter arbetar aktivt med utbildningar, men några tycker att de borde bli bättre på utbildningsfrågan såsom att organisera interna utbildningar mer systematiskt. En annan respondent berättar att utbildningarna som genomförs idag sker mycket ad-hoc och att det saknas rutiner för hur och hur ofta en utbildning ska ske och för vilka. Eftersom det inte finns en sådan rutin är det svårt att få ett svar på om man som organisation gör rätt eller inte. En mindre verksamhet tycker de borde bli bättre på att göra nya, uppdaterade utbildningar och det framgår att det i dagsläget är främst interna diskussioner kring vad man ska göra eller inte ska göra och vilka risker som finns. Det finns en syn på att det mesta kring dessa frågor rör sunt förnuft och inte något man behöver utbildas inom.

Generellt tycker alla att utbildningar är viktigt och något som borde kunna genomföras mer, bättre och mer strukturerat. Samtliga är eniga om att den ökade hotnivån i samhället ställer högre krav på utbildningar.

4.4.2 Övningsverksamhet

Vid intervjuerna frågades respondenterna om de genomför några övningar relaterade till cyberincidenter. Svaret var att ingen av dem gjorde detta regelbundet. En av verksamheternas arbetare hade nyligen deltagit på en övning gällande ransomware. En övning som organiserades av en extern större aktör där de övade tillsammans med andra. Sådana övningar sker kontinuerligt men de påpekar att det inte alltid handlar om IT-incidenter utan övning i krishantering generellt.

Det nämndes att en verksamhet nyligen fått in stora övningar för manuell drift i kontinuitetsplanen. Det är ett stort projekt där de kommer ta ut ett affärsområde åt gången (till exempel vattenproduktion) för att öva och att de ska fortsätta öva på liknande sätt kontinuerligt för alla verksamheter. Dessa har även köpt in ett testsystem, för att kunna ha redundanta system och faktiskt öva på olika händelser och kunna se över och utvärdera rutiner och dokumentationen i ett riktigt system. En annan respondent säger att de inte har möjlighet att öva i sina egna system, det skulle få för

stora konsekvenser, men att de har kört Table-Top-övningar[24] istället som de själva anordnar.

En respondent nämner att de nyligen gjort en övning där processägaren av IT-processer skulle beskriva vad de gör om just deras process ligger nere under ett antal timmar. De skulle då beskriva vad avsaknaden av processerna får för konsekvenser och hur lång tid det krävs för att få tillbaka full funktionalitet. Denna övning gjordes på både IT- och OT-sidan. En respondent säger att de inte har några cyberövningar och att det inte är något de riktigt funderat över, men de har påbörjat ett större informationssäkerhetprojekt där fokus har varit att göra analyser och ta fram åtgärder. Flera nämner att de inte har gjort någon cyberövning men att de har övat att köra manuell styrning på vattenverken. Det är viktigt för dem att kunna köra sina system oavsett anledning till problemet. En verksamhet har velat göra några egna skarpa övningar, bland annat nämns en phishing-kampanj, men dessa har fått nej från ledningsgruppen. Phishing är en metod där angriparen sänder ut e-post för att lura mottagaren att klicka på en länk. Organisationer kan göra egna phishing-kampanjer för att se hur de anställda reagerar och huruvida de klickar på länkar. Dessa interna kampanjer gör däremot ingen riktig skada utan används för utvärdering och medvetandehöjande.

Generellt sett verkar det finnas en stor brist på övningar relaterad till cyberattacker hos samtliga respondenter och de har kommit olika långt i om de har en plan för att påbörja sådant arbete. Det är också en fråga om resurser och prioriteringar, där det verkar som att öva på incidenter kommer lägre ner på prioriteringslistan och att göra analyser och åtgärder prioriteras högre. Majoriteten av verksamheterna övar på att kunna gå i manuell drift, och generellt verkar det som att man satsar på att kunna hantera problem oavsett vad anledningen är till att systemen inte fungerar, och det är inte prioriterat att öva på specifikt en cyberattack.

4.5 Utmaningar

Att bibehålla hög säkerhet på vattenverket medför ett antal utmaningar, inte minst kopplat till digitaliseringen inom branschen. Det lyfts problem

[24] Table-Top-övning är en skrivbordsövning där man diskuterar hur man skulle agera i en viss krissituation.

gällande beroendet av leverantörer, offentlighetsprincipen kontra sekretess, kontinuitetsplanering i en digital verksamhet samt brist på personal med rätt kompetens.

