Granskning av stadens IT- säkerhet

Rapport

Malmö stad

KPMG AB

2020-12-16

Antal sidor 40

Antal bilagor 2

Granskning av IT-säkerhet

Malmö stad
Granskning av stadens IT- säkerhet

2020-12-16

Innehållsförteckning

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Malmö stad fått i uppdrag att genomföra en granskning av stadens arbete med IT-säkerhet. Uppdraget ingår i revisionsplanen för 2020. Granskningen har syftat till att bedöma om kommunstyrelsen och servicenämnden säkerställer att IT-säkerheten är tillräcklig för att reducera risker för obehörigt intrång.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och servicenämnden endast till viss del säkerställer en tillräcklig IT-säkerhet. Ett antal viktiga förbättringsområden har identifierats.

IT-enheten på stadskontoret och IT-service på serviceförvaltningen har i sitt uppdrag för kommungemensam IT investerat i nya tekniska lösningar och säkerhetsfunktioner i nätverk, datacenter, klienter och tjänster. Behov av utveckling samlas årligen i en tjänsteplan och en utvecklingsplan som resurssätts utifrån tilldelad budget. Det saknas dock en övergripande helhetsbild över behov av säkerhetslösningar för att avgöra vad som behöver prioriteras utifrån riskbedömning av eventuella sårbarheter. Detta riskerar i sin tur att inte tillräckliga åtgärder vidtagits för att skydda stadens IT-miljö mot obehörigt intrång.

Det finns till viss del implementerade säkerhetslösningar och tekniska kontroller för att begränsa möjligheten för aktörer att påverka IT-miljön. Kommunstyrelsen och servicenämnden har inte säkerställt att det finns en tillförlitlig övervakning över aktivitet i nät och stadens IT-miljö för att i tid upptäcka och förhindra intrångsförsök och hot. Kommunstyrelsen har inte gett verksamheten i uppdrag att genomföra tester för att utvärdera de införda säkerhetslösningarna, exempelvis sårbarhetsscanning eller penetrationstester.

Kommunstyrelsen ska enligt reglementet ansvara för att leda, strategiskt utveckla och samordna stadens gemensamma digitaliserings- och IT-frågor, informationssystem, digital infrastruktur och telekom. Vår bedömning är att kommunstyrelsen utifrån sitt ansvar delvis har säkerställt att arbetet med IT-säkerhet är tillräcklig. Det finns inte en ändamålsenlig organisation med tydlig ansvarsfördelning för att styra IT-säkerhetsarbetet, därtill saknas dokumenterade uppdragsbeskrivningar och mandatet är otydligt mellan stadskontorets styrande funktion och övriga förvaltningar utifrån ordinarie verksamhetsansvar.

Vår bedömning är vidare att kommunstyrelsen endast till viss del har tillsett att det finns ändamålsenliga styrdokument för IT-säkerhet. Det saknas i nuläget styrdokument på policynivå där den politiska viljeriktningen för stadens informations- och IT-säkerhetsarbete tydliggörs. Styrdokument som tillämpas idag avseende informationssäkerhet tydliggör ansvaret för informationssäkerhet men inkluderar endast i vissa delar IT-säkerhet. De funktioner inom Malmö stad med ansvar inom dessa områden både inom stadskontoret och serviceförvaltningen anser därtill att nuvarande riktlinjer och anvisningar för informationssäkerhet inte är tillräckligt uppdaterade avseende tekniska förutsättningar för att kunna tillämpas i styrningen av IT-säkerhetsarbetet. Innehållet avseende informationssäkerhet upplevs även det vara alltför omfattande och svårgripbart för att vara ett stöd i förvaltningarnas arbete, främst vad gäller informationsklassning och riskbedömning där det framkommit synpunkter

över att frågeställningar i klassningen inte är anpassade efter informationshantering som sker i de moderna tjänster och system som nyttjas i staden.

Det finns i nuläget inte en komplett förteckning över stadens system och IT-komponenter med erforderlig information. Eftersom inte samtliga tillgångar finns dokumenterade och därigenom inte klassats eller riskbedömts går det inte att fastställa om tillräckliga IT-säkerhetsåtgärder är vidtagna för att skydda informationen. Utan en informationsklassning så behöver IT-enheten på stadskontoret och IT-service på serviceförvaltningen vidta de säkerhetslösningar på övergripande nivå som de utifrån sin kompetens bedömer som nödvändiga ur ett tekniskt perspektiv. Arbete med riskanalyser sker till viss del för informations- och IT-säkerhetsarbetet i samband med implementeringar av nya tekniska lösningar. En stor del av ansvaret för riskanalyser finns dock hos förvaltningarna som informations- och systemägare och ska hanteras i enlighet med gällande riktlinjer och anvisningar för informationssäkerhet.

Det finns inte någon dokumenterad riskanalys på stadsövergripande nivå upprättad i samband med förändrade arbetssätt och det ökade antal medarbetare som arbetar hemifrån. I enlighet med informationssäkerhetsansvaret så ska detta upprättas i förvaltningarna innan system tillgängliggörs för distansarbete.

För nämndssammanträden på distans via Teams gjordes en bedömning av IT-enheten på stadskontoret att tjänsten hade tillräcklig IT-säkerhet. Därtill beslutade kommunstyrelsen om tillämpningsanvisningar för att säkerställa informationssäkerheten, främst gällande sekretessbelagd information och personuppgifter. Det saknas kontinuitetsplan för den övergripande IT-driften och nätverk vilken skulle påverka funktionaliteten av distanslösningar vid avbrott eller störning.

Utifrån genomfört penetrationstest är vår bedömning att den tekniska säkerhetsrisken i form av hot mot stadens IT-miljö vid distansarbete via de system som finns för fjärranslutning är låg. Säkerheten överlag är dock beroende på hur användarna säkerställer sitt ansvar i informationshanteringen när de nyttjar systemen och tjänster för distansarbete.

Bristen på medvetenhet är en av de största säkerhetsriskerna med det stora antal användare som finns i stadens IT-miljö. Det finns instruktioner i riktlinjer för informationssäkerhet som riktar sig till användare över användningen av IT-utrustning men vi anser att detta dokument är alltför omfattande för att det ska kunna förväntas att samtliga medarbetare tar del av det då det inte är utformat på ett sätt som medför tillgänglighet och förståelse hos var och en. Utbildningar inom ramen för IT- och informationssäkerhet har endast till viss del erbjudits genom e-utbildning men det har inte skett någon uppföljning över antal som deltagit eller att tillräckliga kunskaper och medvetenhet erhållits genom de insatser som genomförts. Att medarbetarna har kunskap och kännedom om sitt ansvar för informationssäkerhet är delegerat till nämnderna och följer det ordinarie ledningsansvaret.

Det är väsentligt att kunskap finns för att upptäcka och rapportera incidenter i de fall dessa inträffar. Det finns en dokumenterad incidentprocess på IT-service och en hantering i verksamhetssystemet Agera. Det behöver dock säkerställas att rutiner är kända och tillämpas av alla verksamheter så att incidenter kan dokumenteras och följas upp samt att åtgärder vidtas för att hindra att de sker igen.

Varken kommunstyrelsen eller servicenämnden har säkerställt att de får en tillräcklig rapportering av stadens respektive förvaltningens informations- och IT-säkerhetsarbete förutom uppföljning av intern kontroll, de kontrollmål som är beslutade är dock inte tillräckliga för att följa upp efterlevnad av interna riktlinjer för informationssäkerhet eller upprättad IT-säkerhet. Avsaknad av rapporteringsvägar riskerar att leda till att informations- och IT-säkerhetsfrågorna inte når de ledningsnivåer som behövs för att skapa ett engagemang, styrning och acceptans av frågorna som är nödvändiga för att arbetet ska ske på ett systematiskt sätt med tillräckliga resurser.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Etablera en organisation med tydligt ansvar och mandat för stadens informations- och IT-säkerhetsarbete
- Ta fram policy för informationssäkerhet eller revidera befintlig Trygg- och säkerhetspolicy så att informationssäkerhet är inkluderat. Samt komplettera denna med de riktlinjer och anvisningar som behövs för att styra arbetet
- Ge nämnder och förvaltningar i uppdrag att kartlägga samtliga informationssystem och tjänster och dokumentera dessa i förteckning för att säkerställa att det finns en komplett förteckning som är uppdaterad och kan fungera som informationskälla i hanteringen av IT-säkerhetsåtgärder
- Säkerställa att det genomförs risk- och konsekvensanalyser för verksamhetskritiska informationssystem och att det finns tillhörande kontinuitetsplaner för dessa
- Säkerställa att metod för klassning finns som är tillämpbar för dagens informationssystem och tjänstehantering och att klassning genomförs både på system och information som hanteras i förvaltningarna
- Säkerställa att nyanställda samt befintliga medarbetare får information och utbildning i ansvaret för informationssäkerhet och IT-användning
- Besluta om stadsövergripande rutin för incidenthantering och rapportering där ansvar och eskaleringsvägar finns tydliggjorda samt kommunicera denna till verksamheterna. Det behöver även säkerställas att en uppföljning sker av inträffade incidenter så att detta kan beaktas i förbättringsarbetet
- Säkerställa genom intern kontroll att det sker ett tillräckligt arbete med informationssäkerhet i förvaltningarna där efterlevnad av beslutad riktlinje och anvisningar för informationssäkerhet finns
- Skapa struktur för enhetlig uppföljning av informationssäkerhet inklusive IT-säkerhet och etablera rapporteringsvägar till ledning och styrelse

Utifrån vår bedömning och slutsats rekommenderar vi servicenämnden att:

- Utifrån ansvar i reglementet säkerställa att det finns en tilldelad budget för förvaltning av IT-miljö och IT-infrastruktur så att IT-säkerhetsåtgärder vid behov kan vidtas för systemdrift och nät

- Upprätta risk- och sårbarhetsanalyser för nätverk och drift med tillhörande handlingsplaner för åtgärder för att nå önskad nivå av IT-säkerhet
- Upprätta styrdokument avseende drift och teknik med tillhörande kontinuitetsplaner för att det ska finnas reserv- återgång- och återställningsrutiner i händelse av störning eller avbrott och en prioritering av verksamhetskritiska system kan göras
- Säkerställa att förvaltningsspecifik rutin för incidenthantering inkluderar information till berörda funktioner med ansvar för informationssäkerhet, IT-säkerhet och ansvar för driftsäkerhet

2 Bakgrund

KPMG har av de förtroendevalda revisorerna i Malmö stad fått i uppdrag att genomföra en granskning av IT-säkerheten för att bedöma om den är tillräcklig för att reducera risker för obehörigt intrång.

