Granskningsrapport 2020

Genomförd på uppdrag av revisorerna
Januari 2021

Lunds kommun

Granskning av informationssäkerhet

Building a better working world

Sammanfattning

EY har på uppdrag av Lunds kommuns förtroendevalda revisorer genomfört en granskning av kommunstyrelsens arbete med informationssäkerhet. Granskningens syfte har varit att bedöma om kommunstyrelsens interna kontroll kopplat till IT- och informationssäkerhet är ändamålsenlig. Granskningen har fokuserat på styrning, organisation och incidenthantering.

Granskningen visar att kommunstyrelsen har etablerat ett grundläggande ramverk med policy, riktlinjer, mallar och andra dokument som underlättar och tydliggör styrningen av informationssäkerhetsarbetet. Det har dock identifierats brister. Det finns en avsaknad av tydliga kort- och långsiktiga målsättningar för informationssäkerhet. Därutöver saknas en långtgående vision och viljeriktning som är tydligt kopplat till verksamheternas, och kommunens, övergripande strategier.

Lunds kommun har en etablerad struktur med roller och ansvar för informationssäkerhet, men har fortsatt en bit att kvar i att etablera detta i verksamheterna. Det saknas rutiner och riktlinjer som tydliggör och säkerställer genomförande, utvärdering och utveckling av informationssäkerhetsarbetet. Det saknas också en tydlig utbildningsplan för informationssäkerhet.

Vidare framgår av granskning att Lunds kommun har ett grundläggande arbete med operationella rutiner för informationssäkerhetsarbete. Dessa rutiner är i stor utsträckning i linje med riktlinjer och god praxis, men brister har identifierats i bland annat processen för borttagande av behörigheter. Samt att det finns ett behov av att integrera informationssäkerhet som en del av incidenthanteringsprocessen.

Baserat på granskningens slutsatser och sammanfattande bedömning har ett antal huvudsakliga rekommendationer tagits fram. I avsnitt 3 presenteras även granskningens detaljerade rekommendationer. Vi rekommenderar kommunstyrelsen att:

- Tydliggöra processer och ansvar för koordinering och uppföljning av kommunens informationssäkerhetsabete
- Införa kontinuerliga och anpassade utbildningsinsatser
- Kartlägga samhällsviktiga tjänster och hantera dessa utifrån informationssäkerhet
- Etablera en långsiktig strategi och tydliga mål för kommunens informationssäkerhetsarbete
- Uppdatera processen för IT-förändringar med utgångspunkt i ett enat systemstöd
- Uppdatera processen för borttagande av behörigheter i kommunens informationssystem
- Säkerställa att informationssäkerhet är en tydlig del av kommunens risk- och sårbarhetsanalys

- Tydliggöra rutiner för hantering av informationssäkerhetsrelaterade incidenter
- Tydliggöra riktlinjer för uppföljning och övervakning av externa leverantörer
- Formalisera rutiner för säkerhetskopieringar och återläsningstester

Innehåll

1. Inledning

1.1 Bakgrund

Hantering av information i IT-system är idag en grundläggande del av kommuners verksamhet. Bristfällig säkerhet i informationshanteringen kan innebära risker för anställda och invånare. I takt med att den kommunala verksamheten digitaliseras blir fler och fler enheter uppkopplade och fler processer blir IT-beroende. Detta ökar kraven på att känslig information, såsom patientdata eller dokumentation, får ett ändamålsenligt skydd ifrån stöld eller förstörelse. Samtidigt ska informationen vara tillgänglig för rätt personer i rätt tid.

Under 2000-talet har ett antal olika direktiv, lagar och riktlinjer tagits fram för att stötta och tydliggöra, men också sätta krav på organisationer i deras arbete med informationssäkerhet. Under 2018 etablerades i svensk lag EUs dataskyddsförordning (GDPR), vilket har inneburit konsekvenser för hur verksamheter hanterar personuppgifter och information. Senare samma år etablerades lagen om nätverk- och informationssäkerhet för samhällsviktiga tjänster (NIS), som ställer speciella krav på säkerhet i nätverk[1] och informationssystem hos leverantörer av samhällsviktiga tjänster såsom el, vatten och digitala tjänster.

Konsekvenserna av otillräckliga säkerhetsåtgärder kan få effekt på kommunen och dess invånare. Att tappa kontrollen över potentiellt känslig information om kommunens verksamhet, dess anställda eller dess invånare riskerar inte bara att skada kommunens rykte och förtroende, utan kan även kräva kostsamma insatser för att återta kontrollen av den förlorade informationen. Ett bra informationssäkerhetsarbete är därför en förutsättning för effektiv och korrekt informationshantering. För att uppnå god informationssäkerhet krävs att man tar ett helhetsgrepp och skapar metoder som långsiktigt ger verksamheten det skydd den behöver.

Mot bakgrund av dessa utmaningar inom informationssäkerhet har kommunrevisionen i Lund beslutat att genomföra en granskning avseende kommunstyrelsens interna kontroll kopplat till IT- och informationssäkerhet.

1.2 Syfte och frågeställningar

Granskningens syfte är att bedöma om kommunstyrelsen har en ändamålsenlig intern kontroll avseende IT- och informationssäkerhet.
I granskningen besvaras följande frågeställningar:

- Är styrningen av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, ändamålsenlig?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?
- Är Lunds kommuns incidenthanteringsprocess ändamålsenlig?

