Södertälje kommun
Revisorerna

Revisionsskrivelse
2018-09-13

Till: Kommunstyrelsen samt styrelserna för Telge Energi och Södertälje hamn

För kännedom: Kommunfullmäktige

Revisionsrapport nr 4/2018 – Granskning av intrång i system, Telge Energi och Södertälje Hamn

EY har på uppdrag av kommunens revisorer genomfört en granskning med syfte att bedöma om Telge Energi och Södertälje Hamn säkerställt att det finns en tillräcklig styrning och intern kontroll avseende skydd mot intrång i systemen.

EYs samlade bedömning är att de granskade bolagen till viss grad säkerställer att det finns tillräcklig styrning och intern kontroll avseende skydd mot intrång i systemen. Det operativa arbetet med ändamålsenligt skydd och incidenthantering mot intrång i systemen bedöms till stor del tillfredställande. Dock finns en återkommande otydlig definition av begreppet IT-säkerhet och informationssäkerhet där ansvarsfördelning inte beskrivs tillräckligt tydligt i rådande styrdokument och riktlinjer. EY bedömer att koncernens nuvarande utformning av IT-policy bör ses över och utvecklas.

Granskningsrapporten innehåller 12 st rekommendationer för att förbättra skyddet mot intrång.

Svar från kommunstyrelsen och styrelserna i granskade bolag önskas senast 2018-12-15

För revisorerna i Södertälje kommun

Christer Björk

Elisabet Komheden

Bilaga: Revisionsrapport nr 4/2018 – Granskning av intrång i system, Telge Energi och Södertälje Hamn

Södertälje kommun

Granskning av intrång i system, Telge Energi & Södertälje Hamn

31 augusti 2018

Building a better working world

Sammanfattning

EY har på uppdrag av kommunens revisorer genomfört en granskning med syfte att bedöma om Telge Energi och Södertälje Hamn säkerställt att det finns en tillräcklig styrning och intern kontroll avseende skydd mot intrång i systemen. EYs samlade bedömning är att de granskade bolagen till viss grad säkerställer att det finns tillräcklig styrning och intern kontroll avseende skydd mot intrång i systemen. Det operativa arbetet med ändamålsenligt skydd och incidenthantering mot intrång i systemen bedöms till stor del tillfredställande. Dock finns en återkommande otydlig definition av begreppet IT-säkerhet och informationssäkerhet där ansvarsfördelning inte beskrivs tillräckligt tydligt i rådande styrdokument och riktlinjer. EY bedömer att koncernens nuvarande utformning av IT-policy bör ses över och utvecklas.

Det ska noteras att denna bedömning ej tar hänsyn till faktisk efterlevnad av policyer, instruktioner och styrdokument då ingen stickprovstestning har utförts under denna granskning. Bedömningen baseras enbart på vilka förutsättningar som finns i form av styrande dokument.

Styrning och organisation	Inom koncernen har Koncern-IT det övergripande ansvaret för IT-säkerhet medan bolagen ansvarar för informationssäkerhet. Bedömningen är att det finns en ändamålsenlig organisation för IT-säkerhet. Dock bör styrdokument uppdateras där ansvar och roller tydliggörs och eventuella överlapp i riktlinjer mellan bolag och koncern ses över.	
Policyer och styrdokument	Policyer och styrdokument kopplade till IT-säkerhet finns. Telge AB bör överväga att integrera samtliga separata riktlinjer i en enad och sammanhållande IT-policy som innehåller arbetssätt, rutiner, tydlig ansvarsfördelning samt konsekvenser vid bristande efterlevnad.	
Incidenthantering och intern kontroll	En koncernövergripande incidenthanteringsprocess finns dokumenterad. Vid hot eller händelser av intrång klassas incidenten som stor/kritisk och följer separat process. Bedömningen är att framtagna rutiner och riktlinjer följer god praxis. Rekommendationen är att se över behovet att samla dessa i ett gemensamt dokument och att revidera detta på mer regelbunden basis än nuvarande revideringsprocess.	
Identifiering och hantering av risker och hot	Sårbarhetsskanning och införande av skadlig kod i systemen utförs på halv- eller helårsbasis enligt årskontrollplanen. Koncernens databaser övervakas 24/7 för att upptäcka obehörigt intrång eller skada. Bedömningen är att rådande rutiner följer god praxis.	

