Granskning av informationssäkerhet

Rapport

Huddinge kommun

KPMG AB

2020-12-03

Antal sidor 21

Bilaga: 1

Huddinge kommun
Granskning av informationssäkerhet

2020-12-03

Innehållsförteckning

1 Sammanfattning

Vi har av revisorerna i Huddinge kommun fått i uppdrag att översiktligt granska kommunens rutiner kring informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2020.

Informationssäkerhet är ett begrepp som används om säkerhet för information som hanteras i kommunens IT-system. Allt mer information hanteras idag med olika tekniska lösningar och aldrig förr har offentlig sektor hanterat sådana mängder information som görs idag. Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod.

Granskningen har syftat till att bedöma om kommunen har ett ändamålsenligt och systematiskt arbetssätt med informationssäkerhet.

Vår sammanfattade bedömning utifrån granskningens syfte är att kommunstyrelsen inte har ett ändamålsenligt och systematiskt arbetssätt avseende informationssäkerhet.

- **Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i kommunen?**

  Den organisation som finns är ändamålsenlig men begränsad i sin omfattning. Dessutom finns det otydligheter kring roller och ansvarsfördelning, dels mellan kommunstyrelsens förvaltning och verksamhetsförvaltningarna dels mellan kommunstyrelsens förvaltnings funktioner som är uppdelade på olika sektioner och avdelningar.

- **Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrat i kommunens verksamheter?**

  Det finns ett systematiskt och ändamålsenligt arbetssätt dokumenterat genom kommunens styrdokument som behandlar informationssäkerhet. Dock bedömer vi detta arbetssätt inte vara förankrat i kommunens verksamheter.

- **Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?**

  Det finns en ansvars- och rollfördelning mellan verksamheterna och den centrala förvaltningen. Dock framstår denna som inte helt tydlig och det framgår av intervjuerna att verksamheterna inte alltid vet vad som förväntas av dem och vilket stöd de kan få. Fördelningen mellan kommunstyrelsens förvaltnings olika sektioner och avdelningar fungerar bra internt, men uppfattas som otydlig ut mot resten av den kommunala organisationen.

- **Arbetar kommunens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?**

  Nej. Det huvudsakliga ansvaret för riskidentifiering och riskanalys återfinns hos verksamheterna. Där saknas dock i dagsläget kompetens för att genomföra ändamålsenlig identifiering och analys.

- **Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?**

  Nej. Verksamheterna identifierar sårbarheter och åtgärder inom ramarna för internkontrollplanen och uppföljningen av systemsäkerhetsanalyser. Dock framkommer det av intervjuerna att sårbarheterna och åtgärderna ofta återkommer vid upprepade tillfällen. Verksamheterna saknar stöd och resurser för att bedriva detta arbete på ett tillfredställande sätt.

Utifrån granskningens resultat rekommenderar vi kommunstyrelsen att:

- Implementera en informationssäkerhetspolicy.
- Implementera en obligatorisk utbildning om informationssäkerhet med kontinuerliga och regelbundna uppföljningsutbildningar.
- Implementera en systematisk och regelbunden rapportering och uppföljning av informationssäkerhetsarbetet till kommunledningen och kommunstyrelsen.
- Säkerställa att alla verksamheter har tillgång och kännedom om de styrdokument som gäller för verksamheten, samt vilka ansvarsförhållanden som gäller.
- Säkerställa att informationssäkerhetsorganisationen har en tillräcklig omfattning för att möta kommunens behov.
- Ser över möjligheten att implementera nya rutiner för att säkerställa att anställda har rätt behörigheter.
- Implementera en rutin för rapportering av informationssäkerhetsincidenter i ett avvikelserapporteringssystem.
- Säkerställa att det finns en ändamålsenlig organisation för rapportering av incidenter enligt NIS-direktivet.

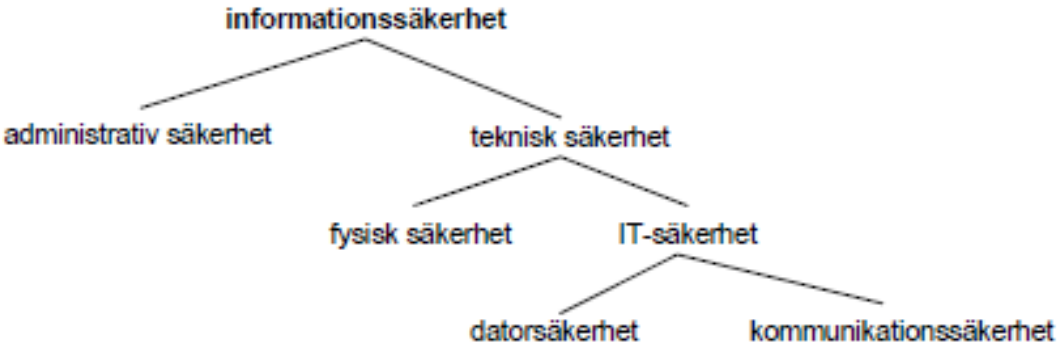
2 Inledning/bakgrund

Vi har av revisorerna i Huddinge kommun fått i uppdrag att översiktligt granska kommunstyrelsens rutiner kring informationssäkerheten. Uppdraget ingår i revisionsplanen för år 2020.

Informationssäkerhet är ett begrepp som används om säkerhet för information som hanteras i kommunens IT-system. Allt mer information hanteras idag med olika tekniska lösningar och aldrig förr har offentlig sektor hanterat sådana mängder information som görs idag. Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod.

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 är involverade och rätt organiserade för uppdraget. IT-säkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av kommunens kärnverksamhet.