[1] För definition, se bilaga 2

1.3 Genomförande och revisionskriterier

Granskningen har genomförts genom intervjuer med identifierade nyckelpersoner för kommunens IT- och informationssäkerhetsarbete. Därutöver har relevant styrdokumentation granskats. Granskningen är utförd mot god praxis inom informations- och IT-säkerhetsområdet och bygger på EYs granskningsprogram Cyber och Informationssäkerhet (GCI), med fokus på offentlig verksamhet.

GCI baseras på erkända ramverk såsom ISO/EC27000 - serien och Myndigheten för samhällsskydd och beredskaps (MSBs) metodstöd för informationssäkerhet.

Intervjuer har genomförts med:

- Digitaliseringschef
- Objektsförvaltare identitet
- IT – tekniker
- Objektsförvaltare Drift
- Chef IT – utveckling

Samtliga intervjuade har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta. Förteckning över intervjupersoner och dokumentation framgår av bilaga 1. En lista över definitioner framgår av bilaga 2.

1.4 Avgränsning

Granskningen syftar till att ge en översiktbild över hur Lunds kommun utformat sitt arbete med IT- och informationssäkerhet. Granskningen täcker således inte enskilda IT-system eller applikationer[2]. Vidare omfattar granskningen endast hantering av incidenter kopplat till IT- och informationssäkerhet och inte kommunens incidenthanteringsprocess i sin helhet.

Inom ramen för granskningen ingår inte att kontrollera att arbetet, såsom det är utformat, har genomförts. Vidare kommer granskningen inte att beröra informationssäkerheten i enskilda system eller hos enskilda verksamheter.

[2] För definition, se bilaga 2

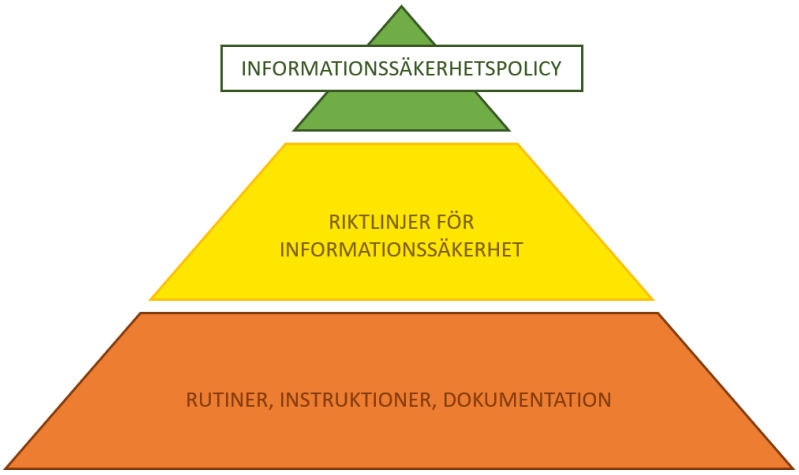
2. Iakttagelser

2.1 Styrdokument

Arbetet med IT- och informationssäkerhet i Lunds kommun utgår huvudsakligen ifrån en pyramidstruktur av styrningsdokument där *informationssäkerhetspolicyn* är tänkt att sätta upp mål och ramar som sedan förtydligas i *riktlinjer för informationssäkerhet,* se schematisk representation nedan. Policyn sätter upp ett antal mål för informationssäkerhetsarbetet, ett antal krav som organisationen har på sig att uppfylla, samt vilka som har det övergripande ansvaret. Ett tydliggörande av ansvarsfördelningen görs också i riktlinjerna som även innehåller kortfattade rollbeskrivningar. Riktlinjerna berör huvudområdena inom IT- och informationssäkerhet såsom:

- Lösenordspolicy
- Behörighetshantering
- Förändringshantering
- Incidenthantering

Vidare har även kommunstyrelsen upprättat ett antal rutiner och instruktioner för hur informationssäkerhetsarbetet ska bedrivas, såsom mallar för riskanalys[3] och kontinuitetsplan[4] samt metodstöd för informationsklassning[5].



Figur 1 visar en schematisk överblick över strukturen av styrdokumenten i Lunds kommun.

För att få hela bilden av Lunds informationssäkerhetsarbete bör även *digitaliserings- och systemförvaltningsmodellen* nämnas. Modellen innehåller en beskrivning av hur IT-avdelningen leder IT- och digitaliseringsinitiativ i kommunens verksamheter.

Kommunstyrelsen har inte initierat något arbete för att undersöka om man faller under säkerhetsskyddslagen eller lagen om informationssäkerhet för samhällsviktiga

[3] För definition, se bilaga 2
[4] För definition, se bilaga 2
[5] För definition, se bilaga 2

tjänster. Det finns en informellt uttalad ambition att initiera detta arbete under året, men vid perioden för granskningen (maj 2020) har detta inte påbörjats.

