Granskning av kontinuitetshantering it-säkerhetshändelse

Rapport

Växjö Energi AB, VEAB Elnät och Wexnet AB

2025-01-23

Antal sidor 20

1 INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING

Azets Revision & Rådgivning har av VEAB-koncernens lekmannarevisorer fått i uppdrag att granska bolagens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa som leder till it-avbrott. Uppdraget ingår i revisionsplanen för år 2025.

Granskningen har genomförts hos de kommunala bolagen Växjö Energi, Växjö Energi Elnät och Wexnet. Syftet med granskningen har varit att bedöma om bolagsstyrelsen och VD har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att bolagsstyrelserna och VD endast delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Bakgrunden till vår samlade bedömning är att det saknas en beslutad och tydlig styrning över krav och förväntningar på bolagen i koncernen vad gäller arbete med kontinuitetshantering. Den styrning som finns genom informationssäkerhetspolicyn bedömer vi vara på en alltför övergripande nivå för att konkretisera hur arbetet ska genomföras. Det saknas därtill etablerad metod eller process för arbetet så att det genomförs på likartat sätt inom VEAB-koncernen.

Vidare är arbetet i en uppstartsfas vilket innebär att dokumenterade och implementerade kontinuitetsplaner saknas i hög grad. Vi vill dock framhålla att samtliga affärsområden har goda rutiner för att genomföra risk- och sårbarhetsanalyser samt vidta åtgärder för att hålla en hög leveranssäkerhet. För att göra det finns dokumenterade rutiner och instruktioner för att hantera kriser och störningar. Vi kan dock inte utesluta att det saknas tillräckliga rutiner och planering för att koncernen ska vara uthållig och säkerställa verksamhetens kontinuitet vid it-säkerhetshändelser. Nuvarande planer och rutiner har inte utvärderats genom övning och arbetet har inte följts upp på ett strukturerat sätt vilket innebär att det saknas kännedom om hur väl planeringen skulle fungera i praktiken.

På nästa sida redovisas våra samlade bedömningar av respektive revisionsfråga.

Finns tydliggjorda krav eller förväntningar avseende kontinuitetshantering och hur denna ska genomföras?	
Växjö Energi AB, VEAB Elnät & Wexnet AB	Nej
Finns dokumenterade kontinuitetsplaner eller motsvarande underlag och inkluderar dessa planering utifrån risk för it-säkerhetshändelse?	
VEAB & VEAB Elnät	Endast delvis
Wexnet AB	I allt väsentligt
Har åtgärder vidtagits för att ha redundans om digitala informationssystem och nätverk inte är tillgängliga?	
Växjö Energi AB, VEAB Elnät & Wexnet AB	Endast delvis
Finns dokumenterade och etablerade reservrutiner för hur verksamheten ska fortgå utan tillgång till digitala informationssystem och nätverk?	
Växjö Energi AB, VEAB Elnät & Wexnet AB	Endast delvis
Har övningar genomförts för att utvärdera kontinuitetsplaner och tillhörande rutiner?	
Växjö Energi AB &VEAB Elnät	Nej
Wexnet AB	I allt väsentligt
Har nuvarande kontinuitetshantering och planer följts upp för att säkerställa att det finns en ändamålsenlig planering?	
Växjö Energi AB, VEAB Elnät & Wexnet AB	Nej

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

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för VEAB att:

- Efterfråga tydlighet avseende hur bolagen i koncernen ska tillämpa den styrning som kommunfullmäktige beslutar om inom krisberedskap och kontinuitetshantering.
- Fastställa styrande dokument som beskriver krav och processer för VEAB-koncernens krisberedskapsarbete, inklusive kontinuitetshantering.
- Etablera metod eller process för kontinuitetshantering och genomföra arbetet för kritiska processer och leveranser.
- Slutföra arbetet med beredskapsplanering och säkerställa att kontinuitetsplaner för bortfall IT/OT dokumenteras.
- Etablera rutiner för uppföljning av kontinuitetsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets förmåga.
- Genomföra övning utifrån scenariot it-säkerhetshändelse/it-avbrott i syfte att utvärdera befintliga planer och rutiner.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för VEAB Elnät att:

- Anpassa det egna säkerhetsarbetet i relation till den styrning som fastställs som gällande för bolagen som ingår i VEAB-koncernen.
- Slutföra arbetet med beredskapsplanering och säkerställa att kontinuitetsplaner för bortfall IT/OT dokumenteras.
- Etablera rutiner för uppföljning av kontinuitetsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets förmåga.
- Genomföra övning utifrån scenariot it-säkerhetshändelse/it-avbrott i syfte att utvärdera befintliga planer och rutiner.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för Wexnet AB att:

- Anpassa det egna säkerhetsarbetet i relation till den styrning som fastställs som gällande för bolagen som ingår i VEAB-koncernen.
- Besluta om riktlinje för kontinuitetshantering efter bedömning om anpassningar utifrån lagkrav och krav från tillsynsmyndigheter.
- Slutföra arbetet med beredskapsplanering och säkerställa att kontinuitetsplaner för bortfall IT/OT dokumenteras.
- Etablera rutiner för uppföljning av kontinuitetsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets förmåga.