Intrång i IT-och informationssystem förekommer och utgör en central risk för en offentlig verksamhet som handhar en stor mängd känslig information.

En omfattande del av Malmö stads totala informationsmängd hanteras i stadens många IT-system och digitala tjänster. Informationen behöver skyddas på ett korrekt och tillräckligt sätt för att upprätthålla och bevara förtroendet för, och kontinuiteten i, stadens olika verksamheter.

Under 2020 har Coronapandemin medfört att användningen av tillgängliga tekniska IT-lösningar har ökat. Exempelvis har kommunfullmäktige möjliggjort deltagande i nämndssammanträden på distans och många medarbetare arbetar hemifrån.

Revisorskollegiet i Malmö stad har efter riskbedömning beslutat att genomföra en granskning av teknisk IT-säkerhet.

2.1 Syfte, revisionsfråga och avgränsning

Syftet med granskningen har varit att bedöma om kommunstyrelsen och service-nämnden säkerställer att IT-säkerheten är tillräcklig för att reducera risker för obehörigt intrång.

Granskningen ska besvara följande revisionsfrågor:

- Finns det en ändamålsenlig organisation med tydlig ansvarsfördelning avseende IT–säkerhetsarbetet?
- Finns det ändamålsenliga styrdokument för IT-säkerhet och säkerställs det att dessa följs?
- Finns det en tillräcklig intern kontroll av IT-säkerheten (t.ex. behörigheter, avslut m.m.)?
- Identifieras och hanteras IT-säkerhetsrisker förknippade med arbete i hemmet och nämndssammanträden på distans?
- Finns det en tillräcklig säkerhet avseende intrång av extern eller intern aktör?
- Hanteras och dokumenteras IT-säkerhetsincidenter på ett ändamålsenligt sätt?
- Finns det dokumenterade och ändamålsenliga kontinuitetsplaner för granskade system?
- Sker det en tillräcklig uppföljning av IT-säkerhetsarbetet och är återrapporteringen till kommunstyrelsen och servicenämnden tillräcklig?

Granskningen avser kommunstyrelsen och servicenämnden.
Granskningen avser revisionsåret 2020.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen (2017:725), kap. 6 §6
- Reglemente för kommunstyrelsen
- Reglemente för servicenämnden
- Reglemente för intern kontroll
- IT-strategi för Malmö stad
- Riktlinjer och anvisningar för informationssäkerhet i Malmö stad

Vissa bedömningar tar sin utgångspunkt i gällande praxis för informationssäkerhetsarbete, ISO27001-standarden, vilken rekommenderas av Myndigheten för samhällsskydd och beredskap, MSB.

2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med tjänstepersoner inom stadskontoret och serviceförvaltningen. (Specificeras i bilaga 1 och 2).

Vidare har ett penetrationstest genomförts av stadens anslutningsmöjligheter för distansarbete och digitala möten. Testet har genomförts för att bedöma sårbarheter för intrång i stadens informationssystem via de system som finns för fjärråtkomst.

Granskningen har genomförts av granskningsledare Sara Linge, certifierad kommunal revisor, Jenny Thörn, kommunal revisor samt Patrick Bladh, IT-säkerhetsexpert.

2.4 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 informationssäkerhetssamordnarens 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.

3 Resultat av granskningen

3.1 Organisation

Trygg- och säkerhetsarbetet i Malmö stad är enligt information på hemsidan, information i intervjuer och styrdokument kopplat till det ordinarie verksamhetsansvaret hos respektive förvaltning och följer linjeansvaret för stadens chefer till medarbetarnivån. Arbetet ska utgå från styr- och ledningssystemet vilket ska ge goda förutsättningar för en tydlig koppling mellan mål, insats, uppföljning och utvärdering.

I beslutade riktlinjer och anvisningar för informationssäkerhet (vilka beskrivs i avsnitt 3.2.2) framgår att det är nämnderna som är ytterst ansvariga för informationssäkerheten och att de ansvarar för att tillse att krav på verksamhetens informationshantering följs genom intern kontroll samt att resurser avsätts för att möta de hot som kan uppstå i verksamheten.

I Malmö stads IT-strategi framgår att styrningen av IT-verksamheten kännetecknas av en tydlig kund och leverantörsrelation med Malmö stads verksamheter som beställare och serviceförvaltningen och andra leverantörer som utförare.

Genom stadens organisering av sitt informations- och IT-säkerhetsarbete finns ett ansvar för detta inom IT-enheten på stadskontoret, enheten för säkerhet och beredskap på stadskontoret, förvaltningarnas eget arbete och IT-service på serviceförvaltningen. Även juridiska enheten arbetar med frågan utifrån lagstiftning och dataskydd.

3.1.1 Kommunstyrelsens ansvar för IT-säkerhet

I kommunstyrelsens reglemente[1] framgår att stadskontoret är styrelsens förvaltning. Förvaltningen leds av en stadsdirektör. Direktören är inför styrelsen ansvarig för kontorets verksamhet.

Styrelsen ska utifrån ett helhetsperspektiv leda kommunens verksamhet genom att utöva en samordnad styrning och leda arbetet med att ta fram nämndövergripande styrdokument för kommunen (styrfunktion).

Styrelsen ska ha ett övergripande ansvar för säkerhet och riskhantering i kommunen. Vad gäller information och kommunikation ska styrelsen ansvara för det övergripande arbetet med informationssäkerhet.

Vad gäller digitalisering och informationssystem ska styrelsen:

- ansvara för att leda, strategiskt utveckla och samordna stadens gemensamma digitaliserings- och IT-frågor, informationssystem, digital infrastruktur och telekom.
- vara systemägare för vissa kommunövergripande system som exempelvis personaladministrativa system och ekonomisystem.

[1] Ant. av kf 17–18/12 1991, senast reviderat 19/6 2019, § 142

Stadskontoret har utifrån reglementet i uppdrag att samordna det övergripande säkerhetsarbetet i staden där informationssäkerhet och tillhörande IT-säkerhet ingår. Samordningen från stadskontoret sker delvis genom flera nätverk med representanter från kommunens verksamheter. Exempelvis finns nätverk för beredskapsarbetet och ett där informationssäkerheten samordnas.

På stadskontoret finns en Kommunikations- och IT-avdelning som leds av en Kommunikations- och IT-direktör som sitter i stadskontorets ledningsgrupp. På Kommunikation och IT-avdelningen finns bland annat en IT-enhet som har en beställarroll av IT-drift och support som hanteras på IT-service, serviceförvaltningen. I beställarrollen ingår att ta fram förvaltning- och utvecklingsplaner samt budgetmedel för de kommungemensamma IT-plattformarna och infrastrukturen. IT-enheten ansvarar bland annat för den stadsövergripande klientplattformen och tillhörande tjänster, intern lagring, identitet- och åtkomsthantering samt förvaltning av stadsövergripande system som HR-system och ekonomisystem. Det är från stadskontoret som stadsövergripande digital utveckling och andra utvecklingsprojekt inom IT drivs.

I detta uppdrag ingår att säkerställa att krav och behov ur ett säkerhets- och informationssäkerhetsperspektiv implementeras. Det ingår även att se till att ändamålsenliga säkerhetslösningar för stadens systemägare finns tillgängliga.

På stadskontoret skiljs det på IT- och informationssäkerhetsansvaret. IT-enheten arbetar med operativ IT-säkerhet och tillämpning. Informationssäkerhet finns organiserat under enheten för säkerhet och beredskap inom avdelningen för Omvärld och näringsliv. Enheten för säkerhet och beredskap ansvarar för riktlinjer och anvisningar för informationssäkerhet men även stadskontorets övriga säkerhetsfrågor som exempelvis säkerhetsskydd.

Inom enheten för säkerhet och beredskap finns två informationssäkerhetssamordnare. Dessa har uppdrag att samordna det stadsövergripande informationssäkerhetsarbetet. Då ingen ytterligare resurs tillsatts för att bedriva det interna informationssäkerhetsarbetet inom stadskontoret har de även tagit sig an det arbete som har behövts göras, i den mån de haft resurser i form av tid att göra det. De har dock påtalat att det behövs andra resurser alternativt ett beslut att samordna frågorna inom stadskontoret.

3.1.2 Servicenämndens ansvar för IT-säkerhet

I servicenämndens reglemente[2] framgår att serviceförvaltningen är nämndens förvaltning. Förvaltningen leds av en direktör.

Vad gäller IT-service som är den verksamhet som omfattas av granskningen, framgår av reglementet att servicenämnden och dess förvaltning ansvarar för:

- förvaltning och support för Malmö stads IT-miljö och IT-infrastruktur, var med bland annat avses systemdrift, övervakning, nät, klientplattform och telefoni.

IT-service ska enligt organisationens beställar- och utförarmodell arbeta på uppdrag från övriga förvaltningar. Det beskrivs dock i intervjuer att IT-service som avdelning anser sig ha ett stort eget ansvar för säkerheten som inte utgår från uppdrag från

[2] Ant av kf 27 – 28/11 1996, senast reviderat 20/12 2018, § 297

beställarna. I det ansvaret arbetar de med att skapa rutiner, processer och genomföra implementeringar av säkerhetslösningar utan andra förvaltningars inblandning.

3.1.3 Övriga nämnders ansvar för IT-säkerhet

Varje verksamhet ansvarar för att äga, förvalta, utveckla och avveckla sina specifika verksamhetssystem och sin information enligt förvaltningsmodell som fastställs av stadskontoret. Förvaltningarna har olika roller tillsatta för sina behov av IT-kompetens, exempelvis finns IT-chefer även inom förvaltningarna, IT-samordnare, systemförvaltare, digitaliseringsstrateger mm.

Det framkommer i intervjuer att IT-samordnarrollen ser helt olika ut mellan förvaltningarna. Runt 2014–2015 togs det fram en rollbeskrivning för IT-samordnare men enligt intervjupersoner implementerades den inte i förvaltningarna. Detsamma gäller för de systemförvaltare som finns i förvaltningarna, uppdrag och ansvar skiljer sig och vissa arbetar med uppdrag på heltid medan andra utför arbetet vid sidan om på en liten del av sin arbetstid.

Ett stort ansvar som ligger inom förvaltningarna är att efterleva och upprätta en tillräcklig informationssäkerhet i enlighet med beslutat styrdokument Riktlinjer och anvisningar för informationssäkerhet.

I arbetet finns utsedda informationssäkerhetssamordnare. Grunden i detta arbete ska leda fram till att risker har bedömts för verksamhetens information så att IT-säkerhetsåtgärder står i relation till risker och skyddsvärde som informationsansvariga har bedömt och dokumenterat.