Existerar tillfredställande

Existerar med utrymme för förbättringar/förtydligande

Existerar ej eller med stora förbättringsbehov

Generella observationer

Telge ABs IT-stab (vidare i rapporten benämnt "Koncern-IT") har ett övergripande ansvar att upprätthålla en god IT-säkerhet inom hela koncernen, vilket även innefattar alla koncernens bolag (Telge Energi och Södertälje Hamn inbegripet). Graden av inblandning varierar beroende på respektive bolags storlek och komplexitet hos IT-miljön.

Det finns en informell överenskommelsekonsensus gällande ansvarsfördelningen mellan koncern och bolag för IT-säkerhet och informationssäkerhet. Enligt denna har Koncern-IT ansvar för IT-säkerhet medan bolagen har ansvar för informationssäkerhet. Denna uppdelning finns dock inte beskriven i något styrande dokument.

Telge Energi har nyligen upprättat en mall för systemsäkerhetsanalys som avser att omfatta riskanalys av informationssäkerhet kopplat till bolagets system. Mallen innefattar klassificering av information, hot- och riskanalys samt fastställande åtgärder. När granskningen ägde rum hade mallen inte tagits i bruk. Dock finns det en ambition att göra det inom snar framtid.

Södertälje Hamn förlitar sig på Koncern-IT som tjänsteleverantör av IT-säkerhet – även gällande informationssäkerhet även om det yttersta ansvaret faller på bolaget.

Telgekoncernen har rådande policyer och styrdokument spridda över olika dokument med olika revideringsdatum. Dessa kan med fördel integreras till en större sammanhållande policy som bör revideras årligen.

Innehåll

1. Bakgrund

Hösten 2017 genomförde EY på uppdrag av de förtroendevalda revisorerna i Södertälje en granskning av informationssäkerhet på övergripande nivå i kommunen. Ett antal förbättringsområden noterades i rapporten. Som ett resultat av 2017 års informationssäkerhets-granskning på kommunnivå har de förtroendevalda revisorerna beslutat att för 2018 begära en fördjupad granskning av skydd mot intrång i systemen i två av de kommunalt helägda bolagen. En viktig del av arbetet med IT-säkerhet kopplat till intrång handlar om att förstå olika hotbilder, hantera sannolikheter för att utsättas för skada samt att arbeta proaktivt, preventivt och reaktivt försvar mot cyberrelaterade attacker. En organisation bör ha tydliga och ändamålsriktiga styrdokument och policyer lättillgängliga och väl inarbetade i organisationen för att kunna säkerställa förutsättningar för en god IT-säkerhet.

1.1 Syfte

Granskningens övergripande syfte är att bedöma huruvida de granskade bolagen säkerställer att det finns tillräcklig styrning och intern kontroll avseende skydd mot intrång i systemen.

I granskningen besvaras följande revisionsfrågor:

- Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policys?
- Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?
- Har bolagen ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?
- Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång?
- Har tester genomförts avseende intrång i systemen?
- Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag?

1.2 Metod

Revisionsfrågorna har besvarats genom en granskning mot så kallad god praxis inom informationssäkerhetsområdet samt mot en rad revisionskriterier. Revisionskriterierna är de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar. I denna granskning utgörs revisionskriterierna av:

- Informationssäkerhetspolicy och tillhörande informationssäkerhetsstandarder
- IT-policy och användarinstruktioner
- IT-strategi
- Riskanalyser IT
- Internationella standarder enligt ISO (International Organization for Standardization) avseende ISO 27001:2013 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet
- Internationella standarder för informationssäkerhet som ryms inom Control Objective for Information and Related Technology Standards (COBIT).

EY har genomfört en övergripande kartläggning av rutiner, kontroller samt kortfattat behandlat styrningsfrågor rörande informationssäkerhet.

