Granskning av kommunens informationssäkerhet

Rapport

Vänersborgs kommun

KPMG AB

2022-11-17

Antal sidor: 19

Vänersborgs kommun
Granskning av kommunens informationssäkerhet

2022-11-17

Innehållsförteckning

1 Sammanfattning

KPMG har av Vänersborgs kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsen och nämndernas rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen till viss del har en tillräcklig intern styrning och kontroll för att säkerställa att arbetet med IT- och informationssäkerhet bedrivs på ett ändamålsenligt sätt. Socialnämnden och barn- och utbildningsnämnden bedöms i huvudsak ha en tillräcklig intern styrning och kontroll inom området. Samhällsbyggnadsnämnden bedöms ha en tillräcklig intern styrning och kontroll inom VA-verksamheten (som står under NIS-direktivets krav). För övriga verksamheter inom samhällsbyggnadsförvaltningen bedömer vi dock att den interna styrningen och kontrollen inom området behöver utvecklas. Kultur- och fritidsnämnden bedöms inte ha säkerställt en tillräcklig intern styrning och kontroll inom området

Kommunstyrelsen har inte säkerställt en tillräcklig styrning då riktlinjen för informationssäkerhet inte är tillräckligt detaljerad och anvisningar saknas för att tydliggöra ansvar och hur informationssäkerhetsarbetet ska bedrivas. Krav och ansvar för IT-säkerheten är inte dokumenterat i styrdokumenten. Det pågår ett arbete med utveckling av IT-säkerheten genom nya tekniska lösningar för infrastruktur och system, Mot bakgrund av de uppgifter vi tagit del av i granskningen och beskrivningar av behov för större investeringar kan vi inte utesluta att det i nuläget saknas vissa tekniska implementationer för att skydda kommunens system och information från intrång och cyberhot.

I nuläget saknas en tillräcklig uppföljning av det arbete som genomförs. Då detta saknas finns inte tillräckliga underlag för kommunstyrelsen för att besluta om handlingsplan och resurser för de förbättringsåtgärder som det finns behov av för att stärka informationssäkerheten.

Socialnämnden och barn- och utbildningsnämnden genomför väsentliga aktiviteter inom informationssäkerhetsarbetet i enlighet med riktlinjerna. Arbetssätt och metoder finns- och det pågår ett aktivt arbete med informationsklassningar och riskanalyser. Därtill har utbildningsinsatser genomförts för att en medvetenhet och kunskap ska finnas.

Samhällsbyggnadsnämnden genomför väsentliga aktiviteter avseende informationssäkerhetsarbetet inom den samhällsviktiga verksamheten, i enlighet med lagkrav och riktlinjer. Arbetssätt och metoder finns och det pågår ett aktivt arbete med informationsklassningar och riskanalyser. Därtill har utbildningsinsatser genomförts för att en medvetenhet och kunskap ska finnas.

Inom kultur- och fritidsnämnden finns i nuläget inte arbetssätt och metoder för att efterleva riktlinjer för informationssäkerhet, exempelvis har inte arbetet med informationsklassningar och riskanalyser genomförts. Utbildningsinsatser har genomförts för att etablera kunskap och medvetenhet om informationssäkerhet.

Slutligen är vår bedömning att kommunstyrelsen behöver etablera gemensamma incidenthanteringsrutiner som är kända och tillämpas av samtliga verksamheter. Kommunstyrelsen bör besluta om dessa rutiner och etablera ansvar och organisation

för att upptäcka, anmäla och hantera incidenter i syfte att vid behov kunna vidta förbättringsåtgärder för att minska risken att incidenter sker på nytt.

Baserat på vår granskning rekommenderar vi kommunstyrelsen att:

- Revidera riktlinje för informationssäkerhet i enlighet med granskningens iakttagelser, bland annat kring ansvar, krav på tekniska åtgärder, incidenthantering samt fastställa och implementera kompletterande anvisningar för informationssäkerhet
- Säkerställa att befintliga resurser för informationssäkerhetsarbetet (inkl. teknisk säkerhet) är tillräckliga och står i relation till identifierade behov och risker.
- Tydliggöra organisation, ansvar och arbetssätt för incidenthantering i linje med nya, upprättade rutiner så att en beredskap finns i händelse av IT-incidenter eller allvarlig störning.
- Säkerställa att former för granskning och uppföljning av informationssäkerhetsarbetet upprättas och tillse att detta regelbundet rapporteras till styrelsen.

Utifrån vår bedömning och slutsats rekommenderar vi samtliga nämnder att:

- Säkerställa att riktlinje för informationssäkerhet efterlevs genom att regelbundet följa upp det arbete som genomförs.
- Säkerställa att befintliga resurser för informationssäkerhetsarbetet är tillräckliga och står i relation till identifierade behov och risker.
- Löpande genomföra utbildning inom informationssäkerhet till samtliga medarbetare samt följa upp de insatser som genomförs.

Utifrån vår bedömning och slutsats rekommenderar vi kultur- och fritidsnämnden att:

Säkerställa att informationsklassning och riskbedömning genomförs avseende den information som hanteras i förvaltningens system för att säkerställa att informationen har tillräckliga skyddsåtgärder

2 Bakgrund

KPMG har av Vänersborgs kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsen och nämndernas rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om informationssäkerhet för 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 görs 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 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.

