Granskning av informationssäkerhet

Rapport

Skinnskattebergs kommun

KPMG AB

2024-09-24

Antal sidor 15

Skinnskattebergs kommun
Granskning av informationssäkerhet

2024-09-24

Innehållsförteckning

1 Sammanfattning

KPMG har av Skinnskattebergs kommuns revisorer fått i uppdrag att granska kommunens arbete med informationssäkerhet.

Granskningen har syftat till att bedöma om kommunstyrelsen har tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

Vår samlade bedömning utifrån granskningens syfte är att det inte bedrivs ett systematiskt informationssäkerhetsarbete.

Vi bedömer att kommunstyrelsen har brustit i sitt ansvar och inte säkerställt en styrning av kommunens informationssäkerhetsarbete. Det saknas till stora delar styrande och vägledande dokument som reglerar ansvar, vilka krav som ställs samt hur arbetet ska bedrivas. Det saknas även kommunövergripande samt verksamhetsövergripande riskanalyser där informationssäkerhetsrisker beaktats samt ett etablerat klassningsarbete av kommunens informationstillgångar. En väl genomförd riskbedömning är nödvändig för att det ska vara möjligt för kommunen att prioritera och vidta erforderliga åtgärder.

Därtill anser vi att de informationsinsatser som genomförts inte är tillräckliga i syfte att stärka kommunens säkerhetskultur. Bristande medvetenhet och kunskap om hot och risker inom informationssäkerhet kan som yttersta konsekvens leda till att kommunens information och system utsätts för risk och allvarliga konsekvenser, både ekonomiska och förtroendeskadliga.

I det följande redovisas våra bedömningar kopplat till respektive revisionsfråga, vilket efterföljs av lämnade rekommendationer.

Revisionsfråga	Bedömning
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?	Nej
Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?	Nej
Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?	Nej
Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?	Nej
Finns fastställda metoder för riskhantering och har informationssäkerhetsrisker beaktats och följts av åtgärder?	Nej
Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?	Delvis
Har kommunstyrelsen säkerställt en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser?	Delvis
Finns en tillräcklig uppföljning och återrapportering av kommunens informationssäkerhetsarbete?	Nej

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Verka för att kommunfullmäktige antar en informationssäkerhetspolicy.
- Till policyn upprätta och anta tillhörande riktlinjer och instruktioner som omfattar ansvarsfördelning samt hur informationssäkerhetsarbetet ska bedrivas.
- Anta en kommungemensam modell för riskbedömning och informationsklassning samt säkerställa att den etableras.
- Säkerställa att riskbedömning av kommunens informationstillgångar genomförs.
- Tillse att en åtgärdsplan upprättas utifrån identifierade åtgärdsbehov.
- Tillse att incidentrutiner dokumenteras, som omfattar eskaleringsvägar samt former för hur inträffade incidenter ska analyseras och dokumenteras.
- Tillse att ett uppföljningsarbete etableras samt att styrelsen erhåller kontinuerlig återrapportering angående kommunens informationssäkerhetsarbete.

2 Bakgrund

KPMG har av Skinnskattebergs kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens ansvar för att kommunen har ett systematiskt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2024.

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 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. 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 att organisationer drabbats av ekonomisk skada eller förtroendeskada. Inledningsvis 2024 utsattes en större leverantör av serverdrift och molntjänster för en ransomware-attack[1] 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 och kritiska funktioner, vilka om de inte fungerar kan leda till skada för såväl enskilda individer som samhället i stort. Det är därför av största vikt att det bedrivs ett systematiskt informationssäkerhetsarbete för att undvika allvarlig påverkan på verksamheten och samhället i stort.

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 kommunen. Det är således väsentligt att kommunen bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att informationssäkerhetsarbetet behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen syftar till att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

[1] En form av skadlig kod eller krypterad fil med syfte att ta filer som gisslan för att sedan pressa informationsägaren på pengar och på så vis återfå filerna.

— Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
— Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
— Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
— Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?
— Finns fastställda metoder för riskhantering och har informationssäkerhetsrisker beaktats och följts av åtgärder?
— Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?
— Har kommunstyrelsen säkerställt en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser?
— Finns en tillräcklig uppföljning och återrapportering av kommunens informationssäkerhetsarbete?

2.2 Avgränsning

Granskningen inriktas till kommunstyrelsens övergripande ansvar för styrning och uppföljning av informationssäkerhet. Avstämningar kan dock behöva göras med representanter från övriga nämnders verksamheter för att verifiera uppgifter.

