Till:
Kommunstyrelsen, Kungälvs kommun

För kännedom till:
Kommunfullmäktige, Kungälvs kommun

Granskningsrapport ”Rapportering av granskning av kommunens informationssäkerhet”

De förtroendevalda revisorerna i Kungälvs kommun har givit KPMG uppdraget att genomföra en granskning av kommunens informationssäkerhet. I bifogade rapport redovisas resultatet av den utförda granskningen, inklusive KPMG:s slutsats och rekommendationer.

Granskningens syfte har varit att bedöma om kommunstyrelsen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt informationssäkerhetsarbete i kommunen.

KPMG:s sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen i huvudsak har en tillräcklig intern styrning av informationssäkerhetsarbetet, men att kontrollen behöver stärkas i syfte att säkerställa ett ändamålsenligt och systematiskt informationssäkerhetsarbete i kommunen.

Utifrån KPMG:s granskning rekommenderas kommunstyrelsen att:

- Säkerställa att informations- och systemägaransvaret etableras i samtliga verksamheter så att aktiviteter genomförs i enlighet med krav i styrande dokument.
- Fastställa hur kommunen i förhållande till externa leverantörer ska hantera de tekniska krav som kommunen beslutat som gällande i informationssäkerhetsarbetet.
- Revidera avtal med extern IT-driftsleverantör där informationssäkerhetskrav tydliggörs tillsammans med former för avtalsuppföljning.
- Tydliggöra mandat och uppdrag för informationssäkerhetsgruppen.
- Säkerställa att efterlevnadskontroller ingår i årlig uppföljning och rapportering av informationssäkerhetsarbetet.
- Säkerställa att incidenthanteringsrutiner är kända och tillämpas av samtliga verksamheter. Inträffade incidenter bör dokumenteras på övergripande nivå och analyser ingå som underlag i förbättringsarbetet.
- Komplettera incidenthanteringsrutiner med beskrivning över hur incidenter ska samordnas och eskaleras mellan kommunen och extern driftsleverantör, exempelvis Soltak AB.

Vi önskar, senast den 27 mars 2023, kommunstyrelsens skriftliga kommentarer till KPMG:s granskningsrapport och våra synpunkter enligt ovan

Kungälv den 11 januari 2023

För kommunrevisionen

.

Göran Johansson (Jan 12, 2023 09:27 GMT+1)

Göran Johansson
Ordförande

KOMMUNREVISIONEN

KUNGÄLVS KOMMUN

ADRESS Stadshuset · 442 81 Kungälv
TELEFON 0303-23 80 00 vx
FAX 0303-182 59
E-POST kommun@kungalv.se
HEMSIDA www.kungalv.se

Granskning av kommunens informationssäkerhet

Rapport

Kungälvs kommun

KPMG AB

2022-12-20

Antal sidor 24

Bilagor 1

Kungälvs kommun
Granskning av kommunens informationssäkerhet

2022-12-20

Innehållsförteckning

Kungälvs kommun
Granskning av kommunens informationssäkerhet

2022-12-20

1 Sammanfattning

KPMG har av Kungälvs kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Vår sammanfattade bedömning utifrån granskningens syfte är att kommunstyrelsen i huvudsak har en tillräcklig styrning av informationssäkerhetsarbetet men att den interna kontrollen behöver stärkas i syfte att säkerställa ett ändamålsenligt och systematiskt informationssäkerhetsarbete i kommunen.

Kommunstyrelsen har genom beslutade styrdokument etablerat en styrning av informationssäkerhetsarbetet. Det finns en etablerad organisation för kommunens interna informationssäkerhetsarbete med centralt utsedd informationssäkerhetssamordnare för att leda och samordna arbetet. Vår bedömning är dock att det ansvar som åligger informationsägare och systemägare i respektive sektor på ett tydligare sätt behöver etableras i enlighet med det linjeansvar som informationssäkerhetsarbetet utgår från.

Kommunens IT-strateg utgör beställarfunktion från kommunens sida i förhållande till Soltak AB som genom avtal är kommunens IT-driftsleverantör. I det ansvaret ingår även ansvar för IT-säkerhet för kommunens system och information. Styrande dokument inom informationssäkerhet inkluderar kravnivåer för IT-säkerhet. Nuvarande avtal med Soltak AB saknar dock tydliggjorda krav för att säkerställa att leverans sker i enlighet med de tekniska krav som kommunen beslutat som gällande. Detta bör regleras i avtal mellan kommunen och Soltak AB samt med övriga externa leverantörer som kommunen har avtal med för system och digitala tjänster. Efterlevnadskontroller bör därtill inrättas som en del i avtalsuppföljning så att ansvar upprätthålls och leveranser sker i enlighet med ställda informationssäkerhetskrav.

Arbete med riskanalyser och informationsklassningar är i en uppstartsfas och har inte slutförts för de informationstillgångar som hanteras i verksamheternas informationssystem. Det finns till viss del arbetssätt och strukturer för att vidta tekniska åtgärder utifrån genomförda klassningar där en dialog sker med externa leverantörer för att hitta lämpliga säkerhetsåtgärder.

Med utgångspunkt i MSB:s rekommendationer för ökad motståndskraft mot cyberhot har kommunen tillsammans Soltak AB ett pågående arbete med säkerhetshöjande åtgärder för IT-infrastruktur som servrar, nätverk och datorer. Det finns dock behov av utvecklade funktioner för övervakning av IT-miljön för att öka möjligheten att detektera cyberhot och andra säkerhetshändelser.

Incidenthanteringsrutiner har beslutats men är ännu inte kommunicerade till verksamheterna så att det finns kännedom hur incidenter ska hanteras. Rutiner saknar därtill beskrivningar av hur incidenter samordnas när externa leverantörer ansvarar för

drift och förvaltning av system. Vi ser främst ett behov av att detta etableras i förhållande till Soltak AB men även för de systemleverantörer som enskilda verksamheter har avtal med.

Utifrån vår bedömning och slutsats rekommenderas kommunstyrelsen att:

- Säkerställa att informations- och systemägaransvaret etableras i samtliga verksamheter så att aktiviteter genomförs i enlighet med krav i styrande dokument.
- Fastställa hur kommunen i förhållande till externa leverantörer ska hantera de tekniska krav som kommunen beslutat som gällande i informationssäkerhetsarbetet.
- Revidera avtal med extern IT-driftsleverantör där informationssäkerhetskrav tydliggörs tillsammans med former för avtalsuppföljning.
- Tydliggöra mandat och uppdrag för informationssäkerhetsgruppen.
- Säkerställa att efterlevnadskontroller ingår i årlig uppföljning och rapportering av informationssäkerhetsarbetet.
- Säkerställa att incidenthanteringsrutiner är kända och tillämpas av samtliga verksamheter. Inträffade incidenter bör dokumenteras på övergripande nivå och analyser ingå som underlag i förbättringsarbetet.
- Komplettera incidenthanteringsrutiner med beskrivning över hur incidenter ska samordnas och eskaleras mellan kommunen och extern driftsleverantör, exempelvis Soltak AB.