2 BAKGRUND

Azets (tidigare KPMG) har av lekmannarevisorerna i VEAB-koncernen fått i uppdrag att granska bolagens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa. Uppdraget ingår i revisionsplanen för år 2025.

En god krisberedskap är en förutsättning för att verksamheterna ska stå väl rustade inför olika former av samhällsstörningar och för att klara av att hantera olika former av krissituationer. Inom ramen för bolagens åtaganden 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.

Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Några av dessa återfinns i koncernens bolag, bland annat el, fjärrvärme och bredband.

Under 2026 förväntas två nya lagar träda i kraft i Sverige:

- Lag om motståndskraft hos kritiska verksamhetsutövare

Med utgångspunkt från CER -direktivet beslutat av EU. Direktivet ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet.

- Cybersäkerhetslagen

Med utgångspunkt från NIS 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 den bristande hanteringen 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.

Lekmannarevisorerna bedömer att de negativa konsekvenserna vid en extraordinär händelse eller annan kris som betydande om det inte finns ändamålsenlig kontinuitetsplanering. Lekmannarevisorerna drar därför slutsatsen att arbetet med kontinuitetshantering och rutiner behöver granskas.

2.1 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

Granskningen har syftat till att bedöma om bolagsstyrelsens och VD har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

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 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 för att säkerställa att det finns en ändamålsenlig planering?

2.2 AVGRÄNSNING OCH ANSVARIG STYRELSE

Granskningen har avgränsats till styrelserna för Växjö Energi AB, Växjö Energi Elnät AB samt Wexnet AB.

Granskningen har inte omfattat information och underlag som omfattas av säkerhetsskyddslagen.

3 REVISIONSKRITERIER

I granskningen har revisionskriterierna utgjorts av:

- 6 kap. 6 § kommunallagen (2017:725), KL
- 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
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (där detta är tillämpbart)

- MSBFS 2018:8 Myndigheten för samhällsskydd och beredskapsföreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (där detta är tillämpbart)
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- Tillämpbara interna regelverk, policys och beslut

4 METOD

Granskningen har genomförts genom dokumentgranskning av:

- Ägardirektiv för Växjö Energi AB
- PLN-1795 v7 Växjö Energi Affärsplan
- PLN-2093 v2 Wexnet Affärsplan
- Växjö kommuns budget för 2025 med plan 2026 &2027: Tillsammans för en stark och hållbar välfärd (Dnr 2024–00560)
- Växjö kommun Policy för säkerhet och beredskap, KS/2017–00245
- Växjö kommun Instruktion för kontinuitetshantering – Förvaltningar och bolag
- Växjö kommun Kriteriemodell för kontinuitetshantering – Förvaltningar och bolag
- Risk- och sårbarhetsanalys (informationsklass under säkerhetsskydd)
- Instruktioner
    - INS-199 v34 Driftstörningsinformation Wexnet
    - INS-1160 v16 Driftstörningsinformation Elnät
    - INS-1161 v22 Driftstörningsinformation Kraft och värme
    - INS-1561 v10 Kommunikation vid kris
    - INS-1881 v3 Krishanteringsplan
- Kontinuitetsplan Wexnet
- Exempel på informationssäkerhetsanalys Wexnet
- Protokoll från styrelsesammanträden
- Presentationsmaterial från kommunikation och rapporteringstillfällen

Intervjuer har genomförts med tjänstepersoner som är ansvariga för övergripande säkerhets- och beredskapsarbete samt säkerheten inom respektive affärsområde. Intervjuer har även genomförts med ordförande för respektive styrelse.

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

Rapporten är faktakontrollerad av utsedda representanter från bolaget.

5 RESULTAT AV GRANSKNINGEN

5.1 INLEDNING

I Växjö kommun är bolagen organiserade i en koncern med Växjö Kommunföretag (VKAB) som moderbolag. Enligt kommunfullmäktiges beslutade Företagspolicy har inte moderbolaget någon egen verksamhet, utan ska fungera som fullmäktiges och kommunstyrelsens formella styrinstrument för dotterbolagen.