Innan granskningen påbörjades hölls ett initialt möte med kommunkoncernens IT-chef och representanter från de granskade bolagen. Under detta möte beskrevs granskningens syfte, upplägg samt de revisionsfrågor som skulle besvaras. Granskningen genomfördes sedan först via insamling och granskning av befintliga styrande dokument. Därefter genomfördes intervjuer med de personer som ansågs kunna ge en fullständig bild över verksamheten, djupare förståelse för aktuella processer, övergripande rutiner och verksamma kontroller. Granskningen ägde rum under maj/juni 2018.

Under granskningen har inga stickprovstester utförts, vilket innebär att EY inte granskat graden av efterlevnad av dessa rutiner och kontroller. Bedömningskriterierna i denna rapport baseras på vilka förutsättningar som finns på plats givet rådande rutiner och styrning att upprätthålla god intern kontroll och skydd mot intrång. Granskningar har alltså inte utformats för att identifiera eventuella fall av bristande efterlevnad och kontrollutförande från koncernen. Med bakgrund till detta rekommenderar EY att Södertälje kommun bör utvärdera möjligheten att utföra en granskning av efterlevnad för att få en faktabaserad bild över till vilken grad anställda i organisationen följer rådande riktlinjer och kontroller.

Under granskningen intervjuades:

- Anders Rosberg – Koncern IT-chef Telge AB.
- Göran Hellström – Förvaltning & Utveckling, Kvalitet, Telge AB koncern IT
- Daniel Rytterlund – IT-säkerhetsansvarig (tf), Telge AB Koncern-IT
- Tomas Zackrisson - IT-chef, kvalitet, miljö, Södertälje Hamn AB

- Åsa Pohl – Chef IT, Projekt & Kundprocesser, Telge Energi AB

Därefter har denna rapport utformats som underlag för revisorernas bedömning av arbetet med att säkerställa en god intern kontroll med avseende intrång i systemen hos de granskade bolagen.

2. Syfte och delfrågor

Följande avsnitt innehåller det övergripande revisionssyftet sammanställt i en omfattande revisionsfråga. För att besvara den övergripande revisionsfrågan har en rad kontrollfrågor utformats i syfte att täcka samtliga aspekter av revisionsfrågan.

2.1 Syfte

Granskningens syfte är att bedöma om de granskade bolagen Telge Energi och Södertälje Hamn säkerställt att det finns en tillräcklig styrning och intern kontroll avseende skydd mot intrång i systemen.

2.1.1 Revisionsfrågor

- **(1) Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policys?**
- **(2) Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?**
- **(3) Har bolagen ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?**
- **(4) Finns tillräckliga riktlinjer för incidenthantering i samband med försök till eller genomförda intrång?**
- **(5) Har tester genomförts avseende intrång i systemen?**
- **(6) Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag?**

3. Bedömning avseende svar på revisionsfrågor

Följande avsnitt innehåller granskningens observationer och rekommendationer.

3.1 Revisionsfråga 1: Finns en tydlig styrning av skydd mot intrång genom tydliga och ändamålsenliga styrdokument? Är dokumenten beslutade på relevanta nivåer och är de tydligt kopplade till kommunkoncernens IT-policys?