Avgränsningen omfattar både organisatorisk säkerhet och teknisk säkerhet.

Granskningen omfattar år 2024. Granskningen avser kommunstyrelsen.

2.3 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

— Kommunallagens 6 kap. 6 §
— Tillämpbara interna regelverk, policys och beslut
— MSB:s metodstöd och rekommendationer avseende Ledningssystem för informationssäkerhet och it-säkerhetsåtgärder
— Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där detta är tillämpbart

2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstepersoner och politiker. Dokumentgranskningen har omfattat dokument så som reglemente, it-policy, styrdokument avseende krisberedskap, civilt försvar, säkerhet samt säkerhetsskydd, kommunstyrelsens protokoll samt andra rutindokument som framgår av rapporten.

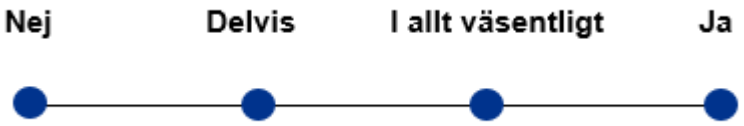
Intervjuer har genomförts med:

- It-chef
- Säkerhetsskyddschef

- Kommundirektör
- Kommunstyrelsens presidium

Samtliga medverkande har erhållits möjlighet att faktakontrollera rapporten.

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



3 Resultat av granskningen

3.1 Ledningssystem för informationssäkerhet

Den 24 april 2024 presenterade kommunens it-chef en uppdragsbegäran[2] för kommunstyrelsens ledningsutskott angående utredning av införande av ett övergripande systematiskt arbete med informationssäkerhet. Ledningsutskottet beslutade att bevilja uppdraget, vilket tilldelades it-chefen.

Uppdraget innebär att kartlägga informationstillgångar i form av system som nyttjas i verksamheterna. Därtill innebär uppdraget att utreda kommunens nuvarande organisation i syfte att identifiera eventuella resursbehov inom informationssäkerhetsarbetet.

3.1.1 Styrande dokument

Kommunen saknar vid tid för granskningen en informationssäkerhetspolicy med tillhörande riktlinjer som beskriver hur informationssäkerhetsarbetet ska bedrivas.

Kommunfullmäktige har under 2023 antagit en it-policy[3]. Policyn definierar kommunens it-miljö samt de centrala standarder, metoder och säkerhetsaspekter som styr både administratörers och användares beteende inom it-frågor. Målet med kommunens it-avdelning är att stötta Skinnskattebergs kommuns verksamheter och det framgår att avdelningen arbetar mot en standardiserad it för att höja säkerheten i drift. Av it-policyn framgår även huvudprinciper för bruk av Skinnskattebergs kommuns it-system samt att policyn omfattar samtliga som i någon form nyttjar kommunens it-system.

3.1.2 Roller och ansvar

Då det saknas styrande dokument som avser informationssäkerhetsarbetet saknas även en dokumenterad ansvarsfördelning samt rollbeskrivning. Av kommunstyrelsens reglemente[4] framgår att kommunstyrelsen ska följa de frågor som kan inverka på kommunens utveckling och ekonomiska ställning. Av kommunens styrdokument avseende bland annat krisberedskap, civilt försvar, säkerhet samt säkerhetsskydd[5] framgår att kommunstyrelsens övergripande uppgifter bland annat är att ansvara för interna säkerhetsfrågor och säkerhetskyddsfrågor i kommunen.

Det saknas i Skinnskattebergs kommun en informationssäkerhetssamordnare med syfte att driva informationssäkerhetsarbetet framåt.

Kommunen har en egen it-avdelning bestående av en it-chef samt tre medarbetare. Som tidigare nämnts har it-chefen tilldelats uppdraget att utreda införande av ett systematiskt informationssäkerhetsarbete. Uppdraget genomförs tillsammans med kommunens säkerhetsskyddschef.