I ägardirektiv för VKAB framgår att ändamålet med moderbolagets verksamhet är att samordna verksamheten direkt inom bolaget eller indirekt genom dotterbolagen i syfte att uppnå ett optimalt resursutnyttjande. Vidare anges syftet vara att uppnå största möjliga kommunnytta genom att VKAB ska vara en aktiv part i utvecklingen av kommunen och samverka med kommunen och övriga kommunala bolag i de fall där bolaget kan tänkas spela en roll. Bolaget ska särskilt tillse att kommunstyrelsen kan fullgöra sin uppsiktsplikt genom att säkerställa bolagens rapportering när kommunfullmäktige eller kommunstyrelsen ställer krav på detta.

I granskningen ingår Växjö Energi AB (VEAB) och dess helägda bolag Växjö Energi Elnät samt delägda bolaget Wexnet AB. I ägardirektiv för Växjö Energi AB ställs inga formella krav på bolagens arbete med krisberedskap eller kontinuitetshantering. Med beröring på området så framgår i ägardirektiv att dotterbolaget Växjö Energi Elnät AB inom sitt geografiska område ska säkerställa trygg elförsörjning.

Enligt ägardirektivet ska det finnas en tillhörande bilaga 1, vilken ska redogöra för de policys som samtliga bolag i koncernen har att efterleva. Bilagan saknas dock i erhållet ägardirektiv.

5.2 STYRNING AV ARBETET MED KONTINUITETSHANTERING

5.2.1 Ägarstyrning kommunen och moderbolaget

Kommunfullmäktige i Växjö har antagit en policy för säkerhet och beredskap[1]. I policyn framgår bland annat att säkerhets- och beredskapsarbetet ska vara en integrerad del i ordinarie verksamhet och att det ska ske ett aktivt och systematiskt säkerhets- och beredskapsarbete inom alla verksamheter. Vidare framgår att bolagen fastställer verksamhetsspecifika rutiner och instruktioner och ansvarar, genom VD, för att säkerhets- och beredskapsarbetet inom eget verksamhetsområde bedrivs i enlighet med lagar, förordningar, policy och instruktioner.

I Växjö kommuns Risk- och sårbarhetsanalys 2023 (öppen version) beskrivs process och förväntningar på verksamheterna, inklusive bolagens, arbete med kontinuitetshantering. Enligt modell som presenteras i dokumentet för Risk- och sårbarhetsanalys (RSA), ska bolag ha lokala RSA:er där samhällsviktig verksamhet och kritiska beroenden identifieras. Bolagen förväntas analysera hur egen verksamhet påverkas av händelser som framgår ur den koncernövergripande RSA:n samt för att ta fram åtgärder för att minska påverkan. Bolagen

[1] Kommunfullmäktige 2017-06-13 § 132

ska med grund i analyserna kontinuitetshantera sin samhällsviktiga verksamhet. Det sista steget i modellen är att arbetet ska följas upp årligen.

Det finns även av Växjö kommun framtagen Instruktion för kontinuitetshantering samt tillhörande kriteriemodell. Av underlagen framgår att dessa är koncerngemensamma och syftar till att vara ett stöd i processen ”Stödja koncernens arbete för en trygg och säker kommun”.

Det finns för granskningsområdet ingen särskild styrning från moderbolaget.

Vi har fått information från intervjuade att de styrdokument som kommunen beslutat om inte utgör styrning för bolagets verksamhet. Detta då styrelsen för VEAB eller dotterbolagen inte fastställt de som gällande för bolagets verksamheter.

Arbetet utgår enligt bolagets representanter i huvudsak från lagkrav samt de krav och rekommendationer som ställs från de sektorsmyndigheter som bolagets verksamhet tillhör. Uppfattningen från intervjuade är att sektorsmyndigheternas krav och bolagets arbetssätt med krisberedskap uppfyller kommunens styrning och arbete varpå det inte har funnits behov av att anpassa beredskapsarbetet i relation till ägarstyrningen.

I kommunfullmäktiges budget för 2025[2] ”Tillsammans för en stark och hållbar välfärd” framgår följande uppdrag till VEAB:

- Riktningsmål: Bättre fungerande och mer miljösmart samhällsplanering
    - Uppdrag till VEAB: Utred för att kunna intensifiera takten av åtgärder för en uthållig energiförsörjning och effektiv energianvändning

- Riktningsmål: Alla som bor, verkar och lever i Växjö kommun ska känna trygghet och tillit:
    - Uppdrag till samtliga bolag: Stärk IT-skydd och säkra informations- och cybersäkerheten

- Riktningsmål: Samhällsplaneringen ska bidra till en ökad trygghet:
    - Uppdrag till VEAB: Fortsätt arbetet med att möjliggöra ö-drift av Växjös kraftvärme - el och uppvärmning - i händelse av skada på anslutande stam- och regionnät

I den uppföljning som presenteras i delårsrapport per 2025-08-31 framgår att Växjö Energi fortsatt det pågående utvecklingsarbetet för att åstadkomma ö-drift där projektet framskrider enligt plan. Vad gäller riktningsmålet om stärkt it-skydd framgår att utbildningsinsatser genomförts för att stärka medarbetarnas kompetens samt att åtgärder vidtagits för att nå efterlevnad av NIS2-direktivet.

