Uppföljande granskning av IT-säkerhet

Rapport

Eskilstuna kommun

KPMG AB

2022-06-27

Antal sidor 10

Eskilstuna kommun
Uppföljande granskning av IT-säkerhet

2022-06-27

Innehållsförteckning

1 Sammanfattning

Vi har av Eskilstuna kommuns revisorer fått i uppdrag att följa upp den tidigare genomförda granskningen av kommunens arbete med IT-säkerhet från 2019. Uppdraget ingår i revisionsplanen för år 2022.

Det övergripande syftet med granskningen har varit att följa upp hur de rekommendationer som lämnats av kommunens revisorer i tidigare genomförd granskning har beaktats av kommunstyrelsen.

Vår sammanfattande bedömning är att kommunstyrelsen i hög grad har beaktat de tidigare lämnade rekommendationerna avseende kommunens IT-säkerhet och vidtagit åtgärder för att förbättra kommunens arbete.

Därtill är vår bedömning att kommunstyrelsen har vidtagit åtgärder utifrån den förhöjda hotbild som råder med ökning av angrepp och intrångsförsök.

Utifrån uppföljningen bedömer vi att följande rekommendation kvarstår:

— Som ett krav för kommunens samtliga förvaltningsobjekt säkerställa att arbete med informationssäkerhetsklassning och riskhantering implementeras fullt ut.

2 Bakgrund

Vi har av Eskilstuna kommuns revisorer fått i uppdrag att följa upp den tidigare genomförda granskningen av kommunens arbete med IT-säkerhet från 2019. Uppdraget ingår i revisionsplanen för år 2022.

Sårbarheter inom IT-säkerhet har uppmärksammats den senaste tiden. Kommuner och regioner har på olika sätt utsatts för IT-attacker vilket orsakat stora problem i verksamheten och inneburit betydande ekonomiska- och verksamhetsrelaterade konsekvenser.
SKR har även uppmärksammat vikten av att kommuner och regioner har en tillfredställande intern kontroll gällande sin säkerhet av IT-verksamhet.

Kommunrevisionen har efter avslutad granskning 2019 lämnat ett antal rekommendationer efter att förbättringsområden identifierats. Styrelsen har därefter svarat kommunrevisionen. För att få en uppfattning i vilken omfattning rapporterna och rekommendationerna tagits tillvara av kommunstyrelsen är en uppföljande granskning viktig att genomföra. Resultatet kan i sin tur ligga till grund för kommande riskanalysarbete.

I tidigare genomförd granskning identifierades brister i kommunens IT-säkerhetsarbete. Sammanfattningsvis bedömde granskningen att kommunstyrelsen inte hade säkerställt ett ändamålsenligt och systematiskt arbete med IT- och informationssäkerhet.

Med hänsyn till uppmärksammade IT-risker har Eskilstuna kommuns revisorer i sin riskanalys dragit slutsatsen att efterlevnaden av kommunrevisionens lämnade rekommendationer behöver granskas avseende åtgärder för att säkerställa en tillräcklig IT-säkerhet.

2.1 Syfte och avgränsning

Det övergripande syftet med granskningen har varit att följa upp hur de rekommendationer som lämnats av kommunens revisorer i tidigare genomförda granskning beaktats av kommunstyrelsen.

De svar vi har efterfrågat i vår uppföljning är:

- Vilka åtgärder har styrelsen vidtagit med anledning av respektive rekommendation?
- Vilken status har eventuella förändringsarbeten med anledning av givna rekommendationer?
- Hur är aktuellt nuläge gällande IT-säkerheten utifrån uppmärksammade brister inom kommuner och regioner?

Granskningen omfattar kommunstyrelsen.

2.2 Revisionskriterier

Utgångspunkt för uppföljning har varit granskningsrapport för kommunens IT-säkerhet från 2019. Vi har utifrån rapporten efterfrågat svar på vilka åtgärder som vidtagits med anledning av revisionsrapporten. För att verifiera uppgifter har vi tagit del av revisionsbevis i form av styrdokument, planer och rutiner.

2.3 Metod

Granskningen har genomförts genom en gruppintervju med utvalda tjänstepersoner samt en översiktlig granskning av styrande dokument. Därtill har kommunstrateg informationssäkerhet förevisat intranät och andra stödprocesser som etablerats i kommunens informations- och IT-säkerhetsarbete.