År 2018 genomförde revisorerna en säkerhetsgranskning av Vänersborgs kommuns cybersäkerhet enligt SANS CIS 20 Critical Security Assessment. I granskningen konstaterades att kommunen inte hade en tillfredsställande intern styrning och kontroll för en effektiv och säker hantering av IT. Ett antal rekommendationer lämnades, vilka presenteras i avsnitt 3.1 i denna rapport.

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

2.1 Syfte och revisionsfråga

Granskningens syfte har varit att bedöma om kommunstyrelsen och utvalda nämnder har en tillräcklig intern styrning och kontroll för att säkerställa att arbetet med IT- och informationssäkerhet bedrivs på ett ändamålsenligt sätt.

Granskningen har även syftat till att följa upp vilka åtgärder som vidtagits med anledning av den granskning som genomfördes år 2018.

Granskningen har besvarat följande revisionsfrågor:

- Vilka åtgärder har styrelsen vidtagit med anledning av lämnade rekommendationer i 2018 års säkerhetsgranskning avseende cybersäkerhet?
    - Vilken status har eventuella förändringsarbeten med anledning av givna rekommendationer?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhet?
- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- 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.)?
- Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?
- Görs systematiska uppföljningar av implementerade säkerhetsåtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

Granskningen omfattar kommunstyrelsen, barn- och utbildningsnämnden, samhällsbyggnadsnämnden, kultur- och fritidsnämnden samt socialnämnden.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

— Kommunallagen 6 kap. 6 §

— Tillämpbara interna regelverk, policys och beslut

— Myndigheten för samhällsskydd och beredskaps (MSB) rekommendationer avseende Ledningssystem för informationssäkerhet

— Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

— Revisionsrapport Cybersecurity hälsokontroll enligt SANS CIS 20 Critical Security Assessment (2018)

2.3 Ansvarig nämnd/styrelse

Granskningen avser kommunstyrelsen, barn- och utbildningsnämnden, samhällsbyggnadsnämnden, kultur- och fritidsnämnden samt socialnämnden.

2.4 Metod

Granskningen har genomförts genom analys av styrdokument, underlag och intervjuer med tjänstepersoner.

Vi har analyserat följande styrdokument och underlag:

- Riktlinje för informationssäkerhet (KF 2021-03-17 § 26.)
- Kommunstyrelsens internkontrollplan 2022
- Revisionsrapport Cybersecurity hälsokontroll enligt SANS CIS 20 Critical Security Assessment (2018)

Vi har intervjuat följande tjänstepersoner:

- Avdelningschef, Juridik och säkerhet
- Informationssäkerhetsspecialist
- Avdelningschef, IT-avdelningen
- Förvaltningschef, socialförvaltningen
- Förvaltningschef, barn- och utbildningsförvaltningen
- Förvaltningschef, samhällsbyggnadsförvaltningen
- Förvaltningschef, kultur- och fritidsförvaltningen
- Utvalda tjänstepersoner inom de berörda förvaltningarna

2.5 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 ämnar 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 oumbärlig 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.

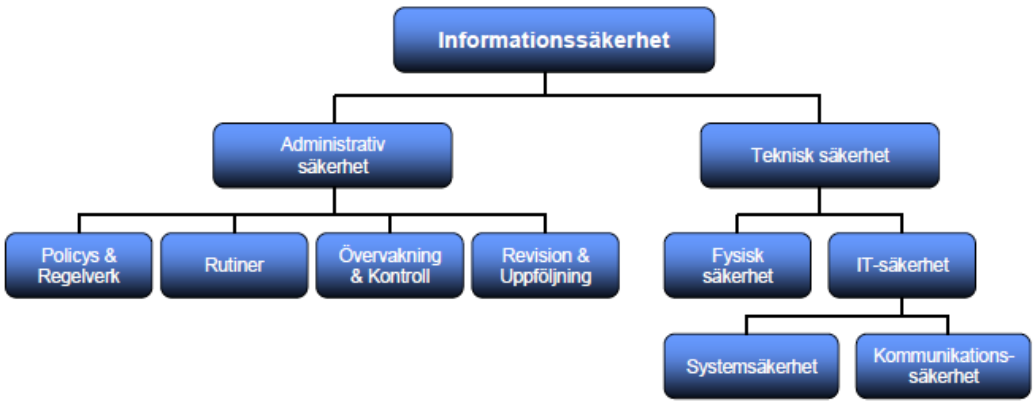
Det är viktigt att tydligt klargöra informationssäkehetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men 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 uppföljande granskning

3.1 Granskning av cybersäkerhet, 2018

Under 2018 genomförde kommunrevisionen en granskning av kommunens cybersäkerhet. Av granskningen konstaterades att kommunen inte hade en tillfredsställande intern styrning och kontroll för en effektiv och säker hantering av IT.

3.1.1 Rekommendationer

De rekommendationer som lämnades i granskningen var:

- Prioritera och öka fokus på arbetet med informationssäkerhet och IT-säkerhet
- Särskilt prioritera de kontrollpunkter som listats under rubriken Prioriteringslista för åtgärder för att höja säkerhetsnivån.
- Stärka cyberförsvarsförmågan och upprätta ett flertal rutiner, processer och dokument.
- Överväga att införa ett ledningssystem för informationssäkerhet (LIS).
- Stärka förmågan att identifiera och reagera på attacker i IT-miljön.
- Förbättra förmågan att detektera intrång.
- Se över informationssäkerheten och begränsa åtkomsten för lågt priviligierade användare.
- Se över rutin för lösenordshantering för konton.