[2] Dnr 2024-00560

5.2.2 Styrning inom VEAB-koncernen

I Växjö Energis Affärsplan fokus 2030 med utblick mot 2035 där även verksamhetsplan ingår lyfts att VEAB-koncernen under 2025 lagt särskilt fokus på fyra viktiga områden, varav ett berör granskningen:

- Förstärkt säkerhet – Vi höjer vår säkerhetsnivå både fysiskt och digitalt. Med reella hot från sabotage och pågående cyberattacker är det avgörande att hela organisationen tar ansvar för säkerhetsarbetet.

Koncernens affärsplan beskriver fokus på cybersäkerhet och anpassningar till kommande lagförändringar och krav, exempelvis Cybersäkerhetslagen (NIS2-direktivet) och CER-direktivet. I affärsplanen lyfts i olika delar vikten av leveranssäkerhet och att bolaget med beaktande av omvärldsläget och nya krav har fokus på säkerhetsarbetet. Bland annat finns mål kopplat till avbrottstid i leveranser och vikten av att uppnå hög cybersäkerhet och beredskap. Inom område *Medarbetare och ledarskap* beskrivs arbetet med säkerhetskultur vilket ska uppnås genom utbildning. Ett antal indikatorer finns beskrivna i syfte att kunna mäta måluppfyllelsen.

I Wexnets affärsplan framgår att bolaget har som intention att klara av de krav som PTS ställer på bredbandsbolag. I affärsplanen beskrivs att bolaget tagit fasta på den reglering som väntas från PTS och att bolaget ligger i framkant för att möta driftsäkerhetskraven. Vi har tagit del av utkast till en Riktlinje för kontinuitetshantering[3] för Wexnet där hänvisningar till krav i relevanta lagrum[4] ingår. Företrädare uppger dock att väntade lagförändringar medfört att riktlinjen inte beslutats av styrelse eller VD då innehållet kan behöva anpassas utefter lagkraven.

Utöver det som beskrivs översiktligt i Affärsplanerna så saknas av styrelserna beslutad styrning av arbetet med krisberedskap och kontinuitetshantering.

Vad gäller arbetet med kontinuitet för system och IT har vi tagit del av beslutad Informationssäkerhetspolicy[5] som på övergripande nivå nämner kontinuitetshantering. Bland annat framgår i policyn reglering genom NIS2-direktivet vilket kräver att energibolag implementerar robusta säkerhetsåtgärder för att skydda sig mot cyberhot. Detta uppges ske genom ett systematiskt arbete med informationssäkerhet. En utgångspunkt i arbetet uppges vara att säkerställa drift och återställande av drift efter störning i verksamheterna. Kontinuitetshanteringen ska beskrivas med hjälp av rutiner samt övas och prövas.

Enligt företrädare från VEAB finns utöver policyn de rutiner och instruktioner som bolaget har behov av för att styra arbetet med utgångspunkt i Cybersäkerhetslagen.

Inom Wexnet finns Instruktion för hantering vid Ransomeware-attack samt ytterligare rutiner som beskriver hantering för att återgå till normalläge vid it-säkerhetsincidenter.

[3] Ej beslutad vid tid för granskningen
[4] LEK (2022:482): Kontinuitet i drift vid störningar samt PTSFS 2022:11, 14 kap. 1–2 §§: Krav på kontinuitetsplanering.
[5] Beslutad av styrelsen i VEAB 2025-02-13

5.2.3 Bedömning

Vår bedömning är att det **inte** finns tydliggjorda krav och/eller förväntningar avseende kontinuitetshantering.

Vi bedömer att styrelsen i VEAB inte har beslutat om styrning och inriktning för de krav och förväntningar som finns på bolagens verksamheter att upprätthålla kontinuitet i kritiska processer och leveranser vid it-säkerhetshändelser. Vi bedömer att bristen på styrning leder till att arbetet inte genomförs tillräckligt samordnat enligt gemensamma ramar och metoder.

De uppgifter som framkommit i granskningen, att arbetet utgår från lagkrav och rekommendationer från sektorsmyndigheter, bedömer vi svåra att bedöma i relation till granskningens avgränsning. Detta då ingen dokumentation över hur kraven tillämpas inom bolaget har presenterats i granskningen. Det är därmed svårt att följa strukturen och sektorsmyndigheternas påverkan på bolagens beredskapsarbete utifrån scenariot för it-säkerhetshändelse.