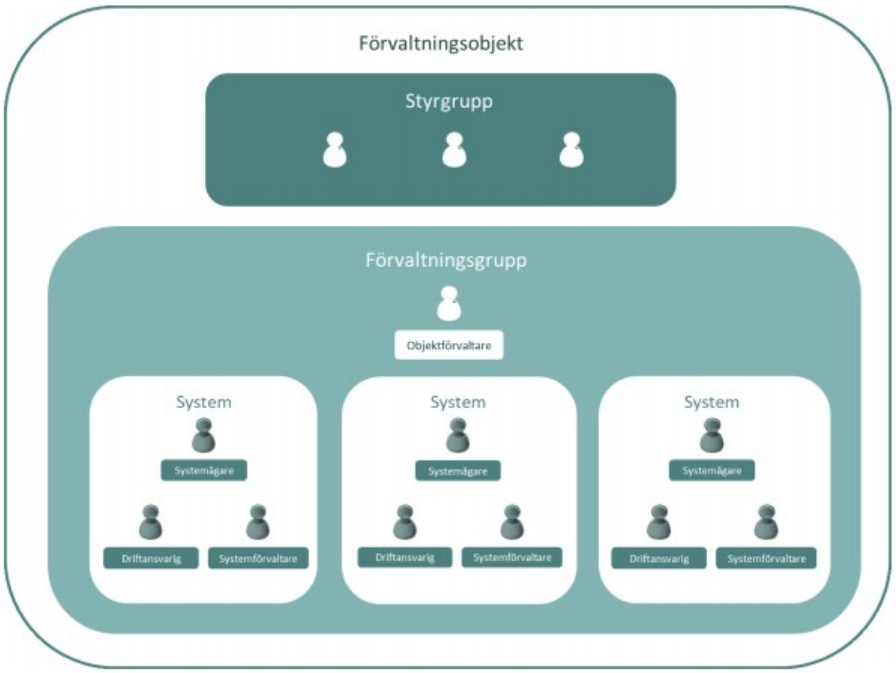
2.2 Ansvarsfördelning och organisation

Organisationen och dess ansvar för Lunds kommuns informationssäkerhetsarbete beskrivs i kommunens informationssäkerhetspolicy, riktlinjer för informationssäkerhet samt i digitaliserings- och systemförvaltningsmodellen.

Lunds kommuns informationssäkerhetspolicy fastställer att det är kommundirektören som ansvarar för att strategiskt leda och samordna kommunens arbete med IT- och informationssäkerhet. Det är sedermera digitaliseringschefen som ansvarar för att utveckla styrande dokument, riktlinjer och andra hjälpmedel samt att följa upp och samordna informationssäkerhetsarbetet. Det faktiska ansvaret för informationen och informationssäkerheten inom ett verksamhetsområde ligger dock på förvaltningarna. Inom förvaltningarna är det huvudsakliga ansvaret fördelat över chefer, medarbetare, systemägare, systemförvaltare[6] och driftansvariga[7]. Det är upp till chefen att säkerställa att varje medarbetare har ändamålsenlig kunskap om informationssäkerhet för att genomföra sitt arbete. Riktlinjerna fastställer också att varje system i kommunen ska ha en systemägare som har det övergripande ansvaret för systemet och dess användning. Detta innebär även ansvar för att systemet ska uppfylla de informationssäkerhetskrav som ställs på systemet utifrån rådande lagar och riktlinjer, samt säkerställa att informationsklassning genomförs, att kontinuitetsplaner tagits fram och fastställts. Under systemägaren finns systemförvaltare, som ansvarar för systemets dagliga funktionalitet. Systemförvaltarens arbete stöds av driftsansvarig, som innehar den tekniska kompetensen att upprätthålla den dagliga IT-systemdriften.

Även kommunens digitaliserings- och systemförvaltarmodell beskriver roller som är relevanta från ett informationssäkerhetsperspektiv. Digitaliserings- och systemförvaltarmodellen antogs 2009. I den framgår att alla kommunens IT-system ska organiseras i så kallade förvaltningsobjekt[8] med en styrgrupp och en förvaltningsgrupp där systemen ingår, se bild nedan.

[6] För definition, se bilaga 2
[7] För definition, se bilaga 2
[8] För definition, se bilaga 2



Figur 1 Lunds kommuns förvaltningsmodell.

Styrgruppen beslutar om förvaltningsplan för objektet. Förvaltningsgruppen har ett rapporteringsansvar till styrgruppen vilket innefattar ett antal processer såsom incidenthantering och behörighetshantering, att rapportera kritiska incidenter eller resultat av periodisk behörighetsgallring.

Utöver nämnda forum och ansvar är det värt att nämna att kommunen även har en säkerhetsgrupp som övergripande ansvarar för säkerhetsfrågor inom kommunen. Säkerhetsgruppen ansvarar för att varje år sammanställa risker och i dessa frågor samarbetar de med förvaltningsobjekten som bistår med interna riskanalyser som genomförts. I dagsläget är informationssäkerhet inte en uttalad del av de riskanalyser som genomförs, något som säkerhetsgruppen identifierat som ett förbättringsområde.

2.3 Personal och utbildning

Vid perioden för denna granskning (maj 2020) är det de intervjuades uppfattning att man har kommit olika långt med att implementera ansvar och organisation i enlighet med riktlinjer och förvaltningsmodell, i de olika förvaltningsobjekten. Detta tros vara en följd av att kunskapen om informationssäkerhet varierar mycket mellan förvaltningsobjekten. Vid en nulägesanalys som genomfördes under 2019 pekades det speciellt på brister i kompetens inom förvaltningsobjekten som resulterat i ofullständiga kontinuitetsplaner.

Vid intervjuer uppges att det finns en ambition om att bredda och öka kunskapsnivån om informationssäkerhet i verksamheterna för att öka deras möjlighet att bedriva sitt arbete självständigt. Det genomförs dock inte några utbildningar och finns i nuläget inte heller en utbildningsplan för förvaltningsobjekten att följa.

Som följd av rådande situation upplever kommunen ett behov av att tillsätta mer resurser med tydligt ansvar för att samordna och stödja förvaltningsobjektens informationssäkerhetsarbete. Ett sådant initiativ påbörjades under mars 2020 och en funktion med titeln ”informationssäkerhetssamordnare” planeras att tillsättas under hösten 2020. Ansvaret som kommer med rollen kommer innefatta att stötta verksamheterna i deras informationssäkerhetsarbete och ta fram en uppföljningsprocess.

