Kungsbacka Kommun

Rapport: Granskning av IT-säkerhet

Juni 2018

Max Wann-Hansson

Jesper Ehrner Vilhelmsson

Hardik Patel

Building a better working world

Innehåll

1. Inledning

1.1 Bakgrund

Vattenförsörjning och avlopp är exempel på samhällsviktiga tjänster. Den globala digitaliseringen har inneburit att styrning och övervakning av dessa tjänsters infrastruktur och processer digitaliserats. Denna utveckling innebär båda nya möjligheter men också nya risker. Utan ett väl fungerande och strukturerat IT- och informationssäkerhetsarbete finns risk för både avsiktliga och oavsiktliga störningar i dessa system vilket kan leda till avbrott i samhällsviktiga funktioner. Detta kan i sin tur få allvarliga konsekvenser för samhället.

Sommaren 2016 antog Europaparlamentet det så kallade ”NIS-direktivet” vilket har som mål att klargöra åtgärder för att uppnå en gemensam grundläggande säkerhetsnivå för nätverk och informationssystem inom EU. De nya reglerna omfattar leverantörer av samhällsviktiga tjänster samt leverantörer av digitala tjänster och har som syfte att öka kraven på säkerhetsåtgärder, incidentrapportering och tillsyn.

Som ett led i detta har regeringen lämnat in en proposition (2017/18:205) till riksdagen i syfte att införa NIS-direktivet i svensk rätt. Regelverket föreslås träda i kraft andra kvartalet 2018, i samband med när EU:s medlemsstater enligt NIS-direktivet ska tillämpa direktivets bestämmelser. En punkt i denna proposition föreslår Livsmedelsverket (SLV) som tillsynsmyndighet för leverans och distribution av dricksvatten. Detta ter sig vara rimligt då SLV idag, på uppdrag av svenska staten, arbetar i konsumenternas intresse för säker mat och kvalitativt dricksvatten.

I Kungsbacka kommun bedriver Miljö & Hälsoskyddsförvaltningen tillsyn av kommunens vatten- och avloppssystem utifrån kontrollpunkter tillhandahållet av SLV. Kungsbackas centrala övervakning och styrning av processer kopplat till vatten och avlopp sköts genom ett SCADA-system (Supervisory Control And Data Acquisition). SCADA-systemet gör det möjligt att övervaka allt, till stor del online, från systemets nuvarande status ner till enstaka temperaturer i en byggnad. Dessa möjligheter medför dock att systemet blir sårbart och nya risker tillkommer, vilket skapar ett behov för ett väl fungerande och strukturerat IT- och informationssäkerhetsarbete.

Mot bakgrund av ovan nämnda utmaningar inom IT- och informationssäkerhet, samt nya regelverk och att revisorerna har identifierat kommunens VA-system som kritiskt för kommunens verksamhet, har en granskning genomförts. Granskningen fokuserar på hur VA-systemets säkerhet och kvalitet säkerställs. Detta inkluderar således de kontroller och rutiner som finns för SCADA, samt en kartläggning av gällande regelverk och tillsynsrutiner som finns för att upprätthålla en god IT-säkerhetsnivå.

1.2 Syfte

Syftet med granskningen är att genomföra en övergripande genomgång av kommunens IT-säkerhet, vad gäller styrande dokument som policys, riktlinjer och hantering av säkerhetsfrågor för kommunens VA-system. Granskningen inriktas på följande revisionsfrågor:

- Hur ändamålsenlig är IT-säkerheten på en övergripande nivå avseende kommunens styrsystem utifrån befintliga lagar och god praxis?
- Hur säkerställer kommunen att IT-säkerheten kring styrsystemen efterlevs?

1.3 Genomförande

Granskningen har genomförts genom dokumentstudier och intervjuer.

