Granskning av kontinuitetshantering it-säkerhetshändelse

Rapport

Svedala kommun, Bostads AB Svedalahem och Svedala Exploaterings AB

2025-09-01

Antal sidor 18

INNEHÅLLSFÖRTECKNING

1 **1**

2 Sammanfattning **3**

3 Bakgrund **8**

4 Syfte och revisionsfrågor **8**

5 Avgränsning **9**

6 Revisionskriterier **9**

7 Metod **9**

8 Resultat av granskningen **11**

8.1 Process för riskbedömning och kontinuitetshantering *11*
8.1.1 Kontinuitetsplaner och kritiska beroende till informationssystem 12
8.1.2 Övning 12
8.1.3 Bedömning 12

8.2 Redundans och reservrutiner *13*
8.2.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet för verksamhetskritiska informationssystem 13
8.2.2 Reservrutiner 14
8.2.3 Bedömning 14

8.3 Uppföljning *15*
8.3.1 Bedömning 15

9 Samlad bedömning och rekommendationer **17**

2 SAMMANFATTNING

Azets har av Svedala kommuns förtroendevalda revisorer och lekmannarevisorer fått i uppdrag att granska kommunens och bolagens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa.

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

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen, nämnderna och bolagsstyrelserna inte har säkerställt en tillräcklig planering och samordning för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Bedömningen grundas i att det saknas etablerade metoder och arbetssätt för hur arbetet med kontinuitetsplaner ska genomföras. Inom vissa verksamhetsområden pågår ett aktivt arbete med kontinuitetsplanering, men det görs med variation som kan bero på att det saknas ett enhetligt arbetssätt. Vår bedömning är att kommunstyrelsen utifrån sitt övergripande ansvar för interna säkerhetsfrågor behöver kravställa nivåer och genomförande av kontinuitetsplanering på ett tydligare sätt.

Vidare gör vi bedömningen att det saknas en tillräcklig analys och bedömning av prioriterade systems eventuella behov om åtgärder för att säkerställa redundans i det fall digitala informationssystem och nätverk inte är tillgängliga. Vi har identifierat att arbetet med manuella rutiner kan stärkas, där det inom vissa verksamheter saknas dokumenterade rutiner för att bibehålla verksamhet vid ett eventuellt it-avbrott.

Då bolagen saknar krav på kontinuitetshantering mot bakgrund av att de inte bedriver samhällsviktig verksamhet, är vår bedömning att bolaget bör göra en riskbedömning och analys avseende vilket behov av kontinuitetsplanering som bolagen är i behov av. Detta för att kunna säkerställa att bolagets verksamhet kan fortgå vid ett eventuellt avbrott.

I kommunens informationssäkerhetspolicy finns krav på samtliga verksamheters kontinuitetsplanering, där arbetet inte har genomförts i tillräcklig utsträckning vilket vare sig nämnd eller styrelser har uppmärksammat genom uppföljning. Vi konstaterar även att det finns behov av att tydliggöra i vilken form det är lämpligt att de förtroendevalda är involverade i uppföljning och rapportering av kontinuitetsplaneringen.

I det följande redovisas samlad bedömning av revisionsfråga per revisionsobjekt.

Finns tydliggjorda krav eller förväntningar avseende kontinuitetshantering och hur denna ska genomföras?	
Kommunstyrelsen	Endast delvis
Tekniska nämnden	Endast delvis
Socialnämnden	Endast delvis
Utbildningsnämnden	Endast delvis
Bostads AB Svedalahem	Endast delvis
Svedala Exploaterings AB	Endast delvis
Finns dokumenterade kontinuitetsplaner eller motsvarande underlag och inkluderar dessa planering utifrån risk för it-säkerhetshändelse?	
Kommunstyrelsen	Nej
Tekniska nämnden	Nej
Socialnämnden	Nej
Utbildningsnämnden	Nej
Bostads AB Svedalahem	Nej
Svedala Exploaterings AB	Nej
Har åtgärder vidtagits för att ha redundans om digitala informationssystem och nätverk inte är tillgängliga?	
Kommunstyrelsen	Endast delvis
Tekniska nämnden	Nej
Socialnämnden	Nej
Utbildningsnämnden	Nej
Bostads AB Svedalahem	Nej
Svedala Exploaterings AB	Nej