Verksamhetsföreträdare har beretts möjlighet att faktagranska rapporten.

3 Resultat av granskningen

3.1 Tidigare genomförd granskning av IT-säkerhet

2019 beslutade de förtroendevalda revisorerna i Eskilstuna kommun att granska kommunens IT-säkerhet.

Granskningen genomfördes genom dokumentstudier, intervjuer med berörda tjänstemän samt en sårbarhetsscanning. Det tekniska testet genomfördes i syfte att granska del av kommunens tekniska miljö för att identifiera eventuella sårbarheter.

Sammanfattningsvis bedömdes i granskningen att kommunstyrelsen inte hade säkerställt ett ändamålsenligt och systematiskt arbete med IT- säkerhet. Flertalet av kommunens styrdokument var ofullständiga, föråldrade och inte fullt ut tillämpbara i den dåvarande organisationen. Därtill identifierades ett starkt personberoende kopplat till centralt utsedda roller. Granskningen bedömde vidare att verksamheterna inte tagit sitt ansvar för att skydda sina informationstillgångar och att informationssäkerhetsarbetet inte var integrerat i övriga styrprocesser. Kommunen hade vid tiden för granskningen påbörjat ett arbete med informationsklassning, arbetet bedömdes däremot inte vara fullt ut implementerat eller systematiskt. Därutöver såg granskningen särskilt allvarligt på att verksamheterna tillät personal att använda datorer och utrustning som inte tillhandahållits av IT-avdelningen.

Under granskningen genomfördes en sårbarhetscanning för att identifiera svagheter i två av kommunens interna nätverk. Testet identifierade ett flertal sårbarheter avseende upprättad IT-säkerhet. Merparten av dessa svagheter grundade sig i ett behov av att uppdatera programvara.

Utifrån granskningsresultatet gav revisionen följande rekommendationer:

1. Säkerställa att styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter revideras och uppdateras.
2. Säkerställa att roller och ansvar mellan verksamheten, kommunstrateg, informationssäkerhet och IT tydliggörs.
3. Säkerställa att IT-avdelningen har kontroll över och ansvar för samtliga datorer som används i kommunens IT-miljö genom att dessa tillhandahålls med den paketering som är nödvändig utifrån ansvaret för IT-säkerhet
4. Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret inom Eskilstuna kommun.
5. Som ett krav för kommunens samtliga förvaltningsobjekt säkerställa att arbete med informationssäkerhetsklassning och riskhantering implementeras fullt ut.
6. Säkerställa att kunskap finns och rutiner är kända över hantering och rapportering av informationssäkerhetsincidenter.
7. Säkerställa att tekniska kontroller implementeras samt att identifierade sårbarheter från sårbarhetsscanningen bedöms och åtgärdas för att skydda Eskilstuna kommuns nätverk och motverka intrång.

Kommunstyrelsen beslutade vid sammanträde 2021-02-16 om ett yttrande till granskningen. Kommunstyrelsen har i yttrandet angett att KPMG:s iakttagelser och rekommendationer var relevanta utifrån rådande situation och att åtgärder för att minska identifierade brister skulle påbörjas omgående, om de inte redan hade startat. Kommunledningskontoret uppdrogs att genomföra de åtgärder som föreslogs i tjänsteskrivelsen.

3.2 Uppföljning av identifierade brister och lämnade rekommendationer

3.2.1 Rekommendation 1

Säkerställa att styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter revideras och uppdateras.

Vidtagna åtgärder

2021-06-23 antog kommunfullmäktige ett nytt styrdokument för kommunens informationssäkerhet. Riktlinje för informationssäkerhet som ersätter den Informationssäkerhetsplan som var föremål för granskning 2019. Riktlinjen anger kommunens inriktning, mål och övergripande principer avseende informationssäkerhetsarbetet. Därutöver anges även roller och definitioner inom informationssäkerhetsområdet. Detta dokument gäller för hela kommunkoncernen.

Anvisningar för informationssäkerhet har fastställts i syfte att konkretisera riktlinjen. Detta dokument innehåller detaljerad information och regler avseende informationshantering inom kommunen. Anvisningarna är tänkta att användas som en uppslagsbok av kommunens anställda och på så sätt säkra tillgången på relevant information rörande informationshantering ur ett informationssäkerhetsperspektiv.