Intervjuer har genomförts med:

- Relevanta medarbetare inom drift på förvaltningen teknik
- Relevanta medarbetare på förvaltningen Miljö & Hälsoskydd
- Förvaltningschef för förvaltningen teknik
- Enhetschefer inom förvaltningen teknik
- IT-chef
- Systemspecialist för styrsystem
- Systemförvaltare

Intervjufrågor har utarbetats utifrån EY:s ramverk för informationssäkerhet, de lagar och regelverk som SLV och Miljö & Hälsoskyddsförvaltningen baserar sin tillsyn på, kommande direktiv, branschorganisationen Svenskt Vattens rekommendationer och myndigheten för samhällsskydd och beredskaps (MSB) vägledning för ökad säkerhet i informations- och styrsystem. Samtliga intervjuande har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

För en fullständig lista över granskade dokument, se *Bilaga 1*.

1.4 Revisionskriterier

Vi har genomfört en granskning mot så kallad god praxis inom informationssäkerhetsområdet. Granskningen har genomförts mot EY:s ramverk Cyber Program Management, vilket är ett brett ramverk som bygger på den svenska och internationella standarden för informationssäkerhet (ISO/SEC 27001), samt mot lagar, direktiv och riktlinjer från tillhörande tillsynsmyndighet.

1.5 Ansvarig nämnd

Ansvarig nämnd för den granskade verksamheten (vatten och avlopp) är nämnden för teknik.

2. Styrning och tillsyn av SCADA för Kungsbacka kommun

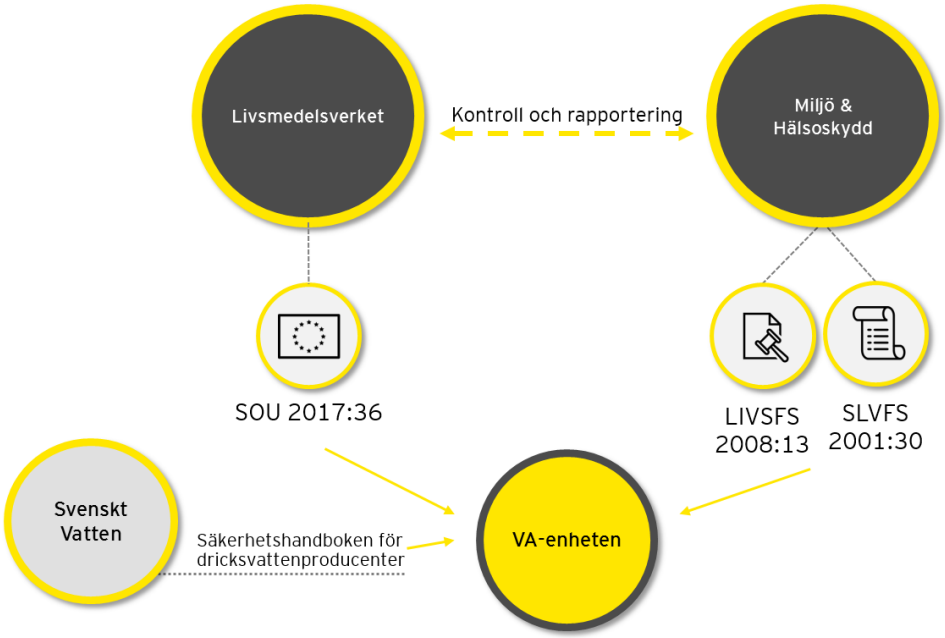
2.1 Vatten- och avloppsenheten

Nämnden för teknik ansvarar för en stor del av infrastrukturen i Kungsbacka kommun, varav ett ansvarsområde är dricksvatten och avloppsrening. Det är alltså teknik som ansvarar för att säkerställa god kontroll och säkerhet av kommunens VA-system. Vatten- och avloppsenheten (VA), vilken är en del av förvaltningen för teknik, ansvarar för styrning och övervakning av kommunens SCADA-system. Med hjälp av ett SCADA-system har en operatör för exempelvis dricksvatten möjlighet att övervaka och styra systemprocesser, från kortsiktiga förändringar i vattenkvalitet till enstaka temperaturer i anläggningar, allt till stor del online. Kungsbacka Kommun använder sig av ett styrsystem som heter EXOscada, framtaget av företaget Regin AB och har även avtal med Systeminstallation AB som ansvarar för säker drift och support av styrsystemet. Vatten- och avloppsenheten består av ca 15 medarbetare och organisationen leds av verksamhetschefen för drift med två enhetschefer ansvariga för VA. Kommunens IT-avdelning har ingen insyn i vatten- och avloppsenhetens egna driftnät, vilket gör att enheten själva ansvarar för att bedriva ett väl fungerande och strukturerat IT- och informationssäkerhetsarbete.