4.5.1 Beroende av extern part

I intervjuerna lyftes beroendet av leverantörerna som en utmaning. Beroendet av leverantörer försvårar insyn och kontroll av säkerheten i systemen. Det kan finnas säkerhetsgarantier som leverantören utlovat som eventuellt inte uppfylls och det uttrycktes att det är svårt att kontrollera då det är extern part som bygger systemet som har den expertkunskapen. Ett annat orosmoment skulle kunna uppstå vid en allvarligare kris på en nationell nivå, där en mindre verksamhet som förser ett mindre antal människor med dricksvatten, skulle behöva prioriteras ned jämfört med större anläggningar eller områden i Sverige med starkare försvarskoppling. Det finns ett problem när all kunskap om systemen finns samlat utanför den egna verksamheten. Man har därmed beroenden som i normaldrift inte är ett problem men som potentiellt skulle kunna bli problematiska vid kris.

4.5.2 Offentlighetsprincipen

Respondenterna lyfter att det är onödigt svårt att veta vad som är sekretess och vad som får sekretessmarkeras och vad som faller under offentlighetsprincipen. Är exempelvis alla ritningar över anläggningar en offentlig handling? De upplever att ritningar borde vara sekretessbelagda men det är inte tydligt om dessa får klassas som sekretess. Ritningar bör enligt respondenterna inte vara en offentlig handling. De uttrycker ett behov av att lagstiftningen behöver blir tydligare kring vad som ska respektive inte ska sekretessmarkeras. Idag läggs mycket tid på tolkning av principen. Här beror svårigheten också på att det bland annat handlar om storleken på vattenverken. Det blir mer komplicerat för de verksamheter som har många små verk som sammantaget förser vatten till många konsumenter. Lagarna upplevs lättare att följa då det är ett fåtal stora verk som levererar vatten till många konsumenter än många små.

4.5.3 Kontinuitetsplanering i en digitaliserad vattenverksamhet

En svårighet som en organisation tar upp handlar om kontinuitetsplanering och att vid kris få fram relevant analog information att använda i fält. Respondenterna frågar sig vilken information som bör finnas tillgängligt på annat vis än digitalt, exempelvis analogt i ett säkerhetsskåp. Arbetet med kontinuitetsplanering har försvårats i takt med digitaliseringen, och det är inte helt tydligt hur man ska hantera det.

En respondent uttrycker att kontinuitetsplanering och reservuttag handlar om ”bondförnuft”. Att rätt behörig personal ska veta var listan med relevant information finns om något skulle hända. En av verksamheterna hade genomfört denna planering och kartläggning tillsammans med kommunen vilket de nyligen blivit tvungna att testa i ett skarpt läge på distributionsnätet. De såg då att planeringen hade underlättat mycket vid incidenten, och att incidenten resulterade i ett bra test, samt gav förslag på åtgärder och förbättringar.

Respondenterna efterfrågar statligt ägda kommunikationsvägar som kan användas av samhällsviktig verksamhet. De ser inte poängen med att varje enskild anläggning ska behöva ansvara för den typen av infrastruktur och dess säkerhet.

4.5.4 Personal

Flera respondenter uttrycker att nyrekrytering tar tid och att det är svårt att hitta personal med rätt kompetens. Någon uttrycker även att de tycker sig se en trend att personal börjat arbeta med frågor som rör totalförsvaret istället. En respondent berättar att de i samband med pandemin gjorde en kontinuitetsplanering gällande personalresurser och att den planen även fungerar bra i andra kriser. Alla uttrycker att de har god beredskap för att ta hand om och arbeta med incidenter under en kortare period. Anläggningarna har underhålls- och driftpersonal som kan arbeta i skift för att producera dricksvatten, men det finns utmaningar på lång sikt.

Det finns i dagsläget ingen riktad utbildning mot just VA-organisationer. Det finns även en svårighet att hitta personal med kompetens inom både IT och OT, vilket har blivit viktigare i takt med digitalisering av produktionsmiljön. Rekrytering bygger istället på att hitta bra personer

som har någorlunda relevant utbildning och som vill lära sig verksamheten. Respondenterna menar även att det är viktigt att man arbetar med att behålla den personal man har och i vissa fall samarbeta mer gränsöverskridande inom den egna verksamheten för att bredda kompetensen och nyttja samarbeten internt.

5 Diskussion och analys

Kapitlet diskuterar några teman utvalda från de presenterade intervjuerna i kapitel 4: hotaktörer, angreppsvektorer och utmaningar. Urvalet baserades på vad de intervjuade själva valde att fokusera på under intervjuerna.

5.1 Hotaktörer

Alla organisationer använder extern personal i olika syften. Extern personal innebär en risk i och med att det blir svårt att garantera att utomstående har det höga säkerhetsmedvetande som krävs. Det är även svårt att kontrollera säkerhetsnivån av externt använd utrustning som till exempel datorer. Extern personal kan även ha tillgång och behörighet att förändra saker i systemen. Det största hotet enligt respondenterna var insiders, både för egen personal och konsulter. Det är delvis en anledning till varför det efterfrågades fler säkerhetskontroller på personal, både ny och gammal. Sekundärt nämns organiserad brottslighet som den grupp som ses som troligast angripare.