Den 1 augusti 2018 trädde NIS (Nätverk och informationssystem) -direktivet i kraft genom lagen (2018:1174) om informationssäkerhet för leverantörer av samhällsviktiga och digitala tjänster. NIS-direktivet skärper kraven på informationssäkerhet vad gäller integritet och tillgänglighet, vilket innebär att personer, processer och teknologi ska beaktas i arbetet för att säkerställa informationssäkerheten inom alla verksamheter som berörs. Överlag krävs en bättre förståelse för risk-klassificering av information och system, konsekvensberedskap och åtgärdsplaner krävs för att skapa bättre motståndskraft vid eventuella attacker.



Bilden ovan illustrerar de olika begreppens relation till varandra.

Revisorerna granskade 2017 kommunens IT-organisation och kunde konstatera att det fanns ytterligare arbete att önska gällande tydligheten i kommunikationen mellan IT-funktionen och övriga verksamheter i kommunen samt i utvecklingsfrågor.

Revisorerna bedömer att det systematiska informationssäkerhetsarbetet fortfarande inte är ändamålsenligt och att det finns risk för brister i kommunstyrelsens organisering och arbetssätt inom området.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att kommunstyrelsen rutiner avseende informationssäkerheten behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera om kommunstyrelsen har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Granskningen ska besvara följande revisionsfrågor:

- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i kommunen?
- Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrat i kommunens verksamheter?
- Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?
- Arbetar kommunens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?
- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- 6 kap. 6 § kommunallagen (2017:725) (KL)
- Tillämpbara interna regelverk, policys och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risk

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier
- Intervjuer med berörda tjänstepersoner, däribland informationssäkerhetssamordnare, IT-säkerhetsansvarig, IT-säkerhetsarkitekt, dataskyddsombud, säkerhetschef, IT-strateg, sektionschef för strategi- och verksamhetsutvecklingssektionen, biträdande kommundirektör samt IT-ansvarig vid barn- och utbildningsförvaltningen och biträdande socialdirektör och systemförvaltningsledare vid socialförvaltningen.

Rapporten är faktakontrollerad av samtliga intervjuade.

2.4 MSB:s rekommendationer

Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram ett omfattande metodstöd och rekommendationer för arbetet med informationssäkerhet. I revisionskriterierna (se 2.2 Revisionskriterier) för denna granskning ingår rekommendationerna för ledningssystem för informationssäkerhet (LIS9, samt NIS-direktivet). Dessa summeras kortfattat i detta avsnitt. För materialet i sin helhet, se referens i fotnoterna.

2.4.1 Ledningssystem för informationssäkerhet (LIS)[1]

Det övergripande syftet med LIS är att utgöra ett stöd för styrningen av informationssäkerhetsarbetet i en organisation. LIS bör enligt dessa rekommendationer utgå ifrån den högsta ledningen och en informationssäkerhetspolicy kan anses vara grunden för LIS, som i sin tur kan kompletteras med ytterligare styrdokument. Detta sammantaget ska utgöra en vägledning för verksamheternas medarbetare att följa ledningens riktlinjer och rutiner.

För att detta arbete ska kunna genomföras enligt styrdokumentens principer och krav är det av stor vikt att innehållet i dessa dokument är väl förankrat bland alla medarbetare i organisationen. Utbildnings- och informationsinsatser framhålls därför som en viktig del av arbetet med att förankra ett ledningssystem.

MSB rekommenderar att LIS tillämpar standarderna som återfinns i den svenska och internationella standardserien SS-ISO/IEC 27000, [2]för att skapa ett enhetligt arbete som följer en tydlig process samtidigt som det underlättar för extern bedömning.

2.4.2 NIS (Network and Information Security)-direktivet[3]

NIS-direktivet infördes i Sverige 2018. NIS-direktivet ställer krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga tjänster och vissa digitala tjänster (leverantörerna kan finnas både i privat och offentlig sektor). Samhällsviktiga tjänster är tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet och dessa är indelade i sju sektorer:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn

[1] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/standardisering-inom-informationssakerhet/lis-iso-27000/
[2]ISO/IEC 27000-serien är en samling standarder för informations- och IT-säkerhet, och omfattar bland annat ledningssystem för informationssäkerhet (27001), riktlinjer för styrning av informationssäkerhet (27002) och Information Security Risk Management (27005)
[3] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/

- Leverans och distribution av dricksvatten
- Digital infrastruktur

Leverantörer har själva ansvaret att undersöka om huruvida de berörs av NIS-regleringen, och om sådana förekommer ska dessa rapporteras till MSB.

3 Resultat av granskningen

3.1 Organisation

3.1.1 Huddinge kommuns organisation för informationssäkerhetsarbetet

Informationssäkerhetsarbetet i Huddinge kommun utgår huvudsakligen från informationssäkerhetssamordnaren vid trygghets- och säkerhetssektionen som är organiserad under kommunstyrelsens förvaltning. Informationssäkerhetssamordnaren ansvarar för att ta fram kommunövergripande riktlinjer och rutiner för informationssäkerhet.

Det finns ett utvecklat och ingående samarbete mellan informationssäkerhets-samordnaren och kommunstyrelsens förvaltnings IT-avdelning med veckomöten där aktuella frågor diskuteras. Det framgår av intervjuerna att det finns ett ömsesidigt beroende mellan de två avdelningarna och att uppdelningen mellan de båda avdelningarna syftar till att motverka oegentligheter och jävssituationer. Generellt ansvarar informationssäkerhetssamordnaren för styrningen och IT-avdelningen för utförandet.

Det förekommer även ett samarbete med dataskyddsombudet men under intervjuerna framgår att detta samarbete borde vara mer omfattande än vad det i dagsläget är. Det begränsas av att tjänsten dataskyddsombud endast omfattar 25 procent.