Vi noterar vidare att det finns en styrning från kommunfullmäktige där hela koncernen inkluderas. Denna har dock inte gjorts formellt gällande av styrelsen för VEAB och dotterbolagen.

För scenariot, it-säkerhetshändelse, som granskningen har som exempelhändelse utgör Informationssäkerhetspolicyn och tillhörande rutiner styrning i arbetet med kontinuitetshantering på systemnivå för hela koncernen. Vi bedömer därtill att det inom Wexnet finns ytterligare rutiner och instruktioner som beskriver hantering vid it-säkerhetshändelse.

5.3 KONTINUITETSPLANER ELLER MOTSVARANDE PLANERING

Som nämnts i tidigare avsnitt saknas av styrelsen beslutade riktlinjer som beskriver hur arbetet med kontinuitetshantering ska genomföras inom VEAB-koncernen. Företrädare menar att styrningen utgörs av dokumenterade krav i form av föreskrifter från exempelvis Svensk Kraftnät och Post- och telestyrelsen samt Energimyndigheten som tillhandahåller fördjupad information om beredskap för energisektorn.

Den dokumentation vi erhållit är tidigare nämnd Riktlinje för kontinuitetshantering som upprättats inom Wexnet (utkast vid tid för granskningen). Motsvarande beskrivande dokument och reglering av hur övriga bolag tolkar och tillämpar regleringen i lag och föreskrifter har inte presenterats. Beskrivningar i rapporten utgår i huvudsak av information som intervjupersoner lämnat om det arbete som genomförts.

Vi har fått muntliga uppgifter om att metoder och processer initieras och samordnas av säkerhetsfunktioner inom VEAB. Bolaget har bland annat en säkerhetschef, samordnare för säkerhetsskydd och beredskapsplanering samt ansvarig för samordning av informationssäkerhet. Ledningen har tillsatt en säkerhetsgrupp som även, enligt

intervjuade, ska vara godkänd av styrelsen. Gruppen leds av säkerhetschefen. I säkerhetsgruppen ingår representanter från alla affärsområden. Gruppen har bland annat i uppgift att samordna arbetet inom kontinuitetsplanering, kompetensutveckling och övningar. I de fall det krävs någon särskild insats inom VEAB-koncernen tillsätts arbetsgrupper som bemannas utifrån berörda affärsområden. Några deltagare från säkerhetsgruppen är även deltagare i Växjö kommuns koncerngemensamma grupperingar gällande säkerhetsarbete.

Vi har i granskningen tagit del av vissa underlag som avser hantering vid kris. Exempelvis krisledningsplan samt rutiner för kriskommunikation och kommunikation vid driftstörningar. Av intervjuerna framgå att arbetet inom bolaget historiskt varit fokuserat på leveranssäkerhet och beredskap för att upprätthålla den dagliga driften.

5.3.1 Beredskaps- och kontinuitetsplanering

Svenska kraftnät har, i rollen som elberedskapsmyndighet, utfärdat föreskrifter om elberedskap och fattade i september 2023 beslut om att aktörer inom elförsörjningen ska upprätta beredskapsplaner för att stärka elsystemets robusthet inför kriser, höjd beredskap eller krig. Syftet enligt myndighetens hemsida är att förbereda aktörerna för att kunna fortsätta verksamhet vid höjd beredskap och krissituationer och främja förmåga att förebygga, motstå och hantera störningar i elförsörjningen som kan påverka samhällsviktiga funktioner.

I våra intervjuer hänvisar flertalet intervjupersoner inom VEAB och VEAB Elnät att arbetet med kontinuitetshantering ingår i det arbete som gjorts och pågår med beredskapsplanerna. Kontinuitetsplanering för eldistribution och elproduktion avseende samhällskritiska leveransen ingår som viktiga delar. Intervjuade har bland annat beskrivit att en kontinuitet- och förmågebedömning ska göras.

Arbetet inom eldistribution (Elnät) och elproduktion (Växjö Energi) har genomförts och färdigställdes enligt intervjuade i september 2024. Intervjuade uppger att arbetet med beredskapsplaner för övrig verksamhet pågår under 2025 och 2026. När detta är slutfört ska den samlade informationen dokumenteras i en gemensam beredskapsplan för VEAB-koncernen.

Vi har inte tagit del av beredskapsplaner då dessa omfattas av säkerhetsskyddslagen och är sekretessklassad enligt lagen. I granskningen är information och underlag som är säkerhetsskyddsklassad utanför granskningens avgränsning. Vi har dock beretts möjlighet att ta del av förteckning av innehåll i beredskapsplanen på rubriknivå, genom det verifieras att beredskapsplanerna avser innehålla planering vid bortfall av IT/OT.