Observationer	Rekommendationer
EY har på förfrågan om gällande policyer fått tillgång till tre policydokument av Telge AB, "Informationssäkerhetspolicy", "Policy för IT" och "Policy för IT-säkerhet". De två sistnämnda dokumenten är undertecknade 2013 av koncernchef Stefan Hollmark och är reviderade under 2016 respektive 2017 av IT-chef Anders Rosberg. Dessa två dokument innehåller vardera 4-5 punkter av rådgivande karaktär som på övergripande nivå beskriver riktlinjer för ett effektivare IT-stöd samt hur koncernen löpande ska arbeta för en säker hantering av information i IT-systemen. Ingen punkt berör specifikt styrning av skydd mot intrång. Informationssäkerhetspolicyn är framtagen av Södertälje kommun och beskriver kommunens arbete med informationssäkerhet på en övergripande nivå. Policyn täcker in organisation och riktlinjer. Telge-koncernen antog policyn under Q2 2018 med förbehållet att den vidareutvecklas och anpassas efter bolagens verksamheter. Informationssäkerhetspolicyn finns i "VETA" bland andra koncerngemensamma policys. Utöver ovan nämnda policydokument finns en IT-strategi av mer omfattande utformning. IT-strategin ägs av koncernchefen, förvaltas av IT-chef och omfattar alla koncernens verksamheter (läs bolag). Detta dokument är daterat till 2016 och innehåller styrande principer	• Telge AB bör överväga att utveckla befintliga policyer kopplat till IT, IT-säkerhet och informationssäkerhet. EY rekommenderar Telge AB att integrera samtliga separata riktlinjer i en, eller möjligtvis två, sammanhållande policy för IT och informationssäkerhet. Denna bör då täcka arbetssätt, rutiner, tydlig ansvarsfördelning samt konsekvenser vid bristande efterlevnad. En enad sammanhållen policy som inkluderar riktlinjer ökar förutsättningarna för lättare efterlevnad och bör bidra till en mer överskådlig bild av rådande policy. Om det utifrån befintlig dokumentstruktur är mer lämpligt att sätta en övergripande policy och låta de detaljerade beskrivningarna ligga i en separat instruktion kan även detta alternativ övervägas. • Vidare rekommenderar EY Telge AB att se över efterlevnaden av den befintliga processen gällande revidering av dokument för att säkerställa att de aktuella och relevanta. Rekommendationen grundar sig på att reviderat datum på insamlade rådande styrdokument varierar i stor grad. För att hänvisa till första punkten i denna sektion så skulle en enad sammanhållen policy underlätta revidering då ett samlat underlag skulle minimera risken att vissa riktlinjer inte revideras på regelbunden basis.

för IT- och informationssäkerhet.

EY har även fått ta del av tre ytterligare dokument som avser riktlinjer för IT-säkerhet kopplat till drift, förvaltning, användare och förebyggande av otillåten åtkomst till systemkomponenter. Ovan nämnda riktlinjer är utgivna av koncernen och reviderade av IT-chef Anders Rosberg 2017 med undantag för dokument "Riktlinje – Förebygg och förhindra otillåten åtkomst till systemkomponenter" som är reviderad av icke-namngiven stabschef 2013. Ovan nämnda riktlinjer ska enligt dokumenten gälla för alla koncernens verksamheter och bolag.

Telge Energi har under våren 2018 utformat två bolagsspecifika styrdokument varav ett omfattande dokument för övergripande riktlinjer för informationssäkerhet inom bolaget och det andra som beskriver styrande riktlinjer för bolagets IT-användare. Riktlinjerna tillämpas ännu inte fullt ut då de nyligen är framtagna. Liknande styrdokument finns inte framtagna för Södertälje Hamn som istället hänvisar till koncernens styrdokument. Bedömningen är att de riktlinjer som är framtagna av Telge Energi är mer omfattande och mer relevanta än de koncernövergripande riktlinjerna som Södertälje Hamn förhåller sig till.

Strategisk IT-ledning (STIL) är det huvudsakliga forumet för samordning och samverkan rörande IT inom Telge AB. Frågor rörande IT diskuteras i STIL där bolagen är representerade. Den strategiska IT-ledningen ska bl.a. diskutera frågor rörande IT- och informationssäkerhet samt risk.