Finns dokumenterade och etablerade reservrutiner (ex. manuella arbetssätt) för hur verksamheten ska fortgå utan tillgång till digitala informationssystem och nätverk?	
Kommunstyrelsen	Nej
Tekniska nämnden	Endast delvis
Socialnämnden	Endast delvis
Utbildningsnämnden	Nej
Bostads AB Svedalahem	Nej
Svedala Exploaterings AB	Nej
Har övningar genomförts för att utvärdera kontinuitetsplaner och tillhörande rutiner?	
Kommunstyrelsen	Nej
Tekniska nämnden	Nej
Socialnämnden	Nej
Utbildningsnämnden	Nej
Bostads AB Svedalahem	Nej
Svedala Exploaterings AB	Nej
Har nuvarande kontinuitetshantering och planer följts upp av styrelsen/nämnden för att säkerställa att det finns en ändamålsenlig planering?	
Kommunstyrelsen	Nej
Tekniska nämnden	Nej
Socialnämnden	Nej
Utbildningsnämnden	Nej
Bostads AB Svedalahem	Nej
Svedala Exploaterings AB	Nej

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Säkerställa tydliga riktlinjer och kravnivåer för kontinuitetsarbete inom kommunkoncernen.
- Upprätta och besluta om verksamhetsövergripande kontinuitetsplan eller på nivå för verksamhet som bedöms lämplig.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Tillse att åtgärdsplanering genomförs och baseras på aktuell informationsklassning och riskbedömning för informationstillgångar som styrelsen ansvarar för.
- Utvärdera behov av intern jourverksamhet för it-verksamheten i förhållande till de samhällsviktiga verksamheternas behov.
- Fastställa former för hur kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.
- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad kommunövergripande systematik.
- Säkerställa att bolagen inkluderas i det koncernövergripande arbetet utifrån behov.

Utifrån resultatet av vår granskning rekommenderar vi socialnämnden, tekniska nämnden samt utbildningsnämnden att:

- Upprätta och besluta om verksamhetsövergripande kontinuitetsplan eller på nivå för verksamhet som bedöms lämplig.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som nämnden ansvarar för.
- Säkerställa att SLA etableras med grund i aktuella analyser och riskbedömningar över tillgänglighetsbehov.
- Säkerställa att reservrutiner i form av manuella arbetssätt upprättas och testas så att de fungerar i enlighet med förväntan.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Fastställa former för hur kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar
- Etablera en dialog med övriga verksamhetsområden och bolag så att kritiska beroenden mellan verksamheter kan omhändertas på ett samordnat och effektivt sätt.

Utifrån resultatet av vår granskning rekommenderar vi Bostads AB Svedalahem och Svedala Exploaterings AB att:

- Utifrån riskbedömning och analys göra en bedömning över behovet av kontinuitetsplaner.
- Säkerställa att reservrutiner i form av manuella arbetssätt upprättas och testas så att de fungerar i enlighet med förväntan.

- Säkerställa att bolagen inkluderas i det koncernövergripande arbetet utifrån behov.

3 BAKGRUND

Azets har av Svedala kommuns förtroendevalda revisorer och lekmannarevisorer fått i uppdrag att granska kommunens och bolagens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa. Uppdraget ingår i revisionsplanen för år 2025.

Inom ramen för det kommunala åtagandet finns en rad samhällsviktiga funktioner knutna till it- och informationssystem. Dessa funktioner behöver fungera varje dag även om incidenter inträffar och det för verksamheten är ett så kallat onormalt läge. Om de inte fungerar kan det leda till skada för såväl enskilda individer som samhället i stort.

Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Ett flertal av dessa återfinns i kommunal sektor; dricksvatten, el, fjärrvärme, energi, avfall samt kommunal hälso- och sjukvård.

Den 1 augusti 2025[1] förväntas två nya lagar träda i kraft i Sverige:

- **Lag om motståndskraft hos kritiska verksamhetsutövare**
  Med utgångspunkt från CER[2]-direktivet beslutat av EU. Direktivet ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet.
- **Cybersäkerhetslagen**
  Med utgångspunkt från NIS[3]2-direktivet beslutat av EU. Direktivet syftar till att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen. Jämfört med nuvarande NIS-reglering kommer tydligare krav ställas på bland annat riskanalyser och olika säkerhetsåtgärder.

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 bristande hantering lett till att organisationer drabbats av ekonomisk skada eller förtroendeskada. 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 och lekmannarevisorerna ser risk att de negativa konsekvenserna vid en extraordinär händelse eller annan kris kan bli betydande om det inte finns ändamålsenlig kontinuitetsplanering. Revisorerna drar därför slutsatsen att arbetet med kontinuitetshantering och rutiner behöver granskas.

4 SYFTE OCH REVISIONSFRÅGOR

Granskningen har syftat till att bedöma om kommunstyrelsen, socialnämnden, tekniska nämnden, utbildningsnämnden samt Bostads AB Svedalahem och Svedala Exploaterings AB har säkerställt en tillräcklig planering och samordning för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

[1] Enligt regeringens tidsplan vid tid för projektplanens upprättande.
[2] Directive on the resilience of critical entities
[3] The Directive on Security of Network and Information Systems

Granskningen har besvarat följande revisionsfrågor:

- Finns tydliggjorda krav eller förväntningar avseende kontinuitetshantering och hur denna ska genomföras?
- Finns dokumenterade kontinuitetsplaner eller motsvarande underlag och inkluderar dessa planering utifrån risk för it-säkerhetshändelse?
- Har åtgärder vidtagits för att ha redundans om digitala informationssystem och nätverk inte är tillgängliga?
- Finns dokumenterade och etablerade reservrutiner (ex. manuella arbetssätt) för hur verksamheten ska fortgå utan tillgång till digitala informationssystem och nätverk?
- Har övningar genomförts för att utvärdera kontinuitetsplaner och tillhörande rutiner?
- Har nuvarande kontinuitetshantering och planer följts upp av styrelsen/nämnden för att säkerställa att det finns en ändamålsenlig planering?

5 AVGRÄNSNING

Granskningen har avsett kontinuitetsplanering och beredskap ur perspektivet it-, informations- och cybersäkerhet.

Granskningen har avsett kommunstyrelsen, socialnämnden, tekniska nämnden, utbildningsnämnden samt bolagsstyrelserna för de kommunala bolagen Bostads AB Svedalahem och Svedala Exploaterings AB.

6 REVISIONSKRITERIER

Granskningen har utgått från nedanstående revisionskriterier:

- 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 föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser
- Tillämpbara interna regelverk, policys och beslut

7 METOD

Granskningen har genomförts genom:

Dokumentgranskning, där bland annat följande dokument har granskats:

- Reglementen/ägardirektiv
- Styrande dokument inom krisberedskap
- Risk- och sårbarhetsanalys (informationsklass under säkerhetsskydd)
- Reservrutiner

Intervjuer har genomförts med:

- tjänstepersoner ansvariga för kommunens/bolagens övergripande arbete med krisberedskap, kontinuitetsplanering och informations- och it-säkerhet.
- ledande tjänstepersoner och förtroendevalda inom berörda nämnder/styrelser och förvaltningar/bolag.

Granskningen omfattade även att granska dokumenterade kontinuitetsplaner och hur kritiska beroenden till informationssystem bedömts.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.

Rapporten samtliga medverkande har delgetts möjlighet att faktakontrollera rapporten.