2 Bakgrund

KPMG har av Kungälvs kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om säkerhet avseende den information som hanteras i kommunens IT-system. Alltmer information hanteras idag med olika tekniska lösningar och aldrig förr har kommunerna hanterat sådana mängder information som idag. Informationssäkerhet innebär att skydda information utifrån dess krav på konfidentialitet, riktighet och tillgänglighet i alla kommunens system. För att kunna hantera detta på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget. Informationssäkerhet är inte bara en IT-fråga, utan en fråga om att säkra och trygga driften av kommunens kärnverksamheter.

Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod. Många verksamheter inom kommunen är idag helt beroende av väl fungerande IT. För flera verksamheter handlar ett väl fungerande IT-stöd såväl om säkerhet som möjlighet till en fungerande verksamhet utan driftstörningar. Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd.

Med anledning av ovanstående har kommunens revisorer utifrån sin riskanalys beslutat att arbetet med informationssäkerheten behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningens syfte har varit att bedöma om kommunstyrelsen har en tillräcklig styrning och intern kontroll som säkerställer ett ändamålsenligt och systematiskt informationssäkerhetsarbete i kommunen.

Granskningen ska besvara följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhet?
- Hur arbetar kommunstyrelsen för att säkerställa beställarkompetens gentemot Soltak AB?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?
- Sker en kravställning av IT-säkerhetsåtgärder utifrån genomförd riskbedömning och klassning av informationstillgångar som hanteras i system?

- Finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.)?
- Görs systematiska uppföljningar av implementerade säkerhetsåtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

2.3 Avgränsning

Granskningen omfattar kommunstyrelsen och avser år 2022.

2.4 Revisionskriterier

Vi har bedömt om informationssäkerhetsarbetet uppfyller:

— Kommunallagen 6 kap.1,6 §§
— MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
— Kommunens styrdokument för informationssäkerhet

2.5 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer/avstämningar med berörda tjänstepersoner.

Dokumentstudier har gjorts av:

— Informationssäkerhetspolicy
— Riktlinjer för informationssäkerhet
— Avtal mellan Kungälvs kommun och Soltak AB
— Kommunstyrelsens internkontrollplan 2022
— Informationsklassningar och riskanalyser för respektive sektor

Intervjuer har genomförts med:

— Kommunchef
— Informationssäkerhetssamordnare
— IT-strateg
— T.f. administrativ chef

- Sektorchef Trygghet och stöd
- Sektorchef Samhälle och utveckling
- Sektorchef Bildning och lärande
- Representanter från sektorerna inom systemförvaltning och IT-samordning utifrån sektorchefernas önskemål
- VD Soltak AB
- IT-chef Soltak AB
- IT-arkitekt Soltak AB

2.6 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet är baserat på den internationella standardserien för informationssäkerhet, ISO/ IEC 27000 och syftar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

Enligt MSB:s metodstöd för hur ett systematiskt informationssäkerhetsarbete ska bedrivas framgår det hur ansvaret för arbetet med informationssäkerhet bör fördelas.

Ledningens förståelse för och engagemang i informationssäkerhet är grundläggande för att lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet. Ledningens stöd är också viktigt för att frågan ska få acceptans och ett engagemang från andra roller i organisationen.

Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, verksamhetschefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten.

Det är viktigt att tydligt klargöra informationssäkehetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men rollen bör generellt vara placerad nära ledningen, exempelvis i ledningsstaben. Vanliga organisatoriska placeringar, enligt MSB:s metodstöd är exempelvis:

- Säkerhet
- Kvalitet
- Juridik

I de fall rollen är placerad i en strategisk IT-funktion bör funktionen vara åtskild från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetssamordnaren både ska granska och vara kravställande gentemot IT-driften och riskerar annars att brista i opartiskhet.

IT-säkerhet är underordnat informationssäkerhet. Av detta följer att beslut om IT-säkerhet styrs av beslutad informationssäkerhetspolicy med tillhörande tillämpningsföreskrifter eller liknande styrdokument.

3 Resultat av granskningen

3.1 Styrande dokument

Kungälvs kommun har beslutat om ett antal styrande dokument avseende informationssäkerhetsarbetet. Det finns en policy och tillhörande riktlinjer som beskrivs nedan.

Av intervjuer framgår att de styrande dokumenten utgör ett gott stöd, men att det finns svårigheter att förankra dem i kommunens verksamheter. Detta uppges till viss del bero på att sektorerna i nuläget till viss del saknar utsedda funktioner för sitt informationssäkerhetsarbete. Som ett resultat så behöver kommunens centralt placerade informationssäkerhetssamordnare stödja sektorerna i hög utsträckning för att genomföra aktiviteter i enlighet med krav i styrande dokument.

Intervjuade uppger att någon kontroll av att de styrande dokumenten efterlevs inte har genomförts. De nya styrdokumenten hade nyligen beslutats vid tiden för den senaste uppföljningen av kommunens informationssäkerhetsarbete och bedömdes därigenom inte vara relevanta att följa upp vid tillfället.

3.1.1 Kungälvs kommuns informationssäkerhetspolicy

Kungälvs kommuns informationssäkerhetspolicy[1] syftar till att ange riktningen för arbetet med informationssäkerhet. I styrdokumentet definieras informationssäkerhet och det beskrivs att kommunens informationssäkerhetsarbete utgår från kraven på konfidentialitet, riktighet och tillgänglighet.

I de styrande principer som framgår av informationssäkerhetspolicyn anges att informationssäkerhetsarbetet ska utgå från ISO 27000.[2]

Vidare så anges kommunens strategiska mål med informationssäkerhetsarbetet, nämligen att:

- systematisk uppföljning av laglighet i behandling av kommunens information och informationstillgångar ska göras,
- kommuninvånare, företag och föreningar känner sig trygga med kommunens behandling av deras uppgifter,
- informationssäkerhet ska vara en integrerad del av kommunens hantering av handlingar, uppgifter och information,

[1] KF, 2021-05-20 § 79
[2] ISO/IEC-27000 är en samling säkerhetsstandarder för att tillse ett systematiskt informationssäkerhetsarbete. Standardserien inbegriper ledningsansvar, administrativa rutiner samt IT-infrastruktur. I Sverige ansvarar Svenska institutet för standarder (SIS) för utvecklingen av standardserien.