[2] Uppdragsbeskrivning, It-chef, 2024-02-29
[3] It-policy, kommunfullmäktige, 2023-10-16
[4] Reglemente för kommunstyrelsen, kommunfullmäktige, senast reviderat 2021-06-07
[5] Styrdokument 2023–2026 avseende krisberedskap, civilt försvar, säkerhet samt säkerhetsskydd, kommunfullmäktige, 2019-12-16

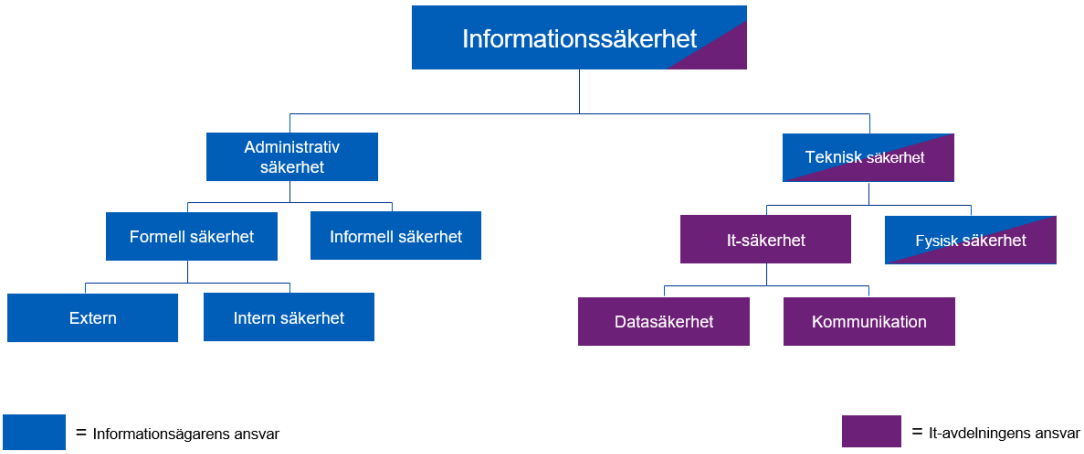


Bild 1. Bilden visar ansvarsfördelningen för informationssäkerheten mellan informationsägare och it-avdelningen.

Ansvaret för den information som hanteras i en verksamhet tillfaller verksamhetsansvariga. Verksamhetsansvarig är även informationsägare. Detta innebär att ansvaret för att ett tillräckligt arbete för en god informationssäkerhet tillfaller verksamhetsansvariga.

Bilden ovan beskriver hur ansvarsfördelning mellan verksamhetsansvarig (informationsägare) och it ser ut. Verksamhetsansvariga ansvarar för att genom genomförda riskanalyser och klassning av system och information identifiera vilka säkerhetsåtgärder som behöver vidtas för att informationen ska vara skyddad. It-avdelning ansvarar för att de *tekniska* säkerhetsåtgärder som identifierats av verksamheten implementeras.

Intervjuade uppger att ansvaret till viss del är känt hos verksamhetsansvariga (i detta fall förvaltningschefer), men att det saknas tydlig kravställning utifrån styrande dokument vilket innebär att ansvaret inte upprätthålls vid tid för granskningen.

Enligt muntliga uppgifter finns en systemförvaltarorganisation i kommunen med roller så som systemägare och systemansvarig. Vi har inte tagit del av någon dokumenterad beskrivning av systemförvaltarorganisationen.

3.1.3 Informationssäkerhetsmål

Det saknas antagna mål för kommunens informationssäkerhetsarbete.

3.1.4 Bedömning

Vår bedömning är att det inte finns styrande dokument som tydliggör ansvar, vilka krav som ställs samt hur arbetet ska bedrivas.

Vi kan konstatera att det finns en it-policy. Dock omfattar den endast den it-tekniska säkerheten, vilket innebär att det saknas styrande dokument avseende den administrativa säkerheten. I MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete framgår att ledningen i en organisation bör säkerställa att organisationen antar en policy för informationssäkerhetsarbetet. Vi

bedömer att det utöver policy finns behov av vägledande riktlinjer för hur arbetet med informationssäkerhet ska bedrivas i kommunen.

Vi bedömer att det saknas en ändamålsenlig organisation för informationssäkerhetsarbetet.

Kommunen har inte utsett en informationssäkerhetssamordnare med ansvar att driva informationssäkerhetsarbetet framåt i enlighet med MSB:s metodstöd.

Vår bedömning bygger även på att ansvaret för informationssäkerhet vid tid för granskningen inte tillämpas hos verksamhetsansvariga, vilket kan vara en följd av att det saknas tydlig kravställning och stöd från centralt håll genom exempelvis styrande dokument.

Vi ser positivt på att it-chefen tagit initiativ till att lyfta behovet av ett systematiskt informationssäkerhetsarbete till kommunstyrelsen men anser att styrelsen ska säkerställa att en funktion utses i enlighet med MSB:s rekommendationer, för att kunna tillförsäkra att ett systematiskt informationssäkerhetsarbete etableras.

Vi kan konstatera att det saknas beslutade informationssäkerhetsmål med tillhörande handlingsplaner.