Värt att notera är att respondenterna inte nämner främmande makt som ett troligt hot. Detta kontrasterar mot den hotbild som Sveriges underrättelsetjänster fört fram. Säkerhetspolisen har varnat för statliga aktörers aktiviteter mot Sverige på cyberområdet och Försvarets radioanstalt (FRA) har också specifikt varnat för cyberangrepp av främmande makt mot kritisk infrastruktur (Säkerhetspolisen, 2023; Försvarets radioanstalt (FRA), u.d.).

5.1.1 Angreppsvektorer

Det är nödvändigt för styrsystemen att ha informationsflöden till omvärlden på grund av att:

- organisationerna vill kunna föra ut driftdata från produktionen till andra avdelningar vilket kräver kopplingar mellan IT- och OT-systemen
- konsulter och leverantörer ofta ställer krav på möjligheter till att fjärransluta från sina egna lokaler

- systemen kan vara geografiskt utspridda så att det blir en arbetsmiljöfråga att den egna personalen kan fjärransluta till olika produktionsplatser (det kan leda till behov av att ansluta sig inifrån de egna lokalerna, men kanske även från fordon eller hem)
- jourpersonal ska kunna ansluta till systemen från sina hem i händelse av incident.

Det finns angrepp som har skett via fjärranslutningar samt genom att utnyttja bryggor mellan kontors- och produktionsnäten (Kelly & Resnick-ault, 2021; Higgins, 2016), vilket visar behovet att både säkra upp bryggorna mellan nätverk och svårigheten att göra det framgångsrikt.

Det finns en komplexitet kring hur man ska säkra kopplingen mellan kontors- och driftnät och man kan tolka respondenterna som att det finns en avsaknad av en standard eller best practice på hur det ska implementeras.

OT-systemen har en historik av att ändras sällan medan IT-produkter länge har haft korta livscykler där man även identifierar och åtgärdar sårbarheter och gör uppdateringar ofta. När man nu har lyft in IT-produkter och funktionalitet i OT-miljön har man flyttat in en del av problemen och behöver då se till att de sårbarheter som upptäcks går att åtgärda. Ju fler datorer som finns i miljön desto fler system och kopplingar behöver säkras upp. Detta tar tid och bidrar till svårigheter att synka uppdateringar med driften som ständigt är igång.

I kombination med att flera av verksamheterna vi pratat med inte själva ansvarar för sina kontorsnät är detta en komplicerad utmaning som kommer att behöva följas upp. En av lösningarna för att begränsa en angripares möjligheter, är att dela upp sina nätverk även mellan olika OT-områden för att förhindra att en angripare, om den trots allt lyckas, skulle få tillgång till hela OT-miljön. Om det i praktiken går att göra detta i en sådan här komplex och geografiskt utspridd miljö som VA-organisationerna har att förhålla sig till skulle behöva utredas vidare. Samverkan och dialog och utbyte av erfarenheter mellan organisationerna blir viktigt inom detta område. Verksamheterna vi talat med arbetar med frågan men säger att det finns en del arbete kvar att göra.

5.2 Utmaningar

Nedan presenteras några av de utmaningar vi sett under förstudien.

5.2.1 Mänskliga misstag

Mänskliga misstag togs upp som ett riskmoment i vattenverket. I många angrepp sker den initiala fasen genom att angriparen lurar personal att utföra vad som för dem verkar vara oskyldiga åtgärder men som försätter systemen i ett osäkert läge, exempelvis via phishing. Att minska riskerna för dessa misstag behöver göras på flera sätt. Det handlar delvis om att se till att det finns faktiska säkerhetsåtgärder som hjälper medarbetarna att inte göra fel. Det ska vara lätt att göra rätt och svårt att göra fel. Det ska finnas fysiska och tekniska begränsningar som minimerar risken att göra fel. Den handlar också om att skydda sig mot mänskliga fel genom utbildning. Personalen behöver utbildning och övning i hur de ska och inte ska agera. Sist men inte minst handlar detta även om medarbetarnas dagliga arbetsmiljö, frånvaro av stress och att våga ta ansvar och informera chefer och ansvariga när man upplever att det finns säkerhetsrisker som bör hanteras. De verksamheter vi intervjuat påtalar att personalen inte får tillräcklig utbildning i IT-säkerhet trots att de kan påverka verksamhetens säkerhet.

5.2.2 Övning kopplat till cyberrelaterade incidenter

Samtliga verksamheter vi talat med upplever att de genomför för få övningar rörande cyberrelaterade incidenter. Förstudien indikerar att det även saknas testanläggningar där organisationerna kan öva cyberrelaterade incidenter. Övningar är viktigt bland annat för att få in det organisatoriska lärandet i hela organisationen och för få förankring kring incidenthantering.