8 RESULTAT AV GRANSKNINGEN

8.1 PROCESS FÖR RISKBEDÖMNING OCH KONTINUITETSHANTERING

Av reglemente[4] framgår att kommunstyrelsen har ett övergripande ansvar för interna säkerhetsfrågor i kommunen och ska för varje mandatperiod ta fram förslag på plan för hur kommunen ska hantera extraordinära händelser. I nämndernas reglemente[5] finns reglering om att de ska följa det som fullmäktige beslutat, i övrigt så saknas uppgift om ansvar i krisberedskapsarbetet i reglementena.

Kommunfullmäktige har beslutat om Program för krisberedskap[6]. Enligt programmet har säkerhets- och beredskapsenheten sedan 2022 ansvar för krisberedskapsarbetet. Säkerhets- och beredskapschefen leder arbetet och har en samordnande roll inom området. Till stöd finns även en beredskapshandläggare.

I programmet beskrivs övergripande styrning av krisberedskap under programperioden. Det framgår att ansvaret vid en oönskad händelse eller hot om oönskad händelse i första hand ligger hos den organisation som drabbats eller de verksamheter som är inblandade. Ansvaret innebär såväl förebyggande arbete för behandling av risk eller sårbarhet som hantering av en inträffad oönskad händelse. Programmet avser kommunens verksamhet, bolag och kommunalförbund.

Kommunen har enligt intervjuade identifierat behov av en tydligare krisledningsorganisation. Det har därför genomförts ett arbete som avser upprättande av en krisorganisation för styrning och ledning i händelse av en kris. Intervjuade informerar om att det har skett organisationsförändringar[7] internt inom kommunen vilket föranlett ett omtag med krisorganisationen. Den nya krisorganisationen väntas bli antagen av ledningsgruppen under maj 2025.

Vi har inom ramen för granskningen tagit del av kommunens risk-och sårbarhetsanalys 2023–2026[8] (en öppen version som inte innehåller sekretessbelagda delar). I dokumentet anges vilka samhällsviktiga åtaganden som finns inom olika verksamhetsområden inom kommunen. Listan är inte fullständig utan avser mest tidskritiska åtaganden. Fullständig tabell går att finna i RSA-rapport från 2019–2022[9]. Av sammanställningen noterar vi att granskade verksamhetsområden inom kommunen finns med på listan. Dock inte de bolag som ingår i den här granskningen, detta mot bakgrund av att de inte har bedömts bedriva samhällsviktig verksamhet.

I Svedala kommuns informationssäkerhetspolicy[10] finns anvisningar för kontinuitets- och avbrottsplanering. Det framgår att det är verksamhetsansvarig chef som ansvarar för att de finns en dokumenterad kontinuitetsplan för kritiska och/eller samhällsviktiga verksamheter (*åtagande*) samt verksamheter vars stödjande system/e-tjänsters krav på tillgänglighet klassificerats som *Mycket viktig* eller *Kritisk*. Därutöver framgår vad kontinuitetsplanerna ska innehålla. Vi informeras om att en ny policy ska antas av fullmäktige i maj 2025.

Den bild som ges är att de övergripande ramarna för kontinuitetsarbetet inte är etablerat. Intervjuade anger att det finns en viss otydlighet av vad som förväntas av dem utifrån den nya RSA

[4] Reglemente för kommunstyrelsen i Svedala kommun, senast revidera av fullmäktige 2023-10-25
[5] Reglemente för tekniska nämnden, senast reviderat av fullmäktige 2024-10-23. Reglemente för socialnämnden, senast reviderad av fullmäktige 2023-11-23. Reglemente för utbildningsnämnden, antagen 2022-12-07.
[6] Upprättad av säkerhets- och beredskapschef, 2022-11-08.
[7] Tidigare var det chef för räddningstjänsten som innehade funktionen säkerhetssamordnare. Numer finns denna funktion i kommunens organisation inom kommunledningskontoret.
[8] Risk- och sårbarhetsanalys för Svedala kommun, 2023–2026. Genomfördes av en extern leverantör och färdigställdes 17 juni 2023.
[9] Risk- och sårbarhetsanalys för Svedala kommun, 2019-2022. Antagen av kommunstyrelsen 2019-12-16.
[10] Antagen av kommunstyrelsen 2016-05-23 och gäller från 2016-06-01. Vi har i granskningen tagit del av en ny version av informationssäkerhetspolicy som avses antas av fullmäktige i maj 2025.