2.4 Externa leverantörer och hantering av leverantörsavtal

Alla upphandlingar av kommunövergripande informationssystem i Lunds kommun underordnar sig lagen om offentlig upphandling och går via kommunens centrala inköpsfunktion. Upphandling av mindre IT-verktyg sker ute på de enskilda förvaltningarna. Instruktioner för hur leverantörer ska handha information de har tillgång till har tagits fram tillsammans med ett metodstöd för IT-upphandling, men inga specifika upphandlings- och leverantörsavtal för informationssäkerhet har definierats.

Vid IT-upphandling ansvarar kommunens inköpsfunktion för att upphandlingen sker och att avtal upprättas. Som en del av detta definieras servicenivåavtal (SLA)[9] mellan leverantör, ansvarig systemägare och systemförvaltare, vilket sedan inköpsfunktionen ansvarar för att föra in i avtalet. Vid implementation av verksamhetssystem flyttas ansvaret från inköpsfunktionen till förvaltningsobjektet. Det finns ett arbete för att öka systemförvaltares delaktighet i upphandlingsprocessen. Detta förväntas bidra till ökad transparens rörande behov och kravställning. Arbetet inkluderar ett initiativ gällande informationsklassning, riskanalys och åtgärdsplan enligt verktyget KLASSA[10] som en del av alla IT-upphandlingar.

För befintliga externa leverantörer och redan upphandlade informationssystem har inga särskilda centrala riktlinjer för uppföljning av informationssäkerhet definierats. Det ingår i systemägares och förvaltares ansvar att ha en kontinuerlig dialog med leverantören rörande driften och säkerheten i systemen. Regelbundna möten som bedrivs med de externa leverantörerna har identifierats, men dessa har oftast varit av driftskaraktär och informationssäkerhetsrelaterade ämnen är inte specificerade.

2.5 Operationella rutiner

2.5.1 Behörighetshantering

Åtkomst till Lunds kommuns IT-miljö hanteras via en e-tjänst för behörighetshantering. Vid nyanställning ansvarar närmsta chef till den nyanställda för att skicka beställning av nytt användarkonto till kommunens Service Desk. Service Desk ansvarar sedan för att lägga upp användare i den gemensamma IT-miljön. Förändrad behörighet samt borttag av behörighet genomförs i nuläget enligt samma process, att ansvarig chef lägger en separat beställning för varje system. Det genomförs inte en gemensam periodisk genomgång av kommunanställdas behörigheter. Detta ansvarar varje

[9] För definition, se bilaga 2
[10] För definition, se bilaga 2

verksamhetssystems förvaltare för, enligt rutinen ska detta genomföras minst en gång årligen. Det är också en informell rutin att följa upp den periodiska genomgången i förvaltningsobjektets styrgrupp. Systemförvaltaren ansvarar även för att ta fram en rutin för behörighetshantering.

2.5.2 Drift och IT-incidenthantering

Lunds kommun ansvarar för driften av ett antal av sina informationssystem. För dessa system definieras det servicenivåavtal (SLA) mellan IT och systemförvaltaren som reglerar vilka driftsnivåer som ska hållas. Detta ska även inkludera vilken mängd säkerhetskopieringar[11] och återläsningstester[12] som ska genomföras. I dagsläget finns ingen rutin för återläsningstester, planer för detta har informellt initieras men det är inget som vid granskningstillfället (maj 2020) ännu fastställts. Informationsklassning ligger till grund för vilken servicenivå som ett system ska ha, och om inte rekommenderad nivå väljs ska detta motiveras i avtalet.

Enligt Lunds kommuns incidenthanteringsprocess rapporteras incidenter in via ärendehanteringssystemet[13] Servis till kommunens support som är uppbyggd med tre olika supportnivåer. Incidenter prioriteras enligt en förutbestämd ordning beroende på hur pass kritisk incidenten bedöms vara för verksamheten. Ordningen är inte specifikt kopplat till ett informationssäkerhetsmässigt perspektiv, incidenter bedöms allmänt enligt en lathund av Service Desk när ärendet registreras.

Om ingen av supportnivåerna klarar av att lösa en incident ska den eskaleras enligt en rapporteringstrappa; 1. Servicechef; 2. Driftschef; 3. Digitaliseringschef. När en incident är löst dokumenteras ärendet i Servis och kommuniceras enligt rutin ut till alla berörda av störningen.

2.5.3 Programförändringar

Förändringshantering i Lunds kommun hanteras enligt en central process för förändringar som sedermera beroende på utfall mynnar ut i olika bi-processer. Behov av förändringar kan inkomma via ett antal olika kanaler men det skapas alltid ett ärende i Servis. Två gånger i veckan sker ett ärendeberedningsmöte där behovet av förändringen klarläggs, ansvar fördelas och ytterligare direktiv fastställs innan beslut tas om förändringen ska delas ut. Därefter hanteras förändringen i olika etablerade processer beroende på förändringens natur. Förändringar i existerande system hanteras via Servis. Det sker dock ingen uppföljning av att processen följs. Om förändringen innebär en större utvecklingsinsats går förändringen vidare som ett enskilt projekt. Projekt hanteras i informationssystemet TFS där testdokumentation och beslut om lansering dokumenteras.