3.1.2 Nuläge

I vår uppföljande granskning har vi tagit del av styrdokument avseende informationssäkerhet som antagits 2021 och kommer presenteras mer ingående i avsnitt 4.1.1. Den kommunövergripande riktlinjen för informationssäkerhet anger att informationssäkerhetsarbetet i kommunen ska utgå från ett LIS. Av intervju framgår att det finns ett LIS etablerat i kommunen. Intervjupersoner upplever även samstämmigt att informationssäkerhetsarbetet har fått en ökad prioritering och fokus i enlighet med lämnad rekommendation.

Av intervju framgår att ett antal tekniska förbättringsåtgärder vidtagits utifrån resultatet i de tekniska tester som genomfördes i granskningen 2018. Exempelvis har kommunen övergått till en ny plattform vilket bidragit till mer moderna system och tjänster där IT-säkerhet är inkluderat. Därtill har ett arbete genomförts med att dokumentera system och samband med tillhörande rutiner och processer. Avseende förmåga att identifiera och reagera på attacker och stärka cyberförsvarsförmågan har kommunen ett pågående pilotprojekt för att gå vidare med lämpliga verktyg för detta. IT-avdelningen har även sett över åtkomsten för lågt priviligierade användare och arbetar i nuläget med införande av multifaktorsautentisering som en säkerhetshöjande insats kopplad till behörighetshanteringen.

3.1.3 Bedömning

Vi bedömer att kommunstyrelsen har vidtagit åtgärder för sex av åtta rekommendationer som lämnades vid 2018 års granskning. Det som kvarstår är att implementera tekniska verktyg och etablera manuella rutiner och arbetssätt i syfte att bättre kunna detektera intrång och agera vid särskilda händelser.

3.2 Slutsats och rekommendationer

3.2.1 Slutsats

Vår sammanfattande bedömning är att kommunstyrelsen har vidtagit vissa åtgärder utifrån de lämnade rekommendationerna i granskning av cybersäkerhet som genomfördes 2018.

3.2.2 Rekommendationer

Utifrån vår uppföljning noterar vi att följande rekommendationer kvarstår:

- Stärka förmågan att identifiera och reagera på attacker i IT-miljön.
- Förbättra förmågan att detektera intrång.

4 Resultat av fördjupad granskning av informationssäkerhet

4.1 Kommunens styrning av informationssäkerhetsarbetet

4.1.1 Riktlinje för informationssäkerhet[1]

Kommunfullmäktige har fastställt en riktlinje för informationssäkerhet vilken anger att kommunens arbete ska ske systematiskt i enlighet med standarden SS-ISO/IEC 27000.[2]

Riktlinjen för informationssäkerhet är ett kommunövergripande styrdokument som reglerar informationssäkerhetsarbetet i Vänersborgs kommun. Enligt riktlinjen ska kommunens informationssäkerhetsarbete skydda information utifrån principerna tillgänglighet, riktighet, konfidentialitet och spårbarhet. Detta innebär att informationen ska vara åtkomlig, korrekt, skyddad från obehöriga och att informationsändringar är spårbara. Riktlinjen beskriver ansvaret för kommunstyrelse, nämnder och kommunala bolag.

Riktlinjen tydliggör på övergripande nivå sambandet mellan informationssäkerhet och IT-säkerhet.

Av riktlinjen framgår att informationstillgångar ska klassas, att inloggningsautentisering ska tillämpas och att spårbarhet i systemlösningar ska appliceras i kommunens verksamhetssystem. Vidare framgår att utbildningar inom informationssäkerhet ska ges till medarbetare och att verksamhetsspecifika anvisningar för informationssäkerhet ska upprättas. Riktlinjen anger att klassning av informationssäkerhet kan påverka krav på IT-säkerhet. Riktlinjen reglerar även att kommundirektören har rätt att besluta om anvisningar.

Av intervjuer framgår att riktlinjen för informationssäkerhet behöver förankras tydligare i samtliga verksamheter. Därtill lyfts att det skulle behövas mer detaljerade anvisningar av vad som ingår i informationssäkerhetsarbetet. Enligt uppgift pågår arbete med att upprätta anvisningar. Intervjupersoner anger dock att det är en utmaning att få dessa på en lättillgänglig och pedagogisk nivå. Avsaknad av anvisningar innebär enligt de intervjuade att det finns stora skillnader i mognad och vilka aktiviteter som förvaltningarna har genomfört i informationssäkerhetsarbetet.

Det finns enligt uppgift en osäkerhet kring vilka styrdokument som är gällande, på grund av en bristande struktur på kommunens intranät. Som exempel har vi i granskningen delgetts inaktuella styrdokument.

I nuläget saknas en samlad dokumenterad uppföljning av kommunens genomförda informationssäkerhetsarbete. Det har inte heller gjorts några kontroller eller uppföljning över hur riktlinjen efterlevs av styrelsen eller nämnderna.

---

[1] KF 2021-03-17 § 26.
[2] SS-ISO/IEC 27000 (hädanefter ISO 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.

4.1.2 Bedömning

Vår bedömning är att det till viss del finns styrande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas. Riktlinjen saknar i nuvarande form en tydlig ansvarsbeskrivning av IT-avdelningens uppdrag i förhållande till förvaltningarna samt vilket uppdrag informationssäkerhetsspecialisten har. Riktlinjen eller kompletterande anvisningar bör även uttrycka det ansvar för informationssäkerhet som ingår i linjeansvaret. Därtill bör riktlinjen kompletteras med krav på tekniska säkerhetsåtgärder.

Vår bedömning är att riktlinjen bör förankras och konkretiseras med tillhörande anvisningar så att det finns en tydlighet i hur informationssäkerhetsarbetet ska genomföras.