samt program för krisberedskap. Uppfattningen är att det saknas ett koncerngemensamt arbetssätt och processer för arbetet med kontinuitetsplaner och reservrutiner. Flera anger att de önskar ett närmare stöd och vägledning från centrala funktioner så att krav och mål kan uppnås.

8.1.1 Kontinuitetsplaner och kritiska beroende till informationssystem

I RSA 2023 beskrivs att krisberedskapen behöver stärkas inom de verksamheter som skulle bli mest drabbad om någon risk skulle realiseras, främst de samhällsviktiga verksamheterna som identifierats i analysen. Det har även identifierats ett behov av att öka reservkraftsförmågan som en del i att säkerställa driften i samhällsviktig verksamhet.

Vi har i intervjuer informerats om att det saknas upprättade kontinuitetsplaner inom samtliga verksamhetsområden som granskningen omfattar. Det pågår ett arbete inom verksamhetsområde vård och omsorg, där verksamheten tagit hjälp av en extern konsult för att upprätta kontinuitetsplaner. Vid tidpunkten för granskningen kvarstår att ta fram kontinuitetsplan för avbrott i it-miljön, vilket innebär att vi inte har kunnat tagit del av något utkast till plan som omfattar granskningsområdet.

Inom serviceenheten (verksamhetsområde miljö och teknik) har det påbörjats ett scenariobaserat arbete som inkluderar framtagande av rutiner och riktlinjer för hur enheten ska agera utifrån olika scenarion. Arbetet sker tillsammans med kommunens beredskapssamordnare. I arbetet inkluderas även kockar och köksmästare där de ombeds att teoretiskt planera för matförsörjning utifrån dessa scenarion. Enheten har även som ambition att genomföra övningar på årlig basis, där senaste övningen syftade till att säkerställa matförsörjning vid elavbrott.

Vi informeras därutöver om att det i kommunen har genomförts ett arbete där verksamheterna har identifierat vilka system som är de mest prioriterade vid en situation som kräver återgångsprioritering. En sammanställning per verksamhet kommer att överlämnas till kommunens it-avdelning, som i nästa steg har i uppdrag att upprätta en kommunövergripande prioriteringsordning. Bolagen har inte ingått i detta arbete.

8.1.2 Övning

I intervjuer informeras vi om att det inte har genomförts någon kommun- eller koncernövergripande övning med fokus på it-avbrott.

Som tidigare nämnts har serviceenheten genomfört en övning som syftade till att säkerställa matförsörjning vid ett eventuellt elavbrott.

8.1.3 Bedömning

Vår bedömning är att det inte finns dokumenterade kontinuitetsplaner eller motsvarande underlag inom kommunstyrelsen, nämnderna eller bolagen.

Vi har i granskningen tagit del av de dokument som reglerar arbetet med kontinuitetsplanering. Dock är vår bedömning att det saknas etablerade metoder och arbetssätt för hur arbetet med kontinuitetsplaner ska genomföras. Vi kan se att det inom vissa verksamhetsområden pågår ett aktivt arbete med kontinuitetsplanering, men att det görs med variation där verksamheterna har kommit olika långt. Vi bedömer att detta kan bero på att det saknas ett enhetligt arbetssätt.