5.3.2 Risk- och sårbarhetsanalyser och åtgärder

Samtliga affärsområden uppges arbeta utifrån ett koncerngemensamt årshjul där årliga risk- och sårbarhetsanalyser genomförs som resulterar i åtgärdsplaner i syfte att säkerställa leveranssäkerheten. Arbetssättet har varit etablerat sedan 2011.

Intervjuade beskriver att medvetenheten höjts på senare år om att i högre grad beakta it-säkerhet i riskanalysarbetet även om riskanalyserna görs i ett helhetsperspektiv.

Inom samtliga affärsområden finns tillgänglighetsmål för samhällsviktiga leveranser. Enligt uppgift som vi erhållit har leveranssäkerheten för samhällskritiska leveranser varit hög över tid och var under 2025 på följande nivåer:

- Wexnet 99,995 %
- Elnät 99,998 %
- Växjö Energi 99,980 %

Företrädare från bolagen anger att skillnaden mellan beredskapsplanering och det kontinuerliga arbetet med risk- och sårbarhetsanalyser med tillhörande åtgärder är att beredskapsplaneringen har en inriktning mot antagonistiska hot medan RSA-arbetet omhändertar exempelvis naturkatastrofer.

5.3.3 Arbetet med informationssäkerhet

Inom ramen för arbetet med informationssäkerhet finns arbetssätt och ansvarsfördelning beskrivet i tidigare nämnd informationssäkerhetspolicy samt tillhörande riktlinjer och rutiner. Det pågår ett koncerngemensamt arbete med anpassningar utifrån nya lagkrav och behov och bolaget deltar i samverkan med Växjö kommun.

Intervjupersonerna beskriver att arbetet inom VEAB-koncernen genomförs enligt motsvarande krav och arbetssätt som finns etablerade inom Växjö kommun. Bland annat görs informationssäkerhetsanalys på nya system, och därefter varje år, samt vid större uppdateringar. Arbetet genomförs tillsammans med Växjö kommuns IT-avdelning och aktuella systemleverantörer. Vidare beskriver intervjupersonerna att alla system inom VEAB-koncernen har utsedda systemägare och systemförvaltare.

Arbetet innebär att det finns dokumenterade riskanalyser och tillhörande åtgärdsplaner för att vidta säkerhetsåtgärder för de system som är kritiska i bolagens leveranser. Gällande OT[6] beskriver intervjupersonerna att verksamheterna försöker hålla OT maskinnära det vill säga så rent som möjligt för att inte utsätta driftsmiljön för externa risker eller sårbarheter.

Det pågår ett arbete inom VEAB med en ”Digital Atlas”. Detta består i att kartlägga och dokumentera it-miljön och olika system och applikationers integrationer och arkitektur för att kunna konstatera olika beroenden och påverkan. I den samlade dokumentationen ingår redovisning och uppföljning av kontinuitetshanteringsplaner och återställningsplaner på systemnivå. Inom bolagen används en mall för kontinuitetsplan för system och IT som har sitt ursprung från Myndigheten för samhällsskydd och beredskap. Mallen uppges ha tillhandahållits från PTS men anpassats i vissa delar utifrån bolagets behov.

I granskningen har vi tagit del av dokumenterad informationssäkerhetsanalys samt kontinuitetsplan för system inom Wexnet AB men inte för några system inom VEAB eller VEAB Elnät. Vi har fått uppgift om att kontinuitetsplanering för IT och OT inom övriga affärsområden är pågående under slutet av 2025.

[6] Operational technology (OT) är ett begrepp som används för att beskriva system och hårdvara som styr, övervakar och automatiserar fysiska processer, exempelvis i industriella miljöer.

5.3.4 Bedömning

Vår bedömning är att VEAB och VEAB Elnät **endast delvis** har dokumenterade kontinuitetsplaner eller motsvarande underlag för att hantera it-säkerhetshändelse.

Vår bedömning är att det inom Wexnet AB i **allt väsentligt** finns dokumenterade kontinuitetsplaner eller motsvarande underlag som inkluderar planering utifrån risk för it-säkerhetshändelse.

Mot bakgrund av att beredskapsplanerna är säkerhetsskyddsklassade har vi inte tagit del av underlag och planer som beskriver VEAB samt VEAB Elnäts kontinuitetshantering vid it-säkerhetshändelser. Vi kan därför inte uttala oss om den dokumentation som finns i nuläget skulle vara tillräcklig för att upprätthålla koncernens samhällsviktiga leveranser på en acceptabel nivå vid it-säkerhetshändelser. Vi bedömer att kontinuitetsplaner på systemnivå kan utgöra visst stöd i hanteringen och att det finns rutiner för att följa upp att sådana är upprättade för system som nyttjas inom bolagets samhällsviktiga leveranser.

