VAGGERYDS KOMMUN
TEKNISKA KONTORET

RAPPORT

Datum
2020-11-12

Tekniska nämnden

Internkontroll 2020- Säkert driftsystem VA

Tekniska nämnden beslutade 2019-03-05 § 21 att ha två kontrollområden för internkontroll 2020. Det ena kontrollområdet är säkert driftsystem VA och det andra är säkert driftsystem fastighet. Kontrollerna ska enligt kommunens internkontrollreglemente göras utifrån ekonomi, prestation, kvalitet och miljö.
Internkontrollernas syfte är att:

- Trygga kommunens tillgångar och förhindra förluster
- Säkerställa att lagar, bestämmelser och avtal efterlevs
- Riskminimering, säkra system och rutiner
- Styrning så att resurserna används i enlighet med tagna beslut
- Säkra en rättvisande redovisning
- Skydda politiker och personal från oberättigade misstankar

Kontroll

Internkontrollen har bestått av följande:

- Inläsning på lagar, föreskrifter, handböcker och publikationer som rör säkerhet inom VA-verksamheten. Inhämtat inläsningsmaterial kommer bland annat från branschorganisationen Svenskt Vatten, Livsmedelsverket samt lagar som till exempel säkerhetsskyddslagen.
- Intervjuer med ansvarig personal (VA-chef Teo Magnusson Bejving samt IT-chef Tomas Johansson)

Bakgrund

Driftsystemet som används inom VA-verksamheten heter Uni-View och är ett svenskt SCADA-system utvecklat av Cactus Uniview AB. Driftsystemet är uppkopplat mot en server som finns inom, driftas och ägs av Vaggeryds kommun. Systemet övervakar bland annat flöden, tryck, nivåer o.s.v. inom vatten och avlopp. Det nuvarande systemet Uni-view är nu helt

Postadress
Box 43
568 21 Skillingaryd
E-post
tekniska@vaggeryd.se

Besöksadress
Bangårdsgatan 2
Skillingaryd
Internetadress
www.vaggeryd.se

Telefon
0370-678 000

Telefax
0370-67 81 40

Bankgiro
5950-7434

Organisationsnummer
212000-0522

uppgraderat från det tidigare systemet (PC Manager) . Övergången från PC-manager började strax efter 2010. Eftersom VA-enheten inte har egen personal som kan programmera i programmet finns det ett serviceavtal upprättat med en programmerare som stöd i arbetet med driftsystemet. Uni-View är ett känt program och finns återkommande hos andra kommuners VA-enheter. Uni-view är ett system som ger betydligt större övervakningsmöjligheter där det i realtid går att se vilken nivå det är i exempelvis en högreservoar. I det förra driftsystemet (PC-Manager) fanns ingen likvärdig översikt. Det fanns ingen möjlighet att kolla vad nivån i en reservoar var vid tidpunkt x. Istället arbetade man i blindo och fick ett larm om nivån exempelvis var hög eller låg i reservoaren.

Totalt sätt finns det ett begränsat antal programlicenser för Uni-view som används dagligen av VA-verksamhetens drifttekniker. Eftersom det finns ett begränsat antal programlicenser (5-6st) minskar risken för att obehöriga (tidigare anställda exempelvis) ska kunna ansluta sig.

För att få åtkomst till Uni-view behöver man ha tillgång till någon av driftteknikernas bärbara datorer där programlicensen är installerad av IT-enheten. Man behöver också vara uppkopplad i det kommunala nätverket så att anslutning med servern finns. För att göra ändringar i Uni-view krävs det att man loggar in med användarnamn och lösenord.

Det finns även fjärrstyrningsmöjligheter där driftteknikerna hemifrån kan ansluta sig till Uni-view via direkt-access. Direkt-access kräver en så kallad tvåfaktorsautentisering. Detta innebär att om man försöker ansluta till Uni-view hemifrån så måste man först logga in på Vaggeryd kommuns nätverk med ett SITHS-kort och lösenord.

