Granskning av kontinuitetsplanering för it-säkerhetshändelser

Rapport

Borgholm Energi

KPMG AB

2024-10-30

Antal sidor 16

Borgholm Energi
Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

Innehållsförteckning

1 Sammanfattning

Granskningen syftar till att bedöma om styrelsen för Borgholm Energi har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att bolagsstyrelsen delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser.

Vår bedömning baseras på att vi i granskningen har tagit del av styrdokument och muntligt redovisade processer som beskriver hur arbetet med kontinuitetsplanering är tilltänkt att bedrivas. Vi kan se att arbetet delvis genomförs i linje med dessa, men kan också konstatera att efterlevnaden till de styrande dokumenten är bristfällig i väsentliga delar. Framför allt handlar det om att det saknas dokumenterade kontinuitetsplaner. Vi anser därtill att det saknas en övergripande styrning och kravställan av nivåer för kontinuitetsplaneringen. Vår bedömning är att denna i sitt grundutförande bör vara likvärdig i kommunkoncernen för att underlätta samordning och samverkan för samhällsviktig verksamhet. Bolagsstyrelsen bör därvid ta initiativ till dialog med ägaren om tydliga riktlinjer och kravnivå för kontinuitetsarbete som komplement till det arbete som genomförs utifrån föreskrifter och rekommendationer från tillsynsmyndigheter och branschorganisationer.

Vi bedömer att det finns behov av att tydliggöra ansvar för uppföljning av kontinuitetsplaneringen så att bolagsstyrelsen kan tillse en tillräcklig uppföljning och rapportering både för egen del, men även som del i rapportering till ägaren.

I tabellen redovisar vi vår bedömning per revisionsfråga och revisionsobjekt.

Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?	
Bolagsstyrelsen	Nej
Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?	
Bolagsstyrelsen	Ja

Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?	
Bolagsstyrelsen	Nej
Har åtgärder för att säkerställa kontinuiteten identifierats och vidtagits?	
Bolagsstyrelsen	Ja
Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?	
Bolagsstyrelsen	Nej
Finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar?	
Bolagsstyrelsen	Nej

2 Bakgrund

KPMG har av lekmannarevisorerna för Borgholm Energi fått i uppdrag att granska bolagets beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa. Uppdraget ingår i revisionsplanen för år 2024.

En god krisberedskap är en förutsättning för att kommunens verksamheter ska stå väl rustade inför olika former av samhällsstörningar och för att klara av att hantera olika former av krissituationer. Förmåga att hantera it-säkerhetshändelser baseras även på att det finns ett systematiskt informationssäkerhetsarbete där hot och risker analyserats för att säkerhetsåtgärder ska anpassas efter dessa och skydda kommunens information och verksamhet.

Ett flertal offentliga organisationer har under de senaste åren utsatts för cyberattacker med stora konsekvenser som följd. Exempelvis har skyddsvärd information förlorats eller röjts till obehöriga eller så har den bristande hanteringen lett till att organisationer drabbats av ekonomisk skada eller förtroendeskada. Inledningsvis 2024 utsattes en större leverantör av serverdrift och molntjänster för en ransomware-attack vilken fått en allvarlig påverkan på ett stort antal statliga myndigheters, kommuners och regioners tillgång till sina informationssystem.

Inom ramen för det kommunala åtagandet finns en rad samhällsviktiga funktioner, vilka om de inte fungerar kan leda till skada för såväl enskilda individer som samhället i stort. Dessa funktioner behöver fungera varje dag även om incidenter inträffar och det för verksamheten är ett så kallat onormalt läge. Det ökande beroendet till it- och informationssystem leder till att ett bortfall av dessa kritiska tillgångar får större konsekvenser än tidigare. I det arbetet krävs väl genomarbetade, förankrade och testade kontinuitetsplaner för att upprätthålla verksamheterna vid sådana händelser.

Revisorerna bedömer att de negativa konsekvenserna vid en extraordinär händelse eller annan kris som betydande om det inte finns ändamålsenlig kontinuitetsplanering. Revisorerna drar därför slutsatsen att både sannolikheten för, och konsekvenserna av kritiska it-säkerhetshändelser är icke-försumbar och att arbetet med kontinuitetsplanering och reservrutiner behöver granskas.