Det saknas både strategiska och mer operativa mål för informationssäkerhetsarbetet. Vi anser att kommunstyrelsen behöver ta ett större ansvar angående styrning av kommunens informationssäkerhetsarbete i enlighet med det ansvar som regleras i reglemente samt styrdokument.

3.2 Säkerhetskultur

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet.

Vid nyanställning genomgår samtliga medarbetare en utbildning i GDPR[6]. Vid utlämnande av it-utrustning tar de nyanställda även del av rutinbeskrivningar för hur utrustningen får hanteras.

Utöver detta informerar it-avdelningen via intranätet och e-postmeddelande om aktuella risker och upplyser medarbetarna att vara uppmärksamma.

Det har även enligt muntliga uppgifter genomförts informationsinsatser på verksamheternas arbetsplatsträffar.

Kommunen har sett över möjligheterna att införa en digital utbildning men har ännu inte infört någon sådan.

Vid intervjuer framkommer att det finns stora behov av att stärka säkerhetskulturen inom kommunen, så att hantering av information sker på ett säkert sett utifrån flera perspektiv så som konfidentialitet, riktighet och tillgänglighet.

[6] General Data Protection regulation

3.2.1 Bedömning

Vi bedömer att styrelsen inte har tillsett att det finns en tillräcklig säkerhetskultur.

Vår bedömning är att kommunstyrelsen bör säkerställa att det genomförs utbildning samt andra nödvändiga insatser för samtliga medarbetare samt förtroendevalda i kommunen som en del i att stärka säkerhetskulturen. Bristande medvetenhet och kunskap om hot och risker inom informationssäkerhet kan i värsta fall leda till att kommunens information och system utsätts för risk och allvarliga konsekvenser, både ekonomiska och förtroendeskadliga.

Ständig utbildning och kommunikation höjer medvetenheten och kunskapen om informationssäkerhet hos medarbetare och förtroendevalda. Därtill bidrar det till en ökad acceptans av och förståelse för de säkerhetsåtgärder som implementeras i organisationen.

3.3 Riskhantering

3.3.1 Riskanalys

Enligt MSB:s metodstöd ska en verksamhet identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen.

Som tidigare nämnts saknas styrande dokument inom granskningsområdet, vilket innebär att det även saknas reglering och kravställning avseende hur arbetet med riskanalys ska se ut.

Intervjuade uppger att det har genomförts en kommunövergripande risk- och sårbarhetsanalys där informationssäkerhetsrisker har beaktats. Det har inte genomförts riskanalyser på verksamhetsnivå.

Vid genomförande av granskningen saknas en kommunövergripande internkontrollplan för år 2024.

3.3.2 Informationsklassning

Enligt MSB:s metodstöd är informationsklassning en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Det saknas inom kommunen dokumenterad styrning och en antagen modell för arbetet med att informationsklassa informationstillgångar.

Intervjuade uppger att arbetet med att informationsklassa kommunens informationstillgångar är eftersatt och det saknas enligt uppgift en överblick angående hur stor andel av de informationstillgångar som hanteras i kommunen som genomgått klassning. De system som genomgått klassning är inom de verksamheter som identifierats som samhällsviktig.

It-avdelningen medverkar till viss del vid nyanskaffning av system och intervjuade uppger att det i sådana fall genomförs klassning av det system som upphandlingen omfattar. Det saknas dokumenterade rutiner för detta vilket intervjuade uppger behöver införas i syfte att säkerställa att klassning genomförs innan upphandlingen äger rum.

3.3.3 Åtgärdsplan

Enligt MSB:s metodstöd ska identifierade behov av säkerhetsåtgärder dokumenteras i en åtgärdsplan.

Det saknas upprättade åtgärdsplaner.

3.3.4 Bedömning

Vi kan konstatera att det saknas fastställda metoder för riskhantering samt att informationssäkerhetsrisker inte har beaktats och följts av åtgärder.

Bedömningen bygger på att det saknas genomförda analyser där informationssäkerhetsrisker har beaktats samt att det saknas genomförda informationsklassningar av informationstillgångarna. Kommunstyrelsen har därmed inte kontroll över de sårbarheter som finns och de informationssäkerhetsrisker som skulle kunna inträffa. Utifrån detta finns även en risk för att konfidentialitet, riktighet och tillgänglighet inte kan säkerställas.