Svenskt vatten är en branschorganisation som består av landets VA-organisationer. Organisationen slår på sin hemsida fast att vatten är vårt viktigaste livsmedel och att det inom vattenförsörjningsverksamheten hanteras uppgifter som i fel händer kan skada vattenförsörjningen och leda till stor samhällsskada. Svenskt vatten nämner hot och risker som kommer från människor men även hot i form av olyckor och föroreningsutsläpp.
Svenskt Vatten har bland annat gett ut publikationen *Råd och riktlinjer om informationssäkerhet – Hantering av skyddsvärda uppgifter inom dricksvattenförsörjningen.*

Enligt publikationen (Svenskt Vatten 2012, 5) produceras det och hanteras uppgifter inom vattenförsörjningsverksamheten som i felaktiga händer kan bidra till störningar och orsaka stor skada i samhället. Publikationen (Svenskt Vatten 2012, 6) slår också fast att det kan finnas många olika syften till att medvetet eller omedvetet orsaka störningar inom dricksvattenförsörjningen och att tillvägagångssätten kan variera med allt från fysisk påverkan på infrastrukturen till påverkan på en medarbetare som ger ifrån sig information som rör skyddsvärda uppgifter kring vattenförsörjningens olika delar. Sabotage och skadegörelse mot vattenförsörjningen kan komma från enskilda personer utanför verksamheten, egen nuvarande eller tidigare personal, grupperingar eller organiserad verksamhet. Svenskt vatten understryker att för att någon ska lyckas med ett angrepp behöver man få tillgång till uppgifter eller kunskap kring ledningsnät, reservoarer eller andra vitala anläggningsdelar. Just därför är ett bra säkerhetsarbete viktigt för att undvika sådant som kan påverka verksamheten negativt.

Ekonomi:
Svenskt vatten understryker också på sin webbplats att säkerhetsarbetet är en del av VA-verksamhetens ordinarie kvalitetsarbete och ska ses som en investering. Vidare kan man läsa på organisationens webbplats att man även när det gäller säkerhet ska arbeta med att planera, genomföra, kontrollera och agera.

Internkontrollen visar att det i dagsläget är rimliga och befogade kostnader som driftsystemet och säkerheten runt omkring har. Kostnaden för driftsystemet varierar från år till år beroende på vilket arbete som utförs i systemet under olika år. Driftsystemet har under 2020, fram till och med sista oktober haft en kostnad på ca 280 tkr. Tittar man bakåt 5 år (201501-202001) så ligger den totala kostnaden på 2 050 000 (410tkr/år) I den kostnaden ingår bland annat att lägga in nya anläggningar, programmera nya maskinkomponenter, backup och felsökningar med mera. Konsultkostnaderna för driftsystemet bedöms därmed vara rimliga.
Ett säkert driftsystem är också till stor del beroende av en fysisk säkerhet. Genom övervakning, staket, larm, begränsningar med hjälp av behörigheter och så vidare begränsas åtkomsten till anläggningarna och driftsystemet. Kostnaderna för övervakning är kopplade till SOS samt Securitas-utryckningar. Totalt har SOS- larm, inbrottslarm och brandlarm under året kostat ca 41 tkr per sista oktober 2020**.** Denna kostnad är dock svår att förutse då det inte går att i förväg

veta till exempel hur många intrångsförsök på anläggningarna som kommer att inträffa under ett år. Intrångsförsöken genererar att larm utlöses och en utryckning av vaktbolag görs, vilket i sin tur leder till en kostnad. Under 2020, fram till och med sista oktober, har just utryckningarna genererat en kostnad på ca 8 700 kr. Märker man dessutom att intrångsförsöken på anläggningarna ökar så är nästa steg att införa kamerabevakning och bättre belysning på aktuella och känsliga anläggningar. Denna eventuella kostnad behöver då också tas med i beräkningarna framåt. I dagsläget ligger antalet larm med utryckning på Va-verksamhetens anläggningar på ca fem stycken per år. Men alla larm beror inte på intrångsförsök. Även kommunikationsfel kan utlösa larm som leder till utryckningar.
En annan oförutsedd kostnad som kan uppstå är om driftsystemet av någon anledning slås ut. VA-chefen gör uppskattningen att om avbrottet kan lösas på några timmar så hamnar kostnaden under 100 tkr. Blir det ett längre avbrott och beroende på vad det är för incident så kan det komma att kräva mycket resurser som gör att kostnaderna kan skena iväg fort.
Målet är att arbeta med att förhindra sådana incidenter. Därför är säkerhetsarbetet något som behöver utvecklas och upprätthållas. Med anledning av detta finns det inför nästa mandatperiod en begäran om cirka 400 -500 tkr per år för säkerhetshöjande åtgärder för både fysiska och digitala åtgärder.