2.1 Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om bolagsstyrelsen har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Granskningen har besvarat följande revisionsfrågor:

- Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?
- Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?
- Har åtgärder för att säkerställa kontinuiteten identifierats och vidtagits?
- Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?
- Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?
- Finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar?

2.2 Avgränsning

Granskningen har inte tagit del av underlag eller information som är säkerhetsskyddsklassade.

Granskningen har avsett bolagets verksamhet inom energi samt och vatten och avlopp.

Stickprov av kontinuitetsplanering har avgränsats till att omfatta kritiska processer med stort beroende till informationssystem.

2.3 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen (2017:725)
- Aktiebolagslagen
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och beredskap.
- Myndigheten för samhällsskydd och beredskaps vägledning för Risk- och sårbarhetsanalyser, MSB245
- MSBFS 2015:5
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (där detta är tillämpbart)
- MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (där detta är tillämpbart)
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- Tillämpbara interna regelverk, policys och beslut

2.4 Metod

Granskningen har genomförts genom dokumentgranskning, intervjuer och stickprov.

Dokumentgranskning

Följande dokument har ingått i granskningen:

- Reglemente för styrelsen
- Ägardirektiv för Borgholm Energi
- Styrande dokument inom krisberedskap och informationssäkerhet
- Risk- och sårbarhetsanalys (informationsklass under säkerhetsskydd)
- Reservrutiner för berörda verksamheter

Intervjuer

Intervjuer har genomförts med:

- Ordförande för bolagsstyrelsen
- Vd
- Säkerhetssamordnare
- It-chef
- Verksamhetsansvarig VA-verksamhet
- Verksamhetsansvarig energi och elnät

Stickprov

Stickprov har gjorts av upprättade kontinuitetsplaner inom berörda revisionsobjekt och mot bakgrund av given avgränsning i de fall dylika underlag erhållits.

Samtliga intervjupersoner har getts möjlighet att faktakontrollera rapporten.

3 Inledning

Kommunens ansvar för krisberedskap och civilt försvar regleras i Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH) med tillhörande förordning och föreskrifter från Myndigheten för samhällsskydd och beredskap, MSB.

Kommunen har ansvar att upprätthålla samhällsviktig verksamhet och ha förmåga att hantera störningar och krishändelser inom dessa. Myndigheten för samhällsskydd och beredskap har definierat samhällsviktiga verksamheter som ”*Verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet*”.

Arbetet med krisberedskap och extraordinära händelser tar sin utgångspunkt i en övergripande Risk- och sårbarhetsanalys som kommuner och regioner enligt lagkrav ska genomföra vid varje ny mandatperiod. En del i RSA-processen är att identifiera vilka samhällsviktiga verksamheter som kommunen bedriver samt att kontinuitetsplanera för dessa.

MSB har även gett ut råd för att säkra tillgången till organisationens information. I den framgår att kontinuitetshantering handlar om att planera för att verksamheten ska kunna bedrivas på en acceptabel nivå oavsett vilken störning den utsätts för.

Ofta är organisationens information nödvändig för att verksamheten ska kunna fungera. Information hanteras idag till stor del digitalt. Kontinuitetshanteringen behöver därför säkerställa tillgång till information och därmed it-resurser. Det kan exempelvis handla om verksamhetsspecifika och administrativa system, e-post, filer, molntjänster och hårdvara som PC, servrar, telefoner och nätverk.

Exempel på arbetssätt som kan behöva planeras är chatt- och videoverktyg för möten, e-post för kommunikation och för att förmedla information samt interna nätverk för att spara eller sprida information. Därtill kan det behövas alternativa arbetssätt i form av utskrivna kontaktlistor, lokala kopior av nödvändig information samt beskrivna rutiner för att övergå till alternativa sätt att bedriva den dagliga verksamheten om tillgång till it saknas.

Mot bakgrund av den ökande hotbilden för cyberattacker med risk att informationssystem och it-miljön inte är tillgänglig för de samhällsviktiga verksamheterna avgränsas denna granskning till kontinuitetsplanering och reservrutiner vid it-bortfall.