- kommunens informationshantering vid normalläge, kris eller höjd beredskap är robust
- kommunen uppfyller kravställningen enligt SS-EN ISO/IEC 27002:2017.[3]

3.1.2 Riktlinjer för informationssäkerhet

Kommunens riktlinjer för informationssäkerhet[4] avser säkerställa ett kommungemensamt informationssäkerhetsarbete. Riktlinjerna syftar till att kommunens informationshantering ska hålla en hög grad av säkerhet med bibehållen effektivitet. Målet med riktlinjerna är att tillse att kommunens informationstillgångar får ett tillräckligt skydd utifrån laglighet och lämplighet i syfte att uppfylla rättsliga krav samt de mål som fastställts i informationssäkerhetspolicyn.

Riktlinjerna innehåller administrativa krav rörande exempelvis lösenordshantering, sekretessmarkering och makulering av sekretessbelagda handlingar. I riktlinjerna finns en klassningsmatris som stöd för den som ska klassa information. I riktlinjerna fastställs även tekniska krav (IT-säkerhet) avseende bland annat dokumentation av IT-miljön, utveckling, anskaffning och utkontraktering, behörigheter, digitala identiteter och autentisering samt kryptering[5].

3.1.3 Bedömning

Vår bedömning är att kommunstyrelsen i enlighet med MSB:s rekommendationer har beslutat om en policy som övergripande styrning av informationssäkerhetsarbetet samt kompletterat det med riktlinjer. Dessa är nyligen upprättade och beslutade vilket också är helt i enlighet med MSB:s rekommendationer som säger att styrande dokument bör ses över med ett intervall om tre till fem år. Styrdokumenten är med andra ord aktuella och tydliggör ansvar och de krav som ställs på hur informationssäkerhetsarbetet ska bedrivas. Det har vid tiden för granskningen inte genomförts någon efterlevnadskontroll av beslutade styrdokument då styrande dokument mot bakgrund att de nyligen beslutats och förankringsprocessen pågick vid tiden för den senaste uppföljningen av informationssäkerhetsarbetet i kommunen.

Vår bedömning är att kommunstyrelsen bör besluta hur de tekniska krav som kommunen beslutat om i styrande dokument ska regleras när externa leverantörer nyttjas för IT-drift och säkerhetsarbete. Detta då beslut finns i informationssäkerhetspolicyn att kommunen ska uppfylla kravställning enligt ISO 27002:2017.

[3] Standard för vägledning i hur organisationer ska välja ut, införa och förvalta säkerhetsåtgärder med utgångspunkt i de informationssäkerhetsrisker som finns i organisationens omgivning.
[4] KS, 2021-05-26 § 177
[5] En mer uttömmande beskrivning av de tekniska kraven finnes i avsnitt 3.3.2 i denna rapport.

3.2 Organisation

3.2.1 Roller och ansvar

3.2.1.1 Ansvar för informationssäkerhet

I de styrande dokumenten framgår följande ansvarsfördelning för informationssäkerhetsarbetet:

- Kommunstyrelsen är ytterst ansvarig för säkerhetsarbetet i kommunen där även informationssäkerhet ingår.
- Övriga nämnder har ett övergripande ansvar för det informationssäkerhetsarbete som bedrivs inom respektive verksamhetsområden.
- Systemägare är ansvariga för säkerheten i sina informationstillgångar, att klassa informationstillgångar samt genomföra riskåtgärder.
- Informationssäkerhetssamordnaren ansvarar för ledning och samordning av informationssäkerhetsarbetet.
- Kommunens medarbetare är skyldiga att följa rutiner, riktlinjer, policys och andra hänvisningar.

Av de intervjuade framgår att kommunen sedan ett antal år har en informationssäkehetssamordnare som är placerad inom kommunkansliet. Ett av informationssäkehetssamordnarens uppdrag är att årligen följa upp det arbete som bedrivs i kommunen och rapportera om detta till kommunstyrelsen. Uppföljningen presenteras i form av en informationssäkerhetsrapport. Av den senaste informationssäkerhetsrapporten[6] som presenterades till kommunstyrelsen den 2022-03-23 och avsåg år 2021 framgick att det i vissa delar saknas förutsättningar för ett systematiskt och kontinuerligt informationssäkerhetsarbete i kommunen. Detta uppges till stor del bero på en viss otydlighet i roller och ansvar där en alltför stor tilltro att en särskild roll eller enhet ansvarar för informationssäkerheten när ansvaret till största delen följer verksamhetsansvaret. Kommunstyrelsen noterade informationen, men fattade inga beslut om åtgärder.

Enligt informationssäkerhetspolicyn ska en informationssäkerhetsgrupp finnas som stöd i informationssäkehetssamordnarens uppdrag. Gruppen består av informationssäkerhetssamordnare, IT-strateg, dataskyddsombud och IT-arkitekt (Soltak AB). Enligt intervjupersoner behöver det ske ett omtag med gruppen då den i nuvarande form inte har ett tydliggjort uppdrag och mandat. Detta finns även med som en rekommendation i informationssäkerhetsberättelsen 2021.

[6] Dnr. KS2022/0332-1, KS 2022-03-23 § 61

3.2.1.2 Organisation för systemförvaltning

Kommunen har sedan ett antal år etablerat en systemförvaltningsmodell. Vi har i granskningen tagit del av en handbok för systemförvaltning. I den beskrivs ett antal roller inom systemförvaltningsarbetet. Däribland systemägare och systemförvaltare. Systemägare ansvarar för verksamhetsspecifika system och är vanligen sektorchefer. Systemägarna delegerar delar av det tekniska ansvaret till systemförvaltare och enligt intervjuade finns ett nära samarbete i arbetet. Av intervjuer framgår att varje sektor har stöd av en systemförvaltare. Sektorcheferna uppges i regel vara systemägare för större och mer övergripande system. För komplexa system med få användare finns dock undantag, där systemägarna inte är sektorchefer. Intervjuade beskriver vidare att etableringen av roller i systemförvaltningsmodellen varit ett sätt att tydliggöra ansvar och arbetssätt för kommunens system mellan kommunen och bolaget sedan övergång till extern drift.