Verksamheterna genomför övningar kopplat till kontinuitetsplanerna samt att gå över till manuell drift. Det verkar dock finnas en avsaknad av att vid dessa övningar fokusera på att hantera orsakerna till störningen. Det vill säga att avgöra om incidenten är orsakad av en olyckshändelse eller ett angrepp. Vid en cyberrelaterad incident är det relevant att begränsa tillgängligheten för en angripare och isolera systemen. Detta kan bland annat göras genom att gå över till manuell drift, men man måste också hindra angriparen från att orsaka nya skador och stänga av den väg angriparen tagit sig in till systemen. Då återställningar normalt raderar

forensiska spår är en viktig uppgift att samla in loggar och annan bevisning för att kunna ta reda på vad som hänt. Skadlig kod kan dölja sig i systemen och finnas kvar efter en omstart vilket kan leda till att angrepp fortsätter eller återupptas. Dessutom saknar man i dessa fall förmåga att lämna sådan information som ska ligga till grund för MSB:s och tillsynsmyndighetens avgöranden om varningar eller understöd är befogat[25]. Det är därför bra att organisationerna förstår att de behöver arbeta mer med cyberrelaterade övningar och eventuellt skulle man även på statlig nivå kunna stödja VA-organisationerna i detta arbete.

5.2.3 Tillsyn

Respondenterna för fram att tillsynen de facto är den enda referens de har för att göra rätt. De upplever att de skyldigheter de har är formulerade på en abstrakt nivå medan lösningarna kräver praktiska bedömningar på detaljnivå i sitt genomförande. Dessa bedömningar är svåra att genomföra utan relevant domänkunskap och risken finns att man uppfyller de formella kraven som tillsynen kräver men inte uppnår den säkerhetshöjning som åtgärderna syftar till.

5.2.4 Personella resurser

Rekrytering av kompetent och kunnig personal inom IT och OT inom VA-branschen tar nästan alla upp som en utmaning. För att bland annat hantera avsaknaden av egen kunnig IT/OT-personal arbetar några organisationer istället med att utveckla sin kompetens som beställare och kravställare av IT-tjänster. Relevant i detta sammanhang blir även hur en sådan organisation ska hantera NIS-direktiven? Frågan är om det kan finnas risk för att organisationen hamnar i en situation där de har OT-system som de driftar men där någon annan ansvarar för IT-säkerheten? Detta är troligen bara ett problem i mindre verksamheter eller i verksamheter som är starkt sammankopplade med en annan part. Här skulle det vara av intresse att utreda hur det går till i praktiken om en IT-incident sker. Vid en pågående IT-incident kan man även få hjälp av

[25] Se formulär för incidentrapportering för leverantör av samhällsviktiga tjänster (Myndigheten för samhällskydd och beredskap).

CERT-SE och det faktum att IT-kunskapen saknas på organisationen kan ställa högre krav på CERT-SE vid en incident.

Om organisationerna har svårt att rekrytera personal blir fördelning av befintliga resurser en utmaning. I några av organisationerna är det tydligt att det är OT som prioriteras vid vattenverket och att IT istället hanteras av extern part och frågan vi ställer oss är om den uppdelningen leder till några specifika konsekvenser och i så fall vilka? Samhället blir mer digitaliserat och det saknas i flera fall IT-kompetens in-house hos organisationer, hur säkerhetsställs det att det sker så få misstag som möjligt gällande IT på OT inom en samhällsviktig bransch som VA? Har den externa parten tillräcklig koll på IT-säkerhet inom OT och produktionsmiljön för att kunna hantera den? För några organisationer verkar det inte finnas ett samlat grepp kring IT-säkerhet för OT, utan det kan skilja mellan vattenverken och andra affärsområden inom samma organisation.

Vissa av respondenterna vill inte enbart förlita sig på extern kunskap, och lägger tyngd på att tillräcklig specialistkunskap ska finnas även inom verksamheten. Den lösningen är svårare att genomföra för mindre organisationer då de inte har lika mycket personal och alltså måste förlita sig på extern kompetens. Frågan blir hur de ska skapa samarbeten, och med vilka organisationer, inom cybersäkerhetfrågorna?

Alla organisationer uttrycker att de har förmågan att gå över till manuell drift snabbt men att det innebär en större personalstyrka om det skulle krävas manuell drift under lång tid.

5.2.5 Stort beroende av andra

En av utmaningarna med säkerheten i vattenverken är det stora beroendet av andra parter och tjänster.

BankID

En verksamhet nämnde att de använder BankID för inloggning vid fjärranslutning. Följdfrågan blir om BankID är ett säkerhetssystem som är utformat för att användas för detta ändamål? Kan det ha blivit en ändamålsglidning? Den frågan har vi inte hunnit fördjupa oss i inom denna förstudie men vi ser att detta kan leda till att det blir en avvägning mellan säkra sätt att ansluta till systemen och beroendet till just den

tjänsten. BankID kan garantera korrekt autentisering men vad sker om tjänsten ligger nere? Går det till exempel att göra en överbelastningsattack mot BankID som skulle leda till problem för vattenverkets produktion? I just detta fall används BankID för att fjärransluta vilket kan kringgås vid en kris men det öppnar upp för att undersöka vidare vilka beroenden som vattenverken har och hur man genom att störa andra tjänster kan få möjlighet att störa vattenproduktionen.