3.1.1 Kontinuitet vid incidenter

Krav utifrån revisionskriterier

Av föreskrift (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster framgår att en leverantör ska ha interna regler och arbetssätt för att minska effekten av en incidents negativa inverkan på den samhällsviktiga tjänsten.

4 Resultat av granskningen

4.1 Riskbedömning och planering för it-avbrott

Kommunfullmäktige har antagit Föreskrifter för Borgholms kommuns arbete med krisberedskap och höjd beredskap[1] som reglerar och kravställer hantering av samhällsstörningar. Dokumentet gäller hela kommunkoncernen och stipulerar att kommunen ska ha en organisation som möjliggör samhällsviktig verksamhet att kunna bedrivas under minst en veckas tid vid samhällsstörning. Vidare anges att kommunen under varje mandatperiod ska genomföra en risk- och sårbarhetsanalys samt ta fram en utbildnings- och övningsplan som ska syfta till att kunna upprätthålla kommunens ledningsförmåga vid samhällsstörningar. Vi har i granskningen tagit del av kommunens Risk- och sårbarhetsanalys 2023[2] (version där sekretessbelagda delar maskats). Dokumentet pekar ut långvarigt IT-avbrott som en typhändelse med risk för allvarliga konsekvenser, där vård och omsorg och teknisk service nämns som kritiskt utsatta. Enligt RSA-dokumentet är krisplaner och kontinuitetshantering av vikt för dessa verksamheter, vilket konstaterats till följd av ett tidigare långvarigt elbortfall.

Inom kommunen finns också informationssäkerhetspolicy[3] och Informationssäkerhetsinstruktioner förvaltning[4] som omfattar bolaget. Dokumenten reglerar kontinuitetsplanering för enskilda it-system. Härigenom finns styrande dokument som kravställer kontinuitetsplanering ur såväl ett krisberedskapsperspektiv som utifrån informationssäkerhetsarbete.

Ur ett kommungemensamt perspektiv samordnas arbetet med kontinuitetsplanering via ett nätverk med funktioner från socialförvaltningen, utbildningsförvaltningen, tekniska avdelningen, Borgholm Energi samt kommundirektör. Grupperingen leds av säkerhetssamordnare och beskrivs ha satts samman delvis i syfte att kunna hantera gemensamma beroenden verksamheter emellan. Muntligen anges att arbetet i första hand kopplar till verksamhetsrisker och planering som krävs för att kunna upprätthålla verksamhet i ett läge med höjd beredskap och krigsberedskap. Kontinuitetsplanering ska vara en del av beredskapsplaneringen, enligt intervjuade.

Intervjuade företrädare för Borgholm Energi beskriver att bolaget främst bedriver sin kontinuitetsplanering genom eget bolagsinternt arbete och inte med grund i det gemensamma nätverket. I kommande avsnitt beskrivs bolagets arbete med beredskapsplanering.

4.1.1 Kontinuitetsplaner och kritiska beroenden till informationssystem

I RSA 2023 beskrivs processen för RSA-arbetet översiktligt. Här framgår att förvaltningarna och bolagen följt upp tidigare RSA från 2019 och åtgärdat brister samt genomfört verksamhetsbaserade risk- och sårbarhetsanalyser. Närmare konkretiseras inte former för det faktiska arbetet.

[1] Beslutad 2023-12-11
[2] Kommunfullmäktige 2023-09-18
[3] 2019-01-02
[4] 2018-12-28

Utöver kommunkoncernens styrande dokument finns ytterligare regulatoriska föreskrifter som berör bolagets verksamheter. Energimyndighetens föreskrifter[5] (STEMFS 2021:3) stipulerar att utförare av samhällsviktig verksamhet inom energisektorn ska identifiera vilka informationssystem som är kritiska för att den samhällsviktiga verksamheten ska kunna upprätthållas. För leverantörer inom leverans och distribution inom dricksvatten anger Livsmedelsverkets föreskrifter[6] (LIVSFS 2022:2) att grundläggande säkerhetsåtgärder måste vidtas för att hantera risker som avser kritiska informationssystem.