Enligt intervjupersoner är en av utmaningarna att få ansvariga chefer att förstå frågorna och deras ansvar och mandat i arbetet och vilka resurser som krävs för att kunna arbeta med dessa frågor. Utan den förståelsen är det svårt att få till det systematiska arbetet som behövs i förvaltningarna. Det framgår av den nulägesanalys som de centrala informationssäkerhetssamordnarna presenterat att förvaltningarnas informationssäkerhetssamordnare ofta har flera roller och att samordningsuppdraget ska skötas på varierande del av sin arbetstid. Det leder inom de flesta förvaltningar till att tiden endast räcker till att lösa frågor som uppstår men inte till att driva ett systematiskt förbättringsarbete.

3.1.4 Samordning av IT-säkerhetsarbetet

Det framkommer i intervjuer att det inte främst är den tekniska säkerheten som är utmaningen i organisationen utan otydligheten i ansvar och roller. Det är svårt att veta var ansvaret finns då det inte är uttalat vem som är ansvarig för vad. Det framkommer vidare att det inte finns någon som håller ihop helheten i arbetet. Enskilda ansvariga driver säkerhetsarbetet inom sina områden och har ett ansvar att vidta åtgärder. Det samlas dock inte ihop på övergripande nivå så att det finns en överblick och gemensam bild av behov av utveckling och åtgärder.

Intervjupersoner beskriver att förvaltningarna vill vara fria men har samtidigt behov av en bättre styrning då de har svårt att hitta säkerhetskompetens själva och mäktar inte med arbetet på egen hand. Det finns ett stort behov och en efterfrågan på styrning och stöttning i den sammanhållna synen på informations- och IT-säkerhet. I riktlinjer för informationssäkerhet framkommer bland annat att stadskontoret ansvarar för att ta

fram en stadsövergripande systemförvaltningsmodell och utgöra stöd till förvaltningarna i arbetet med systemförvaltning. Systemförvaltningen ska bygga på samverkan mellan verksamhetsparter och IT-parter för att säkerställa att verksamhets- och IT-utveckling hänger samman.

När staden avslutade sitt GDPR-projekt hade ett behov att etablera en samordningsgrupp för Malmö stads övergripande arbete med dataskydd och IT-säkerhet identifierats av projektgruppen. Kommunstyrelsen hänvisade till detta i sitt remissvar till stadsrevisionens granskning av informationssäkerheten från 2018 och under våren 2020 bildades en samordningsgrupp för dataskyddsarbete och IT-säkerhet där man samlat kompetenser inom juridik, informationssäkerhet och IT-säkerhet.

Den otydlighet som finns avseende ansvaret uttrycks av flertal intervjupersoner bero på otydlighet i mandat mellan stadskontoret och förvaltningarnas ansvar i enlighet med ordinarie verksamhetsansvar. Enligt intervjuperson så är stadskontorets roll att ta fram styrdokument, följa upp och fånga om det finns brister i hur tillämpning sker och påtala ansvar. Flertal intervjupersoner har dock uttryckt en svårighet att veta hur uppföljning ska ske och var gränsen går över att påtala brister i efterlevnad i förhållande till förvaltningarnas eget ansvar att organisera sitt arbete.

Det lyfts även ett flertal exempel i intervjuer att olika svar ges från exempelvis IT-service inom serviceförvaltningen och från IT-enheten på stadskontoret när verksamheter ber om råd eller stöd i frågor kopplat till IT. Då det inte finns några beslut på övergripande nivå att förhålla sig till så svarar ansvariga utifrån sitt perspektiv och kompetens, svaren ges därför inte från en gemensam syn på säkerhet eller praktisk hantering av IT-frågorna.

Några konkreta exempel som lyfts är om användning av privat utrustning för att koppla upp sig på distans mot stadens IT-miljö vilken i riktlinjer anges förbjudet men i intervjuer framhålls förekomma. Riktlinjen hänvisar dock till att arbetsgivaren tillhandahåller tjänst för uppkoppling till IT-miljön som finns lokalt i Malmö stads datacenter medan Office365 inte är placerad där. Genom behörighetssystemet kan användare vid användning av privat utrustning ansluta sig till Office365 men enligt intervjuperson så är det inte något som rekommenderas. I samband med information om distansarbete som en följd av covid-19 kommunicerades på intranätet en rekommendation att använda utrustning som tillhandhålls av Malmö stad med hänvisning till säkerhet och sekretesskäl.

Hanteringen av att lagra information i molnbaserade tjänster är ett annat exempel som lyfts. Det finns ingen beslutad riktlinje för hantering och tjänsteägare vet inte vad de ska ge för svar till verksamheter som frågar medan verksamheterna förväntar sig att IT-enheten eller IT-service ska kunna svara på dessa frågor. Utifrån ansvarsfördelning för informationen är det upp till varje verksamhet att göra bedömningen utifrån typ av information som ska lagras och de lagrum som behöver beaktas och kan därför inte besvaras av IT-funktionerna. Den generella rekommendationen är alltid att informationen som ska hanteras ska vara klassificerad och en risk- och sårbarhetsanalys ska göras utifrån detta för att avgöra hur hantering och lagring ska ske. Som det är beskrivet längre fram i rapporten finns det dock brister i efterlevnad av riktlinje och anvisning för informationssäkerhet vad gäller klassificering och riskanalyser vilket leder till att den bedömning som behöver ske för informationshantering i vissa fall saknas helt eller delvis. Informationssäkerhetssamordnarna i förvaltningarna har också

återkopplat behov av stöd i fråga om hur lagring i molnet ska hanteras vilket finns dokumenterat i en nulägesanalys som genomfördes 2019 över stadens samlade informationssäkerhetsarbete. Medarbetare inom IT-enheten på stadskontoret har efterfrågat svar om hantering i frågan i tre år utan att beslut har fattats. Den samordningsgrupp som etablerats arbetar med att ta fram rekommendationer för hur stadens förvaltningar bör hantera detta och härigenom skapa tydlighet.

Det pågår ett arbete med att omorganisera IT-funktionen i staden där IT-enheten på stadskontoret framöver ska tillhöra serviceförvaltningen och en ny avdelning för stadens IT ska bildas där även IT-service på serviceförvaltningen ska ingå. Enligt uppgift från intervjuperson så finns det en särskild utredning tillsatt för att säkerställa att området informations- och IT-säkerhet beaktas och vilka krav det ställer på den framtida organisationen.

3.1.5 Finansieringsmodell

I kommunstyrelsens nämndsbudget för 2020 beskrivs under avsnittet för investeringar att dessa utgår från behov som de enskilda förvaltningarna har men att stadskontoret har ett tydligt ägarskap i frågan kring re- och nyinvesteringar av kommunikationsutrustning i stadens lokala datanät. De kapitalkostnader som uppstår ska finansieras av respektive nämnd som omfattas av investeringen. För stadsövergripande säkerhetslösningar beslutas dessa centralt av en ledningsgrupp där budgetchefer inom IT-enheten ingår. Kostnaderna fördelas sedan på förvaltningarna. Ett sådant exempel är investering av ny brandvägg 2020. I Malmö stads delårsrapport 2020 framgår att flera stora re-investeringar kommer att genomföras under 2020 vilket leder till att prognosen för helåret är att utrymmet används med en avvikelse på 1,3 Mkr. Orsaken till avvikelsen är att staden behöver investera i en brandvägg med högre kapacitet på grund av det ökade distansarbetet i samband med covid-19. En effekt av detta blir enligt delårsrapporten att avskrivningar och interna räntor kommer att bli högre än budgeterat.

Det beskrivs i intervjuer att det kan vara en utmaning att pedagogiskt förklara för nämnder och förvaltningar vad syftet är med IT-investeringar och i vissa fall få en förståelse över vad utveckling inom IT och IT-säkerhet kostar. Samtidigt är de IT-säkerhetsåtgärder som vidtas oftast direkt kopplade till att skydda informationen och IT-miljön för förvaltningarnas kärnverksamheter. Intervjupersoner anser att en budget bör tas politiskt så att det finns en viljeriktning om vilken nivå på säkerheten som behövs och vad den får kosta. I nuläget sker beslut om investeringar och prioriteringar på tjänstepersonsnivå och når inte kommunstyrelse eller nämnder.

En tjänsteplan tas fram av IT-enheten på stadskontoret tillsammans med IT-service på serviceförvaltningen. I planen finns aktiviteter för både vidmakthållande och vidareutveckling av stadens IT-plattformar och infrastruktur. I tjänsteplan som vi tagit del av för 2020 framgår ca 100 aktiviteter där behov identifierats. Uppskattad kostnad för att genomföra de investeringar som är resurssatta i planen (10) är 33 mnkr, dock finns aktiviteter där beslut fattats att ej genomföra aktiviteten av orsak som kommenteras i planen. Externa konsultkostnader uppgår till ca 5,5 mnkr på de aktiviteter där detta har angivits vilket är för närmare hälften av aktiviteterna. Av planen framgår också ansvar för aktiviteter samt om den är ej startad, pågående eller avslutad.

Det finns även en utvecklingsplan med aktiviteter för digitalisering och andra insatser för att genomföra aktiviteter som förbättrar kunskap och möjligheter i informations- och IT-säkerhetsarbetet. Innan projekt eller aktiviteter startas tas beslutsunderlag och projektdirektiv fram som enligt intervjuperson på stadskontoret granskas av IT-säkerhetsarkitekter inför beslut. I 2020 års utvecklingsbudget finns dedikerade medel inom både teknik, kompetens och test.

Det framkommer i intervjuer att IT-service saknar egen budget för kunna bedriva ett systematiskt säkerhetsarbete inom drift och nätverk. Med nuvarande beslutsgång avseende IT-projekt saknar IT-service beslutsmandat över vilka projekt och implementeringar som ska genomföras. De upplever därtill att de investeringar de lyfter ett behov av inte erhåller tillräckliga resurser utan ställs i relation till andra utvecklingsprojekt. Även om behov finns dokumenterade i den årliga tjänsteplanen så är det inte säkert att aktiviteten genomförs. IT-service på serviceförvaltningen har endast poster för personalkostnader i sin budget och inga tilldelade resurser för säkerhetslösningar. Det finns en upplevelse att resurser i form av personal utökas inom IT-enheten på stadskontoret och dess ansvarsområden medan det saknas resurser inom IT-service på serviceförvaltningen för att bedriva ett proaktivt och systematiskt arbete med säkerheten för de delar som serviceförvaltningen ansvarar för.