Vi bedömer att kommunstyrelsen inte säkerställt att den får en tillräcklig uppföljning av att beslut och styrdokument avseende informationssäkerhet efterlevs. Detta då det i nuläget saknas en samlad uppföljning och rapportering av det arbete som genomförs. Det är väsentligt att former inrättas för att årligen följa upp kommunens informationssäkerhetsarbete, för att kunna vidta åtgärder utifrån identifierade brister och för att säkerställa att informationssäkerhetsarbetet bedrivs ändamålsenligt. Uppföljning bör även innehålla kontroller av efterlevnad av beslutade dokument samt de lagar och föreskrifter som alla eller vissa verksamheter kan beröras av, exempelvis dataskyddsförordningen (alla) och NIS-direktivet (de som identifierats och anmälts som samhällsviktig verksamhet).

4.2 Organisation och ansvarsfördelning

4.2.1 Ansvar och roller i informationssäkerhetsarbetet

Av den kommunövergripande riktlinjen för informationssäkerhet framgår att kommunstyrelsen är ansvarig för ledning, samordning och granskning av informationssäkerhetsarbetet i kommunen.

Nämnder och styrelser är ansvariga för att upprätthålla informationssäkerheten inom sina respektive områden. Kommunstyrelsen, nämnderna och de kommunala bolagen är personuppgiftsansvariga. Informationssäkerhet är ett linjeansvar och den som är chef för verksamheten är genom det även ansvarig för den information som hanteras i verksamheten, vare sig den är analog eller digital. Detta är inte tydliggjort i interna styrdokument mer än genom ovan skrivelse av nämnderna och styrelsernas ansvar. De intervjuade uppger att ansvarsfördelningen är kommunicerad i organisationen och att förvaltningscheferna är medvetna om det ansvar som åligger dem.

Av riktlinjen framgår att kommundirektören ansvarar för förvaltningarnas organisering av informationssäkerhetsarbetet. Denna organisation ska preciseras i anvisningar utifrån den övergripande riktlinjen för informationssäkerhet. Anvisningarna har ännu inte upprättats.

4.2.2 Informationssäkerhetsarbetets organisation

Kommunens centrala funktion för informationssäkerhetsarbete är organiserat inom juridik- och säkerhetsavdelningen, som är en del av kommunstyrelseförvaltningen.

Inom juridik- och säkerhetsavdelningen finns en informationssäkerhetsspecialist. I dennes uppdrag ingår dels att arbeta med informationssäkerhet (ca 50 %), dels att samordna kommunens arbete med civilt försvar (ca 50 %). Detta uppges vara en förändring mot tidigare, då informationssäkerhetsarbetet var det primära ansvaret för denna funktion. Av intervju framgår att informationssäkerhetssamordnares uppdrag avseende granskning av kommunens verksamheter inte är tydliggjort.

De intervjuade upplever en ökad prioritering av informationssäkerhetsarbetet. Bland annat anges att inrättandet av en informationssäkerhetsspecialist har bidragit till en tydligare rollfördelning i kommunen och att frågorna aktualiserats mer. Ett särskilt fokus uppges ha varit på krav och åtgärder utifrån de verksamheter som är identifierade som samhällsviktiga och står under NIS-direktivet. Dessa är socialförvaltningen och samhällsbyggnadsförvaltningen.

De samarbeten som tidigare funnits, särskilt mellan samhällsbyggnadsnämnden och informationssäkerhetsspecialist uppges ha varit mycket givande och viktigt för informationssäkerhetsarbetet i förvaltningen. De intervjuade lyfter därför en oro över att informationssäkerhetsspecialisten i mindre omfattning kommer att arbeta med dessa frågor.

I kommunstyrelseförvaltningen finns kommunens IT-avdelning.IT-avdelningen har ansvar för den tekniska säkerheten i informationssäkerhetsarbetet. I intervjuer uppges att de har ett nära samarbete med kommunens informationssäkerhetsspecialist.

Det har nyligen inrättats ett säkerhets- och beredskapsråd i kommunen efter förslag från juridik- och säkerhetsavdelningen. I rådet som utgörs av kommundirektör och

förvaltningschefer är tanken att frågor från ledningen inom säkerhet och beredskap ska trattas ner till en beredningsgrupp och arbetsgrupper i respektive förvaltning. Genom strukturen är förhoppningen att få en starkare förankring för frågor från ledning och ut i förvaltningarna samt även åt andra hållet, när frågor behöver lyftas från förvaltningarna och beredas till rådet.

I kommunen finns även ett IT- och digitaliseringsråd sedan 1,5 år tillbaka där frågor kring system och teknik kan lyftas på strategisk nivå.

4.2.3 Användarnas ansvar

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.

Riktlinje för informationssäkerhet reglerar att medarbetarnas kunskap om informationssäkerhet ska säkerställas genom utbildningsinsatser.

Av intervjuer framgår att en kommunövergripande informationssäkerhetsutbildning genomförts i kommunen vid ett flertal tillfällen. Utbildningen kompletterades med simulerade phishing-test[3] för att följa upp de insatser som gjorts. Enligt uppgift var resultatet av testen goda, vi har tagit del av underlag som visar på utfallet som styrker detta. Den första omgången av utbildning uppges ha genomförts med 97 % av medarbetarna. Det är inte tydliggjort om uppföljning av deltagande i utbildningar ska göras av respektive chef, informationssäkerhetsspecialisten eller IT-avdelningen.