Enligt uppgift är merparten av systemförvaltarna centralt organiserade under kommunkansliet. Totalt har kommunen sju centralt placerade systemförvaltare, som är fördelade per sektor. Sektor Trygghet och stöd har tre systemförvaltare, Bildning och lärande har två och ytterligare två förvaltare är fördelade för de centrala systemen. Sektor samhälle och utveckling, som i nuläget har ett stort antal system, har inget stöd från systemförvaltare på central nivå. I stället arbetar vissa medarbetare inom sektorn en procentuell andel av sin tjänst som systemförvaltare. Intervjuade uppger att de ser vissa risker med detta ur ett informationssäkerhetsperspektiv. Exempelvis att det på central nivå finns en bristfällig översikt av sektor Samhälle och utvecklings många system.

I informationssäkerhetsrapporten framgår att sektorchefer inte prioriterat att aktivt leda och följa upp informationssäkerhetsarbetet. Utsedda systemförvaltare har därför fått ett utökat ansvar för uppföljning av sektorernas informationssäkerhetsarbete. Rådande ambitionsnivå är att sektorcheferna ska ha som rutin att med regelbundenhet informera sig om status för informationssäkerhetsarbetet i den verksamhet vederbörande ansvarar för.

3.2.1.3 Extern IT-drift

Kommunen har genom avtal outsourcat sin IT-drift till det gemensamt ägda bolaget Soltak AB (hädanefter bolaget).[7] Bolagets verksamhet styrs av ägardirektiv och bolagsordning. Ägardirektivet syftar till att skapa en aktiv styrning av bolaget, samt underlätta uppföljning och kontroll av bolagets verksamhet. I direktivet anges att bolaget är skyldigt att tillhandahålla tjänster som motsvarar ägarkommunernas beställning, samt att tjänsterna uppfyller aktuella lagkrav. Exempel på lagkrav är offentlighets- och sekretesslagen, GDPR eller annan tillämplig dataskyddslagstiftning.

[7] Soltak AB är ett kommunalt bolag ägt av kommunerna Stenungsund, Orust, Lilla Edet, Tjörn, Ale, Kungälv och Öckerö. Bolaget erbjuder tjänster inom ekonomi, lön, IT och projekt.

Bolagets uppdrag och ansvar regleras genom avtal med kommunen. Avtalet tecknades 2016-03-22. Avtalet reglerar att bolaget inom IT-drift och support ska förvalta ägarkommunernas centrala IT-miljöer och erbjuda samma servicenivå som innan verksamhetsövergången. Ett nytt avtal är under upprättande av bolaget och ska inom kort skickas på remiss till kommunerna. Enligt uppgift kommer det nya avtalet att innehålla bilagor med tjänstebeskrivningar över bolagets leveranser till kommunerna.

Behov av nytt och mer detaljerat avtal är ett identifierat behov i kommunen. Dels framgår det av kommunstyrelsens internkontrollplan där en riskbedömning avseende otydlighet i avtal mellan kommunen och bolaget finns med tillsammans med beskrivning av avsaknad av tjänstekatalog. Detta beskrivs även av intervjuade, att det finns vissa oklarheter mellan kommunens ansvar och bolagets ansvar inom informationssäkerhet. Därtill upplevs det från kommunens sida finnas en otydlighet kring finansieringen av IT-säkerhetsåtgärder. Detta främst kopplat till ägarförhållandet med flera kommuner som äger bolaget som kan inkomma med olika krav och behov. Intervjuade uppfattar att vissa åtgärder stannar av i väntan på beslut om finansiering.

Avtalet anger att kommunen ska utse en beställaransvarig, vi uppfattar att så är gjort genom kommunens IT-strateg. IT-strateg har det sammanhållande ansvaret för kommunens IT och för att tillse en så bra helhet som möjligt för IT-systemen. IT-strateg arbetar enligt intervjuade nära informationssäkerhetssamordnare och de systemförvaltare som finns inom staben. IT-strategens främsta uppgift anges vara att utgöra språkrör och ha en aktiv dialog med bolaget för en så bra beställning och kravställning som möjligt inom IT.

Inom bolaget finns en IT-chef, en IT-arkitekt och ett antal tjänsteägare. Det har enligt intervjuade blivit större fokus på säkerhetsarbetet på senare tid och en säkerhetschef ska inom kort anställas i bolaget.

Ägarkommunerna och bolaget har ett antal etablerade forum för dialog. Enligt uppgift finns ett kundråd för affärsområdet IT där övergripande frågor diskuteras. Kundrådet träffas fyra gånger per år och har mandat att fatta beslut. Utöver kundrådet finns ett forum för kommuncheferna att diskutera och besluta på högre nivå, samt en säkerhetsgrupp där kommunernas informationssäkerhetssamordnare eller motsvarande ingår.

3.2.2 Bedömning

Vår bedömning är att det i huvudsak finns en ändamålsenlig organisation för informationssäkerhetsarbetet. Kommunen har i enlighet med de rekommendationer MSB ger inrättat en central informationssäkerhetssamordnare med uppdrag att leda, samordna och följa upp arbetet.

Vår bedömning är att det ansvar som åligger informationsägare och systemägare i respektive sektor på ett tydligare sätt behöver etableras. Detta för att säkerställa att rollerna upprätthåller det ansvar som åligger respektive roll för att säkerställa

informations- och IT-säkerheten i de system och digitala verktyg som nyttjas i sektorerna. En systemförvaltningsmodell finns i kommunen där roller och ansvar i vissa delar har tydliggjort ansvar i arbetet med system och tillhörande säkerhetsarbete. Ägarna behöver dock säkerställa att de funktioner som tilldelats ansvar i informationssäkerhetsarbete och systemförvaltning har tid och kompetens för att bedriva informationssäkerhetsarbetet för den information och system som de har ansvar för.

Kommunen har säkerställt beställarkompetens i förhållande till Soltak AB för hantering av behov och beställningar inom IT. Vår bedömning är att de tekniska krav som kommunen beslutat om i styrande dokument bör regleras i avtal mellan kommunen och Soltak AB samt övriga externa leverantörer. Efterlevnadskontroller bör därtill inrättas som en del i avtalsuppföljning så att ansvar upprätthålls och leveranser sker i enlighet med ställda informationssäkerhetskrav.

Vår bedömning är att informationssäkerhetsgruppen ytterligare skulle kunna bidra till att arbetet sker mer sammanhållet där flera kompetenser kan samverka och vara involverade i det strategiska arbetet. Vi anser därför att gruppen bör få ett tydliggjort mandat och uppdrag i informationssäkerhetsarbetet.