Ett exempel som framkommer är investering av ny brandvägg vilket har lyfts som ett behov från IT-service inom serviceförvaltningen redan under 2018 då man identifierat sårbarheter i den befintliga brandväggen. Re-investering av brandvägg återfinns i dokumenterad tjänsteplan för 2020. I samband med förändrade arbetssätt inom staden på grund av Corona-pandemin 2020 påskyndades beslut om investeringen. Detta då många medarbetare behövde arbeta på distans vilket krävde nya tjänster för anslutning och kommunikation med IT-miljön. IT-service menar att de brister som varit identifierade sedan tidigare borde varit tillräckliga för att beslut om att genomföra investeringen tagits då brandväggar ur ett säkerhetsperspektiv är en avgörande del för att säkerställa IT-säkerheten.

3.1.6 Bedömning

Vår bedömning är att kommunstyrelsen inte har tillsett att det finns en ändamålsenlig organisation med tydlig ansvarsfördelning för att styra IT-säkerhetsarbetet. Utifrån kommunstyrelsens reglemente framgår ansvaret att leda, strategiskt utveckla och samordna arbetet med informationssäkerhet och IT-frågor. I praktiken utförs detta ansvar i nuläget främst i form av samordning och inte genom att leda arbetet strukturerat och sammanhållet där helheten för stadens IT-miljö och IT-komponenter ingår. Det saknas dokumenterade uppdragsbeskrivningar för var och ens ansvar och mandatet är otydligt mellan stadskontoret och övriga förvaltningar. Detta behöver förtydligas så att stadskontoret kan verkställa sitt uppdrag att på stadsövergripande nivå ansvara för informations- och IT-säkerheten och vara kravställare mot förvaltningarna över det arbete som bör bedrivas inom varje nämnds ansvar för informationssäkerheten.

Kommunstyrelsen bör genom sin uppsiktsplikt över nämnderna säkerställa att dessa tar sitt ansvar för att informationssäkerhetsarbetet genomförs systematiskt och riskbaserat utifrån internt beslutade styrdokument.

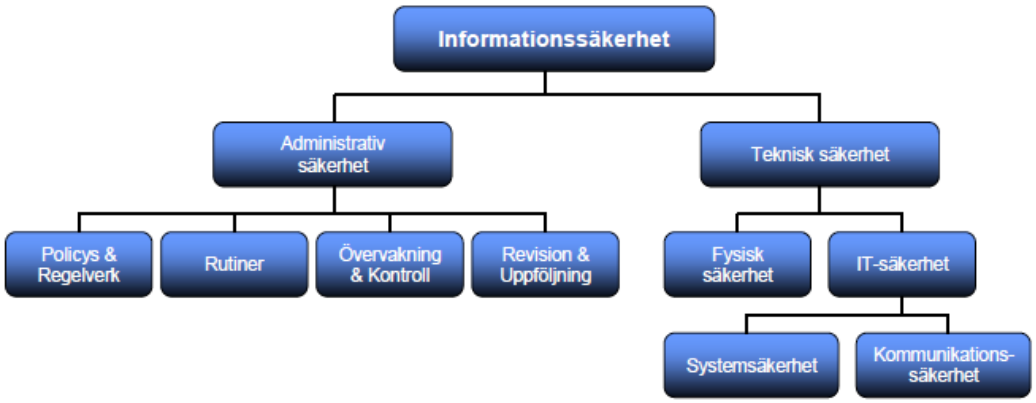
Det saknas därtill en vision, mål eller plan för hur arbetet ska bedrivas och vilka åtgärder som behöver vidtas för att nå dessa. Det finns därför inget underlag inför prioriteringar och gemensamma insatser som utvecklar stadens IT-säkerhet. I avsaknad av detta så tas beslut om investeringar utifrån en årsplanering efter bedömning av tjänstepersoner och förankras inte kommunstyrelsen trots att det i vissa fall påverkar budgeten i övriga förvaltningar.

Vi anser att det i en så stor verksamhet som Malmö stad behöver finnas centralt placerade ansvariga funktioner på stadskontoret (med närhet till förvaltningens ledningsorganisation) som med ett oberoende till andra förvaltningar och operativ IT-organisation kan säkerställa efterlevnad av styrdokument och genomföra revisioner i förvaltningarna för att identifiera brister som kan leda till rekommendendation om förbättringar. Detta för att arbetet på stadsövergripande nivå ska ske systematiskt och riskbaserat i enlighet med ett ledningssystem för informationssäkerhet och standarden ISO27001.

De resurser som finns i nuläget anser vi kommer få svårt att nå en tillräcklig nivå av informationssäkerhet. Det behöver därför utredas och bedömas av förvaltningarna vilka resurser som behöver tillsättas både avseende tid och kompetens för att ta sitt fulla ansvar för systemförvaltning och informationssäkerhet (inklusive dataskyddsarbete) för att dessa ska vara anpassade efter förvaltningens storlek, komplexitet och informationshantering. Då informationssäkerhetsarbetet är grunden för att säkerställa IT-säkerheten i staden så finns ett beroende där emellan som inte kommunstyrelsen och ansvariga för IT-säkerheten kan ta ansvar för på egen hand.

3.2 Styrdokument

Då IT-säkerhet är underordnad Informationssäkerhet så utgår vi i granskningen från den övergripande nivån och de styrdokument som avser att styra informationssäkerhet med den tillhörande IT-säkerheten.



3.2.1 Trygg- och säkerhetspolicy

Malmö stad har sedan 2017 en Trygg- och säkerhetspolicy[3] som har ersatt Säkerhetspolicyn för Malmö stad (KSKOM-1997–01009), IT-säkerhetspolicy för Malmö stad (KS-KOM-2006–00332) samt Policy avseende användning av datorer och internet inom Malmö stad (KS-KOM-2001–00475).

Trygg- och säkerhetspolicyn beskriver det övergripande säkerhetsarbetet vad gäller styrning och ledning samt uppföljning.

Det finns inga specifika delar i policyn som avhandlar informations- eller IT-säkerhet. Det finns inte heller några kompletterande policys som omfattar dessa områden.

3.2.2 Riktlinjer och anvisningar för informationssäkerhet

Riktlinjer och anvisningar för informationssäkerhet[4] (härefter riktlinjer för informationssäkerhet eller endast riktlinjer) finns där det anges att informationssäkerheten utgår från stadens säkerhetspolicy.

Riktlinjer och anvisningar för informationssäkerhet utgår från ISO/IEC 27000-serien där målsättningen är att alla informationssystem minst skall uppfylla de anvisningar som finns i riktlinjen.

I enlighet med intervjusvar anges att den beslutade riktlinjen och anvisning för informationssäkerhet ska fungera som ledningssystem för informationssäkerhet (LIS). Intervjupersoner anger dock att de anser den svårtillgänglig och alltför komplex för att vara ett stöd i det praktiska arbetet och sätta ramar för hur arbetet ska bedrivas, vilket är tanken med ett LIS.

I en tidigare revision av informationssäkerheten som EY genomförde på uppdrag av revisionskontoret under 2018 gjordes denna iakttagelse vilket ledde till en rekommendation om att revidera riktlinjerna. Det framkommer i intervjuer och går också att läsa i nulägesanalysen från 2019 att en större översyn av styrdokument ska genomföras som ska resultera i att dessa bättre stämmer överens med de rekommendationer som MSB har för ett systematiskt informationssäkerhetsarbete, vilka också bygger på gällande standard för informationssäkerhet.

3.2.3 IT-strategi

Det finns en IT-strategi[5] som ska visa viljeinriktningen för stadens arbete där IT stödjer utveckling och förbättring. Det framgår att IT-verksamheten ska bedrivas på ett kostnadseffektivt och säkert sätt och bidra till förverkligandet av Malmö stads övergripande verksamhetsmål. Verksamheternas behov är utgångspunkten för en samordnad, väl fungerande, tillgänglig och kostnadseffektiv IT-verksamhet. Behoven formuleras via IT-rådet som är sammansatt av verksamhetsföreträdare.

I IT-strategin anges att denna ska konkretiseras i handlingsplan för åren 2007–2010. Vi har inte tagit del av några handlingsplaner i granskningen. I samband med att kommunfullmäktige 2017-03-23 beslutade om Malmö stads program för digitalisering, Det digitala Malmö beslutades även att kommunstyrelsen fick i uppdrag att ta fram

[3] Antagen av kommunfullmäktige 2017-05-24
[4] Beslutad av kommunstyrelsen 2013-11-27, senast reviderad av KSAU 2019-06-17.
[5] Antagen av kommunfullmäktige 2007-04-06.

erforderliga riktlinjer för den digitala infrastrukturen och IT vilka skulle ersätta nuvarande IT-strategi. Nya riktlinjer är enligt uppgift från intervjuperson på remiss i nämnderna vid tiden för granskningen.

3.2.4 Bedömning

Vår bedömning är att kommunstyrelsen endast till viss del har tillsett att det finns ändamålsenliga styrdokument för IT-säkerhet. Det saknas i nuläget styrdokument på policynivå där den politiska viljeriktningen för stadens informations- och IT-säkerhetsarbete tydliggörs. I policy bör syfte och mål framgå, roller och ansvar samt hur uppföljning av arbetet ska fungera.

Policyn bör sedan tydliggöras i riktlinjer och anvisningar som konkretiserar hur målen ska uppnås och ansvaret för frågorna fördelas utifrån de olika målgrupper som är delaktiga i stadens informations- och IT-säkerhetsarbete.

Styrdokument som tillämpas idag avseende informationssäkerhet inkluderar endast i vissa delar IT-säkerhet. Nuvarande riktlinjer är omfattande och detaljrika och det finns en hänvisning till de avsnitt som berör IT-funktioner/IT-drift. De funktioner inom Malmö stad med ansvar inom dessa områden både inom stadskontoret och serviceförvaltningen anser därtill att nuvarande riktlinjer och anvisningar för informationssäkerhet inte är tillräckligt uppdaterade avseende tekniska förutsättningar för att kunna tillämpas i styrningen av IT-säkerhetsarbetet. Innehållet avseende informationssäkerhet upplevs även det vara alltför omfattande och svårgripbart för att vara ett stöd i förvaltningarnas arbete, främst vad gäller informationsklassning och riskbedömning där det framkommit synpunkter över att frågeställningar i klassningen inte är anpassade efter de moderna tjänster och system som nyttjas i staden.

