Granskning av it- och cybersäkerhet

Rapport

Räddningstjänst Dala Mitt

KPMG AB

2023-10-19

Antal sidor 9

Räddningstjänst Dala Mitt
Granskning av it- och cybersäkerhet

2023-10-19

Innehållsförteckning

1 Sammanfattning

KPMG har av revisorerna i Räddningstjänst Dala Mitt fått i uppdrag att genomföra en översiktlig granskning av förbundets arbete för att upprätthålla en god it-och cybersäkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Vår samlade bedömning utifrån granskningens syfte är att direktionen delvis har tillsett att det finns ett systematiskt och riskbaserat it-säkerhetsarbete.

Vår bedömning är att direktionen brustit i sitt övergripande ansvar då det saknas fastställda styrdokument för informationssäkerhet (där it- och cybersäkerhet ingår som delar) samt att direktionen inte i riskanalyser för förbundet har inkluderat informationssäkerhetsrisker. Mot bakgrund av omvärldsläget och förhöjd risk för cyberhot mot offentliga organisationer ser vi det som väsentligt för att upprätthålla en tillräcklig säkerhet för förbundets verksamhet och informationstillgångar.

Vi bedömer trots ovan att förbundet med systematik har etablerat tekniska säkerhetsåtgärder i enlighet med de säkerhetsnivåer som MSB rekommenderar för stärkt cyberförsvar. De skydd som är implementerade har varit effektiva mot de hot som förbundet hittills har utsatts för.

Vi bedömer dock att det finns risk att nuvarande resurser inte är tillräckliga för att förbundet ska kunna bedriva ett systematiskt och riskbaserat informationssäkerhets-arbete. Vi uppfattar dock att förbundet i arbetet med de tekniska säkerhetsåtgärderna för infrastruktur och system genom egna resurser och externa leverantörer har tillgång till både personella resurser och kompetens för att de delarna av arbetet ska vara mindre sårbart. Informationssäkerhetsarbetet behöver dock vara integrerat i hela förbundet och ges den uppmärksamhet som krävs för att nå en tillräcklig systematik.

Utifrån våra bedömningar och vår slutsats rekommenderar vi direktionen att:

- Fastställa och etablera styrande dokument för informationssäkerhet som inkluderar ansvarsfördelning och krav avseende tekniska säkerhetsåtgärder.
- Utvärdera om nuvarande resurser är tillräckliga för att etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.
- Inkludera informationssäkerhetsrisker i förbundsövergripande risk- och sårbarhetsanalys samt besluta om åtgärder för att möta risker.
- Fastställa och etablera gemensamma incidenthanteringsrutiner.
- Säkerställa att en årlig uppföljning görs av informationssäkerhetsarbetet, där it- och cybersäkerhet ingår, samt att denna återrapporteras till direktionen.

2 Bakgrund

KPMG har av revisorerna i Räddningstjänst Dala Mitt fått i uppdrag att genomföra en översiktlig granskning av förbundets arbete för att upprätthålla en god it-och cybersäkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete.

Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, konfidentiell och spårbar. Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Utvecklingen och den förändrade användningen av ny teknik innebär också att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Den digitala utvecklingen måste följas av ett anpassat och balanserat säkerhetsarbete för att säkerställa att inte de system och digitala tjänster som nyttjas för informationshantering och lagring är exponerade och tillgängliga för cyberhot och angrepp. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för förbundet. Det är således väsentligt att förbundsdirektionen har en tillräcklig intern styrning och kontroll av sitt it-säkerhetsarbete så att arbetet sker systematiskt och på ett ändamålsenligt sätt.

Med anledning av ovanstående drar förbundets revisorer slutsatsen i sin riskanalys, att arbetet med it-och cybersäkerhet behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen syftar till att bedöma om direktionen har ett systematiskt och riskbaserat it-säkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Granskningen ska besvara följande revisionsfrågor:

- Finns det en ändamålsenlig organisation för it–säkerhetsarbetet?
- Har direktionen i riskanalys för verksamheten identifierat risker i form av cyberhot, exempelvis intrångsförsök eller attacker?
- Finns dokumenterade kravnivåer avseende it-säkerhet och sker det en uppföljning över att dessa följs?
- Har tekniska skyddsåtgärder implementerats som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?
- Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön?

— Finns etablerade rutiner med tydliggjorda eskaleringsvägar vid säkerhetshändelser och incidenter?
— Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?

Granskningen omfattar förbundsdirektionen och revisionsåret 2023.