Inom vissa förvaltningar har kompletterande utbildningsinsatser genomförts. Bland annat inom samhällsbyggnadsförvaltningen där genomgång av krav och hantering i samhällsviktig verksamhet görs innan medarbetare får åtkomst till system och verksamhetsinformation. Inom barn- och utbildningsförvaltningen har filmer spelats in i samarbete med IT-avdelningen i syfte att öka kunskap om informationshantering, lösenordshantering och phishing. Insatser har gjorts mot lärare i förskola och grundskola men tanken är även att inkludera elever i utbildningsinsatsen.

Vid intervju lyfts att det trots de utbildningar som genomförts upplevs finnas en risk med bristande kännedom om bland annat IT-säkerhet hos användarna. Detta bekräftas i kommunstyrelsens internkontrollplan 2022 där risker identifierats i förhållande till kunskap hos medarbetarna.

Bland annat anges för risken *Cyberattack* att ”användarna är en stor del av risken för att obehöriga kan komma åt kommunens information”. Den åtgärd som är beskriven för att möta risken är att fortsätta arbetet att minimera risken för handhavandefel hos användarna. Detsamma gäller för risk att personuppgifter röjs, där kompetenshöjning är föreslagen åtgärd. Vid tiden för granskningen är inte uppföljningen av 2022 års internkontrollplan genomförd. Granskningen har därigenom inte kunnat bedöma om kontrollen varit tillräcklig och bidragit till att minska risker.

[3] Phishing är bedrägerimejl, där avsändaren uppmanar mottagaren att ge ut känsliga uppgifter eller klicka på osäkra länkar. I det här fallet genomförde kommunen ett phishing-test, för att mäta hur de anställda reagerade på phishing efter utbildningen.

De intervjuade ser positivt på genomförda utbildningsinitiativ avseende informationssäkerhet, men anser att det bör tydliggöras att utbildning är obligatorisk och att uppföljning av deltagande därför bör ske noggrant. Det lyfts även under intervjuer att endast närmsta chef har möjlighet att se vilka som genomfört eller inte genomfört utbildningar. Således försvårar detta uppföljning på högre nivå och kräver en ökad dialog mellan chefsleden.

4.2.4 Bedömning

Vår bedömning är att kommunstyrelsen till stor del har etablerat en ändamålsenlig organisation för informationssäkerhetsarbetet utifrån det ansvar som finns reglerat i riktlinjen. Ansvarsfördelningen bör emellertid tydliggöras genom anvisningar för informationssäkerhet. Då anvisningarna för informationssäkerhet ännu inte är färdigställda bedömer vi att ansvaret inte är tydliggjort.

En informationssäkerhetsspecialist finns för samordning och stöd men behöver få ett tydliggjort uppdrag att granska verksamheten, vilket inte görs i nuläget. Vi vill även poängtera att vi ser en risk med att omfördela arbetsuppgifterna för informationssäkerhetsspecialisten. Främst utifrån det arbete som det finns behov av i form av att etablera en tydlig styrning och en stärkt uppföljning, men även det behov av stöd som vi uppfattar att förvaltningarna har från informationssäkerhetsspecialist.

Vi bedömer att det är väsentligt att samtliga nämnder säkerställer att det finns ett tydligt informationsägarskap i förvaltningen. Detta så att det ansvar som vilar på informationsägare etableras och upprätthålls samt att en efterlevnad av riktlinjen för informationssäkerhet säkerställs.

Vi anser att utbildning bör vara obligatorisk för samtliga medarbetare som hanterar information och/eller är IT-användare i kommunen. Uppföljning av genomförd utbildning är ett linjeansvar och krav om utbildning och uppföljning av genomförandet bör därför göras av ansvarig chef.

4.3 Informationssäkerhet

4.3.1 Informationsklassning och riskhantering

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. Då kommunen i vissa delar bedriver samhällsviktig verksamhet och omfattas av NIS-direktivet finns för dessa förstärkta krav av ett systematiskt och riskbaserat informationssäkerhetsarbete.

I kommunens riktlinje för informationssäkerhet finns en beslutad modell för informationsklassning. Av intervjuer framgår att kommunen använder KLASSA[4] som metod för sina informationsklassningar. Enligt uppgift saknas en gemensam lagringsplats för genomförda klassningar. Av intervjuer framgår att det finns skillnader avseende informationsklassning mellan förvaltningarna avseende i hur stor utsträckning dessa har gjorts.

Kommunens centrala IT-avdelning uppger att de bedriver ett aktivt arbete med informationsklassning där cirka 40 system är klassade i nuläget. Totalt har kommunen runt 200 system och applikationer. Det är främst de större systemen som har klassats men även vissa äldre system har prioriterats. Vi har tagit del av exempel på genomförda klassningar som styrker detta.

Av intervju med kommunens IT-avdelning framgår att avdelningen vid behov och efter förfrågan deltar i förvaltningarnas riskanalyser och informationsklassningar tillsammans med informationssäkerhetsspecialisten. Då jobbar avdelningen nära verksamheterna och bidrar med stöd utifrån ett IT-säkerhetsperspektiv. Utifrån genomförda informationsklassningar i förvaltningarna uppger IT-avdelningen att de varit med och hjälpt till att vidta tekniska åtgärder. Som vi tidigare nämnt så har IT-avdelningen i vissa fall nekat redan upphandlade system, då de IT-tekniska riskerna bedömdes vara för stora.