[11] För definition, se bilaga 2
[12] För definition, se bilaga 2
[13] För definition, se bilaga 2

2.5.4 Informationsklassning och riskanalys

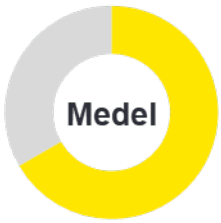
Informationsklassning är en metod som hjälper organisationer att välja rätt åtgärder för att skydda informationen. Lunds kommun har skapat ett verktyg för informationsklassning som är baserat på SKR:s verktyg KLASSA. Verktyget används i arbetet att identifiera vilka av kommunens informationssystem som innehåller skyddsvärd information. För att standardisera och säkra utförande av klassningsrutinerna har mallar tagits fram för hur kommunen ska utföra informationsklassning genom KLASSA-verktyget. Instruktionen beskriver bland annat syftet med klassningsrutinerna och hur klassningen genomförs och dokumenteras. Efter utförd klassning sparas dokumentationen av ansvarigt förvaltningsobjekt. Systemägare ansvarar för att informationsklassning genomförs på sitt system samt att den följs upp och revideras enligt kommunens angivna intervaller om minst en gång per år.

En riskanalys genomförs för att identifiera och bedöma sådana risker som skulle kunna äventyra säkerheten för informationen i kommunens system. Säkerhetsavdelningen genomför årligen en övergripande riskanalys. Den omfattar dock inte explicit informationssäkerhet men visst bidrag har inkommit ifrån förvaltningsobjekten i form av dokumentation på genomförda riskanalyser.

3. Sammanfattande iakttagelser och rekommendationer

Under granskningen har iakttagelser identifierats inom granskade områden. För varje iakttagelse lämnas rekommendationer som syftar till att stödja Lunds kommun i dess framtida arbete med informationssäkerhet. Iakttagelserna har klassificerats enligt tre risknivåer avseende hur omfattande dess eventuella inverkan anses vara:

Prioritering låg: Observation som ej direkt påverkar verksamhetens mål, men som kan medföra ineffektiv verksamhet, mindre brister i IT- och informationssäkerhet, efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.



Prioritering medel: Observation som anses kunna ha påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av verksamhetens resurser.

Prioritering hög: Observation av större karaktär som anses kunna ha hög påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer.

3.1 Strategi, styrning och organisation

3.1.1 Tydliggöra processer och ansvar för koordinering och uppföljning av kommunens informationssäkerhetsabete

Iakttagelse

Långsiktig informationssäkerhet kräver ett helhetsgrepp och fungerande arbetssätt för att säkerställa att kommunens information ges ändamålsenligt skydd. Lunds kommun har etablerat ett grundläggande ramverk i form av förvaltningsmodell, policy, riktlinjer och mallar för sitt informationssäkerhetsarbete. Det har dock noterats att den övergripande styrningen av arbetet med informationssäkerhet saknar tydlighet avseende ansvar, mandat och uppföljning.

Risken med otydligt ansvar, mandat och uppföljning är att kommunens policyer och riktlinjer inte efterlevs och att skyddsåtgärder genomförs på en ojämn nivå runtom i kommunen.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Definiera den roll som ska ansvara för att samordna och driva kommunens arbete med informationssäkerhet med tydliga ansvar kopplat till kommunens mål med informationssäkerhet:
  - Säkerställ att rollen har ett tydligt mandat i relation till berörda parter såsom IT, säkerhetsavdelningen samt kommunens förvaltningar.
  - Utvärdera om rollens ansvar ska inkludera ”omvärldsbevakning” av nya direktiv, riktlinjer eller god praxis som kan vara nödvändig för att kommunens informationssäkerhetsarbete utvecklas i den takt som omvärlden kräver.
- Etablera processer och instruktioner för tydlig uppföljning av verksamheternas informationssäkerhetsarbete, företrädesvis med koppling till kommunens nuvarande systemstöd för aktivitetshantering för förvaltningsplanen.

3.1.2 Införa kontinuerliga och anpassade utbildningsinsatser

Iakttagelse

Ändamålsenlig kunskap om informationssäkerhet är viktig för en organisations förmåga att på kort sikt förebygga, upptäcka och hantera incidenter relaterade till informationssäkerhet. På lång sikt kan avsaknad av kompetensutveckling påverka organisationens förmåga att utveckla sitt informationssäkerhetsarbete i den takt som verksamheten och omvärlden kräver.

Under granskningen har det noterats att Lunds kommun inte har tagit fram en utbildningsplan för IT- och informationssäkerhet. Vidare har Lunds kommun inte säkerställt kontinuerligt anpassade utbildningsinsatser. Exempelvis behöver objektsägare som genomför informationsklassning ha en specifik kunskap medan intern service bör ha mer kunskap om incidenthantering.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Genomföra en analys för att identifiera olika målgrupper och lämpliga aktiviteter anpassade för varje målgrupps kunskapsbehov.
- Ta fram utbildningsplan för kontinuerlig utbildning enligt ovan analys och som tydliggör ansvar och uppföljning av utbildningsinitiativ.
- Säkerställa att alla med direkt ansvar för informationssäkerhet får relevant utbildning utifrån roll och ansvar.

3.1.3 Kartlägga samhällsviktiga tjänster och hantera dessa utifrån informationssäkerhet.

Iakttagelse

Under 2018 etablerades EU-direktivet NIS (Nätverk och Informationssäkerhet) i svensk lag som kräver ett informationssäkerhetsarbete som är specialanpassat för leverantörer av samhällsviktiga tjänster. Samhällsviktiga tjänster är kritiska funktioner för samhällets välmående och löper därför större risk att utsättas för attacker med informationsstöld och samhällspåverkan som följd.

