Revisionsrapport 2021
Genomförd på uppdrag av lekmannarevisorerna
januari-februari 2022

Vätternvatten AB

Granskning av informations- och IT-säkerheten

Örebro kommun

Building a better working world

Innehåll

1. Inledning 2
1.1. Bakgrund 2
1.2. Syfte och revisionsfrågor 2
1.3. Genomförande 2

2. Revisionella utgångspunkter 3
2.1. Ledningssystem för informationssäkerhet – LIS 3
2.2. Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster . 3

3. Granskningsresultat 4
3.1. Vätternvatten AB 4

Bilaga 1: **Källförteckning 6**

1. Inledning

1.1. Bakgrund

Så gott som all verksamhet i kommuner och kommunala bolag bedrivs med någon form av IT-stöd. IT-system har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet. Antalet olika programvaror är stort och mängden ansamlad data och information betydande. För att uppnå målen för kommunens, och dess bolags, verksamheter krävs att informationen i verksamhetsstödet är tillgänglig, riktig, har korrekt konfidentialitet samt är uppfyller krav på ändamålsenlig säkerhet.

Med utgångspunkt från sin riskanalys för 2021 har kommunens lekmannarevisorer beslutat att genomföra en granskning av IT- och informationssäkerhet, med inriktning mot policys, riktlinjer och hantering av säkerhetsfrågor, på övergripande nivå.

1.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma huruvida det föreligger en tillräcklig intern kontroll med avseende på de kommunala bolagens arbete med IT- och informationssäkerhet.

Granskningen har genomförts mot så kallad god praxis inom IT- och informationssäkerhetsområdet. Granskningen görs mot Myndigheten för samhällsskydd och beredskapsverktyg LIS, som är etablerat ramverk inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27001.

I granskningen har följande revisionsfrågor besvarats:

- Är ansvarsfördelningen inom respektive bolag tydlig med avseende på IT-säkerhet?
- Finns tydliga styrdokument (policy, riktlinjer etc.) och följs efterlevnaden av dessa upp regelbundet av styrelsen?
- Genomförs regelbundna riskanalyser med avseende på IT- och informationssäkerhet?
- Kan återrapporteringen till styrelsens bedömas vara tydlig och ändamålsenlig?
- I vilken omfattning används stöd från externa IT-konsulter? Är uppföljning och utvärdering av externa IT-tjänster ändamålsenlig i förekommande fall?

Granskningen avser samtliga bolag inom Örebro Rådhus AB med dess dotterbolag där revisionell bedömning sker för respektive bolag eller i förekommande fall för respektive underkoncern. Granskningen innebär inte att några säkerhetstester, penetrationstester eller dylikt av IT-system har genomförts.

1.3. Genomförande

Granskningen grundas på intervjuer och dokumentstudier (se bilaga 1). Intervjuer har skett med ansvariga för bolagens respektive informations- och IT ansvariga. Samtliga intervjuade har beretts tillfälle att sakgranska rapporten. Granskningen är genomförd januari-februari 2022.

2. Revisionella utgångspunkter

2.1. Ledningssystem för informationssäkerhet – LIS

Ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter[1]. Hur informationssäkerhetsarbetet kan bedrivas på ett systematiskt sätt och i enlighet med ”best practice” finns beskrivet i standarderna för ledningssystem för informationssäkerhet.

Av Myndigheten för Samhällsberedskap, MSB, framgår att en central del i ett ledningssystem är ledningens uttalade stöd. Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet där detta stöd kommer till uttryck. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till mellanchefer och övrig personal.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel användning av Internet och e-post, åtgärder till skydd mot skadlig kod, fysisk säkerhet, incidenthantering, kontinuitetsplanering, mobilt arbete, inventarier och licenser, behörighetsadministration och loggning.