Beslut finns att ta fram nya styrdokument som är anpassade efter målgrupp och upprättade i enlighet med MSB:s metodstöd för ett systematiskt informationssäkerhetsarbete. Vi anser att detta är nödvändigt och att de synpunkter som framkommit i analyser och granskningar avseende styrdokument bör beaktas vid framtagandet för att styrdokumenten ska tillämpas i högre grad och utgöra ett stöd i stadens arbete.

3.3 Informationssäkerhet

I Riktlinje och anvisningar för informationssäkerhet som vi beskrivit i avsnitt 3.2.2 framgår av kapitel 6.6 ”Ledningens ansvar” att informationssäkerhetsarbetet ska vara ett integrerat perspektiv i det dagliga arbetet i samtliga av kommunens verksamheter då det är en del av Malmö stads styr- och ledningssystem. Ytterst ansvariga för informationssäkerheten är nämnderna genom att ställa krav på informationshanteringen genom intern kontroll samt avsätta resurser för att möta de hot som kan uppstå i verksamheten. Som systemägare har nämnden ett ekonomiskt, funktionellt och säkerhetsmässigt ansvar för sina informationssystem och digitala tjänster under hela dess livscykel.

Informationssäkerhetssamordnarna på stadskontoret har genomfört en nulägesanalys under 2019 som en uppföljning över förvaltningarnas arbete med informationssäkerhet. Denna har presenterats i ledningsgruppen för stadskontoret. När nulägesanalysen

presenterades gavs en rekommendation att analysen borde presenteras i förvaltningarnas ledningsgrupper och att de centrala informationssäkerhets-samordnarna skulle bjudas in tillsammans med förvaltningens informationssäkerhetssamordnare och ha en dialog om hur arbetet skulle kunna bedrivas inom förvaltningen utifrån de behov som identifierats i analysen.

I nulägesanalysen framkommer följande stadsövergripande behov i informationssäkerhetsarbetet:

- Det finns önskemål och behov av centralt framtagna ramar och uppdrag för hur förvaltningarnas samordnare ska förvalta sin roll och uppdrag, ansvar, mandat etc. Vem ska utföra vad?
- Reformering av befintliga styrdokument i syfte att bli mer praktiskt användbara i det dagliga arbetet.
- Tydligare stöd och vägledning avseende uppföljning av informationssäkerhetsarbetet.
- Tydligare stöd och vägledning avseende incidentrapportering
- Behov av ett Malmö stadsövergripande ställningstagande till vad Office 365 med tillhörande tjänster kan användas?

Det framkommer även från intervjupersoner att det för att lyckas med ett systematiskt informationssäkerhetsarbete behövs en behovsanpassad och tydligt uttalad och kommunicerad samordnarroll, dialog- och rapporteringsmöjlighet till en engagerad ledning. Dessutom behövs möjligheter att genomföra informationssäkerhetsinriktade aktiviteter och åtgärder både på strategisk och operativ nivå i olika delar inom förvaltningens linjeorganisation, tillsammans med andra berörda funktioner/roller.

Avsaknaden av eller brister i dessa grundläggande förutsättningar riskerar att leda till otydlighet i vad som ska, eller behöver göras, felaktiga prioriteringar och oklara gränsdragningar avseende ansvarsfördelning. I förlängningen riskerar detta att generera ett mer fragmenterat och osammanhållet informationssäkerhetsarbete snarare än det motsatta och önskvärda som är ett sammanhållet och systematiskt arbete.

3.3.1 Informationsklassificering

Det saknas i nuläget en uppdaterad och funktionell registerförteckning, innefattandes kommunens samtliga verksamheters IT-system och tjänster där den information och dokumentationen som behövs i form av klassning, roller/ansvar, riskhantering och kontinuitetshantering kan anses vara komplett. Förteckningen finns delvis i systemet IFacts. Intervjupersoner beskriver systemet som föråldrat och inte anpassat efter de tjänster och system som används idag. Det har skett ett flertal omtag för att alla system ska finnas dokumenterade men den bristfälliga funktionaliteten anges som en av anledningarna till att det inte genomförs fullt ut. Andra anledningar till att detta inte finns dokumenterat anges vara den bristfälliga förmåga som upplevs över efterlevnad beslutade rutiner och processer, däribland kommunövergripande systemförvaltningsmodell.

Det framkommer vidare att det finns ett stort mörkertal i antal system som är dokumenterade i iFacts. IT-service driftar och ansvarar för ca 50–60% av de system

som används. Det finns även många tjänster där informationen finns någon annanstans. Den verksamheten som köper in tjänsten har ett ansvar att säkerheten är upprättad.

Informationsklassning är en genomgång och bedömning av skyddsvärde på information kopplat till riskbedömning för denna. Klassningen ska leda till en åtgärdsplan för att säkerställa skyddet för informationen. Det är därför en avgörande aktivitet att den genomförs så att IT-säkerhetsåtgärder kan vidtas som står i relation till skyddsvärde och risker. Informationsklassning är ett ansvar inom förvaltningarna och bör göras i samråd mellan informationsägare, systemförvaltare, informationssäkerhetssamordnare och IT-säkerhetskunnig.

Intervjupersoner har beskrivit att klassningen genomförs i form av ett antal workshops där deltagarna varierar utifrån processens genomförande. I steg ett deltar verksamhetsrepresentanter som har god kännedom om informationen. I riktlinjen för informationssäkerhet finns det anvisningar hur klassningen ska gå till. Klassningen dokumenteras i ett protokoll som ska bifogas i iFacts när den är klar. Kraven är framtagna utifrån lagar, förordningar, standarder och interna styrdokument som måste beaktas i informationshanteringen. Klassning av icke digital information, dvs fysiska handlingar som hanteras i verksamheten genomförs av respektive handläggare i enlighet med kap 8.1 i riktlinjen med tillhörande klassningsmatris samt stöd i arkivhandboken på respektive förvaltning.

Intervjupersoner lyfter att den klassningsmetod som är beslutad inte fungerar fullt ut och att beslut om en ny modell borde tas som är mer anpassad till dagens moderna system och hantering. Det beskrivs vidare att efter klassningen ska det utifrån skyddsvärde identifieras ett antal säkerhetsåtgärder som leder till anpassade tekniska lösningar. Det som har skett senaste åren är att det har tillkommit nya krav från IT i samband med upphandling av nya system som behöver komplettera kravbilden från klassningen. I intervjuer framkommer att det då har skett att förvaltningarna utgår från kravbiblioteket och inte gör informationsklassningen enligt riktlinjer.

En annan anledning som lyfts i intervjuer till att klassningen inte genomförts fullt ut är att det inte finns tid och resurser för att bedriva arbetet. Det finns ingen likvärdig och enhetlig struktur mellan förvaltningarna för systemförvaltning. Det finns en beslutad systemförvaltningsmodell för staden men i intervjuer framkommer att den förvaltningsmodell som beslutats av stadskontoret, Pm3, inte har implementerats i förvaltningarna i så stor utsträckning. Ett flertal uttrycker ett behov av ett mer närvarande stöd från centrala funktioner för att ta sig an förvaltningsmodellen då den anses alltför omfattande, alternativt få resurser på förvaltningen med den kompetens och tid som krävs för att bedriva arbetet. Bristande kompetens och/eller resurser i form av tid påverkar i stort hur informationssäkerhetsarbetet kan bedrivas.

3.3.2 Riskhantering

Det framkommer en bild i intervjuer att det i nuläget inte finns en gemensam och beslutad rutin för att göra riskanalyser och att verktyg saknas. Stadskontoret har i uppdrag att ta fram en mall för riskanalyser inom IT-verksamheten som följer den stadsövergripande modellen för intern kontroll, COSO-metoden. Arbetet är påbörjat och är ett första steg där sedan kontinuitetsplanering även ska ingå.

Exempelvis lyfts att projekt med implementeringar har ett tekniskt implementationsfokus där mindre vikt läggs vid att beakta risker och konsekvenser juridiskt, kompetensmässigt eller för säkerhet och drift vilket sedan ställer till det efter att implementeringen är genomförd. Ett exempel som lyfts från flera intervjupersoner är implementeringen av Office 365 där man inte beaktade risker som lyftes från driftsidan gällande belastning och påverkan på nät och brandvägg samt den internettrafik som implementeringen skulle medföra. Detta resulterade sedan i att servicedesk fick en ökning av supportärenden med närmare 1000%. I samband med implementeringen beslutades att en molnbaserad lösning skulle ersätta lokal lagring av användarnas hemkatalog. Vi har i granskningen tagit del av en upprättad risk- och konsekvensanalys över informationshanteringen vid migreringen till molnlösningen.

I intervjuer beskrivs att det i projektet för Office 365 informerades på ledningsnivå och skriftlig till varje användare att bla. sekretess och andra känsliga uppgifter inte fick lagras i molnet eller i lokal hemkatalog, utan i avsedda verksamhetssystem. Om användaren trots detta hade sekretess i hemkatalogen skulle detta innan migrering raderas eller sparas över på krypterat USB-minne. Förvaltningarna hade ett eget ansvar att genomföra riskanalyser för sin informationshantering och lagring av information. Vid implementeringen av Office 365 i Malmö stad som skedde under 2017 hade inte dataskyddsförordningen trätt i kraft och de frågeställningar som drivits avseende lagring i molnet har aktualiserats efter detta beslut. I intervjuer beskrivs dock att hanteringen behöver bedömas av förvaltningarna ur flera aspekter beroende på vilken typ av information som hanteras som personuppgifter, sekretess eller andra juridiska perspektiv vilket ska ske genom informationsklassning och riskbedömning i förvaltningarna.

Det genomförs till viss del en riskbedömning i samband med informationsklassning. Då dokumentationen i iFacts upplevs bristfälligt upplever dock ett flertal intervjupersoner att resultat av klassning och riskanalys inte är tillförlitlig för att agera på. Resultatet av klassning och riskbedömning är beroende av deltagarnas kunskap och insikt om den information som hanteras i system eller digital tjänst. För viss information har klassning skett som visar att denna ska hanteras i enlighet med rikets säkerhet, det vill säga, den mest kritiska nivån av klassning. Det är dock få av förvaltningarna som är villiga att implementera säkerhetsåtgärder i enlighet med den kostnad detta medför.

3.3.3 Identitet och åtkomst

Det finns beskrivet i de beslutade riktlinjerna för informationssäkerhet att åtkomst till IT-system och nätverk ska styras utifrån verksamhetens behov och säkerhetskrav. Rutiner ska finnas för att säkerställa behöriga användares åtkomst och för att förhindra obehörigas åtkomst till Malmö stads informationssystem. Det framgår vidare i riktlinjerna att verksamhetschefer beslutar om behörigheter och att behörighetsadministratörer ska utses för hanteringen. Förvaltningarna ansvarar för att det finns tillräckliga funktioner för loggkontroll och övervakning för att transaktioner ska kunna knytas till unika användare. Behov och uppföljning fastställs av systemägare utifrån verksamhetens behov och genomförd informationsklassning.