Säkerhetschefen är chef för trygghets- och säkerhetssektionen och således informationssäkerhetssamordnarens chef. Säkerhetschefen sitter inte i kommunledningsgruppen, utan är organiserad under kommunstyrelsens förvaltnings förvaltningschef. Under intervjuerna framgår att informationssäkerhetsfrågor inte lyfts upp i kommunledningen i den utsträckning som skulle vara önskvärt och en av anledningarna till det uppges vara att säkerhetschefen inte är en del av kommunledningsgruppen. Med uppdelat ansvar i kommunstyrelsens förvaltning anses det föreligga en risk att informationssäkerhetsfrågor fastnar i den stuprörsstruktur som bedöms föreligga i kommunstyrelsens förvaltning i dagsläget. Under intervju med biträdande kommundirektör framhålls att detta dock är något som beaktas i det pågående arbetet med omstrukturering i kommunen.

Av intervjuerna framgår en samstämmig bild av att det inom nuvarande organisation är svårt att nå fram till kommunledningsgruppen med frågor som rör informationssäkerhet. Detta anses leda till att informationssäkerhet är ett område som inte prioriterats och att många av de förslag och projekt som drivs inom området inte slutförts eller implementerats då det saknats beslut eller tilldelade resurser från kommunledningen.

De förvaltningar som intervjuats (barn-och utbildningsförvaltningen och socialförvaltningen) uttrycker att det i stort saknas en organisation inom förvaltningarna för arbetet med informationssäkerhet.

3.1.2 IT-säkerhetsorganisation

IT-säkerhetsorganisationen är en del av kommunstyrelsens förvaltnings digitaliseringsavdelning vilken omfattar ungefär 40 personer med olika typer av tjänster. IT-säkerhet ansvarar bland annat för de kravspecificeringar som ställs vid upphandling av system, vilket har sin grund i de systemsäkerhetsanalyser som genomförs.

Huddinge kommun har en egen IT-drift förlagd till två datahallar. Mycket arbete läggs på att bygga redundans i IT-driften och IT-systemen. Detta har lett till att man har en stabil miljö där det rapporteras få avvikelser och andra händelser. Det framgår dock under intervjuerna en farhåga i att det kan leda till att det inte investeras eller sker lika mycket satsningar inom området.

3.1.3 Dataskyddsorganisation

Dataskyddsorganisationen består idag av ett dataskyddsombud om 25 procent. Dataskyddsombudet är även e-arkivarie till 75 procent och är organiserad under kansliet vid kommunstyrelsens förvaltning. Av intervjuerna framgår att dataskyddsombudets omfattning inte anses tillräcklig för att arbeta med dataskyddsfrågor på ett proaktivt sätt, utan arbetet blir endast reaktiv hantering. Dessutom anses samverkan och samordning mellan dataskyddsombudet och den övriga informationssäkerhetsorganisationen begränsad till följd av detta. Det lyfts fram en önskan om att dataskyddsombudet bör ha en tydligare juridisk specialistkompetens. Den nuvarande lösningen med ett dataskyddsombud på 25 procent är en tillfällig lösning som förlängs var tredje månad.

I rapporten *Dataskyddsombudets roll och omfattning av tjänsten*[4] finns förslag på en ny och mer omfattande dataskyddsorganisation som tagits fram av det nuvarande dataskyddsombudet. I rapporten finns förslag på hur dataskyddsorganisationen kan utvecklas. Bland annat föreslås att ett dataskyddsråd skulle inrättas bestående av informationssäkerhetssamordnare, arkivarie, IT-representant, jurister samt förvaltningsrepresentanter. Rådet syfte skulle vara att arbeta med det operativa och proaktiva dataskyddsarbetet. Till detta anses det behövas ett dataskyddsombud med en omfattning av 100 procent för att uppnå en bättre dataskyddsmognad. Det andra förslaget baseras på att varje nämnd tillsätter ett eget dataskyddsombud med ett operativt ansvar. En sådan tjänst anses behöva omfatta ungefär 20–25 procent. Dataskyddsombud vid kommunstyrelsens förvaltning tilldelas en sammankallande och samordnande roll för att säkerställa ett likartat arbete i varje nämnd, där en omfattning om 100 procent anses önskvärt. Det framgår av intervjuerna att det finns en ambition från ledningen att utöka dataskyddsombudet till 100 procent och organisatoriskt flytta funktionen till trygghets- och säkerhetssektionen för att sedan kunna bygga upp en systematik i hanteringen av bevakning- och tillsyn av dataskyddsfrågor. Under

[4] Dnr KS-2020/284

intervjuerna framgår även att barn- och utbildningsförvaltningen och socialförvaltningen önskar att dataskyddsombudets tjänst utökas.

3.1.4 Bedömning

Huddinge kommun har idag en organisation på plats för arbete med informationssäkerhetsfrågor. Omfattningen av denna organisation är dock begränsad och vår bedömning är att den i dagsläget inte möter kommunens behov och inte heller lever upp till de mål och krav som ställs i lag och styrdokument.

Ansvaret för informationssäkerhet i Huddinge är i hög utsträckning decentraliserat där verksamheterna ansvarar för den praktiska implementeringen och genomförandet. Vår bedömning är dock att en etablerad organisation för ett systematiskt och ändamålsenligt informationssäkerhetsarbete saknas i verksamheterna och att den centrala stödfunktionen i dagsläget inte är tillräcklig för att bidra med ett tillräckligt stöd för verksamheterna. Vi anser att det finns kompetens hos de som arbetar med dessa frågor idag och att det arbete som bedrivs är ändamålsenligt. De brister som vi identifierat bedöms bero på att organisationen inte är tillräckligt omfattande för att driva igenom informationssäkerhetsarbetet i kommunens alla verksamheter.

I dagsläget är ansvaret för informationssäkerhet inom kommunstyrelsens förvaltning fördelat mellan trygghets- och säkerhetssektionen som arbetar med övergripande styrning, digitaliseringsavdelningen som arbetar operativt med tekniska lösningar och system, samt kansliet där dataskyddsombudet återfinns. Vår bedömning är att samarbetet mellan dessa enheter generellt fungerar bra men att det finns otydligheter i roller och ansvarsfördelning utåt i organisationens verksamheter.