Därtill är vår bedömning att styrande dokument ska reglera att riskbedömning och informationsklassning ska genomföras i samband med anskaffning av nya system samt att it-avdelningen ska medverka vid upphandling utifrån behov. Detta som en del i att minska risken för att ett undermåligt system implementeras i kommunens it-mijö.

3.4 It-tekniska säkerhetsåtgärder

3.4.1 Riskanalys och implementerade åtgärder

Intervjuade anger att vidtagna säkerhetsåtgärder grundas i av it-avdelningen genomförda riskanalyser genom bland annat omvärldsbevakning, erfarenhet samt vedertagen praxis i syfte att säkerställa en säker it-miljö. Då riskanalyserna inte har dokumenterats har vi inte kunnat tagit del av dem.

Omvärldsbevakningen består bland annat av informationsinhämtning samt rekommendationer från experter inom it-området som exempelvis it-leverantörer.

En åtgärd som genomförts är att segmentera nätverken som finns i kommunen, som en del i att minska risken för att ett eventuellt intrång sprids till andra nätverk. Detta innebär att dela uppnätverken i flera, för att minska risken för att ett eventuellt intrång når andra nätverk i it-miljön.

Därtill har tvåfaktorautentisering[7] införts för samtliga medarbetare i kommunen. Skyddsåtgärden finns även implementerad på de datorer som nyttjas av flera medarbetare, där en portabel identifikationslösning ska säkerställa användarens identitet.

Det är it-avdelningen som ansvarar för att byta ut it-utrustning i form av datorer och telefoner i hela kommunen utifrån utrustningens livscykel. När utrustningen inte längre kan installera nya uppdateringar sker därför ett byte initierat av it-avdelningen. Beställning av ny it-utrustning genomförs via en blankett på intranätet som hanteras av it-avdelningen. Medarbetarna saknar möjlighet att installera programvaror eller applikationer på datorer och telefoner. Därtill har it-avdelningen möjlighet att fabriksåterställa[8] utrustning som tappats bort eller blivit stulen.

För att kunna återläsa information som gått förlorad sker kontinuerlig backup på den information som hanteras i systemen.

3.4.2 Bedömning

Vår bedömning är att säkerhetsåtgärder har vidtagits och att de delvis står i relation till aktuella hot och risker. Vi kan konstatera att åtgärderna inte utvärderas med regelbundenhet.

Vår bedömning är att genomförd omvärldsanalys behöver kompletteras med underlag så som genomförd riskanalys och informationsklassning från kommunens verksamheter för att säkerställa att skyddet är i relation till aktuella hot och risker. Mot bakgrund av detta kan vi inte fullt ut bedöma om vidtagna åtgärder är i enlighet med aktuella hot och risker. Avsaknad av underlag kan även innebära att informationstillgångarna överskyddas vilket kan utgöra en onödig kostnad för kommunen.

3.5 Incidenthantering

3.5.1 Övervakning och loggar

It-avdelningen har tecknat ett avtal med en it-leverantör avseende funktionen SOC[9] som omfattar kommunens samtliga system. En sådan funktion spårar, upptäcker, analyserar samt reagerar på en eventuell it-säkerhetshändelse i ett system eller ett nätverk.

It-avdelningen kan genom funktionen även få ut loggar där det framgår hur många intrångsförsök som kommunens system har haft. Med hjälp av experter från it-leverantörer analyseras loggarna i syfte att identifiera eventuella behov av åtgärder.

[7] Tvåfaktorautentisering innebär att användaren bekräftar sin identitet genom en kod eller liknande som komplement till inloggning genom lösenord.
[8] Återställa telefonen till standardinställningar där personliga uppgifter inte längre är sparade i telefon.
[9] Security Operations Center

3.5.2 Anmälan, analys och dokumentation av incidenter

Vi har tagit del av en rutinbeskrivning för anmälan av personuppgiftsincidenter. I rutinerna finns beskrivning om när anmälan till IMY[10] ska ske samt vad den ska omfatta. Av dokumentet framgår inte om samma rutiner gäller vid anmälan av andra informationssäkerhetsincidenter eller it-säkerhetsincidenter.

För anmälan om misstanke om eller en inträffad incident eller säkerhetshändelse finns it-avdelningens Helpdesk tillgängligt på intranätet. I samband med anmälan anger anmälaren vilken typ av händelse som de anser har inträffat, ex. it-incident, personuppgiftsincidenter eller lex Maria.

Efter en inträffad incident har ägt rum ska en incidentrapport fyllas i enligt uppgift. Intervjuade uppger att det saknas systematik i arbetet med att dokumentera och analysera inträffade incidenter.