3.2 Revisionsfråga 2: Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?

Observationer	Rekommendationer
Koncern-IT utför riskanalyser med avseende på IT-säkerhet i enlighet med Årskontrollplanen. Årskontrollplanen innefattar 32 kontroller som sker på hel- eller halvårsbasis. Kontrollerna omfattar de områden relaterat till IT-säkerhet som Koncern-IT ansvarar för, vilket innefattar nätverk (interna och externa), servrar, klienter operativsystem och Active Directory. I styrdokument "Rutin-Årskontrollplan IT-säkerhet" beskrivs syfte, ansvarig enhet, förberedelser, genomförande och uppföljning för varje enskild kontroll. Den version av Årskontrollplanen som EY har tagit del av är godkänd av IT-chef Anders Rosberg och senast reviderad 2017-12-14. Huvudansvarig för genomförande av kontroller är IT-säkerhetsansvarig Daniel Rytterlund. Loggar uppdateras efter genomförd kontroll i dokument "Logg – Årskontrollplan – IT-säkerhet Telge AB. EY har inte tagit del av loggdokumentet under granskningen gång. Enligt Årskontrollplanen sker en muntlig genomgång av kontrollresultaten för Koncern-ITs ledningsgrupp vid behov. Rapportering av de större kontrollpunkterna, t.ex. sårbarhetsskanning, rapporteras till Strategisk IT-ledning, övriga kontrollpunkter rapporteras kortfattat där fokus ligger på avvikelser. Kontroller som omfattar risker för intrång på preventiv nivå har av EY identifierats som kontroll 7 "Skanning av organisationens interna nätverk" samt kontroll 8 "Sårbarhetsskanning av externa nätverk". På detektiv nivå omfattas risker för intrång av kontroll 12, "Kontroll av skydd mot skadlig kod", samt kontroll 13, "Kontroll av otillbörlig programvara, logganalys". På proaktiv nivå är kontroll 15, "Kontroll konfiguration av server" under utveckling.	• Telge AB bör överväga att upprätta regelbundna avstämningar med berörda bolag oavsett resultat på kontrollutförande och inte enbart endast vid behov för att upprätthålla en god rapporteringsrutin. • Telge AB bör se över behovet att öka frekvensens av extern sårbarhetskanning till kvartalsvis då det är en rekommenderad frekvens för god praxis.

För detaljerad beskrivning av förberedelser, utförande och uppföljning av ovan nämnda kontroller se referensdokument "Rutin – Årskontrollplan IT-säkerhet".

Koncern-IT utvärderar årligen Årskontrollplanen med syfte att addera nya kontroller eller utveckla befintliga kontroller vid behov. EY har inte tagit del av den riskanalys eller omvärldsanalys som ligger till grund för utvärderingen av Årskontrollplanen.

Samtliga system (med två undantag) som används av Telge Energi och Södertälje Hamn är kopplade till servrar på nätverk som, enligt IT-chef och IT-förvaltningsansvarig, täcks av ovan nämnda kontroller i Årskontrollplanen. De två undantagen är Hogia Terminalsystem och Hogia Affärssystem som används av Södertälje Hamn med Hogia som leverantör. Södertälje Hamn utför inga egna risk- eller sårbarhetsanalyser av ovan nämnda system och begär heller inget liknande från Hogia. Södertälje Hamn är ytterst ansvariga för att utföra riskanalyser med avseende på informationssäkerhet men förlitar sig helt på Koncern-IT i egenskap av tjänsteleverantör gällande säkerhetsfrågor.

Den nyligen framtagna mallen för systemsäkerhetsanalys på Telge Energi omfattar informationssäkerhet med avseende på de system som bolaget använder. Mallen innefattar klassificering av information, hot- och riskanalys samt fastställande åtgärder. När granskningen ägde rum hade denna inte tagit i bruk, men ambitionen är att implementera den inom en snar framtid.

3.3 Revisionsfråga 3: Har bolagen ett ändamålsenligt skydd för sina databaser och system mot utomstående intressen eller utifrån kommande hot om skada?