Kvalitet och prestationer:
Arbetet inom VA-verksamheten styrs till stor del av olika lagar och föreskrifter (*Råd och riktlinjer om informationssäkerhet,* Svenskt Vatten 2012, 7-9) Bland annat Livsmedelsverkets föreskrifter (LIVSFS 2008:13) som innehåller krav på åtgärder för att förebygga skadeverkningar och upptäcka sabotage och skadeverkan.

Andra lagar som reglerar verksamheten är till exempel lag om allmänna vattentjänster, offentlighets- och sekretesslagen (OSL) samt säkerhetsskyddslagen med mera. Säkerhetsskyddslagen (1996: 627) fastställer att det ska finnas ett säkerhetsskydd vid olika verksamhetsställen för att motverka spionerі, sabotage och andra brott som kan hota rikets säkerhet samt ge skydd mot terroristbrott där man hanterar information som gäller rikets säkerhet (*Råd och riktlinjer om informationssäkerhet*, Svenskt Vatten 2012, 9).

Vaggeryds kommun har också ett pågående arbete med GDPR, säkerhetsskydd och informationssäkerhet. Arbetet leds av kommunens säkerhetssamordnare och när det gäller VA-verksamheten är såväl säkerhetssamordnaren, VA-chef samt tekniska kontorets informationssäkerhetsombud involverade i det pågående arbetet med regelbundna uppföljningar. Detta arbete utgår från det faktum att uppgifter som rör dricksvattenförsörjning och avloppshantering är säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddslagen (2018:585)
Säkerhetsskyddslagen 3 kap. 1 § anger att den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas.
Enligt säkerhetsskyddsförordningen, SFS 1996:633, är kommunerna skyldiga att undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. (Livsmedelverkets handbok för Risk- och sårbarhetsanalys för dricksvattenförsörjning, 2007)

Kommunfullmäktige i Vaggeryds kommun antog 2020-10-07 §184 *Riktlinjer för säkerhetsskydd* och 2020-10-26 § 130 antogs en *policy för säkerhetsskydd*. Policyn understryker att en grundläggande förutsättning för ett effektivt säkerhetsskydd är att all berörd personal får den upplysning och utbildning i vad deras arbetsuppgifter och ansvarsområde kräver. Personalen ska också ha insikt i de grundläggande avsikterna med säkerhetsskyddslagen.

I dagsläget är det endast förvaltningschef och VA-chef inom tekniska kontoret som har genomgått en säkerhetsprövning.
Enligt Vaggeryds kommuns riktlinjer för säkerhetsskydd står det att en säkerhetsprövning ska göras av alla personer som på ett eller annat sätt får del av säkerhetsskyddade handlingar, tillträde till säkerhetsskyddade anläggningar eller på annat sätt ska delta i någon verksamhet som rör Sveriges säkerhet och i vilken de kan få inblickar i sådant som inte för röjas.

IT-säkerhet

Intervjun med Vaggeryds kommuns IT-chef visar på att IT-säkerheten i kommunen är bra utifrån de resurser och ekonomiska möjligheter som finns. Dock så behöver man vara medveten om att man aldrig kan vara 100 % skyddad från intrång. Som exempel kan nämnas att Vaggeryds kommun vid tre tidigare tillfällen har drabbats av virus. Det har dock varit med begränsad omfattning och skadan har ganska snabbt kunnat repareras. Om man tittar i brandväggsloggen för kommunens brandväggar ut mot omvärlden kan man se att det ständigt kommer in trafik som försöker hitta öppningar för att lirka in sig på något sätt. Enligt IT-chefen har Vaggeryds kommun väldigt säkra brandväggar men det finns aldrig några garantier.