2.2 Miljö- och hälsoskyddsförvaltningen

Miljö- och hälsoskyddsförvaltningen bedriver tillsyn av kommunens vatten och avlopp och är således de som granskar förvaltningen för teknik arbete med vatten och avlopp. SLV tillhandahåller kontrollpunkter som förvaltningen ska granska, dessa punkter kan till exempel vara vattenkvalitet, lokaler och utrustning. De lagar och regelverk som förvaltningen utgår ifrån är LIVSFS 2008:13 och SLVFS 2001:30, vilket visas nedan i figur 1. Dessa föreskrifter fokuserar huvudsakligen på den fysiska säkerheten och säkerställning av bra vattenkvalitet. Förvaltningen rapporterar en gång per år in den tillsyn som har gjorts till SLV, som inte själv bedriver någon tillsyn av kommunens VA mer än att granska den rapportering som förvaltningen skickar in.

Figur 1: Regulatorisk karta över VA-säkerhet



Utöver SLV och miljö- och hälsoskyddsförvaltningen finns även Svenskt vatten, en branschorganisation för Sveriges VA-organisationer. I sitt arbete för friskt dricksvatten har Svenskt vatten tagit fram en säkerhetshandbok för dricksvattenproducenter vilken innehåller rekommendationer och vägledning för ökad säkerhet och som berör säkerhet i IT-system. Svenskt vatten har även tagit fram en checklista för SCADA-system. Checklistan fungerar som en självutvärdering av IT- och informationssäkerhetsarbetet i SCADA-system.

3. Beskrivning av granskade områden

3.1 Behörighetshantering

Beträffande IT- och informationssäkerhet är det av yttersta vikt att behörigheter i informations- och styrsystem är lämpligt definierade, det vill säga att rätt personer har rätt tillgång vid rätt tidpunkt och av rätt anledning. En hög grad av den information som behandlas i SCADA omfattas av sekretess varvid det föreligger höga krav på tillförlitlig behörighetshantering.

För att kunna lägga en bra grund för en välfungerande behörighetshantering krävs alltid definierade riktlinjer och policys. Några sådana riktlinjer finns inte för kommunens SCADA-system (se iakttagelse 1.1 nedan). När nya användare ska läggas till eller tas bort görs detta ad-hoc. Det finns inte heller någon rutin för att genomföra periodiska genomgångar av behörigheter för att upptäcka olämpliga användare.

Som ett svar på detta har VA-enheten just nu ett pågående genomgripande arbete med att sätta upp en tydlig struktur för IT-säkerhet i SCADA. I detta arbete ingår att ta fram rutiner för tillägg, borttag och periodisk genomgång av behörigheter.

Kungsbacka kommun har idag omkring 15 användare i SCADA. Ett lägre antal användare minskar risken för obehöriga i systemet. För att få åtkomst till systemet krävs tvåvägsauktorisering, vilket betyder att man behöver verifiera sig på två ställen, exempelvis via lösenord i dator och telefon. Planen är också att sätta upp en egen Active Directory (AD) för användarna på VA-enheten, vilket är en katalogtjänst där användares behörighet kategoriseras. Den kommande AD:n ska sättas upp med olika installationer för drift och administration. Detta för att ytterligare begränsa tillgången till SCADA till de som arbetar med systemet. Möjligheten att tidsbegränsa behörigheter för konsulter kommer också att tillkomma och tillsammans med den nya AD-lösningen ska arbetet med periodiska genomgångar av användare startas.