Anvisningarna är uppdelade från A-D. Avsnitt A behandlar informationssäkerhet för medarbetare. B, styrning av informationssäkerhet. C, informationssäkerhet i verksamhetsnära förvaltning och D, informationssäkerhet i IT-miljön. Dokumentet innehåller information för medarbetarna om bland annat ansvar, skyldigheter och informationsklassning. Det finns också verksamhetsspecifika rutiner och instruktioner framtagna av förvaltningen, avsedda för praktisk hantering av information.

3.2.1.1 Bedömning

Vi bedömer att kommunstyrelsen har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation.

3.2.2 Rekommendation 2

Säkerställa att roller och ansvar mellan verksamheten, kommunstrateg, informationssäkerhet och IT tydliggörs.

Vidtagna åtgärder

Som en del i kommunens Anvisningar för informationssäkerhet finns en rollbeskrivning. Bland annat tydliggörs vem som är informationsägare och vilket ansvar de olika rollerna i informationssäkerhetsarbetet innehar. Av intervju med berörda tjänstemän framgår att arbetet förvisso är en ständigt pågående process, men att man i nuläget lagt en god grund avseende tydliggörande av roller och ansvar.

3.2.2.1 Bedömning

Vi bedömer att kommunstyrelsen har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation. Dock är vår uppfattning att ansvar och roller inom de olika avdelningarna för IT-*verksamhet och digitalisering ytterligare kan tydliggöras.*

3.2.3 Rekommendation 3

Säkerställa att IT-avdelningen har kontroll över och ansvar för samtliga datorer som används i kommunens IT-miljö genom att dessa tillhandahålls med den paketering som är nödvändig utifrån ansvaret för IT-säkerhet.

Vidtagna åtgärder

Kommunen arbetar i nuläget med att införa ”Klient som tjänst”, vilket innebär att datorer och på sikt även surfplattor och mobiltelefoner endast kommer att tillhandahållas av IT-avdelningen. Kommunen har även infört åtgärder i sitt nätverk, vilket innebär att det inte är möjligt att få tillgång till kommunens nät utan utrustning som är godkänd med certifikat från kommunen.

3.2.3.1 Bedömning

Vi bedömer att kommunstyrelsen har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation.

3.2.4 Rekommendation 4

Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret inom Eskilstuna kommun.

Vidtagna åtgärder

Kommunen har tagit fram en utbildning som lanserades i slutet av 2021. Utbildningen riktar sig till samtliga medarbetare i kommunkoncernen och är tänkt att förse dem med en grundläggande kunskap avseende informations- och IT-säkerhet. Utbildningen är obligatorisk och är möjlig att genomföra antingen digitalt eller genom sessioner som hålls gruppvis, exempelvis på arbetsplatsträffar. Uppföljningen av den digitala utbildningen görs kontinuerligt, men vad gäller grupputbildningarna arbetar kommunen i nuläget fram en uppföljningsprocess.

3.2.4.1 Bedömning

Vi bedömer att kommunstyrelsen har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation. Vi ser positivt på att en kommunövergripande utbildning även ges gruppvis och således passar även de medarbetare med mindre datorvana och delar kommunens uppfattning att även uppföljningsrutiner för dessa bör inrättas.

3.2.5 Rekommendation 5

Som ett krav för kommunens samtliga förvaltningsobjekt säkerställa att arbete med informationssäkerhetsklassning och riskhantering implementeras fullt ut.

Vidtagna åtgärder

Av Anvisningar informationssäkerhet framgår att kommunen arbetar efter en informationsklassningsmodell. Kommunen har fyra informationsklasser, öppen, intern, konfidentiell och hemlig. Av dokumentet framgår hantering av respektive informationsklass i större detalj.

Av intervjuer framgår att kommunen inlett ett arbete i enlighet med rekommendationen, men att det upplevs tungrott. Arbetets status är pågående och uppdragsledare har utsetts. Projektet utgår från SKR:s[1] rekommendationer avseende informationsklassning. En misstanke till varför arbetet upplevs tungrott tros vara dels att obejktförvaltningsorganisationen (PM[3]) ännu inte inarbetats i verksamheterna, dels att systemförvaltarna konsoliderats till en enhet.