Dela information

Det finns ett behov av att dela information utanför organisationen, till exempel kartor över ledningsnätet, i kris. Här tog några respondenter upp att det inte är helt klarlagt hur de på ett säkert sätt ska dela information utanför organisationen och dess nätverk. Hur skyddas den informationen och vilken avvägning sker mellan att kunna dela informationen och samtidigt säkerhetsställa att ingen obehörig får tillgång till den skyddsvärda informationen? Flera nämnde även att de kommer att ha svårt att leverera korrekt rapportering av data till tillsynsmyndigheten vid manuell drift under en längre period, till exempel vid en incident. Hur man hanterar rapportering eller delning av information vid kris är därmed något som skulle behöva undersökas vidare.

Olika krav

Produktionen av dricksvatten regleras av flertalet olika lagar både gällande dricksvattenkvalitet och cybersäkerhet. Det gör att verksamheten omfattas av många och ibland överlappande krav. Även de som ska se till att organisationen uppfyller kraven, har många krav att förhålla sig till. Det händer till exempel att kommunerna väljer att köpa en viss sorts datorer, men att VA-organisationen då väljer att inte vara med i samma upphandling på grund av andra riskbedömningar. Det kan finnas risker med att VA-organisationerna och kommunen har olika säkerhetskrav, eftersom man aldrig är starkare än sin svagaste länk.

Säkerhetsskyddslagens cybersäkerhetskrav

Ingen av respondenterna nämnde något om säkerhetsskyddslagens krav på cybersäkerhet, inte heller i kontexten av någon av förordningarna som utgår från den. Detta var något förvånande eftersom informationssystem inom dricksvattenproduktionen faller inom lagens råmärken (se kapitel 2.2) vilket gör att deltagarna borde påverkas åtminstone i med

avseende på analyser av nya och förändrade system. Samtidigt tog de upp svårigheter kring kraven i NIS som i väsentliga delar kan överlappa (Myndigheten för samhällsskydd och beredskap, 2024) med säkerhetsskyddslagen.

Inte heller nämnde de Säkerhetspolisen när tillsynsmyndigheter diskuterades, varken som rapportrecipient eller resurs för råd och stöd. En möjlighet är att förfarandet rörande säkerhetsskydd uppfattas som självklart i och med att det pågått under lång tid medan NIS innebär nya rutiner och därmed uppmärksammas.

6 Slutsatser och framtiden

Förstudien visar en övergripande bild på hur respondenterna som arbetar på fem olika VA-bolag i Sverige ser på samt arbetar med säkerhet. Detta kapitel går igenom slutsatser och förslag på vidare utrednings- och forskningsarbete.

6.1 Slutsatser

Syftet med denna förstudie var att bidra med kunskap om hur säkerhetsarbetet vid vattenverk fungerar med fokus på cybersäkerhet. I förstudien har relevanta aktörer, regelverk, informationsflöden och cyberfysiska system identifierats. Vidare har en initial bild skapats över hur de tillfrågade arbetar med cybersäkerhet, vilka hot och risker de ser och vad konsekvenserna av en incident kan bli, samt vilka behov av utbildning och övning som finns. Förstudien bygger på intervjudata med medarbetare som på olika sätt arbetar med säkerhet på vattenverk vid fem olika kommunala bolag i Sverige. Resultatet av studien gav en inblick i hur dessa organisationer arbetar med dessa frågor.

Alla organisationer har datoriserade styrsystem som används i produktionen vid normalläge och har möjligheter att gå över i manuell drift när behov finns. Det sker övningar inom kontinuitetshantering som brister i cyberfokus. Övning och träning i att hantera incidenter verkar vara en generell brist. Tolkningen är att respondenterna oftast ser behovet av övningar men att detta kan vara svårt att realisera på grund av flera orsaker. Ibland finns internt motstånd i organisationen för att det är svårt att genomföra övning och utbildning under pågående produktion då systemen är i drift.

Då IT-komponenter i allt högre grad har flyttat in i de klassiska OT-miljöerna, har det öppnat upp för fler potentiella angreppsvektorer och sårbarheter som kräver åtgärder och ett systematiskt IT-säkerhetsarbete. De intervjuade organisationerna säger att man arbetar med att minimera riskerna av dessa sårbarheter genom att arbeta med säkerhet i olika kombinationer, där fysisk säkerhet, kontroll av personal och tekniska säkerhetsåtgärder går hand i hand i syfte att skydda hela verksamheten. Digitaliseringen av vattenproduktionen har inte bara öppnat upp för flera sårbarheter, utan ställer även krav på att det finns

personal med kompetens inom både IT- och OT-området. Det anses vara en brist på dessa personer både i verksamheterna vi intervjuat och på arbetsmarknaden i stort.