För att minimera möjligheten till fysisk åtkomst till SCADA för obehöriga har VA-enheten ett eget speciellt nyckelsystem. Lokalerna är också kameraövervakade, utrustade med larm och kassaskåp för känslig dokumentation.

3.2 Programförändringshantering

Förändring och utveckling är en kritisk del i en verksamhets hantering av information- och styrsystem. För att applikationer och system ska kunna möta verksamhetens mål avseende funktionalitet, tillgänglighet och integritet behöver kontinuerliga uppdateringar eller rättningar göras. I dessa fall är det viktigt att ha ett väl fungerande utvecklings- och förändringsarbete, för att kritisk information inte ska gå förlorad och för att systemförändringar inte ska medföra oönskad funktionalitet eller driftstopp.

För Kungsbacka kommuns SCADA-system har Systeminstallation AB hand om utveckling och uppdatering. Kommunen har ett uppdateringsavtal som stipulerar att Systeminstallation AB åtar sig att genomföra periodiska uppdateringar. För att minimera risken för eventuell oönskad funktionalitet genomförs uppdateringar en eller två veckor efter att de har släppts, för att buggar på så sätt ska vara identifierade och borttagna innan implementering av uppdatering. En välfungerande programförändringsprocess är enligt god praxis tredelad och innehåller godkännande av förändring, testning och implementation. Mellan dessa steg bör man, enligt god praxis, upprätta en uppdelning av arbetsuppgifter, för att säkerställa att en person inte kan genomföra alla steg. För kommunens SCADA-system sköter Systeminstallation hela processen från initiering av förändring och testning till implementation (se iakttagelse 1.2).

3.3 IT-drift

Rutiner och kontroller inom IT-drift är av stor vikt i syfte att säkerställa en IT-miljö som tillgodoser verksamhetens behov avseende säkerhet och tillgänglighet. För SCADA föreligger höga krav på en tillförlitlig IT-drift för att kunna säkerställa effektiv leverans av styrning av kommunens VA-processer.

Granskningen har fokuserats kring kontroller och rutiner inom följande områden:

- Hantering av incidenter relaterat till SCADA
- Organisation av säkerheten
- Nätverkssäkerhet och övervakning av driftmiljön

Hantering av incidenter relaterat till SCADA

Säkerhetsincidenter utgör ett allvarligt hot mot systemets funktion. På grund av detta ställer NIS-direktivet krav på att leverantörer av samhällsviktiga tjänster utan onödigt dröjsmål ska rapportera incidenter med stor påverkan på kontinuiteten i leverantörens tjänst. För Kungsbacka kommun ska denna rapportering göras till SLV, i form av tillsynsmyndighet. Om detta krav inte efterföljs ska SLV, enligt svenskt lagförslag, ta ut en sanktionsavgift på mellan 5 000 SEK och 10 000 000 SEK.

Kungsbacka Kommuns incidenthantering för VA har sin utgångspunkt i kommunikation till allmänheten. Vid eventuella risker och incidenter, främst kopplat till vattenkvalitet, skickas i första hand ett SMS ut till de konsumenter som är kopplade till Blueidea vilket är ett kommunikationsverktyg för omfattande och korrekt distribution av information. Rutin finns också för att lägga ut information på

kommunens hemsida samt för att gå ut i radio och TV. Vid incidentrapportering till tillsynsmyndighet finns det ingen skriftlig process eller några riktlinjer som fastställer vilka faktorer som bedöms ha tillräckligt stor påverkan på kontinuiteten i SCADA och således bör rapporteras (se iakttagelse 1.3).

Har man som leverantör av samhällsviktiga tjänster en tredje part som hanterar drift av tjänsten, ska man enligt NIS-direktivet säkerställa att denna har tillräckliga kontroller på plats för incidentrapportering och IT-säkerhet. För att kunna säkerställa detta bör man enligt god praxis inom IT- och informationssäkerhet reglera detta i avtal med tredje part, genom att upprätta krav på IT-säkerhet och rätt till att genomföra granskning av tredje parts interna kontroll. Kungsbacka kommuns avtal med Systeminstallation AB saknar dessa delar, vilket försvårar kommunens möjlighet att genomföra granskningar av Systeminstallation ABs interna kontroll (se iakttagelse 1.4).