3.3 Informationssäkerhetsarbetet

3.3.1 Informationsklassning och riskbedömning

För att tydliggöra att olika typer av information har olika värde för verksamheten bör en klassning av information och system genomföras. Kommunen kan därefter skapa förutsättningar för lämpliga skyddsnivåer. Detta görs oftast utifrån en systemöversikt där ansvar och roller är definierade och med stöd av någon metod för informationsklassning och riskanalys.

Eftersom skadeverkningarna av bristande säkerhet uppstår hos informationsägaren, d.v.s. verksamheten, är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning. Efter klassningen ska åtgärdsplaner upprättas. Åtgärdsplanerna handlar om olika saker där IT-säkerhetsåtgärder rent tekniskt är en del. Det kan även vara att göra mer utförliga risk- och konsekvensanalyser, förbättra rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Av intervjuer framgår att kommunens informationssäkerhetssamordnare ägnar en stor del av sin arbetstid åt att stödja sektorerna i deras informationsklassningar. Det anges att detta skapar en viss problematik, då informationssäkerhetssamordnaren även har ett tillsynsansvar, vilket påverkar oberoendet i tillsynen, när samordnaren i hög utsträckning varit del i det operativa arbete som genomförts.

Kommunen använder sig av SKR:s verktyg för informationsklassning, KLASSA. Enligt uppgift är de flesta verksamhetssystem på central nivå klassade. Vi har tagit del av exempel på klassningar och riskanalyser för centrala verksamhetssystem.

Intervjuade i sektorerna Bildning och lärande samt Trygghet och stöd uppger att de har informationsklassificerat en stor del av sina verksamhetssystem. I granskningen har vi tagit del av exempel på klassningar och riskanalyser som styrker denna beskrivning. Sektor samhälle och utveckling uppger att man påbörjat en kartläggning- och informationsklassning av sina system.

Samtliga sektorer beskriver att de har behov av stöd från informationssäkerhetssamordnare eller externa resurser för att genomföra klassningar och riskbedömning. Vissa sektorer uppger därtill att det finns en utmaning med att tillhandahålla resurser för informationsklassning mot bakgrund av att de har många mindre system och i vissa delar komplexa systemintegrationer. Arbetet har nyligen påbörjats och intervjuade beskriver att det ännu inte finns en systematik i hur resultatet av klassningar ska leda till krav om tekniska säkerhetsåtgärder. Intervjupersoner uppger därtill att kravställningen inte är helt tydlig så det kan vara svårt att avgöra vilka tekniska åtgärder som är lämpliga i förhållande till klassningen. Intervjuade beskriver att regelbundna dialoger genomförs med IT-arkitekt på bolaget för att hitta lämpliga åtgärder.

I kommunstyrelsens internkontrollplan 2022 framgår att brister i informationssäkerhet har identifierats i de klassningar som genomförts. Ett exempel på bedömning av risker som inte mötts med åtgärd beskrivs i internkontrollplan. Där framgår att det finns risk att inloggning i verksamhetssystem inte hanteras tillräckligt säkert då det kan saknas tvåfaktorinloggning till system med sekretessbelagd information. Av planen framgår att kontrollmomentet är att systemförvaltare regelbundet ska kontrollera att användare har rätt behörighet.

Som stöd i arbetet med informationsklassningar och dokumentation av informationssäkerhetsarbetet har kommunen implementerat ett systemstöd, DigFrame. Genom systemstödet finns förutsättningar att bedömningar görs på likartat sätt mellan sektorer samt att det finns en samlad dokumentation av kommunens informationsklassningar och systemförvaltning.

3.3.2 Medvetenhet och förståelse

En viktig del i ett systematiskt informations- och IT-säkerhetsarbete är att det finns en tillräcklig medvetenhet hos de som har tillgång till kommunens information. I kommunen är detta bland annat förtroendevalda, medarbetare, elever och externa konsulter.

Av intervjuer framgår att det ännu inte genomförts utbildning på kommunövergripande nivå. Kommunen har dock till alla medarbetare skickat ut information och länk för DISA,

MSB:s introduktionsutbildning avseende informationssäkerhet. Kommunen befinner sig även i en upphandlingsfas avseende en webbaserad tjänst för utbildning, där bland annat informationssäkerhet ingår i utbudet.

Av intervju med sektorerna framgår att bildning och lärande i nuläget arbetar med att ta fram utbildningar avseende bland annat informationssäkerhet. Sektor trygghet stöd uppger att de inte arbetar på något strukturerat sätt med utbildningar avseende informationssäkerhet. Sektor samhälle och utveckling uppger att de genomfört interna utbildningar avseende säker hantering av e-post och användning av internet.

3.3.3 Bedömning

Vår bedömning är att det har påbörjats ett arbete i kommunen med informationsklassningar och riskbedömning i enlighet med rekommendationer från MSB och beslut i kommunens interna styrdokument för informationssäkerhet. Arbetet är dock i stora delar nyligen uppstartat och är ännu inte systematiskt då ytterligare klassningsarbete behöver genomföras och rutiner för att regelbundet omvärdera risker och klassningar behöver säkerställas.

Vi bedömer därtill att utbildning bör genomföras så att fler funktioner i sektorerna har kunskap om riskbedömning och metod för informationsklassning. Detta så att informationssäkerhetssamordnaren inte behöver delta i samtliga klassningar men kan finnas som stöd i mer komplexa frågeställningar och bedömningar.

Vår bedömning är att det i nuläget till viss del finns arbetssätt och dialogvägar för att vid behov vidta tekniska säkerhetsåtgärder som ett resultat av klassningar. Utifrån beskrivningen av risk i internkontrollplan vill vi särskilt påtala att klassningar och riskanalyser som visar att känslig eller sekretessbelagda uppgifter hanteras i system ska emotses med erforderliga tekniska åtgärder, i detta fall tvåfaktorsinloggning, om behov av detta har identifierats. Detta behöver då kravställas till extern leverantör eller Soltak AB.

Som vi tidigare bedömt så finns dock vissa hinder vid etablering av tekniska säkerhetsåtgärder utifrån ägarförhållandet för extern IT-leverantör och den nu gällande finansieringsmodellen. Detta behöver redas ut så att det finns en tydlighet hur kostnadsfördelning för åtgärder ska fördelas.

Vi bedömer därtill att det finns risk att det inte har etablerats en tillräcklig medvetenhet och kunskap inom informationssäkerhet då det i nuläget inte finns obligatoriska utbildningar som medarbetare behöver genomföra. Med det stora antalet användare som finns i kommunens verksamhet så är den mänskliga faktorn i informations-hantering och IT-användning en väsentlig risk om inte en tillräcklig säkerhetskultur finns etablerad.