Resultatet har visat att IT-säkerhet är något samtliga organisationer arbetar med i olika grad. Omfattningen av IT-säkerhetsarbetet har i denna förstudie inte klargjorts fullständigt och kan möjligen undersökas vidare i framtiden. Eftersom de deltagande organisationerna är relativt få, kan inga generella slutsatser om branschen som helhet dras från denna förstudie.

6.2 Förslag till vidare arbete

Nedan följer en punktlista med förslag på fördjupningar och behov av ytterligare arbete. Förslagen har kommit upp under studiens gång och har ingen inbördes ordning. Ibland har förslagen redan beskrivits tidigare i förstudien. Flera av förslagen kan innebära att arbetet behöver genomföras under sekretess, då respondenterna eventuellt behöver dela med sig av sekretessbelagd information vilket skulle resultera i en sekretessklassad rapport.

- Utreda riskerna med integrerade SCADA-system[26]. Bör man ha olika separata SCADA-system för de olika affärsområdena?
- Organisationerna upplever ett stort eget ansvar att själva förstå hur olika krav ska uppfyllas. Här kan man behöva se över hur ett nationellt stöd för VA-organisationerna kan se ut organisatoriskt för att bidra med stöd kring genomförandet av kraven inom denna sektor. Behovet är troligen större de mindre organisationerna.
- En fördjupad analys av vilka aktörer, myndigheter och regelverk som påverkar cybersäkerheten inom VA-sektorn. Se till hela dricksvattenkedjan med avseende på information- och cybersäkerhet och ta hjälp av denna studie för att göra en fördjupningsstudie. Denna studie skulle genomföras med

[26] Termen ska i det här fallet förstås som att organisationernas ofta har flera olika SCADA-system integrerade i samma fysiska datornätverk och telekom-strukturer. Detta medför en potentiell risk för interaktion, eller att ett angrepp kan påverka flera system samtidigt.

ytterligare intervjuer med tydligare fokus på hela dricksvattenprocessen, från intag till leverans hos konsumenten, i syfte att bedöma cybersäkerhetsmognaden. Det skulle kräva att tala med en större mängd organisationer än vad som gjorts i denna studie.

- Undersöka cyberrisker på fler dricksvattenorganisationer, såsom helt kommunala förvaltningar som ansvarar för produktionen av dricksvatten.
- En fördjupning kring hur organisationerna konkret arbetar med implementering, utvärdering och resultat av IT-säkerhetsstrategierna. Denna förstudie går inte in på djupet hur detta görs och vilka brister som kan finnas.
- En studie om vad tillsynsmyndigheten anser är tillräcklig nivå gällande säkerhetsåtgärder samt att jämföra detta mot dagens EU-krav.
- En undersökning av molntjänster i drift inom samhällsviktig verksamhet och hur NIS-direktiven förhåller sig till användningen av molnlösningar.
- En större intervjustudie där både VA-organisationer och leverantörer intervjuas kring cybersäkerhet inom VA-sektorn.

Referenser

'Cyber winter is coming,' warns Israel cyber chief after attack on water systems. (2020). Hämtat från The times of Israel: https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/ den 12 december 2023

2022 Cyber Attacks Statistics. (2023). Hämtat från Hackmageddon: https://www.hackmageddon.com/2023/01/24/2022-cyber-attacks-statistics/ den 12 december 2023

A/RES/64/292. (2010). *The human right to water and sanitation.* Förenta nationerna (FN).

Ansvar för vatten – vem gör vad? (2023). Hämtat från Havs- och vattenmyndigheten: https://www.havochvatten.se/miljopaverkan-och-atgarder/miljopaverkan/vattenbrist/ansvar-for-vatten---vem-gor-vad.html den 20 november 2023

Aslam, M. M., Tufail, A., Kim, K.-H., Apong, R. A., & Raza, M. T. (2023). A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects. *Sensors, 23*, 7999.

Chawaga, P. (2022). *Vermont Water Department Official Secretly Lowered Fluoride Levels For Years*. Hämtat från Water Online: https://www.wateronline.com/doc/vermont-water-department-official-secretly-lowered-fluoride-levels-for-years-0001 den 10 januari 2024

Detta är Stockholm Vatten och Avfall. (u.d.). Hämtat från Stockholm Vatten och Avfall: https://www.stockholmvattenochavfall.se/om-oss/ den 20 december 2023

Dir. 2023:30. (2023). *Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft.* Hämtat från Regeringskansliet.

Direktiv (EU) 2016/1148. (2016). *Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.*

Direktiv (EU) 2022/2555. (2022). *Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.*

Direktiv (EU) 2022/2557. (2022). *Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.* Hämtat från EUR-Lex.