Vi bedömer att det saknas en systematik och tillräcklig samordning som främjar likriktning i arbetet. Vi bedömer att kommunstyrelsen utifrån sitt övergripande ansvar för interna säkerhetsfrågor behöver kravställa nivåer och genomförande av kontinuitetsplanering på ett tydligare sätt.

Därutöver bör berörda nämnder även tillse att de samhällsviktiga verksamheterna prioriterar arbetet med kontinuitetsplanering. Att arbetet bedrivs utifrån en gemensam planering är en avgörande faktor för att en fungerande samverkan ska finnas, exempelvis avseende kritiska beroenden över verksamhetsgränserna både inom kommunen samt gentemot bolagen.

Då bolagen saknar krav på kontinuitetshantering mot bakgrund av att de inte bedriver samhällsviktig verksamhet, är vår bedömning att bolagen bör göra en riskbedömning och analys avseende vilket behov av kontinuitetsplanering som de är i behov av. Detta då it-säkerhetshändelser med störningar eller avbrott som följd riskerar att få en stor påverkan på bolagens verksamhet.

Då en ny policy väntas antas är det av vikt att det upprättas riktlinjer som konkretiserar policyn och som kan utgöra vägledning för nämnder och verksamhetsområden i informationssäkerhetsarbetet. Bland annat avseende krav på kontinuitetsplanering för system som nyttjas inom samhällsviktig verksamhet.

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

Övning är av vikt för att säkerställa en tillräcklig kontinuitetsplanering för it-avbrott. MSB understryker i sin nationella strategi för systematisk övningsverksamhet[11] att just övning är avgörande för en kommuns förmåga att hantera en krissituation. Det är ett viktigt verktyg för kommunen i syfte att förbereda ledning och medarbetare för hur de ska agera vid en skarp händelse. Vi bedömer att kommunstyrelsen behöver tillse att övning genomförs och att samtliga verksamheter och bolag inkluderas.

8.2 Redundans och reservrutiner

8.2.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet för verksamhetskritiska informationssystem

I informationssäkerhetspolicyn framgår att avbrott-/återställningsplan ska redovisa prioriterade åtgärder och aktiviteter vid oplanerade driftavbrott i prioriterade system/e-tjänster. Planen ska tas fram för system-/e-tjänster vars krav på tillgänglighet klassificerats som *Viktig, Mycket viktig* och *Kritisk*. Vi kan genom granskningen konstatera att dessa typer av planer saknas i de verksamheter som granskningen omfattar.

Vidare framgår av policyn att ansvaret mellan ägaren till systemet och driftleverantören ska framgå i Servicenivåavtal (SLA). Enligt intervjuade så saknas upprättade SLA mellan verksamheterna och it-avdelningen som omfattar kravställning om åtgärder för prioriterade system. Kommunens it-avdelning har beredskap som sträcker sig utanför kontorstid, där det finns en informell struktur för vilka som får nyttja it-jouren. Intervjuade uppfattar att beredskapen främst avser verksamhet som är kritisk eller samhällsviktig.

Gentemot externa leverantörer ser det olika ut mellan verksamheterna, men bilden vi får är att det inte har kravställts några särskilda säkerhetsåtgärder utifrån analys och riskbedömning av eventuella behov för prioriterade system.

Vi informeras om att kommunens it-avdelning utifrån omvärldsbevakning, vedertagen praxis samt tidigare inträffade händelser har vidtagit åtgärder för att stärka kommunens redundans samt

[11] Publicerad oktober 2020.

möjlighet att kunna återskapa information genom backup. Åtgärderna saknar dock grund i genomförda analyser och riskbedömning av verksamheterna för de prioriterade systemen.

Angående reservkraft har kommunen tillgång till sådan som kan förflyttas till berört område. Dock uppges i RSA att tillgången är begränsad och intervjupersoner uppger att det finns behov av att kartlägga den reservkraft som finns. Det uppges även finnas behov av att stärka samverkansarbetet över verksamhetsområdena för att säkerställa att prioriteringen vid händelse kan göras effektivt och till de mest kritiska punkterna.