3.2 Styrdokument

I Huddinge kommun finns idag ett antal styrdokument som berör informationssäkerhetsområdet. Det övergripande dokumentet för detta är *Program för trygghet och säkerhet 2018–2021*[5]. Detta ligger sedan till grund för ett antal riktlinjer som berör informationssäkerhet:

- *Riktlinje för informationssäkerhet*[6]
- *Riktlinjer för behandling av personuppgifter*[7]
- *Riktlinje för användning av Internet, e-post och mobila enheter*[8]

Nedan följer en kort beskrivning av ovan nämnda program och riktlinjer.

3.2.1 Program för trygghet och säkerhet 2018-2021

Programmet definierar ansvarsområden för kommunens arbete med trygghet och säkerhet samt fastställer övergripande mål. Ett av dessa mål är informationssäkerhet. Kommunen ska enligt detta mål arbeta med uppsatta krav om konfidentialitet, riktighet,

[5] Beslutad av Huddinge kommunfullmäktige 2018-06-18
[6] Beslutad av Huddinge kommunfullmäktige 2019-12-09
[7] Beslutad av Huddinge kommunfullmäktige 2019-12-09, § 15
[8] Beslutad av Huddinge kommunfullmäktige 2015-01-12. § 17

tillgänglighet och spårbarhet. Programmet definierar även roller och ansvarsförhållanden mellan informationsägare, systemägare, systemansvariga samt för de som hanterar informationstillgångar. Programmet framhåller även att all personal i verksamheterna ska ha tillräcklig kunskap för att informationssäkert handhavande ska säkerställas inom verksamheterna. Till detta tillkommer att risk- och sårbarhetsanalyser ska genomföras för verksamhetskritiska system samt vid nyanskaffning av system. Slutligen lyfts krav som ställs på informationssäkerhetsarbetet genom NIS-direktivet och dataskyddsförordningen (GDPR).

Kommunen har tidigare haft en informationssäkerhetspolicy men den är avvecklad och det som framgick av den har istället förts in i *Program för trygghet och säkerhet 2018-2021.*

3.2.2 Riktlinje för informationssäkerhet

Riktlinjen syftar till att säkerställa spårbarhet, tillgänglighet, riktighet och åtkomstbegränsning för kommunens informationstillgångar och omfattar organisatoriska, fysiska och logiska skyddsåtgärder.

Riktlinjen anger klassificering av information efter konfidentialitet, riktighet, tillgänglighet och spårbarhet som ska bedömas utifrån konsekvensnivå. Detta förtydligas i bilagan *Informationsklassificeringsmodell för informationstillgångar*.

För att uppnå målet med informationssäkerhet formuleras ett antal krav:

- Personal ska ha tillräcklig kunskap för sitt uppdrag och kontinuerligt utbildas.
- Informationstillgångar ska klassificeras.
- Risk- och sårbarhetsanalyser ska genomföras årligen för verksamhetskritiska system samt inför nyanskaffning av verksamhetssystem.
- Baserat på uppföljning av riskanalys ska åtgärdsplaner tas fram årligen.
- Systemägaren säkerställer att säkerhetsbehov identifierade i riskanalys och informationsklassificering åtgärdas. Detta ska dokumenteras i systemförvaltningsplaner som ska fastställas och följas upp.
- Informationsincidenter rapporteras, utvärderas och åtgärdas.
- Kontinuitetsplaner upprättas i alla verksamheter.
- Behörigheter ska tilldelas formellt och kontinuerligt följas upp.
- Kontinuerlig uppföljning sker i enlighet med ledningssystem för informationssäkerhet.
- Upphandlande verksamhet ska samråda med informationssäkerhetssamordnare vid upphandling angående vilka lag- och säkerhetskrav som måste beaktas.

3.2.3 Riktlinjer för behandling av personuppgifter

Riktlinjerna förtydligar de åtaganden och principer som gäller vid behandling av personuppgifter. Syftet är att utgöra ett stöd för kommunens verksamheter att bedriva arbetet med personuppgiftsbehandling på ett effektivt och kvalitativt sätt samtidigt som utifrån gällande lagstiftning.

Riktlinjerna definierar vad personuppgifter och behandling av personuppgifter är, samt förtydligar roller och ansvar för personuppgiftsansvarig och dataskyddsombud. Det formulerar också den juridiska grunden för personuppgiftsbehandling med tillhörande skyldigheter och rättigheter.

Utöver detta formuleras även krav på tekniska och organisatoriska säkerhetsåtgärder som ämnar att säkerställa en lämplig säkerhetsnivå vilket inkluderar konsekvensbedömningar och tillvägagångssätt vid personuppgiftsincidenter.

3.2.4 Riktlinje för användning av Internet, e-post och mobila enheter

Riktlinjen syftar till att rikta ökade krav på informationssäkerhet som följer av flexibla arbetsformer och vänder sig till de som är verksamma inom kommunen eller använder deras verksamhetssystem.

Till detta följer en ansvarsbeskrivelse där kommunstyrelsen har det övergripande ansvaret. Det är ett chefsansvar att personalen utbildas och är medvetna om vilka säkerhetsbestämmelser som gäller för verksamheten. Varje förvaltning ska dessutom utföra riskanalyser, genomföra beslutade säkerhetsåtgärder och vara behjälpliga vid incidentutredningar.

Riktlinjen lyfter även fram principer och regler kring användning av internet, e-post och sociala medier samt förhållningssätt för distansarbete och mobil användning av IT. Det ställs krav på att beslut om mobil tillgång till information i verksamhetssystem ska föregås av en risk- och sårbarhetsanalys. Det framgår även krav på spårbarhet för information och andra tekniska säkerhetsåtgärder tillsammans med uppföljningskrav.