Observationer	Rekommendationer
Koncern-IT har det övergripande ansvaret för alla databaser kopplade till de system som brukas av koncernens bolag, däribland Telge Energi och Södertälje Hamn. Koncern-IT hanterar skydd mot databaserna genom kontroll 8 "Sårbarhetsskanning av externa nätverk" samt kontroll 10 "Kontroll av höga behörigheter i SQL Server (server role: sysadmin, serveradmin, securityadmin, dbcreator, processadmin, setupadmin)" i Årskontrollplanen. Även om kontroll 10 främst avser behörighetsgranskning av höga behörigheter så anser EY att kontrollen mitigerar risken för att externt obehöriga innehar hög behörighet i databasmiljö vilket kan ha skadliga konsekvenser för bolagen. Både Telge Energi och Södertälje Hamn förlitar sig på Koncern-IT för säkerhetshantering och skydd vad gäller databas då det är en tjänst de köper av Koncern-IT. Telge AB köper in övervakningstjänster av Sentor. Sentor är leverantör för all monitorering sett hur ett säkerhetsperspektiv vilket omfattar bl.a. övervakning av applikationer, serverar och databas. Sentor bedriver 24/7 övervakning och hanterar eventuella incidenter i sitt egna incidenthanteringssystem. Återkoppling till Koncern-IT sker via mail till Service Desk eller incidentberedningen beroende på vilken tid på dygnet en incident rapporteras. Då Service Desk får information av Sentor om en eventuell incident så ska problemet hanteras via koncernens interna incidentprocess. Det finns i dagsläget ingen direkt automatisk koppling mellan Sentor och Koncern-ITs interna incidenthanteringssystem. För en mer detaljerad	• Telge AB bör se över möjligheten att stärka kommunikationen med Sentor vid incidenter för att minska risken att information om incidenter som fångas upp av Sentor inte delges Telge AB. En möjlighet är att införa automatiserad kommunikation mellan Sentors övervakningsaktiviteter och Telge ABs incidenthanteringsprocess för att ytterligare förbättra den interna kontrollmiljön avseende incidenter. • Södertälje Hamn bör överväga att begära relevanta tredjepartsrapporter från Hogia för att försäkra sig om att leverantör av terminalsystem och affärssystem uppfyller krav och god praxis i sina interna processer och kontroller.

beskrivning av Koncern-ITs interna incidenthanteringsprocess se avsnitt "3.4 Revisionsfråga 4: Finns tillräckliga riktlinjer för incidenthantering i samband med försök till, eller genomförda intrång?". Enligt IT-säkerhetsansvarig på Koncern-IT så omfattas samtliga system som används av de granskade bolagen av monitoreringsfunktionerna. Koncern-IT är ansvariga för uppsättning av en VPN-tunnel mellan Södertälje Hamn och Hogia för leverantöråtkomst i terminalsystemet och affärssystemet. Regelbundna möten sker månadsvis mellan Koncern-IT och Sentor, där en summering av månadens incidenter presenteras	

3.4 Revisionsfråga 4: Finns tillräckliga riktlinjer för incidenthantering i samband med försök till, eller genomförda intrång?

Observationer	Rekommendationer
Telge AB har dokumenterade rutiner för en koncernövergripande incidenthanteringsprocess vid namn Incident Management. En incident definieras som av kund (läs bolag) upplevd pågående störning i IT-infrastruktur. Incident Management har som ansvar att så snart som möjligt se till att upplevd störning upphör. Enligt processen har bolagen ansvar att själva rapportera incidenter vid upplevda störningar. Incidenthantering sker internt via Service Desk som agerar första instans för rapporterade incidenter. Service Desk ska enligt processbeskrivning identifiera inkommande incident, skapa ett ärende och kategorisera incidenten. Klassas incidenten som en "Stor incident" så ska incidenten eskaleras till medlem i Ledningsgruppen för IT som då blir incidentledare för rapporterad incident. Det finns en tydlig kriterielista över vilka händelser som klassas som en "Stor incident" där hot eller händelser av intrång och övriga säkerhetsrelaterade incidenter ingår. Eskalering ska enligt rutinen vara möjlig både under och utanför kontorstid. Vid eskalering utanför kontorstid ska medlem i Ledningsgruppen kontaktas enligt beredskapsschemat som finns styrdokumentet "Rutin – Incident (Stor Incident) Hantering". Styrdokumentet är reviderat senast 2013 och hänvisar till dokument "Beredskap 2015.docx" för information om vem i Ledningsgruppen som är utvald till att befinna sig i beredskap. Rutinen beskriver incidentledarens uppgifter och förväntad handlingsplan vid eskalerade stora incidenter. Som sista steg vid bekräftat hot uppmanas incidentledaren att utföra ett krislarm och hänvisas till riktlinjer som återfinns i dokument	• Telge AB bör överväga att samla samtliga styrdokument kopplat till rutiner för incidenthantering till ett enat dokument då det ökar förutsättningarna till en bättre efterlevnad och ger en mer överskådlig bild av rådande styrning. • Styrdokument "Rutin - Incident (Stor incident) Hantering" är enligt dokumentet senast reviderat 2013-06-27. Styrdokumentet hänvisar dock till beredskapslista vid namn "Beredskap 2015.docx" vilket ger anledning för läsaren att tro att styrdokumentet är uppdaterat senast 2015. Baserat på ovanstående iakttagelse bör Telge införa en rutin att revidera rådande styrdokument på årsbasis för att försäkra sig om att innehållet i rådande styrdokument är korrekt men även för att förebygga att omvärldsförändringar inte har gjort innefattande rutinbeskrivningar irrelevanta eller förlegade. Även om inga ändringar görs vid revideringstillfälle bör ändå revideringstillfället loggas med datum för att validera aktuell riktighet i reviderat styrdokument. • Styrdokument "Rutin – Incident (Stor Incident) Kommunikationsrutin" är enligt dokumentet senast reviderat 2013-11-01. Styrdokumentet hänvisar till "Krisplan 2013 Telge" vid bedömning av händelse som krislarm, vilket inte är i linje med vad som beskrivs i styrdokument "Rutin – Incident (Stor incident) Hantering", då det hänvisar till "Krisplan 2015 Telge". Det finns anledning att tro att dessa två dokument