8.2.2 Reservrutiner

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

Vår dokumentationsgenomgång visar att det inom verksamhetsområde vård och omsorg samt miljö och teknik finns till viss del dokumenterade reservrutiner. Rutinerna har inte testats, vilket innebär att verksamheterna saknar kunskap om rutinerna är tillräckliga för att kunna säkerställa drift av verksamheten vid ett eventuellt it-avbrott.

Vi har från miljö och teknik även tagit del av en krisledningsplan, som ska utgöra stöd vid kris som påverkar verksamheten i den utsträckning att anpassningar behöver göras i ledning- och mötesstruktur. Därutöver har vi för samma område delgetts planering för minsta bemanning vid exempelvis semester eller personalbortfall för områdena serviceenheten, stab, strategisk planeringsenhet, enheten för gata/park samt projektenheten.

Därtill har vi i faktakontrollen informerats om att det på samtliga skolor och förskolor finns manuella arbetssätt för att kunna bedriva viss skolverksamhet, dock har inget underlag bifogats uppgifterna.

Av verksamhetsområde utbildning av vi mottagit ett organisationsschema för krigsberedskap samt personalhantering vid nedstängning av verksamheter.

Vi informeras om att bolagen konstaterat att tillgängligheten till nybyggda lokaler och fastigheter kan försvåras vid ett eventuellt it-avbrott och att det därför finns behov av att säkerställa detta.

8.2.3 Bedömning

Vår bedömning är att åtgärder endast delvis har identifierats eller vidtagits för att ha redundans om digitala informationssystem och nätverk inte är tillgängliga.

Vi bedömer att det saknas en tillräcklig analys och bedömning av prioriterade systems eventuella behov om åtgärder samt upprättade SLA för att verksamheterna ska kunna kravställa i enlighet med behov.

En betydelsefull kontinuitetsbefrämjande åtgärd är jourberedskap för it-händelser och förmåga att bedöma misstänkta eller pågående incidenter i tidigt skede. Vi anser att kommunens interna it-beredskap utgör en möjlighet för att kunna upprätthålla kommunens samhällsviktiga verksamhet.

Mot bakgrund av att strukturen för vilka som får nyttja it-jouren är informell, ser vi behov av att den utvärderas i förhållande till behov som de samhällsviktiga verksamheterna identifierar i arbetet med riskhantering och kontinuitetsplanering.

Vår bedömning är att det endast delvis finns dokumenterade och etablerade reservrutiner i form av manuella arbetssätt för hur verksamheterna ska fortgå utan tillgång till digitala informationssystem och nätverk.

De rutiner vi tagit del av bedömer vi inte vara tillräckliga för att säkerställa kontinuitet i verksamheten vid ett eventuellt it-avbrott. Därutöver saknas det dokumenterade rutiner inom vissa av de verksamhetsområden som omfattas av granskningen. Vi anser därför att det finns behov av att upprätta reservrutiner samt testa dem för att säkerställa att de fungerar enligt förväntan vid ett it-avbrott.

8.3 Uppföljning

Enligt program för krisberedskap så har den aktör som innehar ett visst ansvar under normala förhållanden även detta ansvar vid en oönskad händelse. Detta innebär att den nämnd vars verksamhet som drabbas av en oönskad händelse också ansvarar för att hantera den.

Av granskningen har det framkommit att det saknas ett systematiskt arbete för uppföljning av kontinuitetsplaneringen i kommunen, både inom nämnderna och kommunstyrelsen samt bolagen. Det anges att samtliga nämnder har fått viss återrapportering om att det pågår ett arbete inom verksamheterna som rör krisberedskap, dock sker återrapportering inte med någon systematik.

De förtroendevalda som intervjuats inom ramen för granskningen uppger att de inte ser ett behov av ökad delaktighet i kontinuitetsplanering då frågan till största del ses som en verksamhetsfråga.