För att uppnå så hög säkerhet som möjligt och förhindra samt begränsa skador från möjliga intrång jobbar man på flera olika plan.

Servern som driftsystemet är uppkopplat mot står på en plats med begränsad åtkomst. Det är låst, övervakat, och har ett passagesystem. Man kör regelbundna backuper. Man kör även en så kallad image på servern varannan dag. Det betyder att det går att återställa servern inom ett par timmar till exakt så som det en såg ut efter den sista imagen upprättades. Vid uppdateringar görs dessutom en så kallad ”snapshot”, det vill säga att en ögonblicksbild tas av servern på hur den ser ut innan uppdateringen. Därmed kan servern återställas på 15 sekunder om något skulle gå snett under uppdateringen. Det finns även en handlingsplan i händelse av till exempel en brand i serverrummet. Den går ut på att bandbackuper hanteras cirka en mil från serverrummet. Sedan finns ytterligare ett reservserverrum där ett antal servrar finns i beredskap och väntar för att kunna startas upp och återställa servarna från imagen med det nödvändigaste vi behöver för att kunna komma igång snabbt igen. Driftskopia och reservkopia är alltså av säkerhetsskäl åtskilda med en mils avstånd.

Såväl VA-verksamhetens drifttekniker som den externa konsult som jobbar i systemet kan jobba på distans med en fjärruppkoppling men som ytterligare en säkerhetsåtgärd krävs det då en tvåfaktorsautentisering för att kunna komma in i systemet.

När det gäller den externa konsulten så använder man sig av en lösning som heter Mobilityguard som gör att konsulten inte kan föra över virus från sin dator in i systemet, utan det är som en så kallad glasvägg mellan konsult och server. IT-chefen understryker dock att konsulten i praktiken skulle kunna ladda ner saker från internet och lägga in på servern. Servern har kontakt med internet för att till exempel kunna uppdatera virusskydd. Där finns en risk för

att konsulten ska kunna orsaka skada. Det ligger på verksamheten att säkerställa att de konsulter man jobbar med är ”säkra”. Från IT-enheten säkerställer man endast funktionen, det vill säga att på verksamhetens uppmaning så ser IT-enheten till att de konsulter som ska ha uppkoppling också får det.

Tillsammans med tillämpliga lagar, föreskrifter, policys samt det egna arbetet med säkerhet och säkerhetsskydd pågår ett kontinuerligt arbete för att säkerställa en god kvalitet och ett säkert driftsystem. Det finns dock områden som kan förbättras och systematiseras. Internkontrollen visar att den övergripande bilden är att inom VA-verksamheten jobbas det med säkerhet och man har koll på densamma. Man har till exempel begränsad behörighet för vilken personal (två personer) som kan göra större ändringar i driftsystemet men även ändringar i larmsystem på befintliga anläggningar. Driftsäkerheten är även beroende av den fysiska säkerheten som ska förhindra att obehöriga tar sig in på verksamhetens anläggningar. Den säkerheten anses i dagsläget vara god. Så gott som alla livsmedelsanläggningar har inbrottslarm. Alla livsmedelsanläggningar har staket för att förhindra obehörigt intrång på området. Allt sabotage polisanmäls och upptäcker man att någon anläggning återkommande drabbas av intrångsförsök ses övervakningen över och installation av t.ex. kameraövervakning övervägs. Det finns även ett pågående arbete med att uppmärksamma personal att tänka på vad det är för information man skickar ut via till exempel e-post.

Om driftsystemet skulle slås ut (t. ex på grund av misstag, sabotage, elavbrott och så vidare) går varje enskild anläggning även att driva manuellt. Till en början kan kommunen vid ett avbrott i systemet bli utan vatten en kortare tid. Det finns en backup som säkerställer funktion i 24 timmar i framförallt Skillingaryd och Vaggeryd. Dessa orter är bättre rustade för ett avbrott än de mindre orterna i kommunen. Det beror dels på att det mellan Vaggeryd och Skillingaryd finns en överföringsledning. I övriga orter är det manuell drift som gäller. Om elektriciteten försvinner får man också problem med pumparna. Det finns tillgång till reservkraftverk idag, både mobila och befintliga på plats. Dessa reservkraftverk utförs det årliga besiktningar på och regelbundna kontroller av reservkraftverk sker enligt egenkontrollprogrammet. När det gäller den manuella driften visar internkontrollen att det finns goda rutiner. Det finns en teknisk beskrivning på varje anläggning om hur man kör manuellt. Det finns en upplärningsperiod på