I stadens IT-miljö nyttjas funktion i Microsoft som heter Active Directory, AD, för att styra det mesta av åtkomsten till stadens plattform och nätverk. I AD registreras IT-komponenter som skrivare, datorer och användare. Säkerhetsgenomlysning genomförs återkommande.

Stadskontoret tillhandahåller säkra inloggningsmetoder (olika lösningar och säkerhetsnivåer, ex MFA) och rekommendationer. Det är informationsägaren som bär det yttersta ansvaret och beslutar om sina system och vilken typ av inloggningsmetod som ska implementeras. Detta krav framkommer vid klassificering i iFacts. Beskrivningar finns i kravbibliotek för att systemägare ska kunna kravställa rätt sätt vid upphandling. Den brist som upplevs är att säkerställa efterlevnad, dvs att rätt lösning, verkligen, används utefter krav i iFacts.

Sedan några år har IT-enheten på stadskontoret förespråkat att förvaltningarna ska använda de säkerhetslösningar som erbjuds när det finns behov av att ytterligare skydda information. Förstärkt inloggning till Office 365-plattformen finns men det har varit lågt intresse för detta från förvaltningarnas sida. Genom implementering av Office 365 ingår moderna tekniska lösningar som vid behov kan användas för att öka säkerheten om dessa tjänster nyttjas. Microsofts Azure Multi Factor Autentication, MFA är en sådan tjänst där verifiering sker via annan teknisk kanal. Vid användande av MFA så sker en automatisk bedömning över när användare behöver verifiera sig med ytterligare moment än användarnamn och lösenord utifrån förinställda parametrar. Detta är ett stöd för säkerhet utifrån användningen av plattform och tjänster.

Det framkommer därför att det skulle utveckla säkerheten om det beslutas över generella krav på hur tillgång och åtkomst ska hanteras för vissa roller, exempelvis det stora antal chefer i staden som har tillgång till känsliga personuppgifter och personuppgifter samt annan känslig information. Inom stadskontoret upplever man svårigheter att få igenom krav på rutiner och följsamhet efter en implementering.

Tjänster och system finns men det är förvaltningen som avgör vilka som ska nyttjas och för vilka funktioner. Under hösten 2020 införs multifaktorautentisiering som heter Freja-ID och kan liknas vid en inloggning med Bank-ID. Det finns dock inget beslut eller rekommendation över hur detta ska tillämpas av förvaltningarna och om det ska finnas krav för användning av multifaktorautentisering för vissa utsedda roller eller funktioner i stadens verksamheter. I tjänsteplanen för 2020 finns ett flertal förslag på aktiviteter kopplat till identitet och åtkomst.

Det saknas enligt uppgift av intervjupersoner en förteckning över vilka personer som har mandat att göra beställningar av förändring av behörighet och åtkomst vilket leder till att tjänsteägare på stadskontoret inte vet hur detta är beslutat inom förvaltningarna och om beställningar som kommer är gjorda av de med mandat att göra det.

Det finns en tjänst från Microsoft i plattformen som övervakar ovanliga beteendemönster eller konkret identitetsstöld som leder till larm och att användarkontot spärras så ett lösenordsbyte krävs. När detta sker så tas kontakt med den person som är drabbad och då har det gett ett resultat för att även börja använda förstärkt inloggning för att skydda kontot bättre.

3.3.4 Medvetenhet och förståelse

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

I riktlinjerna för informationssäkerhet framgår att informationssäkerhet är en del av Malmö stads styr- och ledningssystem för att upprätthålla och bibehålla tjänster och förtroende. Förankringen och medvetandet hos medarbetare är grunden för att lyckas med detta arbete. Det är därför varje chefs ansvar att kommunicera vikten av god informationssäkerhet.

Trots denna beskrivning i riktlinjer framgår i intervjuer att det finns en otydlighet över vems ansvar det är att det finns en tillräcklig medvetenhet hos stadens medarbetare och förtroendevalda. Det måste ske en regelbunden kommunikation för att uppmärksamma användare på hot i form av mail eller identitetsstöld och hur detta ansvar ser ut för varje användare. Användare hör i stor utsträckning av sig till IT-service och behöver fråga hur de ska logga in, vad de får göra och vilka system som ska användas vilket enligt intervjupersoner tyder på att linjeansvaret brister inom IT-säkerhet kopplat till användarna.

I uppföljning av intern kontroll för kommunstyrelsen för tertial 2, 2020 framkommer att det finns brister i introduktion av nya medarbetare där Informations- och IT-säkerhet lyfts som särskilda områden. För att följa upp resultatet ska fördjupade intervjuer genomföras under hösten 2020. Det framgår av uppföljningen att det pågår ett förbättringsarbete för stadskontorets introduktionsprocess där synpunkterna kommer att beaktas.

3.3.5 Utbildning

Varje förvaltning ansvarar för egen utbildning av sina medarbetare. I riktlinje för informationssäkerhet och i dialog med informationssäkerhetssamordnare hänvisas till utbildningen DISA som tillhandahålls av MSB.

Vissa förvaltningar har utbildning som en obligatorisk del i introduktionsprogram. Stadskontoret genomför utbildning två gånger per år för nyanställda. Vissa förvaltningar har endast en länk till utbildningen på intranät men det är valfritt att genomföra den. Flera förvaltningar har efterlyst en central utbildning som ett helhetsgrepp i introduktion. Uppdraget ligger hos HR.

I granskningar genomförda av de centralt utsedda informationssäkerhetssamordnarna och kommunrevisionen åren 2014, 2015, 2019, 2020 har det funnits delmoment där utbildning granskats. Vid samtliga tillfällen har det framkommit brister, vilka påtalats i samband med redovisning av resultaten.

3.3.6 Bedömning

Det finns i nuläget inte en komplett förteckning över stadens system och IT-komponenter med erforderlig information. Eftersom inte samtliga tillgångar finns dokumenterade och därigenom inte klassats eller riskbedömts går det inte att fastställa om tillräckliga IT-säkerhetsåtgärder är vidtagna för att skydda informationen. Utan en informationsklassning så behöver IT-enheten på stadskontoret och IT-service på serviceförvaltningen vidta de säkerhetslösningar på övergripande nivå som de utifrån sin kompetens bedömer som nödvändiga ur ett tekniskt perspektiv.

Klassning har genomförts till viss del men metoden som används upplevs inte vara anpassad efter dagens tekniska lösningar och arbetet med klassningen är inte fullt ut implementerad i staden. Förvaltningarna arbetar till viss del med riskanalyser i

samband med klassningar men vår bedömning är att detta än så länge inte sker systematiskt. Arbete med riskanalyser sker till viss del för informations- och IT-säkerhetsarbetet i samband med implementeringar av nya tekniska lösningar. En stor del av ansvaret för riskanalyser finns dock hos förvaltningarna som informations- och systemägare och ska hanteras i enlighet med gällande riktlinjer och anvisningar för informationssäkerhet.

Det yttersta ansvaret för informationssäkerheten finns hos respektive nämnd. Detta innebär att kommunstyrelsen genom sin uppsiktsplikt behöver säkerställa att nämndernas arbete sker i enlighet med gällande lagar och beslutade riktlinjer. Vår bedömning är att nuvarande kontrollmål för intern kontroll inte är tillräckligt för att följa upp nämndernas arbete med informationssäkerhet och att detta sker i enlighet med beslutade riktlinjer.

Behovet av en ökad medvetenhet och gemensam förståelse kring informations- och IT-säkerhet har under ett flertal intervjuer med nyckelpersoner lyfts som avgörande för hur kommunen ska få ett systematiskt arbete inom området. Bristen på medvetenhet är en av de största säkerhetsriskerna med det stora antal användare som finns i stadens IT-miljö. Det finns instruktioner i riktlinjer för informationssäkerhet som riktar sig till användare över användningen av IT-utrustning men vi anser att detta dokument är alltför omfattande för att det ska kunna förväntas att samtliga medarbetare tar del av det då det inte är utformat på ett sätt som medför tillgänglighet och förståelse hos var och en. Utbildningar inom ramen för IT- och informationssäkerhet har endast till viss del erbjudits genom e-utbildning. I de uppföljningar som skett i samband med nulägesanalys för informationssäkerhetsarbete eller revisioner har det i resultat i samtliga dessa lyfts att brister finns avseende utbildning. Att medarbetarna har kunskap och kännedom om sitt ansvar för informationssäkerhet är delegerat till nämnderna och följer det ordinarie ledningsansvaret. Det är väsentligt att kunskap finns för att upptäcka och rapportera incidenter i de fall dessa inträffar.

Då brister i tydlighet finns över var och ens ansvar medför det svårigheter att avkräva ansvar och efterlevnad för att vid behov vidta disciplinära åtgärder vid bristande hantering, vare sig den är uppsåtlig eller icke uppsåtlig. Bristen på medvetenhet visar sig dels i att det saknas kunskap om vad som är informationssäkerhetsincidenter som därför inte upptäcks och rapporteras i tillräckligt hög grad dels i form av många ärenden till servicedesk över hantering och frågor över vad som gäller avseende hantering av information och IT.

En viktig del för att begränsa användares möjligheter till påverkan på information och system är en restriktiv behörighet- och åtkomsthantering. Hantering och ansvar anges i riktlinjer för informationssäkerhet. Ansvaret ligger till stor del inom förvaltningarna att säkerställa sin åtkomsthantering varpå vår bedömning är att det finns behov av ytterligare informationsinsatser och rekommendationer från ansvariga för informations- och IT-säkerhet över när det finns behov av utökade tjänster för behörighetskontroll. Utifrån att det inte funnits så stort intresse för dessa tjänster är vår bedömning att det inte finns en tillräcklig förståelse och kunskap i förvaltningarna för att själva kunna avgöra när det finns behov av det.

Vår bedömning är att det på stadsövergripande nivå finns en tydlig styrning av åtkomst via Active Directory, AD där Malmö stads IT-komponenter finns registrerade. Åtkomst till verksamhetssystem och förvaltningsspecifika tjänster är ett ansvar inom varje

förvaltning att hantera och har inte genomlysts i denna granskning utifrån granskningens avgränsning.