Organisation av säkerheten

I sin vägledning till ökad säkerhet i informations- och styrsystem rekommenderar MSB att regelbundet genomföra riskanalyser. Kungsbacka kommuns VA-enhet genomförde 2018-01-11 en genomlysning och riskanalys av sin IT-säkerhet tillsammans med en extern aktör, Endera Networks. Utifrån denna har en åtgärdsplan tagits fram och enheten bedriver ett pågående arbete med att genomföra dessa åtgärder.

En av åtgärderna var att ta fram en styrande IT-policy specifikt för VA-enheten och SCADA. En sådan har ännu inte tagits fram men förväntades vid granskningens genomförande att bli klar under sommaren (se iakttagelse 1.5). I samband med detta ska även den befintliga handlingsplanen för hur sabotage och annan skadegörelse ska avhjälpas kompletteras med IT-säkerhet.

Nästa steg i att ta fram policys och riktlinjer är att säkerställa efterlevnad genom utbildning och uppföljning tillsammans med anställda. VA-enheten har tagit del av den webbaserade IT-säkerhetsutbildningen som genomförts för alla Kungsbacka kommuns anställda. Någon ytterligare utbildning specifikt för säkerheten i styrsystem har inte genomförts (se iakttagelse 1.6).

Nätverkssäkerhet och övervakning av driftmiljön

Den av branschorganisationen Svenskt Vatten framtagna checklistan för SCADA rekommenderar att man som leverantör av dricksvatten loggar händelser som sker i organisationens SCADA-system. VA-enheten i Kungsbacka kommun har två typer av loggning aktiverat. Dels loggar man de händelser och förändringar som sker i själva SCADA men även trafiken i brandväggen loggas för att kunna spåra eventuella intrång. Vid misstänkta försök till intrång skickas också ett larm till en systemteknikers e-post. För att skydda sig mot eventuella virus finns anti-virusprogram installerat som veckovis söker igenom nätverket. Programmet uppdateras också kontinuerligt för att kunna upptäcka nya hot mot SCADA och dess nätverk. En segmentering av nätverken har också gjorts för att separera det nätverk som SCADA ligger på från resterande nätverk och verksamheter i Kungsbacka kommun.

4. Iakttagelser och rekommendationer

Under granskningen har EY identifierat iakttagelser inom granskade områden. För varje iakttagelse har EY lämnat rekommendationer som syftar till att stödja förvaltningen för teknik i dess framtida arbete med IT-säkerhet för VA-system. De av EY identifierade iakttagelserna har klassificerats enligt tre risknivåer avseende hur omfattande dess eventuella inverkan anses vara:

HÖG	Observation av större karaktär som anses kunna ha hög påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer.
MEDEL	Observation som anses kunna ha påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av verksamhetens resurser.
LÅG	Observation som ej direkt påverkar verksamhetens mål, men kan medföra ineffektiv verksamhet, mindre brister i IT- och informationssäkerhet, efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.

1.1 Riktlinjer och policys för behörighetshantering är inte definierade

Iakttagelse	Processen för behörighetshantering i SCADA är inte tydligt definierad av Kungsbacka kommun. Varken för tillägg eller borttag av behörigheter finns riktlinjer eller tidsreferenser definierade för hur användare ska läggas till eller när användare ska tas bort. Beställning och borttag av behörighet genomförs ad-hoc. Det finns inte heller någon process för periodisk genomgång av användare. Det låga antalet användare i systemet ökar dock möjligheten till att få en överblick över lämpliga behörigheter. Efter att granskningen genomfördes ska, enligt enhetschef för drift, nya riktlinjer ha tagits fram under sommaren 2018.
MEDEL	
Rekommendation	Kungsbacka kommun rekommenderas att se över möjligheten att upprätta riktlinjer för tillägg och borttag av användare. Genom tydliga riktlinjer för hur processen ska se ut minskar man risken för obehöriga användare i SCADA. Detta rekommenderas att göras i samband med den åtgärdsplan som tagits fram utifrån årets genomförda riskanalys. Som ett nästa steg bör kommunen utvärdera möjligheten att kontinuerligt genomföra periodiska genomgångar av alla användare i SCADA.