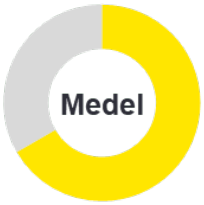
Lunds kommun har inte genomfört en analys om någon del av organisationen omfattas av lagstiftningen, vilket lagen kräver. Det innebär också att potentiella samhällsviktiga tjänster som Lunds kommun ansvarar för kan ha bristfälligt skydd vilket ökar risken för IT- och informationssäkerhetsincidenter med stor samhällspåverkan som följd.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Genomföra en grundläggande analys av kommunens tjänsteutbud där potentiella leverantörer av samhällsviktiga tjänster kan identifieras och rapporteras till tillsynsmyndighet.
- Utarbeta ändamålsenliga processer i enligt med lag och föreskrifter för leverantörer av samhällsviktiga tjänster samt säkerställa kontinuerlig genomlysning av kommunens tjänsteutbud.
- Med utgångspunkt i kommunens nuvarande ramverk för informationssäkerhet, etablera ändamålsenliga processer för rapportering av incidenter till tillsynsmyndighet.

3.1.4 Etablera en långsiktig strategi och tydliga mål för kommunens informationssäkerhetsarbete



Iakttagelse

För att långsiktig informationssäkerhet ska kunna uppnås är det viktigt att kommunen har strategiska mål som definierar viljeriktning för de kommande 3-5 årens informationssäkerhetsarbete. Lunds kommun har mål för sin informationssäkerhet, men det är inte tydligt hur dessa mål kopplas till andra relevanta strategiska mål inom kommunen såsom kommunens övergripande strategi, säkerhetsstrategi samt IT- och digitaliseringsstrategi.

För att viljeriktningen ska vara tydlig för organisationen är det viktigt att även ha kortsiktiga mål som definierar hur den långsiktiga strategin ska realiseras de kommande 1-2 åren. Lunds kommun har krav som ställs på verksamhetens arbete, men inte tydligt definierat mål som kan stämma av och mäta kommunens utveckling.

Avsaknaden av en tydlig strategi på lång och kort sikt kan påverka effektiviteten i arbetet med informationssäkerhet, samt arbetets integration med andra digitaliserings- och säkerhetsinitiativ.

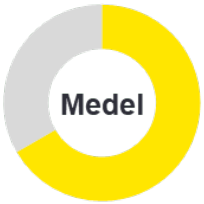
Rekommendation

Kommunstyrelsen rekommenderas att:

- Tydligt definiera och prioritera ramverkets innehåll, omfattning, kortsiktiga och långsiktiga mål och vision med avseende på kommunens dagliga verksamhet och övergripande vision och strategi.
- Etablera en process för utvärdering, uppföljning och utveckling av uppsatta mål.

3.2 IT-drift, förändringar samt behörigheter

3.2.1 Uppdatera processen för IT-förändringar med utgångspunkt i ett enat systemstöd



Iakttagelse

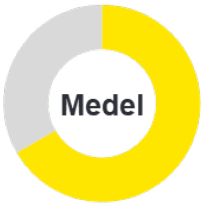
Att ha god insikt i de förändringar som görs i kommunens informationssystem är viktigt för säkerställandet av ändamålsenlig driftnivå och säkerheten för informationen som hålls i systemen. I dagsläget har Lunds kommun en stor och komplex förändringsprocess som använder flertalet olika systemstöd för att hantera och dokumentera flödet. Brist på tydlighet i processen medför en risk att den inte efterföljs och skapar flera, potentiell konflikterande, källor för information. Detta ökar risken för komplikationer till följd av obehöriga eller felaktiga ändringar i systemen.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Ta fram en ny förändringsprocess för IT-förändringar som är harmoniserad med den översiktliga förändrings- och projektprocessen. Företrädesvis supporteras den nya processen för IT-förändringar av ett systemstöd istället för flera.

3.2.2 Uppdatera processen för borttagande av behörigheter i kommunens informationssystem



Iakttagelse

Borttagande och ändring av behörigheter är en viktig process för att motverka informationsstöld och obehöriga ändringar samt säkerställa ansvarsfördelning i kommunens informationssystem. Det finns ingen central, kommungemensam process för borttagande av behörighet. Processen för ändring och borttagande av användare är personberoende vilket ökar risken för att behörigheter inte tas bort i tid.

Rekommendation

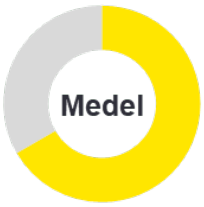
Kommunstyrelsen rekommenderas att:

- Ta fram en central process för borttagande och ändring av behörigheter.
- Utreda möjligheten att inkludera processen i den pågående omstruktureringen av centrala HR-processer vid nyanställning och vid avslut av anställning.

3.3 Incident-, risk- och informationshantering

3.3.1 Säkerställa att informationssäkerhet är en tydlig del av kommunens risk- och sårbarhetsanalys

För att kommunen ska vara beredd att hantera nuvarande och kommande hot är det viktigt att kontinuerligt genomföra risk- och sårbarhetsanalys av IT- och informationssäkerhet. Lunds kommun har inte genomfört en övergripande riskanalys av informationssäkerhet.



Iakttagelse

Kommunens säkerhetsavdelning ansvarar för att sammanställa en övergripande risk och sårbarhetsanalys men den tar inte specifikt informationssäkerhet i beaktning. Därmed ökar risken för allvarliga systemfel med störningar i processer som är kritiska för samhället, samt informationsläckage som följd.

Risken blir särskilt stor då kommunen inte tagit fram en övergripande kontinuitetsplan som innefattar hantering av incidenter relaterade till informationssäkerhet. Kommunen har inte heller säkerställt via uppföljning att ändamålsenliga kontinuitetsplaner tagits fram för alla förvaltningar.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Säkerställa att risk och sårbarhetsanalyser för IT- och informationssäkerhet genomförs i alla kommunens förvaltningar, samt att processen för att föra in dem i säkerhetsavdelningens övergripande risk och sårbarhetsanalys tydliggörs och formaliseras.
- Samordna att kontinuitetsplaneringen i förvaltningarna genomförs och att de inkluderar informationssäkerhet. Förslagsvis genom en övergripande kontinuitetsplan som sammanfattar de åtgärder som tas runtom i alla förvaltningar.