3.5.3 Reserv- och återgångsrutiner

Vid avbrott i elförsörjningen finns åtgärder för att säkerställa strömförsörjning genom reservkraft inom vissa delar av kommunens verksamhet.

It-avdelningen har internt en prioriteringslista över nätverk och system i kommunen vid uppstart av it-infrastrukturen efter ett avbrott.

Dessa reserv- och återgångsrutiner har testats och justerats utifrån behov. I faktakontrollen framgår även att rutinerna har nyttjats i skarpt läge med resultat att rutinerna fungerade som förväntat.

3.5.4 Bedömning

Vi bedömer att det delvis finns en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser.

Bedömningen grundas i att kommunstyrelsen via it-avdelningen har säkerställt förmågan genom en teknisk lösning för att upptäcka och hantera en händelse i kommunens it-miljö. Därtill är vår bedömning att det sker ett systematiskt analysarbete avseende inträffade it-säkerhetshändelser.

Vi konstaterar dock att det finns risk för en bristande förmåga att upptäcka och hantera informationssäkerhetsincidenter internt i kommunen. Detta då rutiner och etablerade arbetssätt saknas för incidenthantering tillsammans med tidigare konstaterade risker avseende avsaknad av tillräcklig säkerhetsmedvetenhet och otydliga roller och ansvar i informationssäkerhetsarbetet. Därtill finns en risk för att efterföljande analysarbete samt dokumentation av händelsen inte genomförs då det saknas krav om detta.

[10] Integritetsskyddsmyndigheten

3.6 Uppföljning och återrapportering

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i kommunen behöver det enligt MSB:s metodstöd ske en kommunövergripande uppföljning av arbetet som rapporteras under ledningens genomgång. Uppföljning utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning.

3.6.1 Uppföljning

Då kommunen är i ett tidigt stadie av etableringsfasen för införandet av ett systematiskt informationssäkerhetsarbete saknas det ett etablerat uppföljningsarbete.

3.6.2 Ledningens genomgång och annan återrapportering

Ledningens genomgång är inte infört i kommunen.

Intervjuade uppger att kommunstyrelsen inte har erhållit någon kontinuerlig återrapportering av arbetet då det nyligen initierats att utreda implementering av ett systematiskt informationssäkerhetsarbete.

Vi kan av dagordning konstatera att kommunstyrelsen på sammanträdet i juni 2024 informerades om NIS2[11], vilket kommer att ersätta det NIS-direktiv som började gälla genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Av kommunstyrelsens protokoll framgår en stående punkt på dagordningen där rapportering ska ske av inträffade personuppgiftsincidenter.

3.6.3 Bedömning

Vår bedömning är att det saknas ett etablerat uppföljningsarbete och vi kan konstatera att det inte har skett någon återrapportering till kommunstyrelsen avseende kommunens informationssäkerhetsarbete.

Bedömningen grundas i att det i kommunen saknas ett etablerat uppföljningsarbete. Det är av stor vikt att kommunstyrelsen erhåller en kontinuerlig återrapportering som utgör underlag för att kunna fatta beslut om erforderliga åtgärder i syfte att stärka kommunens robusthet.

[11] The Directive on security of network and information system – även förkortat the NIS Directive, är ett direktiv från EU i syfte att stärka medlemsländernas cybersäkerhet.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelsen tillsett att det bedrivs ett systematiskt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att det inte bedrivs ett systematiskt informationssäkerhetsarbete.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Verka för att kommunfullmäktige antar en informationssäkerhetspolicy.
- Till policyn upprätta och anta tillhörande riktlinjer och instruktioner som omfattar ansvarsfördelning samt hur informationssäkerhetsarbetet ska bedrivas.
- Anta en kommungemensam modell för riskbedömning och informationsklassning samt säkerställa att den etableras.
- Säkerställa att riskbedömning av kommunens informationstillgångar genomförs.
- Tillse att en åtgärdsplan upprättas utifrån identifierade åtgärdsbehov.
- Tillse att incidentrutiner dokumenteras, som omfattar eskaleringsvägar samt former för hur inträffade incidenter ska analyseras och dokumenteras.
- Tillse att ett uppföljningsarbete etableras samt att styrelsen erhåller kontinuerlig återrapportering angående kommunens informationssäkerhetsarbete.

Datum som ovan

KPMG AB

Maria Schultz
Kundansvarig

Ida Larsson
Verksamhetsrevisor

Jenny Thörn
Verksamhetsrevisor, Specialist