"Krisplan 2015 Telge". Krisplanen revideras årligen.

Uppföljning av incidenter, både incidenter klassade som stor och vanliga, behandlas som protokollspunkt i så kallade servicemöten. Servicemöten sker med Telge Energi och Södertälje Hamn månadsvis.

inte skiljer sig nämnvärt mellan varandra, dock bör det enbart finnas en officiell uppdaterad krisplan att referera till.

3.5 Revisionsfråga 5: Har tester genomförts avseende intrång i systemen?

Observationer	Rekommendationer
Det genomförs inga tester med avseende på intrång i system eller servrar utöver de interna och externa sårbarhetsanalyser som återfinns i kontroll 7 och kontroll 8 samt införandet av skadlig kod på utvalda servrar som återfinns i kontroll 12 och kontroll 13 i Årskontrollplanen beskrivna i stycke 3.2 "Revisionsfråga 2: Görs riskanalyser avseende IT-säkerhet på ett strukturerat sätt och omfattar dessa risker för intrång?".	• Telge AB bör se över möjligheten att som komplement till den redan befintliga sårbarhetsskanningen införa regelbundna penetrationstester utförd av objektiv tredjepart på utvalda servrar och applikationer med syfte att identifiera sårbarheter och ingångar som inte nödvändigtvis redan är uppdagade genom tidigare skanning. Föreslagen frekvens på penetrationstest är på årsbasis men även i samband med implementation av nya applikationer/system eller servrar.