3.4 Drift och teknik

3.4.1 Systemförvaltning

I kommunens systemförvaltningshandbok beskrivs kommunens ansvarsfördelning och väsentliga processer i systemförvaltningsarbetet. Systemägare är enligt riktlinjer för informationssäkerhet skyldiga att vid utveckling, anskaffning eller utkontraktering av informationssystem identifiera vilka tekniska krav som det finns behov av för att nå en tillräcklig säkerhet. Vidare är systemägare skyldiga att inför driftsättning eller förändring med bäring på säkerhet i informationssystemen genomföra säkerhetstester och granskningar för att kontrollera att aktuella säkerhetsåtgärder är tillräckliga.

Av intervjuer framgår att sektorerna i stora delar arbetar enligt den systemförvaltningsmodell och handbok som finns. Det uppges dock svårt för vissa sektorer som hanterar ett stort antal mindre system att kunna tillsätta roller och bedriva systemförvaltningsarbetet i enlighet med handboken.

Intervjuade uppger att kommunen har etablerade rutiner vid anskaffning av nya system där bedömningar av informationssäkerhetskrav görs. Det uppges av intervjupersoner ha skett en förbättring avseende dialog där Soltak AB involveras i tidigare skeden i processen nu än vad som gjordes tidigare.

3.4.2 IT-säkerhetsåtgärder

I informationssäkerhetspolicyn framgår att ett kommunens långsiktiga mål är att uppfylla kravställningen i SS-EN ISO/IEC 27002:2017. Av kommunens riktlinjer för informationssäkerhet som beskrivits i avsnitt 3.1.2 framgår mer detaljerade krav avseende IT-säkerhet. Vi uppfattar att dessa i stora delar utgår från de krav som ingår enligt ISO-standarden.

Bland annat kravställs att kommunstyrelsen för egen del samt för övriga nämnder upprätthåller en dokumentation över:

- den hård- och mjukvara som används i informationssystemen,
- beroenden mellan interna informationssystem samt beroenden av informationssystem hos externa parter,
- vilka informationssystem som har behov av utökat skydd, exempelvis genom säkerhetsskyddslagen eller NIS-direktivet,
- vilka informationssystem som är av central betydelse för kommunens förmåga att utföra sitt uppdrag.

Intervjuade uppger att det inte finns en samlad systemdokumentation i nuläget.

Riktlinjerna anger därtill ett stort antal tekniska krav, i enlighet med de standarder som kommunen beslutat att informationssäkerhetsarbetet ska utgå från. Vi presenterar dessa mer i detalj i bilaga 1. Kraven är som vi beskrivit tidigare i vissa delar

kommunicerade till extern IT-leverantör. Vi uppfattar dock av intervjuade att det i nuläget inte finns en systematik i att kravställningar dokumenteras eller att kontroller görs över att de tekniska kraven efterlevs.

I intervju har en övergripande beskrivning av arbetet med drift och IT-säkerhet presenterats av representanter från bolaget. Ett säkerhetsråd finns med representation från bolaget och kommunen, från Kungälvs kommun deltar informationssäkerhetssamordnare och IT-strateg. I säkerhetsrådet sker en dialog om säkerhetsåtgärder innan införande och utveckling genomförs.

Vidare beskrivs att bolaget genomfört ett antal säkerhetshöjande insatser inom flertalet IT-komponenter som servrar, nätverk och klientnivå. Vidare beskrivs att risker analyseras löpande men att det inte finns någon beslutad modell eller arbetssätt för att upprätta riskanalyser inom bolaget. Bedömningar görs främst utifrån den interna kompetensen hos medarbetare tillsammans med en omvärldsbevakning. En stor del av de säkerhetshöjande åtgärderna har därtill vidtagits genom nya licenser och programvaror samt i samarbete med externa leverantörer till bolaget.

Säkerhetsrådet har under året arbetat med åtgärder utifrån MSB:s rekommendationer för ökad motståndskraft mot cyberhot.[8] Bland annat har en åtstramning av lokala administratörer gjorts och åtkomsthanteringen har stärkts genom införande av multifaktorautentisering. Intervjuade uppger att krav ställs om stärkta inloggningsfunktioner när användare loggar in från externt nät, exempelvis vid distansarbete, samt vid inloggning till kommunens plattform.

Det pågår arbete med förstärkta åtgärder kring segmentering. Intervjuade anger att det finns etablerade rutiner för att säkerhetsuppdatera IT-komponenter som bolaget har ansvar och kontroll över men att det finns vissa system som kommunen själva hanterar som inte bolaget kan managera i nuläget. Det finns etablerade rutiner för säkerhetskopiering och tester har genomförts för att säkerställa att dessa är återläsningsbara utan att information går förlorad. Dock framhålls att ytterligare tester bör genomföras genom samarbete mellan bolaget och kommunen där verksamheterna verifierar den data som är återläst.

Bolaget har identifierat behov av mer proaktiva övervakningsfunktioner och loggning av säkerhetshot. Det finns i nuläget vissa skydd för olika typer av hot och flertalet åtgärder finns planerade att genomföras under år 2023. Bolaget har vi två tillfällen genomfört kontroller av vidtagna säkerhetsåtgärder i form av penetrationstest. Dessa har inte enligt intervjuuppgifter visat på några betydande sårbarheter.

[8] Se: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/rekommenderade-sakerhetsatgarder/

3.4.3 Bedömning

Vår bedömning är att det till viss del finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. Arbetet kan dock utvecklas genom en fastställd metod för riskanalyser samt att rutiner och processer dokumenteras i högre grad. I avsaknad av dokumenterade riskanalyser saknas i nuläget underlag för att besluta om säkerhetsåtgärder utifrån en prioritering av hot och risker.

Vår bedömning är att implementerade säkerhetsåtgärder vid tillfällen har testats men att uppföljningsarbetet i nuläget inte sker på ett systematiskt sätt.

Vår bedömning är vidare att kommunen bör tydliggöra och formalisera kravställning av informationssäkerhet och de tekniska krav som ska gälla då detta ingår för att efterleva ISO 27002-standarden. Vår bedömning är, som vi uttryckt tidigare i rapporten att avtal och kravställning inte uppfyller detta i nuvarande form. Att detta inte är dokumenterat kan leda till risk i otydlighet över om det är kommunens eller den externa leverantörens ansvar att de säkerhetsåtgärder som det finns behov av är etablerade. Krav behöver därför skriftligen avtalas och följsamhet kontrolleras regelbundet. Detta så att kommunen erhåller de säkerhetsnivåer som de beslutat i sina styrande dokument.