3.2.5 Bedömning

Huddinge kommun har etablerat en styrning för informationssäkerhetsfrågor genom styrdokument. Av dessa är *Program för trygghet och säkerhet 2018–2021* det övergripande dokument som utgör vision och mål för kommunens informationssäkerhetsarbete. Därtill följer riktlinjer som syftar till att uppfylla de mål som programmet sätter upp.

Vår bedömning är att de styrdokument som finns i dagsläget är ändamålsenliga och delvis innehåller vad som krävs för ett systematiskt informationssäkerhetsarbete. Däremot anser vi att det finns en lucka mellan de övergripande mål som återfinns i programmet och de krav och bestämmelser som riktlinjerna utgör samt att styrdokumenten bitvis brister när det gäller uppföljning. Tidigare har det funnits en informationssäkerhetspolicy men kommunen har valt att avveckla denna.

3.3 Informationssäkerhetsarbete

3.3.1 Systemsäkerhetsanalys

Vid nyanskaffning av system ska, i samband med upphandling, en systemsäkerhetsanalys genomföras. Analysen ligger sedan till grund för en kravspecificering som IT-avdelningen genomför, där den internationella standarden ISO 27001 samt NIST 800-53[9] utgör grunden för arbetet. Det är upp till verksamheterna att inkludera informationssäkerhetsorganisationen vid upphandling av system för att genomföra en systemsäkerhetsanalys. Det finns en framarbetad grundmall för hur en systemsäkerhetsanalys ska genomföras med en tillhörande instruktion. Upphandlingsenheten har upprättat en rutin att alltid koppla in informationssäkerhetssamordnaren samt IT-avdelningen vid alla kommunövergripande upphandlingar.

Systemsäkerhetsanalysen utgår från den information som ska behandlas i systemet, förvaltning av systemet, GDPR, vilka som förväntas använda systemet och informationsklassificering. I systemsäkerhetsanalysen inkluderas även kontinuitetsbehov, back-up samt sårbarheter med systemet.

Av *Instruktion för genomförande av SSA, systemsäkerhetsanalys* framgår att kommunens verksamhetssystem regelbundet ska följas upp med en ny systemsäkerhetsanalys. För system som kategoriseras som verksamhetskritiska ska detta ske årligen, och för övriga system var tredje år. Av intervjuerna framgår dock att denna uppföljning inte sker enligt rutin, endast ett fåtal av de verksamhetskritiska systemen ses över regelbundet.

3.3.2 Informationsklassificering

Idag arbetar kommunen efter modellen som återges i *Informationsklassificeringsmodell för informationstillgångar*. Det har förekommit diskussioner att övergå till KLASSA[10], men detta har inte beslutats än.

Av intervjuerna framgår att omfattningen av förvaltningarnas informationsklassificering är begränsad och att mognadsnivån och medvetenheten kring dessa frågor i verksamheterna generellt är mycket låg. Det finns dock en variation mellan förvaltningarna, de som regelbundet hanterar känslig information har en högre medvetenhet och kompetens än de andra. Under intervjuerna framgår att det behövs pedagogiska instrument för att förankra informationsklassificeringsmodellen i kommunens respektive verksamhet.

Det har skett ett arbete där man tittat på verktygslösningar som Microsoft Information Protection. Det har förts diskussioner mellan de som arbetar med IT-säkerhet, kansliet, kommunjurist och kommunregistrator men det har inte fattats något beslut på

[9] National Institute of Standards and Technology (NIST) är ett amerikanskt institut som erbjuder standardiseringar inom teknologiområdet. NIST 800-53 är ett ramverk som innehåller kontroller och bedömningsprocesser för informationssäkerhet och dataskydd.
[10] KLASSA är ett självskattningsverktyg som hjälper dig KLASSA era verksamhetssystem och datalagring. Verktyget är skapat för SKR:s medlemmar; kommuner och regioner.

kommunledningsnivå om någon verktygslösning och därför har det således inte blivit något utav det.

3.3.3 Incidentrapportering

Personuppgiftsincidenter av allvarlig karaktär anmäls direkt till Datainspektionen av förvaltningarna enligt en gemensam rutin, *Riktlinje för behandling av personuppgifter*. Ibland behöver förvaltningarna stöd i bedömningen om en händelse utgör en incident som ska anmälas vidare till Datainspektionen. Då utgör dataskyddsombudet ett stöd och vid behov involveras även informationssäkerhetssamordnaren i dessa bedömningar. Det finns i dagsläget en tillgänglig rutin för anmälan av incidenter, men förvaltningarna framhåller i intervjuerna att det saknas kompetens för att göra de nödvändiga bedömningar som krävs och att de behöver mer stöd i dessa frågor.

Ansvaret för personuppgiftsincidentrapportering skiljer sig mellan förvaltningarna. Vissa förvaltningar har utsedda personer, oftast inom förvaltningarnas IT-organisationer, medan det i andra är respektive avdelningschef som anmäler incidenter. Det har inte förekommit någon särskild utbildning för de som ansvarar för rapporteringen av personuppgiftsincidenter.

Anmälningar av personuppgiftsincidenter ska anmälas till dataskyddsombudet och diarieföras. Det har tagits fram en ärendekategori för personuppgiftsincidenter i Helpdesks system (system för avvikelser) men av intervjuerna framgår det att alla incidenter inte placeras i denna kategori. Detta är ett viktigt verktyg för att kunna följa upp hur många personuppgiftsincidenter som har skett. Ett arbete har påbörjats för att förbättra kategoriseringsarbetet av avvikelser i Helpdesks system.

Det framkommer också att det inte finns några systematiska eller återkommande orsaker till personuppgiftsincidenter men att det i stort är samma personer som anmäler personuppgiftsincidenter. Detta i kombination med brister i ärendekategorisering anses utgöra en grund för att det kan finnas ett mörkertal i incidenter som aldrig rapporteras till dataskyddsombudet. Det framgår även under intervjuerna att det inte finns någon hantering av de personuppgiftsincidenter som inte anmäls till Datainspektionen. Detta är dock personuppgiftsincidenter som ska hanteras inom kommunen, precis på samma sätt som andra avvikelser. Det tillämpas således inte en systematisk avvikelserapportering av personuppgiftsincidenter.