3.6 Revisionsfråga 6: Finns en ändamålsenlig organisation, ansvar och roller avseende IT-säkerhet i berörda bolag

Observationer	Rekommendationer
EY har vid granskning av gällande styrdokument och insamlat intervjuunderlag noterat viss otydlighet kring var ansvar ligger för IT-säkerhet kontra informationssäkerhet. Enligt koncernens riktlinje för "IT-säkerhet, användare" omfattas styrdokumentets regler av all informationshantering som sker med hjälp av koncernens IT-system samtidigt som dokumentet hävdar att alla användare av koncernens IT-system ska upprätthålla en god IT-säkerhet. Med "alla användare" tolkar EY det som att även alla anställda i koncernens olika bolag omfattas av rådande riktlinjer. Det råder därmed enligt EY otydlighet kring vad som i koncernens riktlinjer definieras som IT-säkerhet och vad som definieras som informationssäkerhet. Utöver detta så finns det vissa skillnader i Telge Energis egna utformade riktlinjer för användare jämfört med den som koncernen beskriver där den mest påtagliga skillnaden är att Telge Energis riktlinjer är mer omfattande och täcker ett större riskspektrum än vad koncernens nuvarande rådande riktlinjer för användare gör. Detta gap ger anledning till att tro att bolag inom koncernen som inte har utformat en egen bolagsspecifik riktlinje för användning av IT-system efterlever lägre krav på informationssäkerhet, vilket i sin tur kan öka risken till intrång i systemen.	• De styrande principer som avser IT- och informationssäkerhet som återfinns i IT-strategin saknar tydlighet gällande ansvarsfördelning. EY rekommenderar därför Telge AB att förtydliga ansvarsfördelningen och mer specifikt definiera skillnaden mellan IT-säkerhet och informationssäkerhet då det enligt intervjuer finns en enad bild över att koncernen har ansvar för att upprätthålla en god IT-säkerhet medan bolagen ansvarar för att hantera all verksamhetsinformation på ett säkert sätt. • EY rekommenderar Telge AB att se över möjligheten att utveckla sina rådande riktlinjer gällande användning av IT-system med avsikt att omfatta alla bolag. En alternativ rekommendation är att upprätta riktlinjer för användning av IT-systemen av samma omfattande natur som Telge Energis för samtliga koncernens bolag och därmed inte ha egna riktlinjer för detta som omfattar bolagen då det kan leda till risk för otydlighet kring vilka riktlinjer man som bolag ska följa.

4. Slutsatser

Nedan följer en sammanställning av de slutsatser som denna granskning har resulterat i.

Med hänvisning till insamlat material, intervjuer och uppföljningsfrågor med Koncern IT på Telge AB och representanter från de granskade bolagen så bedömer EY att koncernen operativt arbetar tillfredställande med att upprätthålla god intern kontroll för att förhindra och upptäcka intrång i databas, servrar och applikationer som driftas av koncernen och som används av Telge Energi och Södertälje Hamn.

EY bedömer att det finns relevanta forum för uppföljning och samspel mellan koncern och bolag. Bedömningen är dock att det finns ett behov av att göra regelbundna uppföljningar istället för vid behov.

EY bedömer koncernens rådande IT-policy och IT-säkerhetspolicy vara otillräckligt utformad för att följa god praxis. Koncernens riktlinjer för IT-säkerhet är inte samlade och senast reviderad version skiljer sig mellan respektive riktlinje. Koncernens riktlinjer för IT-säkerhet och incidenthantering innehåller vid tillfällen inkonsekvent hänvisning till andra dokument vilket ökar risken till svårighet av efterlevnad.

EY anser att Södertälje Hamn och Telge Energi har olika förutsättningar att via styrning upprätthålla samma nivå av informationssäkerhet då Telge Energi har bolagsspecifika riktlinjer som är på en mer omfattande nivå än de koncerngemensamma riktlinjer som Södertälje Hamn hänvisar till. Telge AB har enligt insamlat intervjumaterial ett begränsat samarbete med ägare Södertälje kommun.

Bilagor

Följande huvudområden har granskats och utvärderats:

- Policyer och styrdokument
- Kontroll och uppföljning av policyer och styrdokument
- Risker kopplade till intrång i system
- Ansvarsfördelning
- Intern kontroll
- Hot om risker för intrång i systemen

Granskade dokument

- Telgekoncernens strategi för användning av IT, (*2016*)
- Rutin – Årskontrollplan IT-säkerhet, (*2013, reviderad 2017*)
- Policy för IT, Telgekoncernen (*2013, reviderad 2016*)
- Policy för IT-säkerhet, Telgekoncernen (*2013, reviderad 2017*)
- Riktlinjer för IT-säkerhet, användare (*2016*)
- Riktlinjer för IT-säkerhet, drift och förvaltning (*2016)*
- Riktlinje – Förebygg och förhindra otillåten åtkomst till systemkomponenterna (*2013*)
- Riktlinjer informationssäkerhet Telge Energi (*2018*)
- Systemsäkerhetsanalys – Protokoll för krav och klassificering (*2018*)
- Rutin – Incident Management hantering (2017)
- Rutin – Incident (Stor Incident) Hantering (2013)
- Rutin – Incident (Stor Incident) Kommunikationsrutin (2013)
- Informationssäkerhetspolicy (2018)