Socialförvaltningen bedriver ett aktivt informationssäkerhetsarbete, där informationsklassning ingår som en del. Förvaltningen uppger vidare att de har ett samarbete med IT-avdelningen och informationssäkerhetsspecialisten utefter behov vid informationsklassningar. Förvaltningen har i sitt arbete upprättat rutiner utifrån krav i NIS-direktivet. Avseende uppföljning av informationsklassningar uppger förvaltningen att de har rutiner och arbetssätt för omprövning av genomförda klassningar och

[4] KLASSA är ett verktyg för informationsklassificering som tillhandahålls av Sveriges kommuner och regioner (SKR).

riskanalyser. Vi har tagit del av informationsklassningar genomförda av socialförvaltningen.

Samhällsbyggnadsförvaltningen uppger att de endast till liten del har genomfört informationsklassningar för system och information som används i verksamheter som inte är samhällsviktiga och således inte omfattas av NIS-direktivet.[5] Det finns en systemöversikt och utsedda ansvariga för dessa system, vilket uppges vara runt 40.

Det uppges finnas en god systematik avseende informationsklassning och riskanalys inom de verksamheter som omfattas av NIS. Det framgår vidare att förvaltningen saknar kompetens för att genomföra informationsklassningar och riskanalyser. Stöd från kommunens informationssäkerhetsspecialist har nyttjats i hög grad för att etablera ett mer systematiskt informationssäkerhetsarbete, inom framför allt VA-verksamheten. 2018 gjorde Livsmedelsverket en tillsyn utifrån efterlevnad av NIS-direktivet. Tillsynen resulterade i ett antal åtgärder som kommunen behövde vidta, bland annat att tillsätta en informationssäkerhetssamordnare, vilket gjordes på central nivå. Det fanns därtill ett antal tekniska åtgärder som behövdes och förvaltningen uppger i intervju att de arbetat nära IT-avdelningen för att få detta på plats. Åtgärder har följts upp av Livsmedelsverket efter tillsynen och de har varit nöjda med den progression som gjorts inom förvaltningen.

Barn- och utbildningsförvaltningen uppger att de aktivt arbetar med informationsklassning, exempelvis vid införande av nya verksamhetssystem. Uppföljningen av informationsklassningarna ses dock som ett utvecklingsområde och uppges ske utan en högre grad av systematik. Vi har tagit del av informationsklassningar för förvaltningen.

Kultur- och fritidsförvaltningen uppger vid intervju att de inte klassat information inom sina verksamheter.

4.3.2 Bedömning

Kommunstyrelsen

Vi bedömer att kommunstyrelsen i stora delar bedriver ett systematiskt arbete med riskanalyser och informationsklassningar för kommungemensamma system genom IT-avdelningens arbete. Vår bedömning är vidare att kravställning av IT-säkerhetsåtgärder görs utifrån genomförda riskbedömningar och informationsklassningar.

Informationsklassningar genomförs i kommunen utifrån en vedertagen modell. Då modellen är etablerad bör riktlinjen revideras med ett tydliggörande att det är KLASSA som ska användas. Uppföljning av arbetet skulle även underlättas av en gemensam lagringsplats och hantering av resultat från klassningar. Detta skulle innebära att informationssäkerhetsspecialist och IT-avdelningen vid behov skulle kunna kontrollera klassningar och använda relevant information i uppföljande eller utvecklande syfte.

[5] Network and Information Security Directive (2016/1148), översatt till Nätverks- och informationssäkerhetsdirektivet (NIS) innehåller krav på säkerhet i nätverk och informationssystem i verksamhet som bedöms som samhällsviktig. Exempel på sådan verksamhet är hälso- och sjukvård, leverans och distribution av dricksvatten, energi och digital infrastruktur.

Socialnämnden

Vi bedömer att socialnämnden bedriver ett systematiskt arbete med riskanalyser och informationsklassningar. Kravställning av IT-säkerhetsåtgärder görs utifrån analys och bedömning av skyddsvärdet.

Samhällsbyggnadsnämnden

Vi bedömer att samhällsbyggnadsnämnden i de delar av verksamheten som omfattas av NIS-direktivet bedriver ett systematiskt arbete med informationsklassning och riskanalyser. För de samhällsviktiga verksamheterna kravställs IT-säkerhetsåtgärder utifrån analys och bedömning av skyddsvärdet. Det är dock av vikt att nämnden tillser ett systematiskt arbete med informationsklassning och riskanalys även för den information och de system som hanteras i övriga verksamheter.

Barn- och utbildningsnämnden

Vi bedömer att barn- och utbildningsnämnden i stora delar bedriver ett systematiskt arbete med riskanalyser och informationsklassningar. Kravställning av IT-säkerhetsåtgärder görs utifrån analys och bedömning av skyddsvärdet. Vi anser emellertid att förvaltningen bör tillse att genomförda klassningar och riskanalyser följs upp regelbundet för att möta nya hot och risker.

Kultur- och fritidsnämnden

Vi bedömer att kultur- och fritidsnämnden i nuläget inte arbetar systematiskt med vare sig riskanalyser eller informationsklassning. Vi anser att nämnden bör tillse att ett sådant arbete initieras i dess verksamheter för de system och den information som förvaltningen ansvarar för.

4.4 IT-säkerhetsåtgärder

Det har genomförts ett antal förbättringar de senaste åren. Exempelvis har IT-avdelningen fått medel för nya licenser under 2021. Det anges av intervjupersoner att arbetet mot den nya plattformen i huvudsak påbörjades i och med detta. I och med den nya licensmodellen har kommunen väsentligt höjt sin IT-säkerhetsförmåga. Bland annat finns aktiva cyberskydd och analysverktyg.