En annan faktor som identifieras under intervjuerna är att de som ansvarar för incidentrapportering ute i förvaltningarna inte har fått någon utbildning i dataskyddsfrågor och att det därför föreligger en risk för att personuppgiftsincidenter inte upptäcks eller rapporteras.

Utöver personuppgiftsincidentrapportering ska leverantörer av samhällsviktiga tjänster rapportera incidenter som orsakar störningar som får betydande inverkan på kontinuiteten i den samhällsviktiga tjänster till MSB. Huddinge kommun har en instruktion för rapportering av sådana incidenter. Den som är identifierad som ansvarig för en samhällsviktig tjänst har en skyldighet att rapportera identifierade incidenter till kommunens IT-Helpdesk. Därifrån tas ärendet vidare till kommunens NIS-grupp, bestående av IT-säkerhetsansvarig, informationssäkerhetssamordnare, säkerhetschef och enhetschef för IT-stöd. NIS-gruppen och verksamhetsansvarig för den

samhällsviktiga tjänsten anmäler sedan incidenten gemensamt till MSB. Av våra intervjuer framgår dock att denna rutin inte är allmänt känd eller förankrad i verksamheterna.

3.3.4 Ledningssystem för informationssäkerhet

Kommunen har haft ett pågående utvecklingsåtagande för att införliva ett ledningssystem för informationssäkerhet. Man har genomfört en gap-analys men det har inte fattats något beslut om projektet trots att det finns en projektbeställning och att ärendet har dragits för kommunledningsgruppen. Under intervjuerna framgår att man nu inväntar pågående revisionsrapport innan ledningssystemsarbetet slutförs.

3.3.5 Kontinuitetsplanering

IT-avdelningen har haft ett uppdrag att ta fram en kontinuitetsplan. Man har gjort en värdering och prioritering för de verksamhetssystem som förvaltningarna använder. Dock är det förvaltningarnas ansvar att ta fram kontinuitetsplaner för den tid eventuella avbrott varar.

Det har även skett en prioritering av de verksamhetssystem som kommunen idag använder sig av, för att se till vilka som innebär störst risker och sårbarheter. Detta arbete har resulterat i en lista över samhällskritiska och verksamhetskritiska system. De prioriterade systemen ska enligt rutin följas upp årligen, men det framgår av intervjuerna att detta inte genomförs för alla system.

3.3.6 Logg- och behörighetskontroller

Loggkontroller är idag begränsade. Man har inhandlat en SIEM-tjänst (System Incident and Event Manager). I dagsläget används detta bara för ett fåtal system och att inkludera fler anses vara en resursfråga. Vid tidpunkt för granskningen sker bara loggrapportering för infrastrukturen, men det framgår av intervjuerna att det önskas få ut detta i verksamheterna i större utsträckning. Loggarna kontrolleras i dagsläget endast vid misstänkta intrång eller attacker, det förekommer således ingen regelbunden och systematisk screening av loggarna.

Digitala behörigheter sköts automatiskt. Information matas från personalsystemet till ett system för behörighetsansökningar. Systemet flaggar när personal avslutar sin tjänst eller byter tjänst inom kommunen. En uppmärksammad brist är vid tjänsteförflyttningar då behörigheter från tidigare tjänst ofta ligger kvar. Utöver detta belyses under intervjuerna en sårbarhet i att kontobehörigheter förblir öppna i 30 dagar efter att en tjänst har avslutats. Förvaltningarna vi har pratat med framhåller att behörighetsarbetet innebär en manuell handpåläggning där mycket av ansvaret ligger på cheferna. Man har identifierat risker i det manuella arbetet, dels till följd av misstag dels att komplexa och tidskrävande processer ökar risken för fusk och genvägar.

Det framgår under intervjuerna brister i hanteringen av fysiska behörigheter. I många fall avslutas inte behörigheter i samband med att en tjänst avslutas och det finns generellt en låg kontrollgrad av dessa behörigheter.

3.3.7 Intern kontroll och riskanalyser

Trygghets- och säkerhetssektionen arbetar övergripande med risk- och sårbarhetsanalyser. Riskanalyserna baseras på konsekvens och sannolikhet, men viktas även mot kontroll där högre grad av kontroll genererar en lägre risk. Risk- och sårbarhetsanalyser genomförs i samband med upphandling av system och är en del av systemsäkerhetsanalysen.

Generellt arbetar man i Huddinge kommun med ett etablerat system för intern kontroll. Det finns dock en uppfattning om att det saknas systematik och avgränsning i detta arbete. Arbetet utgår från en bottom-up-princip där risker ska genereras från verksamheterna. Det anses innebära fördelar då risker kan iakttas ute i förvaltningarna, men eftersom det saknas systematik i hur risker identifieras kan det leda till att alla risker inte identifieras.

Av intervjuerna med förvaltningarna framgår det att det inte sker någon systematisk eller regelbunden riskanalys särskilt för informationssäkerhet. Däremot kan dessa frågor i viss mån inkluderas i internkontrollplanen. Inom socialförvaltningens digitala ledningssystem för kvalitet finns systemstöden som används i alla verksamheters processer publicerade.

3.3.8 Utbildning

Idag finns MSB:s utbildning *Digital informationssäkerhet för alla* (DISA) tillgänglig via kommunens e-learningsystem. I intervjuerna uttrycks en önskan om att göra denna utbildning obligatorisk för alla anställda. Dessutom anses det behövas kontinuerlig och regelbunden utbildning för att säkra kompetensen och medvetenheten hos medarbetare. Idag finns det ingen utbildningsplan för informationssäkerhet och det framgår av våra intervjuer att många verksamheter inte är medvetna om att det finns en tillgänglig e-utbildning inom informationssäkerhet.