2.1.1. Internationella standarder enligt ISO/IEC 27001

I verksamheternas arbete med ledningssystem för informationssäkerhet finns det vissa standarder att beakta. De grundläggande standarderna har tagits fram inom ramen för samarbetet i de internationella standardiseringsorganen ISO (International Organization for Standardization) och IEC (International Electrotechnical Commission) och berör främst krav och riktlinjer för vilka säkerhetsåtgärder ledningssystemet generellt ska innehålla[2]. I ISO 27001:2017 framgår att ledningen ska säkerställa att en informationssäkerhetspolicy och informationssäkerhetsmål är upprättade och integrerade i verksamhetsprocesser. Vidare bör det finnas en tydlig ansvarsfördelning med rapporteringsstruktur[3]. Kapitlen i 27002 har fokus på säkerhetsåtgärder men omfattar även frågor om styrning av informationssäkerhet såsom regelverk för informationssäkerhet (policy), organisation och efterlevnad.

2.2. Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

Med syfte att genomföra NIS-direktivet beslutades om en ny lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen trädde i kraft den 1 augusti 2018 och innehåller ytterligare krav för organisationer som driver samhällsviktiga verksamheter, exempelvis flygplatser, hamnanläggningar, energidistribution och leverans/distribution av dricksvatten[4]. Den nya lagen innebär att det kommer att ställas nya krav på att företagen ska arbeta systematiskt och riskbaserat med informationssäkerhet samt rapportera incidenter.

[1] MSB:s definition av informationssäkerhet: Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
[2] ISO 27001:2017
[3] MSB rekommenderar exempelvis att ett organisationsövergripande dokument klargör det mandat och den rapporteringsplikt som personen med ansvar för att leda och samordna informationssäkerhetsområdet har
[4] Där statens energimyndighet är tillsynsmyndighet

3. Granskningsresultat

3.1. Vätternvatten AB

Vätternvatten AB är ett kommunalägt bolag som bildades 2018. Vätternvatten ägs av Hallsbergs kommun, Kumla kommun, Lekebergs kommun och Örebro kommun. Ägarförhållandena ändras varje år och justeras utifrån befolkningsmängd per den 1 november varje år. För 2021 äger Örebro kommun 76,65 procent av bolaget. Vätternvatten har som mål att på ett långsiktigt, ekonomiskt och hållbart sätt ansvara för och främja en god vattenförsörjning till delägarkommunerna. Bolagets verksamhet är uppdelad i tre faser. Produktionstiden för projektet är cirka tio år från bolagsbildandet.

Bolaget har för tillfället nio anställda, vilket är en ökning från de tre anställda som bolaget hade i början av 2021. Därtill anlitar bolaget flera konsulter med expertkunskap kopplat kring vissa delar i projektet med att främja en god vattenförsörjning.

3.1.1. Ansvarsfördelningen avseende IT-säkerhet

Bolaget anlitar för tillfället VD från Futurum Fastigheter i Örebro AB i väntan på att en heltidsanställd VD rekryteras. Ytterst faller ansvaret på IT- och informationssäkerhet på VD. Bolaget har anlitat IT-resurs/support från Futurum Fastigheter för att säkerställa en fungerande struktur kring hårdvaror (datorer och mobiler) samt mjukvara. Bolagets IT-miljö har funnits i Futurum Fastigheter fram till januari 2022. Vid tiden för granskningen köper bolaget även IT-support vid behov från Futurum Fastigheter.

3.1.2. Styrdokument och efterlevnad

Det saknas ett upprättat styrdokument som behandlar IT- och informationssäkerhet. Vidare saknas skriftliga rutiner och riktlinjer för området. Intervjuade redogör för att bolaget till viss del inte vill styra detta innan utredningen kring säkerhetsskyddslagstiftningen är färdigställd, se 3.1.3.