3.4 Drift och teknik

IT-enheten och IT-service har i sitt uppdrag för kommungemensam IT investerat i nya åtkomstlösningar, nytt datacenter med bättre säkerhetsfunktioner, nya brandväggar, autentiseringslösningar, identitetslösningar, managering och säkerhetslösningar för enheter som telefoner, plattor och datorer. I årliga tjänsteplaner och utvecklingsplaner finns säkerhetsaktiviteter identifierade och budgetsatta, som exempelvis utveckling av övervakning och loggning, penetrationstester m.fl. Det finns ett strukturerat planeringsarbete mellan IT-enheten och IT-service i form av förvaltningsplaner som ska fånga nya behov och förslag på åtgärder. Ett arbete pågår med en genomlysning över vilka områden inom drift och teknik det behövs förstärkning för. En IT-säkerhetsanalys är planerad att genomföras som en del i detta arbete. Den ska kunna användas för att prioritera säkerhetsfunktioner och på vilka sätt olika miljöer behöver skyddas. Det saknas i nuläget en helhetsbild över vad som pågår för att utveckla IT-säkerheten och upplevs finnas ett stort behov av att få en mer sammanhållen bild av det arbete som pågår och vilka som är delaktiga.

Den största begränsning i nuläget beskrivs i intervjuer vara att vissa verksamhetssystem i förvaltningarna är föråldrade och inte kompatibla med moderna lösningar och säkerhetslösningar inte finns på plats i de gamla tjänsterna. IT-enheten på stadskontoret upplever sig ha svårt att kräva en förändring som innebär en investering i förvaltningarna. Det finns också inom vissa verksamhetsområde fåtal alternativ till verksamhetssystem och de som finns till stor del bygger på en teknik som inte nyttjas i så hög grad längre. Det innebär dock att det inte bara påverkar det faktiska systemet utan även andra system och tjänster i IT-miljön. Sedan några år har IT-enheten på stadskontoret arbetat med ett kravbibliotek som ställs mot verksamheten i deras kontakt med leverantörer men med det arv som finns med befintliga system så är det ett tiotal år kvar tills allt är utbytt. Inte förrän dess så finns det ett kravbibliotek som följs fullt ut.

I dialog med verksamheterna har IT-enheten på stadskontoret och IT-service på serviceförvaltningen försökt få förvaltningarna att agera och förstå hur detta påverkar det övergripande säkerhetsarbetet men har fått till svar att det är en IT-fråga som behöver lösas, inte en åtgärd i förvaltningen. Det finns ett stort antal verksamhetssystem och många leverantörer som arbetar med Malmö stad så det hade varit önskvärt med tydligare mandat för de med ansvar för IT-säkerhet att följa upp följsamhet till riktlinjer, kravbibliotek och andra beslut som fattas för att det ska finnas en tillräcklig säkerhet för stadens information och IT-miljö.

3.4.1 IT-säkerhetsåtgärder

Närverk är segmenterade mellan förvaltningar och kommunikation mellan dessa sker via router och brandvägg. Även wifi-nät är separerade och säkerhetsklassade. Det finns en del strukturella problem som leder till sårbarheter som påverkar effektivitet i övervakning. Det har skett ett arbete med re-investeringar i nytt datacenter, brandväggar och åtkomsthantering. I intervjuer beskrivs dock att arbetet med IT-

säkerhetsövervakning behöver utvecklas och att det till viss del saknas verktyg för detta. I utvecklingsplanen för 2020 bekräftas detta då behov har lyfts att genomföra en förstudie med syfte att hitta lösningar för en central överblick av säkerhetshändelser. Det anges att nuvarande hantering där detta ansvar och utförande sker inom förvaltningarna är resurskrävande och osäkert. Det pågår en teknisk uppdatering av system för övervakning av servrar men det enda den kan göra är att skicka ett mail när det sker något vilket är en stor risk för driften och säkerheten då arbetet sker reaktivt när något händer och inte som en proaktiv lösning. I nuläget sker larm när intrång gjorts och en identitetsstöld skett.

Intervjupersoner framhåller att det finns bra IT-säkerhetslösningar som standard i alla datorer som tillhandahålls av Malmö stad. Genom implementering av Office 365 och Windows 10 har säkerheten förbättrats. Det har också lett till ett ökat fokus på IT-säkerhet genom att användning av tidigare tjänster med lägre säkerhetsnivåer har kunnat begränsas eller avslutats.

Många av de standardlösningar som Microsoft erbjuder i grunden används men intervjupersoner beskriver att dessa kan behöva anpassas utifrån olika behov och nivåer. Det anges vara för mycket som är valbart och frivilligt genom att ansvaret till stor del är förflyttat till förvaltningarna och det inte finns en tydlighet i vad som gäller. Det finns tilläggslicenser som kan kopplas till roller i staden som anses hantera mer skyddsvärd information men inget beslut är fattat över införandet av detta eller hur kostnaden i sådana fall skulle fördelas. I intervjuer beskrivs att en ökning av skyddsnivåerna generellt för all personal i Malmö stad innebär att användande och tillgång försvåras. Därför måste en ökad skyddsnivå vara motiverad och belagd utifrån identifierat hot eller behov. Även kostnadsaspekter behöver vägas in i en sådan bild. Inga sådana hot eller behov är identifierade och framlagda av förvaltningarna i nuläget.

Malmö stads IT-verksamhet tillhandahåller en centralt hanterad klientplattformsdator. Denna används av i stort sett samtliga anställda (ej elever/utbildning). Denna hålls uppdaterad med säkerhetspatchar, virusprogram och brandvägg. Åtkomst hanteras med centralt automatiserade behörighetslösningar och certifikathantering. Kryptering av lokala data såväl som molnbaserad data kan göras. Smartphones och plattor hanteras (tvingande) via EMS och Intunes för att bla. forcera lösenordsskydd samt att enheterna kan raderas på distans vid borttappande eller stöld.

I nuläget kan inte IT-enheten eller IT-service se den kommunikation som sker i nätet. Stadskontoret har inte mandat att övervaka aktivitet för att förhindra intrång eller upptäcka att någon har tillgång till information som den inte ska ha behörighet till. Detta har dock efterfrågats och finns med som aktivitet för utveckling. Utdrag från loggar kan göras vid misstanke om brott och initieras i dessa fall av polis eller förvaltningschef. I intervjuer anges att det skulle vara värdefullt för att öka kunskapen och kunna arbeta med fördjupade analyser och övervakning i ett tidigare skede.

Det framkommer i intervjuer att det sker incidenter i form av intrångsförsök löpande och att incidenterna ofta är kopplade till den mänskliga faktorn genom att användare klickar på länkar i mail som leder till identitetsstöld eller att virus sprids. På IT-service inom serviceförvaltningen så får man kännedom om detta om det leder till driftsstörning och rutiner och processer finns för att hantera detta.

Intervjuperson beskriver att investeringar görs kontinuerligt i säkerhetshöjande lösningar baserat på behov och underlag. Utmaningar finns däremot i att implementera

tekniska lösningar samt att höja säkerhetsmedvetandet hos stadens anställda så att arbetet kan ske mer proaktivt.

3.4.2 Testning och utveckling

Stadskontoret styr utveckling och utifrån sitt ansvar för plattformar och system så sker en kontinuerlig utveckling av säkerhet och funktionalitet. Intervjusvar visar att kommunen bedriver egen utveckling i liten utsträckning, merparten av all utveckling sker genom nyttjandet av externa konsulter och leverantörer.

Varje år tas tjänsteplaner fram där behov identifierats över investeringar. Det upplevs tungrott att få beslut om investeringar i konkurrens med andra aktiviteter som prioriteras. Genom omvärldsbevakning och kunskap så vet man att det finns nya, moderna lösningar med högre säkerhet i grunden som skulle utveckla IT-säkerheten generellt.

Intervjusvaren visar att kommunens förvaltningar själva avgör vilka miljöer som dess utveckling ska ske i men att beställningar om förändringar i tjänster och system läggs till stadskontoret som kan avgöra hur dessa påverkar andra delar i IT-miljön. Om det finns behov av att göra avsteg från styrande dokument för informationssäkerhet kan förvaltningen besluta om det så länge det inte äventyrar infrastrukturen generellt.

Vid nyinköp sker alltid en bedömning av säkerhetskrav och IT-enheten är med i processen från början. Processen utgår från det kravbibliotek som tagits fram.

Det framkommer också i intervju att IT-service på serviceförvaltningen inte blir tillfrågade att delta i projekt där de har kompetens utan att IT-enheten på stadskontoret tar in externa konsulter. Det finns även exempel på projekt där det upplevs ha funnits en bristande förankring så att väsentliga funktioner inte blir delaktiga i genomförandet eller kopplas in försent och därför inte ges möjlighet att påtala tekniska eller säkerhetsmässiga risker eller avvägningar.

I intervju beskrivs att IT-enheten har en projektmetodik som kallas ProjektStegen som följs vid IT-projekt. Intervjupersoner upplever dock att uppföljningen av genomförda projekt är bristfällig och att det saknas en bedömning av effekthemtagning för de investeringar som beslutats. I intervju uppges att reella effekter ofta uppstår på andra ställen i organisationen än på IT-enheten och IT-service varpå det är en utmaning att följa upp och utvärdera.

Vidare visar intervjusvaren att en strukturerad testning av tekniska miljön, genom sårbarhetsscanning alternativt penetrationstestning, inte genomförs. Det finns ett pågående uppdrag att genomföra en IT-säkerhetsanalys på stadsövergripande nivå. Denna behöver dock upphandlas så är i planeringsfas vid tiden för den här granskningen.

3.4.3 Kontinuitetshantering och planering

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.

Avseende driftssäkerhet så anges i intervjuer att staden har hög tillgänglighet med få störningar och avbrott i fibernätet. Det finns två åtskilda datahallar och intervjupersoner

menar att staden har en välbyggd teknisk driftsmiljö med redundant nät och redundanta system som körs parallellt så det finns ett i reserv om det andra går ner. I och med det har en bedömning gjorts att det inte finns behov av dygnet runt-personal. I dialog med förvaltningarna har det framkommit att man inom vissa delar önskar tillgång till dygnet runt service men det är inte i nuläget reglerat i några servicenivåöverenskommelser, så kallade SLA. IT-service har lyft detta som en säkerhetsrisk då vissa verksamheter har verksamhetskritiska system som inte får ha avbrott mer än en mycket begränsad tid enligt klassning i iFacts. Om det skulle uppstå larm utanför kontorstid anger intervjuperson att det finns möjlighet att beordra in personal och påbörja felsökning och åtgärder utifrån en prioriteringslista som finns inom IT-service på serviceförvaltningen.