3.2.5.1 Bedömning

Vi bedömer att kommunstyrelsen till viss del har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation. Det är positivt att kommunen beslutat om en modell för klassning och att arbetet har påbörjats. Vi rekommenderar att kommunstrateg för informationssäkerhet får i uppdrag att undersöka vilka behov av stöd som förvaltningarna skulle behöva för att arbetet med informationsklassningar och riskanalyser ska bli mer systematiskt.

3.2.6 Rekommendation 6

Säkerställa att kunskap finns och rutiner är kända över hantering och rapportering av informationssäkerhetsincidenter.

Vidtagna åtgärder

I Anvisningar för informationssäkerhet beskrivs kommunens incidenthantering. Ansvarsfördelningen framgår och att incidenter rangordnas efter allvarsgrad. I dokumentet beskrivs hantering av incidenter. I samma sektion av dokumentet beskrivs även kontinuitetsplaner.

Vi har i uppföljningen fått en visning av det system som IT-avdelningen har infört för att hantera incidenter. Då alla incidenter anmäls i systemet kan en analys göras av inträffade incidenter. Ett flertal nyckelfunktioner i kommunen med ansvar inom

[1] Sveriges kommuner och regioner

informationssäkerhet och IT analyserar gemensamt statistiken för att kunna se vilken typ av angreppsförsök som är aktuella i nuläget. IT-avdelningen har därtill inrättat interna rutiner och processer för incidenthantering som leds av en utsedd incident manager. Det är incident manager som vid behov hanterar eskalering av incidenter.

3.2.6.1 Bedömning

Vi bedömer att kommunstyrelsen har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation. Vi ser positivt på att kommunen analyserar statistik över incidenter och angreppsförsök och att den utbildningen som getts i kommunen tycks ha ökat benägenheten att rapportera incidenter.

3.2.7 Rekommendation 7

Säkerställa att tekniska kontroller implementeras samt att identifierade sårbarheter från sårbarhetsskanningen bedöms och åtgärdas för att skydda Eskilstuna kommuns nätverk och motverka intrång.

Vidtagna åtgärder

De sårbarheter som identifierats i den föregående granskningen har åtgärdats och det framgår av intervju att kommunen numera har infört interna verktyg för sårbarhetsskanning.

Av intervju framgår vidare att det finns ett behov av systematik i arbetet avseende att hålla system och digital utrustning uppdaterade. Vidare framgår att kommunen utefter det förändrade säkerhetsläget intensifierat sin omvärldsbevakning och utbildningsinsatser avseende informationssäkerhet. Efter Rysslands invasion av Ukraina sammanställde kommunen en lista på prioriterade initiativ. Exempelvis så tidigarelade kommunen segmentering av sina nätverk i och med förändringen i säkerhetsläget. Utifrån incidenten i Kalix kommun inledde kommunen ett arbete där det ingick att identifiera kritiska verksamhetssystem och hur detta skulle påverkas av IT-bortfall.

3.2.7.1 Bedömning

Vi bedömer att kommunstyrelsen har vidtagit åtgärder i enlighet med tidigare lämnad rekommendation. Därtill är vår bedömning att kommunstyrelsen har vidtagit åtgärder utifrån den förhöjda hotbild som råder med ökning av angrepp och intrångsförsök.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning är att kommunstyrelsen i hög grad har beaktat de tidigare lämnade rekommendationerna avseende kommunens IT-säkerhet och vidtagit åtgärder för att förbättra kommunens arbete. Därtill är vår bedömning att kommunstyrelsen har vidtagit åtgärder utifrån den förhöjda hotbild som råder med ökning av angrepp och intrångsförsök.

4.1 Rekommendationer

Utifrån uppföljningen bedömer vi att följande rekommendation kvarstår:

— Som ett krav för kommunens samtliga förvaltningsobjekt säkerställa att arbete med informationssäkerhetsklassning och riskhantering implementeras fullt ut.

Datum som ovan

KPMG AB

Jenny Thörn	William Andreasson	Mikael Lind
Kommunal revisor	*Kommunal revisor*	*Certifierad kommunal revisor*