1.2 Kungsbacka kommun har begränsad insikt i programförändringsprocessen för SCADA

Iakttagelse	Processen för programförändringar genomförs uteslutande av Systeminstallation AB vilka sköter allt från initiering av programförändringar, testning och slutligen implementation. Kommunen har ofullständig insikt och delaktighet i processen för att säkerställa att programförändringar är korrekta.
MEDEL	
Rekommendation	Kungsbacka kommun rekommenderas att se över möjligheten att öka sin delaktighet i processen för programförändringar, förslagsvis genom egna acceptanstester för användare av nya programförändringar innan implementation.

1.3 Riktlinjer och policys för IT-incidentrapportering är inte definierade

Iakttagelse	Kungsbacka kommun har inte några definierade riktlinjer eller policys för hur och när incidenter relaterat till SCADA ska rapporteras till tillsynsmyndigheten. Kraven på en välfungerande rapporteringsprocess stärks i samband med NIS-direktivet. Efter att granskningen genomfördes ska, enligt enhetschef för drift, nya riktlinjer ha tagits fram under sommaren 2018.
HÖG	
Rekommendation	EY rekommenderar kommunen att definiera riktlinjer för hur och när incidenter relaterat till SCADA ska rapporteras och när enheten för hantering av IT-säkerhetsincidenter ska kontaktas. Kungsbacka kommun rekommenderas också att utvärdera möjligheten att se över sina IT-incidentrapporteringsprocesser för alla kommunens samhällsviktiga tjänster med tillhörande styrsystem.

1.4 Möjlighet till insyn i leverantörs arbete med IT-säkerhet är inte avtalat

Iakttagelse	Kungsbacka kommun har inte skriftligt avtalat följande två punkter med sin leverantör av SCADA: ► Ingen rätt till att genomföra revision av leverantör. ► Inga avtalade krav på leverantörens IT-säkerhet. Utan dessa två punkter begränsas kommunens möjlighet att säkerställa god intern kontroll och IT-säkerhet hos leverantören.
MEDEL	

Rekommendation	Kungsbacka kommun rekommenderas att utvärdera om möjligheten finns att inkludera ovanstående punkter vid nästa förnyelse av avtalet. Kommunen rekommenderas också att se över möjligheten att öka beställarkompetensen för att minska risken för liknande brister i framtida avtal.

1.5 Det finns ingen generell IT-policy för SCADA och VA-enheten

Iakttagelse	Under EYs granskning framkom att det inte finns någon specifik IT-policy för SCADA och VA-enhetens arbete med IT-säkerhet. Det finns en handlingsplan vid katastrof och sabotage, vilken till största del fokuserar på förändringar i vattenkvalitet.
MEDEL	En IT-policy syftar till att möjliggöra ett välfungerande IT-säkerhetsarbete som genomsyrar hela organisationen och öka förståelsen hos de anställda.
Rekommendation	EY rekommenderar kommunen att fortsätta det arbete som pågår med att ta fram en IT-policy för SCADA och VA-enheten. Fortsättningsvis rekommenderas kommunen också att fortsätta arbetet som pågår med att inkludera IT-säkerhet i sin handlingsplan för SCADA.

1.6 Kontinuerlig utbildning inom IT- och informationssäkerhet för SCADA genomförs inte

Iakttagelse	VA-enheten har tagit del av de utbildningsinsatser inom IT- och informationssäkerhet som genomförts för hela Kungsbacka kommun. För VA-enhetens anställda finns dock inga kontinuerliga utbildningsinsatser inom IT-och informationssäkerhet specifikt kopplat till styrsystem, till exempel SCADA, som säkerställer god kompetens och efterlevnad av riktlinjer i verksamheten. Efter att granskningen genomfördes ska, enligt enhetschef för drift, en ny plan ha tagits fram som möjliggör att utbildning ska ske minst en gång per år eller oftare vid behov.
MEDEL	
Rekommendation	Kungsbacka kommun rekommenderas att se över möjligheten att införa en process för att säkerställa kontinuerlig utbildning inom IT- och informationssäkerhet, delvis med fokus på SCADA, för alla anställda som jobbar med systemet. Utbildning rekommenderas att ske minst årligen antingen fysiskt eller genom en digital lösning.