3.3.2 Tydliggöra rutiner för hantering av informationssäkerhetsrelaterade incidenter

Incidenthanteringsprocessen är avgörande för riskbaserad hantering av incidenter som minimerar skada och tiden för återställning till normal drift.

Iakttagelse

Kommunen har en dokumenterad incidenthanteringsprocess som är etablerad och kommunicerad inom verksamheten, men den saknar harmonisering med processerna för informationsklassning och riskanalys.

Detta innebär att prioriteringen av incidenter inte tillräckligt tydligt beaktar klassningen och riskanalysen, vilket ökar risken för att incidenter relaterade till informationssäkerhet inte hanteras riskbaserat och med nödvändig prioritet.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Säkerställa att processen för incidenthantering uppdateras och tydligt belyser hanteringen av informationssäkerhetsrelaterade incidenter. Speciellt fokus bör läggas på att stötta prioriteringen av incidenter med avseende på utfallet av informationsklassning och riskanalys.

3.3.3 Tydliggöra riktlinjer för uppföljning och övervakning av externa leverantörer

Organisationer förlitar sig mer och mer på tredjepartsleverantörer av IT-lösningar för att uppnå sina mål. Det ökade beroendet av externa leverantörer introducerar nya risker.

Iakttagelse

Kommunen har i dagsläget inga rutiner för standardiserad kravställning rörande informationssäkerhetsrelaterad övervakning och rapportering för IT-leverantörer. Det är systemförvaltarnas ansvar att följa upp på driftsnivåer samt hantering av incidenter med respektive IT leverantör.

Det saknas dock riktlinjer på vilka områden, främst relaterat till informationssäkerhet, som bör följas upp. Detta leder till att uppföljningarna håller olika nivå, samt ökar risken för påverkan av incidenter som är bortom kommunens kontroll.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Komplettera processen för att granska tredjepartsleverantörer av IT-lösningar med tydligare riktlinjer och krav på innehåll samt deltagande av sakkunniga i avstämningar.
- Se över hur informationssäkerhet inkluderas som en faktor i kravställningen vid upphandling. Initiativet med att genomföra informationsklassning som en del av upphandlingen är ett bra exempel på detta, men kan kompletteras ytterligare med rapporteringskrav och granskningsrätt som standard.

3.3.4 Formalisera rutiner för säkerhetskopieringar och återläsningstester

Iakttagelse

Säkerhetskopieringar av kommunens information är den process som säkerställer att ingen kritisk information går förlorad vid eventuella incidenter och störningar. Återläsningstester som säkerställer fullständighet och riktighet i kopierad information är en förutsättning för ändamålsenligt arbete med säkerhetskopiering.

I dagsläget har Lunds kommun ingen formaliserad rutin för under vilka förutsättningar eller hur ofta återläsningstester ska genomföras. Detta ökar risken för att säkerhetskopieringar inte går att återläsa och kritisk information går förlorad.

Rekommendation

Kommunstyrelsen rekommenderas att:

- Säkerställa att det tas fram en process för årliga återläsningstester som specificerar hur de bör genomföras, för vilka system, vem som ansvarar samt hur ofta som det rekommenderas att genomföras. Processen bör anpassas efter olika IT-system och ta i beaktning faktorer såsom klassning av informationen i systemet samt hur pass kritiskt systemet är för verksamheten.

4. Svar på revisionsfrågor

Granskningen har syftat till att på uppdrag av revisorerna genomföra en övergripande genomgång av kommunens IT- och informationssäkerhet. Granskningen har utgått från tre revisionsfrågor, vilka besvaras nedan.

Är styrningen av arbetet med IT- och informationssäkerhet, för de behov som kommunens verksamhet har, ändamålsenlig?

Ett ledningssystem för informationssäkerhet är den del av ledningssystemet som styr verksamhetens informationssäkerhet. Styrningen av informationssäkerhetsarbetet i Lunds kommun gentemot LIS-ramverket, bedöms vara **delvis ändamålsenligt**. Detta grundar sig i att Lunds kommun har tillsett att rutiner samt grundläggande riktlinjer och policyer finns, så som informationssäkerhetspolicy, riktlinjer, förvaltningsmodell samt mallar. Det finns även en ambition att tillsätta resurser för att möta ett ökat behov av välfungerande informationssäkerhetsarbete. Vi har dock noterat brister rörande kommunens mål och vision med sitt informationssäkerhetsarbete och hur man ska uppnå en god kommungemensam nivå av säkerhet. Vidare har brister noterats i utbildningsinsatser, behörighet- och åtkomsthantering samt styrning av tredjepartsleverantör och hur man säkerställer tillräcklig insyn i leverantörers arbete med informationssäkerhet.

Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till IT- och informationssäkerhet efterlevs?

Arbetet med uppföljning av efterlevnad av beslut och styrningsdokument relaterat till informationssäkerhet bedöms vara **delvis ändamålsenligt**. Svaret grundar sig i att Lunds kommun inte har upprättat en ansvarsfördelning rörande uppföljning av arbetet. Det saknas en ändamålsenlig uppföljning av att nämndernas arbete med informationssäkerhet har implementerats och genomförts. Detta inkluderar exempelvis uppföljning av externa leverantörsavtal avseende informationssäkerhet och kontroll för borttag av användares behörigheter. Kommunen saknar en ansvarig funktion eller roll för samordning och koordinering mellan processer inom IT- och informationssäkerhetsarbetet vilket blir synligt i avsaknaden av övergripande informationsklassning och kontinuitetsplan samt brister i den övergripande riskanalysen.