Av de internkontrollplaner vi tagit del av för nämnder och kommunstyrelsen så saknas kontrollmoment med bäring på området. Vi har inte heller tagit del av underlag för någon formell rapportering eller uppföljning som presenterats på sammanträden för styrelser och nämnder.

8.3.1 Bedömning

Vår bedömning är att nuvarande kontinuitetshantering och planer inte har följts upp av styrelsen/nämnderna/bolagen för att säkerställa att det finns en ändamålsenlig planering.

Vi konstaterar att det i informationssäkerhetspolicyn ställs krav på samtliga verksamheters kontinuitetsplanering. Vi kan samtidigt konstatera att arbetet på flera håll inte har genomförts i tillräcklig utsträckning vilket vare sig kommunstyrelsen, nämnderna eller bolagen har uppmärksammat genom intern kontroll eller annan uppföljning.

Som vi bedömt i tidigare avsnitt så har nuvarande beredskap endast testats i begränsad form på enhetsnivå och utvärdering av kontinuitetsplaner och rutiner har inte ingått för att bedöma att beredskapen är tillräcklig.

Sammantaget ser vi därför att uppföljningen är i behov av att stärkas avseende efterlevnad av styrande dokument samt för att säkerställa att kommunkoncernens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser.

I policyn ställs även krav på att den nämnd vars verksamhet som drabbas av en oönskad händelse också ansvarar för att hantera händelsen. Mot bakgrund av vad granskningen visar konstaterar vi att det finns behov av att tydliggöra i vilken form det är lämpligt att de förtroendevalda är involverade i uppföljning och rapportering av kontinuitetsplaneringen i syfte att kunna säkerställa nämndernas styrning inom området.

9 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

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

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen, nämnderna och bolagsstyrelserna inte har säkerställt en tillräcklig planering och samordning för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Säkerställa tydliga riktlinjer och kravnivåer för kontinuitetsarbete inom kommunkoncernen.
- Upprätta och besluta om verksamhetsövergripande kontinuitetsplan eller på nivå för verksamhet som bedöms lämplig.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.
- Tillse att åtgärdsplanering genomförs och baseras på aktuell informationsklassning och riskbedömning för informationstillgångar som styrelsen ansvarar för.
- Utvärdera behov av intern jourverksamhet för it-verksamheten i förhållande till de samhällsviktiga verksamheternas behov.
- Fastställa former för hur kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.
- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad kommunövergripande systematik.
- Säkerställa att bolagen inkluderas i det koncernövergripande arbetet utifrån behov.

Utifrån resultatet av vår granskning rekommenderar vi socialnämnden, tekniska nämnden samt utbildningsnämnden att:

- Upprätta och besluta om verksamhetsövergripande kontinuitetsplan eller på nivå för verksamhet som bedöms lämplig.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som nämnden ansvarar för.
- Säkerställa att SLA etableras med grund i aktuella analyser och riskbedömningar över tillgänglighetsbehov.
- Säkerställa att reservrutiner i form av manuella arbetssätt upprättas och testas så att de fungerar i enlighet med förväntan.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

- Fastställa former för hur kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar
- Etablera en dialog med övriga verksamhetsområden och bolag så att kritiska beroenden mellan verksamheter kan omhändertas på ett samordnat och effektivt sätt.

Utifrån resultatet av vår granskning rekommenderar vi Bostads AB Svedalahem och Svedala Exploaterings AB att:

- Utifrån riskbedömning och analys göra en bedömning över behovet av kontinuitetsplaner.
- Säkerställa att reservrutiner i form av manuella arbetssätt upprättas och testas så att de fungerar i enlighet med förväntan.
- Säkerställa att bolagen inkluderas i det koncernövergripande arbetet utifrån behov.

Datum som ovan

Azets Revision & Rådgivning AB

Fredric Gyllensten
Certifierad kommunal revisor

Jenny Thörn
Verksamhetsrevisor

Ida Larsson
Verksamhetsrevisor