Som vi belyste i föregående rapportavsnitt genomförs bolagets kontinuitetsplanering med fokus på beredskapsarbete. De intervjuade menar att det arbete som görs inom ramen för RSA-arbetet är på en mer bolagsövergripande nivå medan den verksamhetsbaserade kontinuitetsplaneringen ingår i de beredskapsplaner som upprättas per verksamhetsområde. Beredskapsplanerna förklaras ha en högre detaljeringsgrad och utgå från exempelvis lagkrav och föreskrifter som gäller för det specifika verksamhetsområdet, vilket också påverkar hur planerna dokumenteras. Gällande just risken för it-bortfall anges att scenariot är snarlikt oavsett verksamhetsområde varför grunden i planeringen är gemensam för hela bolaget.

I granskningen har ingått att göra stickprov av underlag för kontinuitetsplanering för att kontrollera om kritiska beroenden till informationssystem har ingått i analys och planering. Vi har efterfrågat att ta del av dokumenterat underlag för kontinuitetsplanering, vilket avslagits av bolaget med hänvisning till att befintliga underlag dels innehåller känslig information, dels är under framtagande varför kompletta kontinuitetsplaner ännu inte är färdigställda.

För VA-verksamheten ingår kontinuitetsplaneringen i nödvattenplanen. Muntligen uppges att it-avbrott är ett av två scenarier som planeringen utgår från.

För energi- och elnätsverksamheten tillämpas elberedskapsmyndigheten Svenska Kraftnäts struktur för beredskapsplanering, vilken framgår av ett beslut[7] från Svenska Kraftnät som tillhandahålls av bolaget. Här kravställs att planeringen ska utgå från bland annat följande aspekter:

- Interna och externa samband
- Bortfall av it-system
- Upprätthållande av verksamhetens funktion

För samtliga verksamhetsområden uppges kritiska it-system ha identifierats. Exempel på sådana beskrivs också i samband med intervju.

[5] Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn
[6] Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten
[7] Daterat 2023-09-05

4.1.2 Övning

Intervjuade bolagsrepresentanter likställer en skarp situation som inträffade 2022 vid en övning. Utöver den har det inte skett någon planerad övning med specifikt fokus på it-avbrott i bolaget.

4.1.3 Bedömning

Vår bedömning är att det saknas dokumenterade kontinuitetsplaner eller motsvarande underlag inom Borgholm Energi.

Vi kan konstatera att arbete med kontinuitetsplanering pågår inom bolaget, men att det vid tid för granskningen saknas fullständiga kontinuitetsplaner. Arbetet bedrivs enligt verksamhetsanpassad systematik och utgår från specifika krav som bolagets verksamheter står under i förhållande till tillsynsmyndigheter och branschorganisationer. Vi ser det som positivt då det främjar att planeringen inkluderar viktiga aspekter som kan saknas i den kommungemensamma styrningen. Samtidigt har bolaget krav på att efterleva de av ägaren beslutade styrdokumenten och följa de processer för riskhantering och kontinuitetsarbete som beslutats. Detta är särskilt viktigt för en fungerande intern samverkan inom koncernen, exempelvis avseende kritiska beroenden med påverkan inom hela kommunkoncernen.

Bolagsstyrelsen bör tydliggöra kravställning och genomförande av kontinuitetsplanering för de samhällsviktiga verksamheterna och tillse att uppföljningsrutiner etableras för att kontrollera att planeringen är tillräcklig.

Vår bedömning är att kritiska beroenden till informationssystem beaktats i kontinuitetsplanering för Borgholm Energi.

Vi vill poängtera att bedömningen baseras på muntliga uppgifter då vi inte tagit del av dokumenterade underlag. Bolaget har emellertid pekat ut vissa specifika system varför vi anser oss kunna bedöma att sådan analys genomförts.

Vår bedömning är att övningar inte har genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

Övning är viktigt i syfte att säkerställa en tillräcklig kontinuitetsplanering för it-avbrott. Därvid anser vi att bolagsstyrelsen behöver tillse att sådan genomförs med avseende på samtliga verksamheter.