2.2 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

— Kommunallagen 6 kap. 6 §
— Tillämpbara interna regelverk, policys och beslut
— MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet och it-säkerhetsåtgärder
— NIS-direktivet där detta är tillämpbart

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av:
    - Informationssäkerhetspolicy (utkast)
    - Riktlinjer för informationssäkerhet (utkast)
    - Incidenthantering IT (ej implementerade)
    - Incidentrapportering IT (ej implementerade)
    - Beskrivning av it-miljö och etablerade säkerhetsåtgärder

- Intervjuer har genomförts med förbundsdirektör, IT-ansvarig och verksamhetsstrateg.

Rapporten har faktakontrollerats av intervjupersoner.

3 Resultat av granskningen

3.1 Organisation för it-säkerhetsarbetet

KPMG genomförde under 2022 en granskning av förbundets arbete med informationssäkerhet och dataskydd. Intervjuade beskriver att förbundsdirektör utifrån de rekommendationer som lämnades i granskningen initierat ett projekt med målet att etablera ett systematiskt informationssäkerhetsarbete i förbundet. Verksamhetsstrateg är utsedd projektledare och övriga i projektgruppen har varit IT-ansvarig och HR-chef. Vid tid för intervjuer uppges att HR-chef sagt upp sig och arbetet försvårats på grund av bristande resurser för arbetet.

Inom ramen för projektet ingår att tydliggöra ansvarsfördelning för informationssäkerhet och it-säkerhet. I nuläget utgörs förbundets organisation för it-säkerhetsarbetet av it-ansvarig som är ansvarig för it-miljön och de system som nyttjas inom förbundet och en it-tekniker som ansvarar för användarnära it-frågor.

Förbundet har avtal med externa leverantörer för system och även för mer avancerade infrastrukturfrågor inklusive it-säkerhetslösningar.

3.1.1 Bedömning

Vår bedömning är att direktionen i allt väsentligt har säkerställt att det finns en ändamålsenlig organisation för it-säkerhetsarbetet.

Förbundet har en intern it-organisation som består av två personer. Vi bedömer att förbundet genom avtal med externa leverantörer har säkerställt att it-säkerhetsarbetet kan bedrivas med tillräckliga resurser och kompetens.

Vi bedömer däremot att det finns risk för att förbundets informationssäkerhetsarbete inte i tillräcklig utsträckning är en del i förbundets ordinarie verksamhet för att arbetet ska genomföras systematiskt. Med nuvarande resurser att tillgå i arbetet ser vi att det kan finnas risk att det inte ges den uppmärksamhet som krävs. Vi ser därför det pågående projektet som väsentligt att prioritera så att förbundet kan hitta den nivå på arbetet som bedöms tillräcklig i förhållande till hot och risker inom informationssäkerhet.

Vi bedömer dock att det finns risk att nuvarande resurser inte är tillräckliga för att förbundet ska kunna bedriva ett systematiskt och riskbaserat informationssäkerhets-arbete. Vi uppfattar dock att förbundet i arbetet med de tekniska säkerhetsåtgärderna för infrastruktur och system genom egna resurser och externa leverantörer har tillgång till både personella resurser och kompetens för att de delarna av arbetet ska vara mindre sårbart.

3.2 Riskhantering

Enligt intervjuade har inte direktionen i övergripande riskanalys beaktat informationssäkerhetsrisker. Förbundet har påbörjat informationsklassningsarbete utifrån metoden KLASSA och tar enligt uppgift stöd i MSB:s råd och rekommendationer för systematiskt informationssäkerhetsarbete.

3.2.1 Bedömning

Vår bedömning är att direktionen inte har identifierat risker i form av cyberhot, exempelvis intrångsförsök eller attacker, i dokumenterad riskanalys för förbundet.

Mot bakgrund av säkerhetsläget och höjd risk för cyberhot så ser vi det som väsentligt att informationssäkerhetsrisker ingår och kan mötas med beslut om åtgärder för vid behov stärka säkerheten. Vi ser det som positivt att informationsklassningsarbetet har påbörjats, detta så att skyddsbehov för informationstillgångar kan identifieras och komplettera redan etablerade säkerhetsåtgärder när analyser visar att behov finns.

3.3 Tekniska säkerhetsåtgärder

I styrande dokument anges endast på övergripande nivå vilka krav som finns för informationssäkerhet och inget specifikt regleras avseende krav på tekniska säkerhetsåtgärder. Vi har tagit del av sammanställning av förbundets it-miljö och de säkerhetsfunktioner som är etablerade. Vi kan utifrån beskrivningen konstatera att säkerhetsåtgärder i hög grad är i nivå med de rekommendationer som MSB ger för en stärkt cyberförsvarsförmåga.

Intervjuade beskriver att de avtalade externa leverantörerna inom it har lämnat förslag på relevanta säkerhetsåtgärder och skydd för förbundets system och information. Dels avseende nätverkssäkerhet men för olika klientskydd, backup, dels segmentering av nätverk. Det finns en etablerad övervakning med automatiska larm om avvikelser sker som kan indikera på säkerhetshändelser.