Doris, T. (2019). *IN DEPTH: How Riviera Beach left the door wide open for hackers*. Hämtat från The Palm Beach Post: https://eu.palmbeachpost.com/story/news/local/2019/06/21/in-depth-how-riviera-beach-left-door-wide-open-for-hackers/4848254007/ den 11 mars 2024

Dricksvatten och vattenskydd. (2022). Hämtat från Havs- och vattenmyndigheten: https://www.havochvatten.se/avlopp-och-dricksvatten/dricksvatten-och-vattenskydd.html den 10 oktober 2023

Dricksvattenförsörjning. (2023). Hämtat från Krisinformation.se: https://www.krisinformation.se/detta-gor-samhallet/mer-om-sveriges-krishanteringssystem/samhallets-ansvar/kommuner/dricksvattenforsorjning den 15 december 2023

EU och arbetet med att stärka motståndskraften i samhällsviktig verksamhet. (2023). Hämtat från Myndigheten för samhällsskydd och beredskap: https://www.msb.se/sv/om-msb/internationella-samarbeten/eu-samarbete/eu-och-skydd-av-samhallsviktig-verksamhet/ den 12 december 2023

Federal Office for Information Security (BSI). (2014). The State of IT Security in Germany 2014.

Försvarets radioanstalt (FRA). (u.d.). *Cyberförsvar*. Hämtat från FRA: https://fra.se/cyberforsvar.4.55af049f184e92956c42bb9.html den 10 januari 2024

Gjendemsjø, M. (2013). *Creating a Weapon of Mass Disruption: Attacking Programmable Logic*. Norwegian University of Science and Technology. Hämtat från NTNUOpen.ntnu.no.

Greenberg, A. (2021). *A Hacker Tried to Poison a Florida City's Water Supply, Officials Say*. Hämtat från Wired: https://www.wired.com/story/oldsmar-florida-water-utility-hack/ den 9 januari 2024

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering 146*.

Higgins, K. J. (2016). *Lessons From The Ukraine Electric Grid Hack*. Hämtat från Dark Reading: https://www.darkreading.com/vulnerabilities-threats/lessons-from-the-ukraine-electric-grid-hack den 25 januari 2024

Informationssäkerhet, cybersäkerhet och säkra kommunikationer. (2023). Hämtat från Myndigheten för samhällsskydd och beredskap: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/eus-cyberregleringar/ den 28 november 2023

ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Hämtat från International Organization for Standardization.

ISO/IEC 27002:2022. (2022). *Information security, cybersecurity and privacy protection — Information security controls*. Hämtat från International Organization for Standardization.

Kelly, S., & Resnick-ault, J. (2021). *One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators*. Hämtat från Reuters: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ den 25 januari 2024

Lee, R. M., Assante, M. J., & Conway, T. (2014). German Steel Mill Cyber Attack. *Industrial Control Systems*, 1-15. Hämtat från AssetsContentstack.io.

Livsmedelsverket. (2023). *Handbok i krisberedskap och civilt försvar för dricksvatten, Modul 4*. Hämtat från Livsmedelsverket.

MSB1501. (2020). *Kontinuitetshantering - kommunalt vattenverk : ett förenklat exempel*.

MSB1773. (2021). *MSB:s roll och ansvar inom NIS*. Hämtat från Myndigheten för samhällsskydd och beredskap.

MSB2032. (2023). *Vägledning : säkerhetsåtgärder i informationssystem*.

MSBFS 2021:9. (2021). *Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster*. Hämtat från Myndigheten för samhällsskydd och beredskap.

Myndigheten för samhällskydd och beredskap. (u.d.). Välkommen till MSB:s incidentrapporteringsformulär för leverantörer av samhällsviktiga tjänster! (version 1.4). Hämtat från https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/incidentrapportering-for-nis-leverantorer/incidentrapportering-for-leverantorer-av-samhallsviktiga-tjanster/ den 18 januari 2024

Myndigheten för samhällsskydd och beredskap. (2024). Hämtat från NIS-regleringen och säkerhetsskyddslagen: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/nis-regleringen-och-sakerhetsskyddslagen den 9 februari 2024

Naturvårdsverket. (2001). *Egenkontroll: en fortlöpande process*. Naturvårdsverket. Hämtat från Naturvårdsverket.

PMFS 2022:1. (2022). *Säkerhetspolisens föreskrifter om säkerhetsskydd*.

Prop. 2019/20:137 . (2020). *Förbättrad tillsyn på miljöområdet.*

Reningsprocesser i vattenverk. (2023). Hämtat från Svenskt Vatten: https://www.svensktvatten.se/vattentjanster/dricksvatten/vattenverk-och-reningsprocesser/reningsprocesser-i-vattenverk/ den 20 november 2023

SFS 2006:412. (2006). *Lag (2006:412) om allmänna vattentjänster.*

SFS 2018:1174. (2018). *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.* Hämtat från Sveriges riksdag.

SFS 2018:1175. (2018). *Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.* Hämtat från Sveriges riksdag.

SFS 2018:585. (2018). *Säkerhetsskyddslag (2018:585).* Hämtat från Sveriges riksdag.