4.2 Tillgänglighet till informationssystem och redundans

4.2.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet

Kommunens informationssäkerhetspolicy definierar informationssäkerhetsarbetet på övergripande nivå. Ur ett systemperspektiv konkretiseras detta i Instruktion för förvaltning där krav på informationsklassning, riskanalys och kontinuitetsplanering pekas ut som delar i kommunens systematiska informationssäkerhetsarbete.

Även Svenska Kraftnäts beslut om beredskapsplanering (se rapportavsnitt 4.1.1) förtydligar att informationsklassning ska genomföras löpande.

De intervjuade framför att informationsklassning ska genomföras i samband med upphandling av it-system, vilket senast skedde för ett antal år sedan. Däremot genomlyste bolaget hela verksamheten i förhållande till NIS-direktivet under 2020. Del i arbetet omfattade informationsklassningar, för vilket vi också delges dokumenterade underlag. Konklusioner från genomlysningen uppges ha legat till grund för en kravspecifikation avseende it-säkerhetsåtgärder som ska användas som underlag vid upphandlingar.

I granskningen har ingått att analysera huruvida underlag för kontinuitetsplanering innefattar bedömningar över kritiska verksamhetssystem och informationstillgångar samt redundans. Avseende reservrutiner finns det rutiner som är kopplade till den kravställan som verksamheten ställer mot leverantör eller interna it-avdelningen på exempelvis underhåll, beredskap och svarstid på incidenter. Med extern leverantör är detta ett formellt avtal, kallat SLA (service level agreement). Den överenskommelse som finns enligt SLA eller motsvarande interna it-drift är en del av att säkerställa kontinuiteten. Krav på att sådan ska upprättas ställs i Instruktion för förvaltning.

Bolaget ingår i kommunens gemensamma it-miljö och har således system som både driftas av kommunens interna it-avdelning samt andra som ligger på extern drift. Samtliga system uppges ha prioriterats enligt tre kategorier: ”prioriterade”, ”vanliga” samt ”icke-prioriterade”. System som identifierats som kritiska finns både internt och externt via leverantör. För system som driftas internt uppges kravställning avseende it-drift finnas, men inte inkludera SLA. För kritiska system som driftas internt har bolaget identifierat behov av it-beredskap men detta uppges saknas i nuläget då kommunen inte har it-beredskap på jourtid.

För externt driftade system har accepterad återställelsetid fastställts, dock saknas SLA.

4.2.2 Reservrutiner

En del i att säkerställa verksamhetens kontinuitet är en planering för att upprätthålla sin verksamhet vid ett it-avbrott. Detta kan ske exempelvis genom manuella instruktioner eller rutiner som medarbetare kan utgå från vid bortfall av kritiska system eller funktioner i system eller genom olika sätt tekniska reservåtgärder i verksamheten.

Vi har inte tagit del av några dokumenterade reservrutiner, detta då dessa ingår i det underlag som bolaget bedömer som känsligt. Muntligen anges att det finns reservrutiner för både elnätsverksamheten och VA-verksamheten.

4.2.3 Bedömning

Vår bedömning är att åtgärder har identifierats för att säkerställa kontinuiteten inom Borgholm Energi.

Aktuella informationsklassningar och riskanalyser utgör grund för att bedöma risker, konsekvenser och skyddsnivåer för bland annat aspekten tillgänglighet. Genomförda klassningar ger underlag för att påbörja åtgärder och planering.

Vår bedömning är att det inte finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem.

Vi konstaterar att åtgärder har vidtagits med kravställning i förhållande till externa leverantörer, men att det internt i nuläget inte finns förutsättningar för högre beredskap eller jour internt inom kommunen. Vår bedömning är att bolagsstyrelsen bör ta initiativ till dialog med ägaren avseende behovet av it-jour, vilken har en betydande funktion i syfte att kunna upprätthålla samhällsviktig verksamhet om kritiska it-säkerhetshändelser sker.

Då aktuell informationsklassning inte genomförts bedömer vi även att det saknas sakligt underlag för upprättade SLA.

4.3 Intern kontroll

4.3.1 Bolagsstyrelsens kontroll avseende kontinuitetsplaneringen

Enligt de intervjuade återrapporteras arbetet med beredskapsplanering löpande till bolagsstyrelsen, då som del i vd-information. Av de fyra protokoll som vi i granskningen fått del av gällande sammanträden 2024 finns ingen notering om att information från vd inkluderat beredskaps- eller kontinuitetsplanering.