3.5 Incidenthantering

Av informationssäkerhetspolicyn framgår hur informationssäkerhetsrelaterade avvikelser ska rapporteras. Avvikelser av mindre betydelse sammanställs i informationssäkehetssamordnarens årliga rapport till kommunstyrelsen, medan avvikelser av större betydelse rapporteras till förvaltningsledningen samt vid behov även kommunstyrelsen.

Kommunen arbetar efter en anvisning för informationssäkerhetsincidenter vilken syftar till att kommunen ska ha en effektiv, rättssäker och robust hantering av informationssäkerhetsincidenter. Vid informationssäkerhetsincidenter framgår en särskild organisation och rollfördelning mellan incidentanmälare, incidentmottagare och åtgärdsansvarig.

En incidentanmälare är i regel en medarbetare eller extern part som noterar en pågående incident. En medarbetare är alltid skyldig att rapportera incidenten till incidentmottagaren. Incidentmottagaren är kommunens centralt placerade systemförvaltargrupp under kontorstid och tjänsteman i beredskap övrig tid. Incidentmottagaren vidtar initiala åtgärder för att skademinimera och påbörja en dokumentation kring incidenten.

Åtgärdsansvarig är chef för berörd verksamhet. Om incidenten påverkar flera verksamheter inom samma sektor är sektorchef ansvarig. Vid incidenter i kommunövergripande informationssystem ansvarar respektive stabsenhetschef för åtgärder. Orsakar incidenten mycket ansträngande bortfall av funktionalitet och kapacitet ska kommunens krisorganisation aktiveras.

I anvisningen saknas beskrivning av hur kommunens interna incidenthantering ska samordnas med incidenthantering inom Soltak AB och vilken organisation som ska upprättas för att hantera allvarligare incidenter.

I anvisningen tydliggörs även hur mindre incidenter ska hanteras, hur dokumentation av incidenter ska ske och hur anmälan till myndighet görs. Anmälningsvägar finns tillgängliga på intranätet. Anvisningen innehåller även en lathund för incidentrapportering.

Av intervjuer framgår att incidentrapporteringen skiljer sig mellan olika sektorer. Enligt uppgift har kommunen från central nivå gjort ett utskick till chefer så att de i sin tur kan informera om incidentrapporteringsrutiner. Intervjuade bekräftar att det vid tiden för granskningen pågår ett arbete för att implementera rutinen och informera medarbetare om incidenthantering i kommunen.

3.5.1 Bedömning

Vår bedömning är att kommunen i enlighet med informationssäkerhetspolicyn och krav enligt ISO 27000-serien har beslutat om incidenthanteringsrutiner. Rutinen är dock vid tiden för granskningen inte känd så att den tillämpas av samtliga verksamheter.

Anvisningen är i sin form detaljerad och har förutsättningar att utgöra en god vägledningen i den interna hanteringen vid informationssäkerhetsincidenter. Vi ser dock behov av att kommunen i anvisningen eller genom annan kompletterande dokumentation tydliggör hur incidenthanteringsorganisationen ska se ut när externa leverantörer, främst IT-driftsleverantör, behöver involveras. Det saknas i nuläget en tydlighet över hur allvarliga händelser samordnas och eskaleras mellan kommunen och extern IT-driftsleverantör. Den externa leverantören är en avgörande part när händelser sker i system eller nätverk då kommunen inte har vare sig insyn, tillgång eller kompetens att hantera tekniska åtgärder vid säkerhetshändelser.

Mot bakgrund av tidigare bedömning att det till viss del saknas etablerade utbildningar inom informationssäkerhet i kommunen, kan vi inte utesluta att det kan finnas en risk för att incidenter inte upptäcks och rapporteras i tillräckligt hög grad.

4 Slutsats och rekommendationer

4.1 Slutsats

Vår sammanfattade bedömning utifrån granskningens syfte är att kommunstyrelsen i huvudsak har en tillräcklig styrning av informationssäkerhetsarbetet men att den interna kontrollen behöver stärkas i syfte att säkerställa ett ändamålsenligt och systematiskt informationssäkerhetsarbete i kommunen.

Utifrån granskningens resultat ser vi ett behov av att rollen informationsägare och systemägare etableras så att ansvar i enlighet med interna styrdokument upprätthålls. Arbete med riskanalyser och informationsklassningar är i en uppstartsfas och har inte slutförts för de informationstillgångar som hanteras i verksamheternas informationssystem. Vår bedömning är att det till viss del finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. Arbetet kan dock utvecklas genom en fastställd metod för riskanalyser samt att rutiner och processer dokumenteras i högre grad. I avsaknad av dokumenterade riskanalyser saknas i nuläget underlag för att besluta om säkerhetsåtgärder utifrån en prioritering av hot och risker.

Vår bedömning är vidare att kommunen bör tydliggöra och formalisera kravställning av informationssäkerhet och de tekniska krav som ska gälla då detta ingår för att efterleva ISO 27002-standarden. Avtal och kravställning uppfyller inte detta i nuvarande form. Att detta inte är dokumenterat kan leda till risk i otydlighet över om det är kommunens eller den externa leverantörens ansvar att de säkerhetsåtgärder som det finns behov av är etablerade.

Incidenthanteringsrutiner har beslutats men är ännu inte kommunicerade till verksamheterna så att det finns kännedom hur incidenter ska hanteras. Rutiner saknar därtill beskrivningar av hur incidenter samordnas när externa leverantörer ansvarar för drift och förvaltning av system. Vi ser främst ett behov av att detta etableras i förhållande till Soltak AB men även för de systemleverantörer som enskilda verksamheter har avtal med.

4.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att informations- och systemägaransvaret etableras i samtliga verksamheter så att aktiviteter genomförs i enlighet med krav i styrande dokument.
- Fastställa hur kommunen i förhållande till externa leverantörer ska hantera de tekniska krav som kommunen beslutat som gällande i informationssäkerhetsarbetet.
- Revidera avtal med extern IT-driftsleverantör där informationssäkerhetskrav tydliggörs tillsammans med former för avtalsuppföljning.
- Tydliggöra mandat och uppdrag för informationssäkerhetsgruppen.
- Säkerställa att efterlevnadskontroller ingår i årlig uppföljning och rapportering av informationssäkerhetsarbetet.
- Säkerställa att incidenthanteringsrutiner är kända och tillämpas av samtliga verksamheter. Inträffade incidenter bör dokumenteras på övergripande nivå och analyser ingå som underlag i förbättringsarbetet.
- Komplettera incidenthanteringsrutiner med beskrivning över hur incidenter ska samordnas och eskaleras mellan kommunen och extern driftsleverantör, exempelvis Soltak AB.