Intervjuer påvisar emellertid att det finns behov av ett antal tekniska implementationer i IT-infrastrukturen för att stärka IT-säkerheten. Det finns enligt uppgift ett antal föråldrade system som kommunen har avtal om och ett beroende mellan olika system och integrationer som försvårar att uppdatera IT-miljön enligt nuvarande praxis och standarder. IT-avdelningen uppger dock att de anser sig ha mandat att påtala till berörda förvaltningar om sårbarheter finns för att uppmärksamma dem om att åtgärder behöver vidtas.

I intervjuer beskrivs att vissa processer och samarbeten behöver utvecklas, bland annat kring kravställning av säkerhet vid inköp av nya system. Där har IT-avdelningen vid tillfällen fått stoppa inköp sent i processen eller när system redan köpts in då de bedömt att systemen inte är tillräckligt säkra att integrera i IT-miljön.

Det saknas en komplett systemdokumentation av IT-miljön men uppges finnas en bra överblick över separata delar samt en god kontroll av respektive systemförvaltare. Dock så anges att det finns olika nivåer av systemförvaltare och även ett flertal system som inte har någon utsedd förvaltare. Det finns etablerade rutiner för att regelbundet uppdatera system och applikationer så att de får nya säkerhetsrutiner installerade.

Vid intervjuer framgår att IT-avdelningen arbetar med ett projekt avseende detektering av intrång för att hitta lämpliga verktyg anpassade efter kommunens behov och förutsättningar.

Åtkomst och behörighet för användare har skärpts och användare uppges i nuläget ha olika roller, med olika behörighet, vilka baseras på arbetsuppgifter och yrkesroll. IT-avdelningen arbetar också i nuläget med att införa multifaktorsautentisering, vid tiden för granskningen är det endast en förvaltning där detta inte är slutfört.

Av intervjuer framgår att IT-säkerhetsarbetet följts upp genom tekniska test under 2020. Då anlitades en konsult för att genomföra ett penetrationstest avseende kommunens system. Intervjupersoner uppger att resultatet utifrån testet var tillfredsställande. En genomlysning av IT-miljön gjordes även under 2021 vilken bidragit till en nulägesbild över åtgärder som IT-avdelningen planerar för. Enligt uppgift omvärldsbevakar IT-avdelningen, för att fånga upp hot och risker. Omvärldsbevakningen görs emellertid inte per rutin och dokumenteras inte.

En kontinuitetsplan ska beskriva hur verksamheten ska bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas av störning under en längre specificerad tidsperiod. Dessa ska även finnas tillgängliga vid bortfall av IT. IT-enheten uppger vid intervju att de har en kontinuitetsplan. Den uppges dock vara i behov av revidering.

4.4.1 Bedömning

Vi bedömer att det i stora delar finns ett systematiskt arbetssätt med IT-säkerhet avseende central IT-infrastruktur. Vi uppfattar dock att det finns identifierade behov av ett flertal tekniska implementationer för att stärka kommunens IT-säkerhet. Vår bedömning är att kommunstyrelsen bör efterfråga en sammanställning från IT-avdelningen som redovisar behov utifrån en riskanalys. Detta så att investeringar kan prioriteras och planeras utifrån en bedömning av kritiska sårbarheter som riskerar att leda till stora konsekvenser.

IT-avdelningen har med regelbundenhet genomfört penetrationstest och genomlysningar för att identifiera tekniska sårbarheter. Vår bedömning är därför att det görs systematiska uppföljningar av implementerade säkerhetsåtgärder. Utifrån nuvarande säkerhetsläge med en ökad hotbild uppmanar vi även att IT-enheten inrättar rutiner för att löpande omvärldsbevaka säkerhetsläget med cyberhot och uppmärksammade sårbarheter inom IT för att vid behov vidta skyndsamma åtgärder för att skydda kommunens system och information.

4.5 Incidenthantering

Information om incidenthantering saknas i den kommunövergripande riktlinjen för informationssäkerhet. Av intervjuer framgår att det saknas en gemensam rutin för incidenthantering. Det innebär att incidenter i nuläget inte sammanställs så att det finns en samlad bild av inträffade incidenter. Det finns dock ett pågående arbete och ett förslag till rutin har upprättats men inte fastställts.

Intervjupersoner beskriver att kommunens IT-avdelning är mottagare av de incidenter som anmäls och att incidenterna loggas i IT-avdelningens ärendehanteringssystem. Det är supporten som tar emot incidenterna. Det går att ta fram listor över inträffade incidenter om behov av detta finns.

Medarbetare från socialförvaltningen uppger att arbetet med incidenthantering sker förvaltningsvis. Användare inom förvaltningen rapporterar inträffade incidenter till kommunens IT-avdelning, genom mejl eller telefonkontakt. Incidenter diarieförs därefter. Intervjupersoner uppger att incidentrapporteringen inom socialförvaltningen ses som ett förbättringsområde. Rutiner och arbetssätt gällande incidentrapportering utifrån NIS-pliktig verksamhet finns inom förvaltningen.

Av intervju med kultur och fritidsförvaltningen framgår att medarbetare enligt rutin ska kontakta närmsta chef vid personuppgiftsincident. Vid misstanke om dataintrång finns inga rutiner. Intervjupersoner framhåller att medarbetarna vid sådana misstankar tar kontakt med kommunens IT-avdelning.