Vid behov har anställda fått ta del av Försvarshögskolans kurs i grundläggande säkerhetsskydd.

När GDPR infördes hölls utbildningar om personuppgiftsbehandling av en extern aktör. Utbildningen riktade sig till de centrala befattningarna vid förvaltningarna. Efter detta har det inte skett några utbildningsinsatser inom dataskyddsområdet på kommunövergripande nivå. Barn- och utbildningsförvaltningen köpte in en GDPR-utbildning för alla medarbetar inom förvaltningen men trots uppföljning mot förvaltningsledningen uppfattade man att det var svårt att få de anställda att genomföra utbildningen trots att den var obligatorisk.

Ansvaret för att klassificera information efter kommunens informationsklassificerings-modell är förlagd på förvaltningarna. Dock har det inte genomförts några utbildningar i detta och det anses saknas kompetens för att på ett adekvat sätt genomföra den klassificering som är nödvändig.

Digitaliseringsavdelningen har tagit fram utbildningsmaterial i samband med projektet för Microsoft 365.

Av intervju med biträdande kommundirektör framgår att en ny utbildningsstruktur är en del av det övergripande omstruktureringsarbete som pågår. I den nya strukturen är ombordstigningsprocessen för nya medarbetare i kommunen ett prioriterat område. Tanken är att vissa centrala delar, däribland informationssäkerhet, ska inkluderas i ett utbildningspaket och ska omfatta alla nya medarbetare.

3.3.9 Måluppfyllelse och uppföljning

Huddinge kommun har upprättade styrande dokument kring informationssäkerhet men av de intervjuer som har genomförts framgår en tydlig och enhetlig bild av att den praktiska implementationen brister. Framförallt anses verksamheternas mognad, medvetenhet och kompetens inom informationssäkerhetsområdet högst bristfällig. Det framhålls att det förekommer skillnader mellan förvaltningarna men även på individnivå.

Det framkommer även av intervjuerna att det saknas systematisk rapportering och uppföljning av nyckeltal mot ledningen vilket anses kunna leda till utveckling av arbetet med informationssäkerhet för systemägare och ansvariga.

Informationssäkerhetsorganisationen utför mycket arbete men det saknas uppföljning av personuppgiftsincidenter, utvecklingsåtaganden samt annat arbete. Många projekt anses fastna i beslutsskedet och som resultat slutförs de aldrig och dess resultat implementeras inte. Ett exempel på detta är processen där verksamheterna ska ta fram risker och sårbarheter för sina system för att sedan presentera åtgärdsplaner. Av intervjuerna framgår att dessa åtgärdsplaner sällan implementeras.

Det framkommer även under våra intervjuer att strategisk och långsiktig uppföljning saknas, det framgår att det krävs åtgärder för struktur och organisation men även systemförvaltning och tydligare ansvarsfördelning.

3.3.10 Bedömning

Vår bedömning är att Huddinge kommuns informationssäkerhetsarbete endast till viss del sker enligt befintliga styrande dokument, och att ändamålsenligheten och systematiken är bristfällig.

Arbetet med systemsäkerhetsanalyser inför upphandlingar bedömer vi vara den processen inom informationssäkerhet som tillämpas idag. Denna process fungerar generellt bra och är ändamålsenlig. Genom centraliseringen av upphandlingsfunktionen till kommunstyrelsens förvaltnings upphandlingsenhet ökar också systematiken kring involvering av informationssäkerhetsorganisationen och att det sker vid rätt tidpunkt, det vill säga inför en upphandling. Det finns idag brister med uppföljningen av dessa analyser, de sker inte med den regelbundenhet som framgår av rutiner för säkerhetsskyddsanalys.

Vi bedömer även att det finns brister i kommunens hantering av behörigheter, såväl för system som fysiska lokaler. Risker och sårbarheter har identifierats vid avslut och förändring av tjänster.

Med ett decentraliserat ansvar för informationssäkerhet där förvaltningarna förväntas sköta det dagliga arbetet blir kunskap, medvetenhet och kompetens avgörande faktorer för förvaltningarnas möjlighet att utföra ett ändamålsenligt och systematiskt informationssäkerhetsarbete. Vår bedömning är att detta till stor del saknas i dagsläget vilket bland annat beror på bristande utbildning. Det finns inga obligatoriska utbildningar inom vare sig informationssäkerhet, dataskydd eller informationsklassificering.

Vi bedömer även att det idag saknas en systematisk kring hantering av personuppgiftsincidenter. Personuppgiftsincidenter som inte anmäls till Datainspektionen rapporteras inte vilket försvårar uppföljning, riskidentifiering samt åtgärder. Omfattningen av dataskyddsombudets tjänst bedöms idag vara för liten för att kunna arbeta förebyggande och bygga upp en kompetens och medvetenhet ute i verksamheterna.

Det finns inte heller en systematik i hur kommunen ska arbeta med incidentrapportering enligt NIS-direktivet.

4 Slutsats och rekommendationer

Vår sammanfattade bedömning utifrån granskningens syfte är att kommunstyrelsen inte har ett ändamålsenligt och systematiskt arbetssätt avseende informationssäkerhet.

Vi bedömer att kommunstyrelsen har ett övergripande ramverk för arbetet med informationssäkerhetsfrågor men att det finns brister i utförandet. Det finns upprättade styrdokument men förankringen och medvetenheten om dessa i verksamheterna anses vara låg. Dessutom saknar kommunen en informationssäkerhetspolicy vilket skulle kunna bidra med att tydliggöra roller och ansvarsförhållanden ytterligare. I de riktlinjer som finns upprättade för informationssäkerhetsarbetet ställs krav som är förenliga med en ändamålsenlig och systematisk informationssäkerhetsorganisation men efterlevnaden och uppföljningen av dessa krav är högst bristfällig.