Kungälvs kommun
Granskning av kommunens informationssäkerhet

2022-12-20

DocuSigned by:
Erik Söderberg
2AE86DF94405495...
2023-01-04

Erik Söderberg
Kvalitetssäkrare
Certifierad kommunal yrkesrevisor

DocuSigned by:
Jenny Thörn
F1872C8AB3D4FC...
2023-01-04

Jenny Thörn
Projektledare
Kommunal yrkesrevisor

DocuSigned by:
William Andreasson
2023-01-04

William Andreasson
Kommunal yrkesrevisor

5 Bilaga 1

5.1 Tekniska krav

Denna information är hämtad från kommunens riktlinjer för informationssäkerhet.[9]

5.1.1 Utveckling, anskaffning eller utkontraktering

Systemägare är skyldiga att, vid utveckling, anskaffning eller utkontraktering av informationssystem identifiera flera tekniska krav. Exempel är nätverkssegmentering, behörigheter, kryptering, säkerhetsloggning och analys, skydd mot skadlig kod, redundans och återställning samt kontinuitet.

Vidare är systemägare skyldiga att inför driftsättning eller förändring med bäring på säkerhet i informationssystemen genomföra säkerhetstester och granskningar för att kontrollera att aktuella säkerhetsåtgärder är tillräckliga, samt verifiera att det finns nödvändig dokumentation för drift och förvaltning. Nödvändig dokumentation för drift och förvaltning bör omfatta exempelvis arkitektur, ingående komponenter, konfiguration, dataflöden och annan relevant systeminformation. Av dokumentationen bör systemägare framgå.

5.1.2 Utvecklings-, test- och utbildningsmiljöer

Systemägarnas arbete med utveckling och tester med bäring på informationssäkerheten ska ske i en från produktionsmiljön avskild del av den digitala miljön.

5.1.3 Uppdelning i nätverkssegment och filtrering av nätverkstrafik

Kommunstyrelsen ska för egen och övriga nämnders räkning förhindra incidentspridning och konsekvensminimera genom nätverkssegmentering av informationssystem. Exempel på funktioner i produktionsmiljön som bör placeras i separata nätverkssegment är användarklienter, administrationsklienter, servrar och trådlösa nätverk. Kommunstyrelsen ska även filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

5.1.4 Behörigheter, digitala identiteter och autentisering

Kommunstyrelsen ska för egen och övriga nämnders räkning tillse en funktionell behörighetshantering. Behörighetshanteringen bör bland annat säkerställa unika digitala enheter i produktionsmiljön, att digitala identiteter och behörigheter är godkända innan de kopplas till användare eller system, att tilldelade behörigheter kontrolleras årsvis. Digitala identiteter med systemadministrativ behörighet ska tilldelas restriktivt och flerfaktorsautentisering ska tillämpas för bland annat åtkomst till

[9] KS, 2021-05-26 § 177

produktionsmiljön via externt nätverk, systemadministrativ åtkomst till informationssystem samt åtkomst till informationssystem med behov av utökat skydd.

5.1.5 Kryptering

Kommunstyrelsen ska identifiera och hantera behov av kryptering för att skydda informationstillgångarna mot obehörig åtkomst- och eller förändring, överföring och lagring. Kommunstyrelsen ska även ha ett system för att kryptera sin e-post.

5.1.6 Säkerhetskonfigurering

Systemägaren ska, för att skydda informationssystem, byta ut förinställda autentiseringsuppgifter, stänga av, ta bort eller blockera överflödiga systemfunktioner samt i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet.

5.1.7 Säkerhetstester och granskningar

Kommunstyrelsen ska egen och övriga nämnders räkning säkerställa att säkerhetstester och granskningar möjliggör identifiering av sårbarheter. Kommunstyrelsen ska upprätta externa bestämmelser över hur informationssystem hålls uppdaterade, hur valda säkerhetsåtgärder införs samt hur det bedöms att genomförda säkerhetskonfigurationer är tillräckliga.

5.1.8 Ändringshantering, uppgradering och uppdatering

Kommunstyrelsen ska för egen och nämndernas räkning säkerställa att förändringar i informationssystemen genomförs på ett sådant sätt att ändringarna är strukturerade och spårbara. Kommunstyrelsen ska ha interna regler för bland annat kriterier för godkännande av hård- och mjukvara inför installation, hur incident- och avvikelserisker i samband med förändring identifieras och hanteras samt hur mjukvara ska hållas uppdaterad.

5.1.9 Korrekt och spårbar tid

Systemägaren bör använda sig av tjänsten Swedish Distributed Time Service för att hålla en korrekt och spårbar tid.

5.1.10 Säkerhetskopiering

Systemägaren ska på regelbunden basis säkerhetskopiera information. Detta ska ske varje dag för information som är påverkar kommunens förmåga att utföra sina uppdrag och årsvis, eller vid större förändringar i produktionsmiljön ska förmåga att återställa information från kopior verifieras. Säkerhetskopiorna ska förvaras separat från produktionsmiljön.

5.1.11 Säkerhetsloggning och övervakning

Systemägaren ska upprätthålla säkerhetsloggar. Dessa ska inkludera obehörig åtkomst och försök till obehörig åtkomst till IT-miljö och informationssystem, förändringar av konfigurationer och säkerhetsfunktioner som kräver priviligierade rättigheter, förändringar av behörighet, åtkomst till information med behov av utökat skydd.

Kommunstyrelsen ska för egen och nämndernas räkning analysera innehållet i säkerhetsloggarna. Detta för att upptäcka och hantera incidenter eller avvikelser. Säkerhetsloggana ska möjliggöra sådan utredning och utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar.

5.1.12 Skydd mot skadlig kod

Kommunstyrelsen ska för sin egen och nämndernas räkning använda mjukvara som ger skydd mot skadlig kod. För informationssystem där sådan mjukvara inte finns tillgänglig ska andra åtgärder vidtas som ger motsvarande skydd.

5.1.13 Skydd av utrustning

Kommunstyrelsen ska för sin egen och övriga nämnders räkning skydda den utrustning som informationssystem består av mot skador eller intrång, genom att placera centrala servrar och central nätverksutrustning i särskilt avsedda utrymmen och tilldela behörighet till sådana utrymmen restriktivt.

5.1.14 Redundans och återställning

Kommunstyrelsen ska, för att säkra tillgänglighet till information och informationssystem vid incidenter eller ha interna regler för återställning av produktionsmiljön och för enskilda informationssystem samt öva återställning av kritiska informationssystem och placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika avsedda utrymmen.