De säkerhetsåtgärder som är etablerade har fungerat effektivt mot de hot som förbundet utsatts för.

3.3.1 Bedömning

Vår bedömning är att det saknas dokumenterade kravnivåer avseende it-säkerhet och därigenom finns inte förutsättningar att göra uppföljning över att dessa efterlevs.

Vi bedömer att förbundet har tekniska skyddsåtgärder och funktioner för övervakning så att olika typer av attacker, intrång eller säkerhetshändelser i it-miljön kan stoppas, upptäckas och hanteras. Den säkerhet som är etablerad är i nivå med de rekommendationer som MSB ger för stärkt cyberförsvarsförmåga och har genomförts efter råd från externa specialister inom it. Den säkerhet som är etablerad har inte utvärderats genom tekniska test men har varit effektiva mot de hot som förbundet hittills utsatts för och inga allvarliga incidenter har skett.

3.4 Incidenthantering och reservrutiner

Vi har tagit del av utkast till rutiner för hantering av it-incidenter samt rapportering av it-incidenter. Rutinerna uppges dock vid tid för granskningen inte vara fastställda och etablerade.

I händelse av en incident finns arbetssätt i praktiken som anpassas efter vilka system eller vilken it-komponent som incidenten gäller. Det finns en dokumenterad lista över system med tillhörande prioriteringsordning. Det innebär att om någon sker i ett högt prioriterat system så sker en skyndsam hantering där externa leverantörer involveras.

För den mest kritiska verksamheten finns kontinuitetsplanering för att upprätthålla verksamheten om det inte finns tillgång till informationssystem. Det avser bland annat insatsdata, geografisk kartinformation samt information om fastigheter mm som kan vara avgörande i den operativa verksamheten. För denna typ av information finns lokala kopior och analog tillgång till information i pärmar mm. Därtill uppges av intervjuade att det finns hög säkerhet för kritiska processer genom att förbundet delar lokaler med SOS Alarm som har höga säkerhetskrav som även innefattar skyddad infrastruktur, nätverk och även tillgång till reserv-el.

Återläsning av säkerhetskopior har testats och informationen verifierats för att säkerställa att de fungerar ändamålsenligt.

3.4.1 Bedömning

Vår bedömning är att det saknas etablerade rutiner med tydliggjorda eskaleringsvägar vid säkerhetshändelser och incidenter. Vi har dock tagit del av utkast för rutiner samt konstaterar att det i praktiken delvis finns etablerade arbetssätt med tillhörande eskaleringsvägar i händelse av incidenter.

Vi bedömer att det finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system. Det finns bland annat etablerade rutiner för säkerhetskopiering samt tekniska funktioner för att säkerställa att information kan återställas i händelse av allvarlig incident eller avbrott.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om direktionen har ett systematiskt och riskbaserat it-säkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Vår samlade bedömning utifrån granskningens syfte är att direktionen delvis har tillsett att det finns ett systematiskt och riskbaserat it-säkerhetsarbete.

I nuläget saknas beslutade styrdokument för informationssäkerhet där it-säkerhet ingår. I avsaknad av detta finns i nuläget inte tydliggjorda krav för arbetet och ansvaret är inte fördelat. Vi ser behov av att direktionen i förbundsövergripande riskanalyser inkluderar informationssäkerhetsrisker så att beslut om åtgärder kan fattas i syfte att stärka säkerheten inom förbundet.

Vi bedömer att förbundet, trots avsaknad av styrning och krav för arbetet, har etablerat tekniska säkerhetsåtgärder utifrån aktuella hot och risker. Dessa är i nivå med de rekommendationer som MSB ger för stärkt cyberförsvarsförmåga.

Med nuvarande resurser att tillgå i arbetet ser vi att det kan finnas risk att det inte ges den uppmärksamhet som krävs. Vi ser därför det pågående projektet som väsentligt att prioritera så att förbundet kan hitta den nivå på arbetet som bedöms tillräcklig i förhållande till hot och risker inom informationssäkerhet.

Utifrån våra bedömningar och vår slutsats rekommenderar vi direktionen att:

- Fastställa och etablera styrande dokument för informationssäkerhet som inkluderar ansvarsfördelning och krav avseende tekniska säkerhetsåtgärder.
- Utvärdera om nuvarande resurser är tillräckliga för att etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.
- Inkludera informationssäkerhetsrisker i förbundsövergripande risk- och sårbarhetsanalys samt besluta om åtgärder för att möta risker.
- Fastställa och etablera gemensamma incidenthanteringsrutiner.
- Säkerställa att en årlig uppföljning görs av informationssäkerhetsarbetet, där it- och cybersäkerhet ingår, samt att denna återrapporteras till direktionen.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Linnéa Grönvold
Certifierad kommunal yrkesrevisor