Av intervju med samhällsbyggnadsförvaltningen framgår att det finns en god struktur för incidenthantering inom deras NIS-verksamheter i enlighet med lagkrav. Dessa rutiner uppges vara kända av all personal inom VA. För de resterande verksamheterna kontaktas IT-avdelning, registrator eller närmsta chef för att anmäla incidenter.

Av intervju med barn- och utbildningsförvaltningen framgår att de rapporterar incidenter till kommunens IT-avdelning. De har även tagit fram interna rutiner avseende personuppgiftsincidenter.

4.5.1 Bedömning

Vi bedömer att det i nuläget saknas tydliga och övergripande rutiner för incidenthantering. Vi anser att det är av vikt att kommunstyrelsen fastställer incidenthanteringsrutiner och kommunicerar dessa till kommunens verksamheter för att säkerställa en likvärdig incidenthantering i kommunen. IT-avdelningen har i vissa delar en etablerad organisation med beredskap för att hantera allvarligare incidenter eller störningar. Det är av vikt att denna upprätthålls och anpassas efter aktuella hot och risker.

Inträffade incidenter bör sammanställas, analyseras och följas upp så att åtgärder kan vidtas så att de inte inträffar på nytt. Det är utifrån nuvarande rutiner och hantering svårt att avgöra huruvida rapporteringsfrekvensen är tillräcklig. Vi bedömer att det är väsentligt att tillse att medarbetarna i kommunens verksamheter har god kännedom om vad incidenter är och hur dessa ska hanteras och anmälas.

5 Slutsats och rekommendationer

5.1 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen till viss del har en tillräcklig intern styrning och kontroll för att säkerställa att arbetet med IT- och informationssäkerhet bedrivs på ett ändamålsenligt sätt. Socialnämnden och barn- och utbildningsnämnden bedöms i huvudsak ha en tillräcklig intern styrning och kontroll inom området. Samhällsbyggnadsnämnden bedöms ha en tillräcklig intern styrning och kontroll inom VA-verksamheten (som står under NIS-direktivets krav). För övriga verksamheter inom samhällsbyggnadsförvaltningen bedömer vi dock att den interna styrningen och kontrollen inom området behöver utvecklas. Kultur- och fritidsnämnden bedöms inte ha säkerställt en tillräcklig intern styrning och kontroll inom området

Kommunstyrelsen har inte säkerställt en tillräcklig styrning då riktlinjen inte är tillräckligt detaljerad och anvisningar saknas för att tydliggöra ansvar och hur informationssäkerhetsarbetet ska bedrivas. I nuläget saknas en tillräcklig uppföljning av det arbete som genomförs. Då detta saknas finns inte tillräckliga underlag för kommunstyrelsen för att besluta om handlingsplan och resurser för de förbättringsåtgärder som det finns behov av för att stärka informationssäkerheten.

Socialnämnden och barn- och utbildningsnämnden genomför väsentliga aktiviteter inom informationssäkerhetsarbetet i enlighet med riktlinjerna. Arbetssätt och metoder finns- och det pågår ett aktivt arbete med informationsklassningar och riskanalyser. Därtill har utbildningsinsatser genomförts för att en medvetenhet och kunskap ska finnas. Detta gäller även samhällsbyggnadsnämndens samhällsviktiga verksamheter (som omfattas av NIS). Inom kultur- och fritidsnämnden och i samhällsbyggnadsnämndens ordinarie verksamhet finns i nuläget inte arbetssätt och metoder för att efterleva riktlinjer för informationssäkerhet.

Slutligen är vår bedömning att kommunstyrelsen behöver etablera gemensamma incidenthanteringsrutiner som är kända och tillämpas av samtliga verksamheter. Kommunstyrelsen bör besluta om dessa rutiner och etablera ansvar och organisation för att upptäcka, anmäla och hantera incidenter i syfte att vid behov kunna vidta förbättringsåtgärder för att minska risken att incidenter sker på nytt.

5.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Revidera riktlinje för informationssäkerhet i enlighet med granskningens iakttagelser, bland annat kring ansvar, krav på tekniska åtgärder, incidenthantering samt fastställa och implementera kompletterande anvisningar för informationssäkerhet
- Säkerställa att befintliga resurser för informationssäkerhetsarbetet (inkl. teknisk säkerhet) är tillräckliga och står i relation till identifierade behov och risker.
- Tydliggöra organisation, ansvar och arbetssätt för incidenthantering i linje med nya, upprättade rutiner så att en beredskap finns i händelse av IT-incidenter eller allvarlig störning.
- Säkerställa att former för granskning och uppföljning av informationssäkerhetsarbetet upprättas och tillse att detta regelbundet rapporteras till styrelsen.

Utifrån vår bedömning och slutsats rekommenderar vi samtliga nämnder att:

- Säkerställa att riktlinje för informationssäkerhet efterlevs genom att regelbundet följa upp det arbete som genomförs.
- Säkerställa att befintliga resurser för informationssäkerhetsarbetet är tillräckliga och står i relation till identifierade behov och risker.
- Löpande genomföra utbildning inom informationssäkerhet till samtliga medarbetare samt följa upp de insatser som genomförs.

Utifrån vår bedömning och slutsats rekommenderar vi kultur- och fritidsnämnden att:

- Säkerställa att informationsklassning och riskbedömning genomförs avseende den information som hanteras i förvaltningens system för att säkerställa att informationen har tillräckliga skyddsåtgärder.

Datum som ovan
KPMG AB

Jenny Thörn	William Andreasson	Liz Gard
Kommunal revisor	Kommunal revisor	Certifierad kommunal revisor