Granskningens bedömning är att det finns en medvetenhet om nuvarande brister i informationssäkerhetsarbetet på alla nivåer i organisationen men att det saknas kompetens och resurser för att åtgärda detta. Omfattningen av informationssäkerhetsorganisationen bedöms idag vara begränsad vilket leder till reaktivt arbete med låg grad av uppföljning och utveckling.

Samtidigt noteras även att det pågår ett utvecklingsprojekt inom området och att den kommunövergripande omstruktureringen kan utgöra en grund för ett fortsatt utvecklingsarbete. Vidare bedöms det fortsatta arbetet med implementering av ett ledningssystem för informationssäkerhet som avgörande för att säkerställa regelefterlevnad samt att uppnå de krav och mål som kommunen ställer på informationssäkerhet. Rekommendationerna i denna granskning kan utgöra ett underlag i ett sådant arbete.

4.1 Rekommendationer

Rekommendationerna som denna granskning resulterat i kan alla inkluderas i det övergripande arbetet med införandet av ett ledningssystem för informationssäkerhet som för tillfället pågår i Huddinge kommun. Vi anser att ett sådant ledningssystem utgör grunden för den fortsatta utvecklingen av Huddinge kommuns arbete med informationssäkerhet och att denna fråga bör prioriteras.

Utifrån granskningens resultat rekommenderar vi kommunstyrelsen att:

- **Implementera en informationssäkerhetspolicy.**

  En informationssäkerhetspolicy skulle kunna brygga det gap som i dagsläget finns mellan *Program för trygghet och säkerhet 2018-2021* och de tillhörande riktlinjerna. Det skulle även verka för att samla informationssäkerhetsarbetet på ett ställe där de övergripande målen utvecklas. En sådan policy kan även underlätta arbetet med måluppföljning och kontroll. Det skulle dessutom förtydliga roll- och ansvarsfördelningen i informationssäkerhetsorganisationen. MSB uttrycker i sina rekommendationer att en informationssäkerhetspolicy är ett viktigt verktyg i arbetet med ledningssystem för informationssäkerhet.

- **Implementera en obligatorisk utbildning om informationssäkerhet med kontinuerliga och regelbundna uppföljningsutbildningar.**

  En grundläggande faktor för att säkerställa en medvetenhet och kunskap om informationssäkerhet är utbildning. En obligatorisk utbildning för alla anställda skulle kunna bidra till att garantera en adekvat lägstanivå i kommunen. En sådan utbildning kan med fördel inkluderas i de utbildningar nyanställda tar del av.

  För att säkerställa att medvetenhet och kunskap bevaras över tid anser vi även att utbildningarna regelbundet bör följas upp. Uppföljande utbildningar behöver inte vara lika omfattande som den ursprungliga.

  Utbildningen bör innefatta delar som övergripande informationssäkerhet med gällande styrdokument, dataskydd och personuppgiftshantering samt informationsklassificering.

- **Implementera en systematisk och regelbunden rapportering och uppföljning av informationssäkerhetsarbetet till kommunledningen och kommunstyrelsen.**

  För att informationssäkerhetsarbetet ska förankras i kommunens alla verksamheter är det viktigt att följa upp arbetet för att kunna genomföra utvärderingar av regelefterlevnad och måluppfyllelse.

- **Säkerställa att alla verksamheter har tillgång och kännedom om de styrdokument som gäller för verksamheten, samt vilka ansvarsförhållanden som gäller.**

  Kommunen behöver säkerställa att denna dokumentation finns samlad på en lättillgänglig samlingsplats där alla anställda kan ta del av denna. Det krävs även informationsinsatser för att nå ut med denna dokumentation.

- **Säkerställa att informationssäkerhetsorganisationen har en tillräcklig omfattning för att möta kommunens behov.**
- **Ser över möjligheten att implementera nya rutiner för att säkerställa att anställda har rätt behörigheter.**

  Framförallt krävs en förbättrad rutin för behörigheter vid förändring och avslut av tjänst inom kommunen.
- **Implementera en rutin för rapportering av informationssäkerhets-incidenter i ett avvikelserapporteringssystem.**
- **Säkerställa att det finns en ändamålsenlig organisation för rapportering av incidenter enligt NIS-direktivet.**

Datum som ovan

KPMG AB

Emma Garpenholt

Emma Garpenholt
Kommunal verksamhetsrevisor

Martin Forslund

Martin Forslund
Kommunal verksamhetsrevisor

Micaela Hedin

Micaela Hedin
Certifierad kommunal yrkesrevisor

5 Bilaga 1 – Material och intervjuer

Denna granskning har genomförts genom dokumentstudier och intervjuer med tjänstepersoner.

Dokument:

Program för trygghet och säkerhet 2018-2021

Riktlinje för informationssäkerhet

Riktlinje för användning av Internet, e-post och andra mobila enheter

Riktlinje för behandling av personuppgifter

Riktlinje för säkerhetsskydd i Huddinge kommun

Instruktion för genomförande av SSA

Instruktion för anmälan av NIS-incident

Dataskyddsombudets roll och omfattning av tjänsten

Grundmall SSA

Verksamhetsberättelse Huddinge kommun 2019

Intervjuer:

Biträdande kommundirektör

Säkerhetschef, kommunstyrelsens förvaltning

Dataskyddsombud, kommunstyrelsens förvaltning

Informationssäkerhetssamordnare, kommunstyrelsens förvaltning

IT-säkerhetsansvarig, kommunstyrelsens förvaltning

IT-säkerhetsarkitekt, kommunstyrelsens förvaltning

Sektionschef strategi och verksamhetsutveckling och *IT-strateg*, kommunstyrelsens förvaltning

Socialchef och systemförvaltningsledare, socialförvaltningen

IT-ansvarig, barn- och utbildningsförvaltningen