SFS 2021:955. (2021). *Säkerhetsskyddsförordning (2021:955).*

Sjukdomsinformation om cryptosporidiuminfektion. (2019). Hämtat från Folkhälsomyndigheten: https://www.folkhalsomyndigheten.se/smittskydd-beredskap/smittsamma-sjukdomar/cryptosporidiuminfektion/ den 12 december 2023

Statistiska centralbyrån (SCB). (2022). *Vattenanvändningen i Sverige 2020 MI27 - Vattenuttag och vattenanvändning 2022:1.* Hämtat från Statistikmyndigheten (SCB).

STEMFS 2021:3. (2021). *Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn.*

Säkerhetspolisen. (2023). *Säkerhetspolisens årsbok 2022/2023.*

Säkerhetspolisen. (2023). *Vägledning Säkerhetsskyddsanalys.* Hämtat från Säkerhetspolisen.

Tillsyn av livsmedelsverksamhet. (2023). Hämtat från Stockholm stad: https://tillstand.stockholm/tillstand-regler-och-tillsyn/servering-av-mat/vad-som-kontrolleras/ den 20 november 2023

Vattenverk och reningsprocesser. (2023). Hämtat från Svenskt vatten: https://www.svensktvatten.se/Vattentjanster/Dricksvatten/Vattenverk-och-reningsprocesser/ den 20 november 2023

Bilaga A

I det följande presenteras intervjuguiden. Denna modifierades med några ytterligare frågor under studiens gång.

Intervjuguide

Respondenten och lokala förutsättningar

- Vilken roll har du/ni i din organisation?
- Hur många anställda har er organisation?
- Hur omfattande är organisationens verksamhet? Hur spridd är organisationen geografiskt
    - personalmässigt?
    - produktionsmässigt?
- Vilka andra organisationer samarbetar ni med, särskilt med avseende på cybersäkerhet, rörande
    - dricksvattenproduktion?
    - distribution?

Övergripande om dricksvattenframställningen

- Kan du översiktligt beskriva hur dricksvattenprocessen går till?
- Vilka delar av den är styrda av datoriserade kontrollsystem?
- Vilka av dessa delar kan man köra utan datorsystem om nödvändigt t ex om man kör med reducerad drift eller andra inskränkningar.
- Vilka informationsflöden krävs för att dricksvattenproduktionen ska fungera?
    - Kan dricksvatten produceras utan dessa, t ex om man kör med reducerad drift eller andra inskränkningar.
- Interagerar era system med system från andra organisationer?
- Finns det beroenden till externa system?

- Är ni beroende av kompetens från andra organisationer t ex entreprenörer eller konsulter?
- Vilka av de system ni har tagit upp är viktigast för produktionen?

Regelverk och policyer

- Finns riktlinjer/strategier/policyer? Tas dessa fram enligt någon standard/ramverk/best practices?
- Vad finns det för regelverk och myndigheter ni behöver förhålla er till? Hur ser ni till att dessa följs?

Organisationens arbetssätt

- Hur arbetar din organisation med säkerhetsfrågor relaterat till era cyberfysiska system?

Utbildning och övningar

- Hur utbildas er personal för att upprätthålla och förbättra säkerheten? Sker denna typ av utbildning kontinuerligt? Vem organiserar utbildningarna och vad täcker utbildningarna?
- Har ni genomfört några övningar relaterat till cybersäkerhet? Sker denna typ av övningar kontinuerligt? Vem organiserar övningarna och vad övas?

Hot- och riskbedömningar

- Hur sker hot- och riskbedömning? Är det något som sker kontinuerligt?
- Hur sker inventering av tillgångar? Är det något som sker kontinuerligt? (i termer av applikationer, mjukvaruplattformar, nätverk, nätverkskomponenter, servrar, OT-system, administrativa komponenter etc.)?
- Finns process för att hantera organisationens ändpunkter (genom säkerhetsåtgärder som antivirus, kryptering, härdning etc.), och process för säker introduktion av nya enheter (som acceptanstester)?

- Finns en plan för kontinuitets- och krishantering relaterat till cyberrelaterade händelser? Uppdateras och testas/övas detta kontinuerligt?
- Genomförs säkerhetskontroller för personal som arbetar med IT- och OT-system?
- Vidtas åtgärder för att begränsa obehörig tillgång till system? Och behörigas, som externa konsulter etc.
- Använder ni molntjänster? Hur utvärderas effekt och risker med molntjänster?
- Hur hanterar ni backuper för era system? Finns backup för (de mest kritiska av) era system?
- Hur skulle er verksamhet påverkas av en cyberattack?
- Finns det någon aspekt kring skydd av cyberfysiska system som du känner dig bekymrad för, idag och i framtiden, för din egen organisations del/för branschens del? Hur utsatta är cyberfysiska system inom branschen?
- Något du önskar tillägga som vi inte ställt här men som du tänker är relevant för studien?

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se