Är Lunds kommuns incidenthanteringsprocess ändamålsenlig?

Lunds kommun bedöms ha en **ändamålsenlig** incidenthanteringsprocess. I och med att kommunens incidentprocess är utformad enligt god praxis och är väl fungerande. Visst utrymme för förbättring finns, till exempel i form av harmoniserande av prioriteringsordning med avseende på IT- och informationssäkerhet.

5. Slutsats och sammanfattande bedömning

Digitaliseringen skapar inte bara utvecklingsmöjligheter utan möjliggör fler sätt att attackera verksamheters information och system. De senaste åren har antalet cyberattacker ökat kraftigt, och bakom dem finns inte bara kriminella och hackare utan även statsstödda aktörer som har stor uthållighet och substantiella resurser. Genom att påskynda åtgärder för att öka säkerheten inom kritisk infrastruktur, höjs hela samhällets robusthet mot yttre störningar. IT och informationssäkerhet med stödjande lagstiftning i form av GDPR, Säkerhetsskyddslagen och NIS-direktivet är sätt att göra detta.

Granskningen har syftat till att bedöma om kommunstyrelsen har en ändamålsenlig intern kontroll avseende IT- och informationssäkerhet. Utifrån granskningens syfte och grunderna för ansvarsprövning bedömer vi att kommunstyrelsen delvis har en ändamålsenlig intern kontroll avseende arbetet med IT- och informationssäkerhet.

Kommunen har ett grundläggande informationssäkerhetsramverk i form av styrande dokument, roller och ansvar men brister i att inkorporera IT- och informationssäkerhet i verksamhetens dagliga arbete samt övrigt säkerhetsarbete. I kommunens arbete med att implementera och befästa ramverket bör därför fokus vara på att etablera processer och dokumentationsstöd för samordning, uppföljning och utbildning som säkerställer en ändamålsenlig säkerhetsnivå runtom i kommunen.

Lund den 20 januari 2021

Aleksandar Jovanovic
EY

Max Wann Adebahr
EY

Johan Andersson
EY

Bilaga 1: Källförteckning

Intervjuade roller:

- Digitaliseringschef
- Objektsförvaltare identitet
- IT – tekniker
- Objektsförvaltare Drift
- Chef IT – utveckling

Dokumentation:

- Informationssäkerhetspolicy för Lunds kommun
- Riktlinjer för informationssäkerhet
- Digitaliserings- och systemförvaltningsmodellen
- Rutinbeskrivningar
  - Incidenthanteringsprocessen
  - Hantera tekniska förändringar
  - Hantera förändringsbehov
- Exempel på utföranden:
  - Risk- och sårbarhetsanalys_W3D3 2016 ver.1.0
  - Ks Kontinuitetsplan för W3D3 2016
  - Informationssäkerhetsklassning Procapita BoU 2019 - Handlingsplan - 2019-11-21
- Informationssäkerhet - Behovsbeskrivning av tjänster
- Servicenivåbeskrivning var 203.2

Bilaga 2: Definitioner

Active Directory (AD): Katalogtjänst vilken lagrar information om resurser (såsom användare). Separata IT-system kan kopplas till Active Directory och både inloggning och behörighetsroller i systemen kan således styras genom inställningar och rolluppsättning i Active Directory. Detta möjliggör för central användarhantering och automatisk inloggning.

Applikation: Datorprogram med olika typer av funktionalitet beroende på applikationens syfte. Applikationen finns lagrad på en dator eller en server.

Driftansvarig: Ansvar innefattar att ta fram och underhålla driftdokumentation till ett informationssystem samt assistera vid eventuella incidenter eller problem.

Databas: En databas är en katalogtjänst med indexerad information om resurser (såsom tex. användare).

Förvaltningsobjekt: Styrande enhet inom vilken ett antal olika informationssystem för en viss typ av kommunens verksamhet innefattas. Förvaltningsenheten styrs av en styrgrupp som beslutar om förvaltningsplan och budget. System är uppdelade på olika förvaltningsgrupper inom ett förvaltningsobjekt.

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

KLASSA: Klassa är ett verktyg för att genomföra en kombinerad informationsklassning, riskanalys och åtgärdsplan, framtagen av Sveriges Kommuner och Regioner (SKR). Verktyget är framtaget i enlighet med ISO27001.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.

Penetrationstester: Test av informationssystem, nätverk eller webbapplikationer för att identifiera sårbarheter vilka kan utnyttjas av angripare.

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats.

Systemförvaltare: Ansvarar för att operativt sköta ett systems förvaltning inom givna ekonomiska ramar.

Systemägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.

Säkerhetskopiering: Kopia av den information som finns i en databas eller på en server.

Återläsningstest: För att säkerställa att en säkerhetskopia fungerar som den ska och inte är sönder eller ofullständig så är det god praxis att genomföra tester av de säkerhetskopior som genomförts. Testet går ut på att återläsa in kopian in på servern eller databasen igen och granska innehållets korrekthet och fullständighet.

Ärendehanteringssystem: Ett ärendehanteringssystem är en typ av informationssystem som används för att dokumentera information rörande genomförandets av olika processer eller rutiner inom verksamheten, såsom exempelvis förändringsprocessen eller incidenthanteringsprocessen. Exempel på ärendehanteringssystem som Lunds kommun använder är Servis, TFS och Stratsys.