Bolagets internkontrollplan innehåller tre kontrollmoment som de intervjuade anser tangerar kontinuitetsplanering och informationssäkerhet, och därmed genererar uppföljning till styrelsen. Det avser ”risk att brister i uppfyllnad av lagar och myndighetskrav finns”, ”risk att distribution av beslut uteblir eller hamnar fel” samt ”risk att det finns fel i kundbasen så att till exempel upplägg av kunder missas eller att kunder feldebiteras”. Vi har tagit del av uppföljning av internkontrollen[8], vilken inte ger uppfattning av att kontrollmomenten har direkt bäring på området.

4.3.2 Bedömning

Vår bedömning är att det inte finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

Vi konstaterar att det finns krav i styrande dokument avseende bolagets kontinuitetsplanering, till exempel kopplat till strukturen för informationssäkerhetsklassning samt externa regulatoriska krav. Vi kan samtidigt konstatera att arbetet på flera håll inte har genomförts i tillräcklig utsträckning vilket bolagsstyrelsen inte har uppmärksammat genom intern kontroll eller annan uppföljning. Angivna kontrollmoment i internkontrollplanen visar att bolaget uppmärksammat risker med bäring på kontinuitetsplanering, men vi anser inte att detta är tillräckligt för att bolagsstyrelsen ska ha kontroll i frågan. Vi ser inte heller att det finns någon annan strukturerad eller dokumenterad uppföljning av området.

Därmed anser vi att uppföljningen är i behov av att stärkas avseende efterlevnad av styrande dokument samt för att säkerställa att kontinuitet i samhällsviktiga verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser.

[8] Delårsbokslut augusti 2024 Borgholm Energi

5 Samlad bedömning och rekommendationer

Granskningen syftar till att bedöma om styrelsen för Borgholm Energi säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att bolagsstyrelsen delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser.

Vår bedömning baseras på att vi i granskningen har tagit del av styrdokument och muntligt redovisade processer som beskriver hur arbetet med kontinuitetsplanering är tilltänkt att bedrivas. Vi kan se att arbetet delvis genomförs i linje med dessa, men kan också konstatera att efterlevnaden till de styrande dokumenten är bristfällig i väsentliga delar. Framför allt handlar det om att det saknas dokumenterade kontinuitetsplaner. Vi anser därtill att det saknas en övergripande styrning och kravställan av nivåer för kontinuitetsplaneringen. Vår bedömning är att denna i sitt grundutförande bör vara likvärdig i kommunkoncernen för att underlätta samordning och samverkan för samhällsviktig verksamhet. Bolagsstyrelsen bör därvid ta initiativ till dialog med ägaren om tydliga riktlinjer och kravnivå för kontinuitetsarbete som komplement till det arbete som genomförs utifrån föreskrifter och rekommendationer från tillsynsmyndigheter och branschorganisationer.

Vi bedömer att det finns behov av att tydliggöra ansvar för uppföljning av kontinuitetsplaneringen så att bolagsstyrelsen kan tillse en tillräcklig uppföljning och rapportering både för egen del, men även som del i rapportering till ägaren.

I det följande redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Utifrån resultatet av vår granskning rekommenderar vi **bolagsstyrelsen** att:

- Fastställa och besluta om kontinuitetsplaner för samhällsviktig verksamhet
- Ta initiativ till dialog med ägaren om tydliga riktlinjer och kravnivå för kontinuitetsarbetet så att de interna styrdokumenten efterlevs
- Säkerställa att kontinuitetsplanering genomförs i enlighet med interna och externa krav på samhällsviktig verksamhet
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Överväga att etablera servicenivåöverenskommelser för samhällsviktig verksamhets informationssystem när detta är tillämpligt, detta i syfte att höja beredskapen
- Initiera dialog med ägaren om behovet av intern jourverksamhet för it-verksamheten
- Fastställa former för hur kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Sofie Ernerudh
Verksamhetsrevisor

Fredrik Ottosson
Kundansvarig och certifierad kommunal revisor