strax över en månad där nyanställda får följa med respektive drifttekniker en vecka för att lära sig hur samtliga anläggningar fungerar. Det finns också en årlig genomgång med befintlig personal på hur samtliga anläggningar fungerar inför semestern då bemanningen är begränsad. Detta är en kvalitetssäkring som minskar sårbarheten då det finns flera personer som kan utföra samtliga arbetsmoment.

Internkontrollen belyser det faktum att det finns vissa delar inom säkerhetsarbetet som har brister och behöver åtgärdas. Bristerna kan kopplas till att det inte finns dokumenterade och/eller uppdaterade risk- och sårbarhetsbeskrivningar, konsekvensanalyser och handlingsplaner. Enligt VA-chefen finns det en medvetenhet kring dessa men man behöver kunna säkerställa att om till exempel personal slutar att kunskap och information på ett smidigt sätt kan överföras till ny personal genom att informationen är skriftlig, samlad på ett ställe, lättillgänglig samt att all personal vet var den finns. Även säkerhetsrutiner behöver vara tydliga och skriftliga. Det går till exempel inte att anta att personal loggar ut från sin dator och därmed från driftsystemet när de går hem för dagen. Det måste finnas klara rutiner som ser till att dessa, liksom andra viktiga rutiner, inte glöms bort. Därför bör dessa vara skriftliga och delges all ny personal samt att man har regelbundna genomgångar och uppföljningar av dessa med befintlig personal.
En annan säkerhetsrisk som framkommer i intervjun med både VA-chef som IT-chef är den egna personalen. Om någon ur den egna personalen till exempel skulle klicka på en fel länk kan det leda till att man drar in ett virus på datorn som skulle kunna låsa filer, ta bort filer eller skicka filer någon annanstans. Säkerheten blir inte bättre än de medarbetare som hanterar systemet. Konsulter kan också utgöra en risk då de sitter och jobbar med systemet. Konsulter och medarbetare är helt enkelt den största risken. För medarbetare handlar det om utbildning och förståelse om vad det är man arbetar med. För konsulter gäller det att verksamheten gör en bakgrundskontroll och säkerställer att konsulter man tar in har en förståelse för vad det är de gör.
Man kan inte utesluta att de som har behörigheter att göra ändringar i systemet kan vara angripare. Interna angripare kan vara farligare än externa eftersom de både har behörighet till lokalerna samt känner till kritiska funktioner och svagheter i systemet. Men alla störningar

behöver inte vara orsakade av angripare. Personalen kan också orsaka driftstörningar av misstag.(*Säkerhethandbok för dricksvattenproducenter*, Svenskt Vatten 2012, 51)
Internkontrollen påvisar att den personal som inom VA-verksamheten har behörighet att göra ändringar i systemet skulle kunna göra detta utan att något larm utlöses. Det innebär att problemet skulle upptäckas först i efterhand och därmed kunna ställa till med skada. Sannolikheten för detta får dock bedöms som liten då det endast är två personer som har behörighet för att göra ändringar. En säkerhetsprövning av den personal som har behörigheten är också en möjlig åtgärd för att minimera risken ytterligare.
Det finns även rutiner som man inte har implementerat i säkerhetsarbetet. Till exempel finns tillgång till loggar (inloggningar, misslyckade inloggningsförsök och inpassage). När det gäller dataloggar till driftsystemet är det verksamheten själv som ansvarar för att kontrollera dessa. Misslyckade inloggningsförsök kan till exempel vara ett tecken på angripare. Många loggposter med fel som har begåtts av behöriga användare kan till exempel också visa att det finns behov av kompletterande utbildning (*Säkerhethandbok för dricksvattenproducenter*, Svenskt Vatten 2012, 53). Men dessa kontrolleras i dagsläget inte alls när det gäller VA-verksamhetens driftsystem. Det innebär att eventuella obehöriga aktiviteter och annat inte upptäcks den vägen. Personal som dagligen arbetar i systemet upplever att systemet är enkelt att arbeta i och att risken för att göra fel är liten.
När det däremot gäller inloggning på det kommunala nätverket så ligger det ansvaret på IT-enheten. Om en användare försöker logga in på nätverket flera gånger så blir de utelåsta. Sedan behöver användaren höra av sig till IT för att de ska låsa upp behörigheten. IT-enheten har precis beställt en ny programvara som är en loggningsprogramvara. Anledningen till det är att kommunen behöver uppfylla vissa GDPR-krav och behöver därmed kunna logga på ett bättre sätt än vad man gör idag. Programvaran kommer logga alla inloggningar och på den kommer det sättas larmnivåer där IT-enheten då omedelbart kommer att få ett larm när någon till exempel försöker logga in ett visst antal gånger eller när det blir felaktiga inloggningar på ett visst användarkonto. För även om systemet stänger ute en användare efter ett visst antal inloggningsförsök så kan det finnas någon automatfunktion som fortsätter att testa lösenord. Med den nya programvaran så kommer det då utlösas ett larm och möjlighet finns då för IT-enheten att se vem och varifrån inloggningsförsöken kommer.