Baserat på muntliga uppgifter har vi fått en uppfattning om att det finns goda rutiner för att regelbundet genomföra risk- och sårbarhetsanalyser samt vidta åtgärder för att hålla en hög leveranssäkerhet. Det pågår därtill arbete med beredskapsplanering där analys av kontinuitet- och förmågebedömning ingår. Arbetet är dock endast delvis slutfört vid tid för granskningen.

Vi bedömer att Wexnet AB i allt väsentligt har dokumenterade planer och rutiner som beskriver hantering av it-säkerhetshändelser. Det finns dels dokumenterade analyser och riskbedömning med tillhörande åtgärdsförslag för kritiska system. Det finns även kontinuitetsplaner och instruktioner som beskriver hantering vid it-säkerhetshändelser.

5.4 REDUNDANTA LÖSNINGAR OCH RESERVRUTINER

5.4.1 VEAB och Elnät

Intervjupersonerna beskriver att bolaget har stort fokus på driftsäkerhet och krav på hög tillgänglighet, vilket gör att redundans finns utifrån det arbete som löpande pågår för att upprätthålla leveranserna. I bolagens ledningssystem finns ett mycket stort antal instruktioner och rutiner för specifika system och processer. Dessa uppdateras årligen i samband med riskanalysarbetet. Rutiner och instruktioner finns digitalt men även i analog form.

De intervjuade beskriver att kontinuitetshanteringen för de samhällsviktiga leveranserna till stor del består av att inte vara helt beroende av system utan att vid behov kunna övergå till manuell drift. Detta är delar som beskrivs i beredskapsplanen för elförsörjning och som planeras att ingå även i den koncerngemensamma beredskapsplanen.

5.4.2 Wexnet

De intervjuade beskriver att kritiska system alltid byggs med redundans. Respondenterna beskriver att det finns dokumenterade rutiner i de situationer där redundansen inte fungerar samt mer detaljerade checklistor mm. Redundansen kan även bestå av serviceavtal med externa leverantörer. Instruktioner och rutiner finns i dokument som lagras på en digital yta, de finns ej utskrivna men man tar regelbundet ut dokumentationen offline. Det görs regelbundet uppdateringar i såväl instruktioner som kontinuitetsplaner.

5.4.3 Bedömning

Vår bedömning är att det **endast delvis** vidtagits åtgärder för att ha redundans och **endast delvis** finns dokumenterade och etablerade reservrutiner.

Vi baserar vår bedömning på att det finns dokumenterade underlag med rutiner och instruktioner för att upprätthålla den dagliga driften och ha en leveranssäkerhet. Vi kan dock inte utesluta att mer omfattande störningar, exempelvis vid it-säkerhetshändelse, skulle innebära behov av andra åtgärder och rutiner för att ha redundans och kunna upprätthålla de samhällsviktiga leveranserna på en acceptabel nivå.

Vi ser det pågående arbetet med beredskapsplanering och anpassning efter cybersäkerhetslagen som väsentliga delar i att identifiera ytterligare behov.

5.5 Övning

De intervjuade beskriver att det genomförts ett antal olika utbildnings- och övningsinsatser dels internt inom VEAB-koncernen, inom respektive bolag eller i samverkan med kommunen eller andra externa parter.

Säkerhetsgruppen arrangerar återkommande övningar, exempelvis under beredskapsveckan, då övning genomfördes i syfte att öva ledningsfunktionen. Ett av de scenarion som övades var cyberattack. Övningar har enligt uppgift inte inkluderat utvärdering av kontinuitetsplaner och reservrutiner.

Inom Wexnet har medarbetare deltagit i en större övning, TELÖ24, som arrangerades av Post- och telestyrelsen. Därtill har två övningar genomförts tillsammans med andra stadsnät inom Svenska Stadsnätsföreningen/Crisis. En intern övning har genomförts utifrån scenariot för en ransomwareattack.

Företrädare från Wexnet uppger att de interna övningar som genomförts har syftat till att öva olika händelseförlopp, hantering av situationen samt återställning. Utvärdering har enligt uppgift resulterat i uppdaterade rutiner och kontinuitetsplaner.

5.5.1 Bedömning

Vår bedömning är att VEAB och VEAB Elnät **inte** har genomfört övningar för att utvärdera kontinuitetsplaner och tillhörande rutiner.

Vår bedömning är att Wexnet **i allt väsentligt** har genomfört övningar för att utvärdera kontinuitetsplaner och tillhörande rutiner.

Vi baserar vår bedömning på vissa övningar inom VEAB och VEAB Elnät har genomförts men att dessa inte har inkluderat utvärdering av kontinuitetsplaner och tillhörande rutiner hantering av it-säkerhetshändelser. De övningar som genomförts har varit fokuserade på ledningsorganisationen inom bolagen eller haft andra scenarios i fokus.