3.1.3. Riskanalyser avseende IT- och informationssäkerhet

Bolaget anlitar en konsult för att utreda hur bolaget påverkas av säkerhetsskyddsförordningen och vilka åtgärder som behöver vidtas. Vi har i och med detta inte kunnat ta del av dokument och riskanalyser då dessa är under utredning gällande informationssäkerhetsklassning. De dokument som finns framtagna är klassade med sekretess. Intervjuade uppger att bolaget avser ta ett större grepp kring styrningen av IT- och informationssäkerhetsfrågorna när det har tydliggjorts vilka krav som gäller utifrån säkerhetsskyddslagstiftningen. Bolaget uppger dock att man är medvetna om att en sådan utredning kan ta tid och att verksamheten behöver påbörja arbetet med styrningen av dessa frågor parallellt.

Enligt uppgift arbetar bolaget med att fastställa arbetssätt för bolagets internkontrollarbete inför 2022. Det finns exempelvis ett behov av att upprätta en detaljerad attestinstruktion som är uppdaterad till den nya organisationen. Enligt uppgift har inte IT- och informationssäkerhetsrelaterade risker inkluderats i någon samlad riskanalys eller internkontrollplan för bolaget som helhet.

3.1.4. Återrapportering till styrelsen

Styrelsen tar inte del av någon regelbunden rapportering rörande IT- eller informationssäkerhet. Enligt uppgift har enskilda ärenden varit uppe som berört IT-säkerhet, exempelvis kring arbetet med säkerhetsskyddslagstiftningen.

3.1.5. Användandet av externa IT-konsulter

Vätternvatten AB använder sig av externa IT-konsulter då alla IT-frågor hanteras av den IT-resurs som hyrs in av Futurum Fastigheter. Resursen är ej säkerhetsprövad. Bolaget har en projektchef som ansvarar för uppföljningen av externa konsulter som anlitas i projektrelaterade frågor, ingen av dessa är att betrakta som IT-konsulter. Inga externa konsulter, bortsett från de som anlitas av Futurum, släpps idag in i Vätternvatten AB:s IT-system. För konsulter anlitade att arbeta med säkerhetskyddsfrågor har säkerhetsskyddsavtal tecknats och säkerhetsprövning gjorts. Vissa tekniska konsulter har även tecknat sekretessavtal.

3.1.6. Bedömning

Sammanfattad bedömning – Vätternvatten AB

Det saknas ett upprättat styrdokument som behandlar IT- och informationssäkerhet och ett systematiskt arbete kring frågorna. Detta beror delvis på att bolaget är relativt nystartat och bedrivs i projektform samt att det bedrivs en utredning kring säkerhetsskyddsförordningens påverkan på bolaget. Det är rimligt att ett övergripande styrdokument fastställs av styrelsen när utredningen kring säkerhetsskyddsförordningen är färdigställd. Det finns ett behov av att inarbetade arbetssätt och rutiner skyndsamt dokumenteras. Det saknas en samlad formaliserad riskanalys inom IT- och informationssäkerhet för bolaget som helhet. IT- och informationssäkerhetsrelaterade risker bör inkluderas i riskanalysarbetet för bolagets övergripande internkontrollarbete som kommer att utvecklas framgent. Bolagets anlitar medarbetare vid systerbolaget Futurum Fastigheter i Örebro AB för stöd kring IT, vilket är nödvändigt då bolaget själva saknar denna kompetens.

Vår bedömning är att bolaget inte har en tillräcklig hantering av IT- och informationssäkerhet. Vi rekommenderar att styrelsen säkerställer att vissa rutiner för IT-och informationssäkerhet upprättas samt att roller och ansvar tydliggörs. Det saknas en regelbunden rapportering till styrelsen rörande verksamhetens IT- och informationssäkerhet, vilket vi bedömer är en brist. Styrelsen rekommenderas även att inkludera IT- och informationssäkerhetsrelaterade risker i det övergripande riskanalysarbetet kopplat till bolagets internkontrollarbete.

Bilaga 1: Källförteckning

Intervjuade funktioner:

- Ekonomichef Vätternvatten (från 1 oktober 2021)
- *anlitad* Ekonomichef från Futurum Fastigheter (fram t.om. den 1 oktober 2021)
- *anlitad* IT-ansvarig från Futurum Fastigheter