Sammanfattningsvis kan man konstatera att det är av största vikt att skydda hela kedjan i dricksvattenförsörjningen, även driftsystemet, från hot och angrepp. Förutom att ett angrepp eller försök till angrepp kan orsaka skada i form av en ökad kostnad så kan det även leda till att dricksvattenproducenten förlorar konsumenternas förtroende. Ibland kan förtroendet även påverkas av ett misslyckat angreppsförsök (*Säkerhetshandbok för dricksvattenproducenter*, Svenskt Vatten , 25).

Miljö

Inget miljöperspektiv har framkommit under kontrollen av rutiner kopplade till driftsystemet inom vatten- och avlopp.

Förslag på åtgärder/förbättringar:

För att uppnå ett säkert driftsystem är det många faktorer som ska samspela. Som internkontrollen visar så hänger säkerheten ihop med såväl IT-säkerhet, personalsäkerhet, fysisk säkerhet samt framtagna och dokumenterade rutiner. Detta har resulterat i flera förslag på åtgärder som kan göras för att förbättra säkerheten för driftsystemet inom VA men även för VA-verksamheten överlag:

- Att VA-chef samt IT-chef går kursen i systematiskt säkerhetsarbete som anordnas av branschorganisationen Svenskt Vatten. Kursen ska ge ett underlag för hur man kan planera säkerhetsåtgärder. Utbildningen behandlar informationssäkerhet med fokus på såväl personsäkerhet, fysisk säkerhet och cyberhot och lär bland annat ut hur man gör riskanalyser och upptäcker säkerhetshot.
- Att VA-personalen går en intern utbildning hos kommunens informationssäkerhetssamordnare för att få kunskap om hur man kan arbeta med informationssäkerhet och vilka krav som ställs på informationshantering inom VA-verksamheten utifrån till exempel säkerhetsskyddslagen samt GDPR.
- Att VA-chefen får i uppdrag att se till att eventuella befintliga rutiner ses över och rutinbeskrivningar upprättas och/eller uppdateras.
- I de fall där det inte finns risk- och sårbarhetsanalyser, konsekvensanalyser och handlingsplaner ska de tas fram, dokumenteras och följs upp kontinuerligt för att bland annat kunna ha tydliga

skriftliga dokument som till exempel kan visa vilka konsekvenser ett avbrott eller störningar i systemet kan få för såväl samhället som för verksamheten.

- Att skapa en rutin för att kontinuerligt följa upp dataloggar kopplade till driftsystemet för att på så vis kunna upptäcka eventuella intrångsförsök och/eller misslyckade inloggningar.
- Att se över att samtliga medarbetare som har tillgång till säkerhetsskyddade handlingar eller tillträde till säkerhetsskyddade anläggningar säkerhetsprövas eller/och har ett säkerhetssamtal.
- Att se över extern konsult och göra en bakgrundskontroll på denne för att ytterligare höja säkerheten.