5. Svar på revisionsfrågor

Granskningen har syftat till att på uppdrag av revisorerna genomföra en övergripande genomgång av kommunens IT-säkerhet vad gäller deras VA-system. Granskningen har utgått från två revisionsfrågor, vilka besvaras nedan.

Hur ändamålsenlig är IT-säkerheten på en övergripande nivå avseende kommunens styrsystem utifrån befintliga lagar och god praxis?

Kontroller och rutiner för att säkerställa att endast lämpliga personer har åtkomst till kommunens VA-system finns. Det finns tydliga processer för att säkerställa att inte obehöriga har fysisk åtkomst till VA-enhetens avdelning. Kommunen har också väletablerade rutiner och handlingsplaner för att säkerställa hög vattenkvalitet.

EY har dock noterat iakttagelser inom området för behörighetshantering, vilka anses viktiga för Kungsbacka kommun att adressera för att på så sätt stärka kontrollen kring användares behörigheter och aktiviteter i SCADA. Primärt rekommenderas kommunen att ta fram riktlinjer för hur tillägg och borttag av behörigheter ska hanteras. Som ett nästa steg rekommenderas kommunen att etablera en process för att regelbundet se över användarna i SCADA.

Vid granskningen noterades också att Kungsbacka kommun har begränsad insikt i programförändringsprocessen, då denna uteslutande genomförs av den externa leverantören Systeminstallation AB. Kommunen har inte, genom nuvarande avtal, möjlighet att genomföra revision av Systeminstallation AB för att säkerställa att de upprätthåller god intern kontroll. Primärt rekommenderas kommunen att genomföra acceptanstester på egen hand innan nya programförändringar implementeras, samt att se över möjligheten att inkludera rätten till att genomföra revision i avtalet.

EY noterade även att processen för IT-incidentrapportering inte är definierad. För att kunna leva upp till de nya kraven i NIS-direktivet rekommenderas Kungsbacka kommun att ta fram riktlinjer och handlingsplan för att säkerställa att IT-incidenter rapporteras till tillsynsmyndighet i de fall det krävs och att detta görs i god tid.

Hur säkerställer kommunen att IT-säkerheten kring styrsystemen efterlevs?

Beaktat ovan bedömer EY att Kungsbacka kommuns mognadsgrad för IT-säkerhet kring SCADA är relativt hög. Detta eftersom man har pågående initiativ för att säkerställa att verksamhetens IT-säkerhet stärks, där ett av initiativen är att utforma policys och riktlinjer för IT- och informationssäkerhet. Primärt rekommenderas Kungsbacka kommun att fortsätta detta arbete och genomföra det som en del i den åtgärdsplan som togs fram efter årets riskanalys. Fortsättningsvis rekommenderas också kommunen att stärka utbildningsinsatserna för verksamheten i syfte att säkerställa kunskap och efterlevnad inom IT-säkerhet.

Bilaga 1 – Granskade dokument

- Lagstiftningsområden dricksvatten
- Miljö & hälsoskydds kontroll av dricksvatten Fjärås Bräcka VV
- Svenska livsmedelsverkets operativa mål för dricksvatten
- SLVFS 2001:30 – föreskrift
- LIVSFS 2008:13 - föreskrift
- Regeringsproposition 2017/18:204 – Informationssäkerhet för samhällsviktiga och digital tjänster
- Svenskt Vattens checklista för SCADAsäkerhet
- MSB & Svenskt Vattens kartläggning av SCADAsäkerhet 2010
- MSBs vägledning till ökad säkerhet i informations- och styrsystem
- Regin informationsblad om EXOscada

-