Vi baserar vår bedömning av Wexnet AB på att flertalet övningar har genomförts och att det i dessa har skett en utvärdering av befintliga planer och rutiner.

5.6 Uppföljning av arbetet med kontinuitetshantering

Intervjuade uppger att det sker en löpande uppföljning och rapportering till ledning och styrelse men inte enligt någon fastställd rutin eller regelbundenhet. Exempelvis har vi erhållit en agenda och presentation för presentation av säkerhetsarbetet för styrelserna i både VEAB och Wexnet AB under 2024 i samband med styrelseseminarier för respektive bolag. Vi har inte erhållit något motsvarande för år 2025 riktat till styrelserna i VEAB eller VEAB Elnät. Däremot har styrelsen i Wexnet AB erhållit en presentation av säkerhetsarbetet vid sammanträdet i augusti 2025.

Inom verksamheten beskrivs att uppföljning sker i linjen där även eventuella incidenter rapporteras. Det sker även rapportering via säkerhetsgruppen. Vi har i granskningen tagit del av presentationsmaterial från koncerndagar under 2025. Ett tema var säkerhet och beredskap där dels samtliga deltagare fick en omvärldsspaning av säkerhetsläget, dels information om bolagets pågående och kommande arbete med beredskapsplanering. En del av informationen avsåg cybersäkerhet och diskussion om kontinuitetsfrämjande åtgärder.

Respondenterna beskriver att den operativa uppföljning som sker till kommunens säkerhetsavdelning sker efter förfrågan och de instruktioner som kommer från kommunen.

5.6.1 Bedömning

Vår bedömning är att kontinuitetshanteringsarbetet och planer **inte** har följts upp för att säkerställa att det finns en ändamålsenlig planering.

Då inte nuvarande planer och rutiner inom VEAB och VEAB Elnät har utvärderats genom övning saknas tillräcklig kännedom avseende hur väl dessa skulle fungera vid en it-säkerhetshändelse.

Vi baserar därtill vår bedömning på att det saknas strukturerad uppföljning och rapportering till respektive styrelse. Då styrelserna är ytterst ansvariga för krisberedskaps- och kontinuitetshanteringsarbetet så bedömer vi att det är väsentligt att rutiner för uppföljning och rapportering etableras så att styrelsen erhåller information löpande för att kunna fullgöra sitt ansvar.

6 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

Granskningen har syftat till att bedöma om bolagsstyrelsens och VD har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning utifrån granskningens syfte är att styrelserna för VEAB, VEAB Elnät och Wexnet samt VD endast delvis har säkerställt en tillräcklig planering för att upprätthålla kontinuitet vid kritiska it-säkerhetshändelser.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för VEAB att:

- Efterfråga tydlighet avseende hur bolagen i koncernen ska tillämpa den styrning som kommunfullmäktige beslutar om inom krisberedskap och kontinuitetshantering.
- Fastställa styrande dokument som beskriver krav och processer för VEAB-koncernens krisberedskapsarbete, inklusive kontinuitetshantering.
- Etablera metod eller process för kontinuitetshantering och genomföra arbetet för kritiska processer och leveranser.
- Slutföra arbetet med beredskapsplanering och säkerställa att kontinuitetsplaner för bortfall IT/OT dokumenteras.
- Etablera rutiner för uppföljning av kontinuitetsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets förmåga.
- Genomföra övning utifrån scenariot it-säkerhetshändelse/it-avbrott i syfte att utvärdera befintliga planer och rutiner.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för VEAB Elnät att:

- Anpassa det egna säkerhetsarbetet i relation till den styrning som fastställs som gällande för bolagen som ingår i VEAB-koncernen.
- Slutföra arbetet med beredskapsplanering och säkerställa att kontinuitetsplaner för bortfall IT/OT dokumenteras.
- Etablera rutiner för uppföljning av kontinuitetsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets förmåga.
- Genomföra övning utifrån scenariot it-säkerhetshändelse/it-avbrott i syfte att utvärdera befintliga planer och rutiner.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för Wexnet AB att:

- Anpassa det egna säkerhetsarbetet i relation till den styrning som fastställs som gällande för bolagen som ingår i VEAB-koncernen.
- Besluta om riktlinje för kontinuitetshantering efter bedömning om anpassningar utifrån lagkrav och krav från tillsynsmyndigheter.
- Slutföra arbetet med beredskapsplanering och säkerställa att kontinuitetsplaner för bortfall IT/OT dokumenteras.
- Etablera rutiner för uppföljning av kontinuitetsarbetet som säkerställer att styrelsen får den information som krävs för att ha insyn i bolagets förmåga.

Datum som ovan

Azets Revision & Rådgivning AB

Jenny Thörn

Verksamhetsrevisor

Helena Olsson

Verksamhetsrevisor