Vissa verksamheter har avtal med externa parter om servicenivåer utanför kontorstid med jourtjänster. Det framkommer dock att även om vissa system skulle ha ett högre behov av SLA så speglas inte det för driften av infrastruktur för nätet.

Enligt riktlinjer för informationssäkerhet så har verksamhetsansvarig chef ansvaret för att det finns en dokumenterad kontinuitetsplan för kritiska och/eller samhällsviktiga verksamheter samt verksamheter vars stödjande systems krav på tillgänglighet klassificerats som Mycket viktig eller Kritisk. Intervjusvar bekräftar att kommunens förvaltningar självständigt ansvarar för framtagande av de kontinuitetsplaner som behövs. Det framkommer i intervjuer att det är en del i dokumentationen i iFacts men att det har skötts bristfälligt de senaste åren. I samband med krisledning utifrån Corona-pandemin var IT beroende av en prioriteringslista över vilka verksamheter och system som skulle prioriteras att hantera för verksamhetens kontinuitet. Då upptäcktes att mycket av informationen i iFacts var ouppdaterad och inte användbar varpå det gick inte att verkställa en prioriteringslista och kontinuitetsplanering.

För enskilda verksamheter inom serviceförvaltningen har vi fått beskrivet att det finns väl utvecklade och regelbundet testade kontinuitetsplaner, exempelvis för verksamhet som hanterar färdtjänst.

Förvaltningarnas kontinuitet är beroende av bibehållen drift av IT och digitala system, vilket står under IT-service inom serviceförvaltningens ansvar att upprätta kontinuitetsplaner för. Granskningen har genom intervjusvar kunnat fastställa att en övergripande och gemensam kontinuitetsplan för kommunen saknas.

I den operativa driften finns framtagna processer enligt ITIL-ramverket som används för att upprätthålla kontinuiteten för verksamhetskritiska system. Processerna är incident, problem och change. IT-service har i dessa processer tagit fram en prioriteringslista för att vid större incidenter kunna koppla resurser till de mest verksamhetskritiska systemen. Det finns även en process för major incident.

3.4.4 Incidenthantering

I riktlinjer för informationssäkerhet finns ett avsnitt som beskriver stadens incidenthantering. Bland annat beskrivs att incidenter ska rapporteras snarast för att minimera skada, åtgärda brister och utreda eventuell brottslighet. Ett antal exempel på incidenter beskrivs.

Allvarliga informationssäkerhetsincidenter ska enligt riktlinjen:

- Omgående rapporteras till tjänstgörande TIB (Tjänsteperson i beredskap).
- Rapporteras till Malmö stads informationssäkerhetssamordnare för kännedom.
- I det fall händelsen endast berör enskild förvaltning också rapporteras till berörd förvaltnings kontaktperson.

Stadsövergripande ska vissa incidenter rapporteras i ett system som heter Agera. Där rapporteras informationssäkerhetsincidenter, personuppgiftsincidenter men inte IT-incidenter. IT-incidenter är ett ansvar för IT att hantera och sker i ett system inom IT-enheten på stadskontoret och IT-service på serviceförvaltningen.

Enheten för säkerhet och beredskap har fått i uppdrag att i samverkan med andra funktioner se över rutin för hantering och rapportering av incidenter och vara sammanhållande för detta arbete.

Informationssäkerhetssamordnarna finns inte med som en roll i Agera och får därigenom ingen information om inträffade incidenter i nuläget. Enligt intervjusvar sker ingen rapportering till nämnd eller styrelse över incidenter utan hanteras i tjänstepersonsorganisationen.

Det framkommer i intervjuer att det behövs ett förbättringsarbete för att tydliggöra rutin och hantering av incidenter oavsett typ av incident. I rapporten för den nulägesanalys av informationssäkerhetsarbetet som genomförts finns dokumenterat att förvaltningarna har behov av tydligare stöd och vägledning avseende incidentrapportering. Det framgår vidare i rapporten att det ska arbetas in med övriga behov av säkerhetsuppföljning i Malmö stads styr- och ledningssystem.

Det har gjorts försök att upprätta en incidentstatistik men det har varit svårt att få att fungera. Det finns inte heller någon samlad rapportering av incidenter. I en omorganisation av IT-funktionen anses detta vara ett prioriterat område att diskutera och förankra samt kommuniceras med verksamheterna så att alla har gemensamma rutiner och kännedom om dessa.

För IT-incidenter kunde det tidigare anges vilken typ av IT-incident som inträffat och på så sätt få en överblick över vilken typ av intrång eller sårbarhet som identifierats. Nu rapporteras allt på övergripande nivå och anges i ärendehanteringssystemet som IT-säkerhet.

Internt inom IT-service upplevs det finnas en tydlig och dokumenterad incidenthanteringsprocess. Vid en allvarlig incident så har incident manager, som är en roll inom IT-service ansvar att skyndsamt vidta åtgärder och sammankalla resurser för att lösa situationen.

Incidenter i form av identitetsstöld ökar och larm om detta leder till att kontot spärras av IT-service. Det sker en ökning av denna typ av incident och en risk som diskuterats är om det är kopplat till att medarbetare kan logga in på privata enheter.

Incidenter händer till stor del som följd av att medvetenheten hos medarbetare och förtroendevalda är alltför låg, vilket vi beskrivit tidigare i rapporten. Det behövs kontinuerliga informationsinsatser för att uppmärksamma användare på hot som finns

som kan orsaka incidenter. Incidenter är enligt intervjupersoner kostnadsdrivande och ineffektivt då IT behöver lägga resurser på att vidta åtgärder utifrån inträffade incidenter trots att dessa till stor del hade kunnat undvikas med en grundläggande kunskap i verksamheten.

3.4.5 Bedömning

Vår bedömning är att det pågår ett kontinuerligt arbete utifrån ansvar som regleras i reglemente för kommunstyrelsen och servicenämnden. Vi anser däremot att styrelse och nämnd bör vara mer aktiva och ta del av det arbete som pågår och efterfråga uppföljning för att ha en förståelse och insikt i de hot och risker som finns för kommunens information och IT.

Det saknas konkreta former avseende organisation och ansvar för att säkerställa ett strukturerat arbete med stadens IT-säkerhet. I nuläget finns inte en övergripande helhetsbild över säkerhetshot och behov av säkerhetslösningar för att avgöra vad som behöver prioriteras utifrån riskbedömning av eventuella sårbarheter. Detta medför en risk att inte tillräckliga åtgärder vidtagits för att skydda stadens IT-miljö mot obehörigt intrång. Detta kan försvåra förutsättningar för ett systematiskt arbete och en tillräcklig uppföljning av vidtagna säkerhetsåtgärder.

IT-enheten på stadskontoret och IT-service på serviceförvaltningen har i sitt uppdrag för kommungemensam IT investerat i nya tekniska lösningar och säkerhetsfunktioner i nätverk, datacenter, klienter och tjänster. Behov av utveckling samlas årligen i en tjänsteplan och en utvecklingsplan som resurssätts utifrån tilldelad budget. Det saknas dock en övergripande helhetsbild över behov av säkerhetslösningar för att avgöra vad som behöver prioriteras utifrån riskbedömning av eventuella sårbarheter. Detta riskerar i sin tur att inte tillräckliga åtgärder vidtagits för att skydda stadens IT-miljö mot obehörigt intrång.

IT-service inom serviceförvaltningen har inom driftsorganisationen vissa kontroller att system och programvaror som nyttjas fungerar i enlighet med förvaltningarnas behov, där kontroller utförs med huvudsakligt syfte att säkerställa funktionaliteten genom uppdateringar och löpande underhåll. Det saknas för närvarande tillräcklig övervakning av nätverk och system för att upptäcka och i tid förhindra att intrång sker. I övrigt har inte kommunstyrelsen eller servicenämnden säkerställt att det finns en tillförlitlig övervakning över aktivitet i nät och stadens IT-miljö för att i tid upptäcka och förhindra intrångsförsök och hot. Kommunstyrelsen har inte gett verksamheten i uppdrag att genomföra tester för att utvärdera de införda säkerhetslösningarna, exempelvis sårbarhetsscanning eller penetrationstester.

Vår bedömning är att det till viss del finns rutiner och processer för incidenthantering. I riktlinjer finns rutin beskriven för allvarliga incidenter. Det finns en dokumenterad incidentprocess på IT-service och i intervjuer beskrivs en hantering i verksamhetssystemet Agera. Det behöver dock säkerställas att rutiner är kända och tillämpas av alla verksamheter så att incidenter kan dokumenteras och kan följas upp samt att åtgärder vidtas för att hindra att de sker igen. Eskaleringsvägar är inte kända och efter att IT-service har registrerat incidenter och meddelat ansvarig chef inom den verksamhet där incidenten inträffat så sker ingen uppföljning över den fortsatta hanteringen. Ansvariga i form av IT-säkerhetsarkitekter eller centralt utsedda informationssäkerhetssamordnare tar inte del av rapporterade incidenter och det sker

ingen övergripande dokumentation över incidenter så att dessa kan analyseras och utgöra underlag i det systematiska förbättringsarbetet.

Det saknas i nuläget tillräckliga styrdokument inom drift och teknik. Då övriga verksamhetsområden är beroende av kommunens IT-verksamhet, bedömer vi bristen på styrdokumentation inom drift och teknik som en risk vad avser kontinuitets- och avbrottshantering. I samband med Corona-pandemin skulle IT-enheten på stadskontoret ta fram en prioriteringslista för verksamhetskritiska system men det gick inte att verkställa på grund av den bristfälliga systemdokumentationen i iFacts. Detta riskerar att få stora konsekvenser vid extraordinära händelser, denna gång i form av en pandemi men det kan även ske genom direkt attack på IT-miljön med stora konsekvenser för verksamheternas kontinuitet och säkerhet. För enskilda verksamheter finns kontinuitetsplaner framtagna som testats under 2020 där även avtal om jourverksamhet mm har gjorts för att det ska finnas en planering och hantering vid störningar och avbrott.

3.5 Förändrade arbetssätt och förutsättningar på grund av Corona-pandemin 2020

I Riktlinjer och anvisningar för informationssäkerhet finns i avsnitt 12.8 information om vad som gäller vid mobil datoranvändning och distansarbete. I inledningen av avsnittet framgår följande:

> ”Skyddet av information ska säkerställas vid användning av mobil utrustning och vid distansarbete. Med mobil utrustning menas avancerade s.k. smarta telefoner, bärbara datorer, handdatorer, pekplattor och liknande enheter som kan användas för informationsbehandling från annan plats än arbetsplatsen. Med distansarbete avses ”Av arbetsgivaren tillhandahållen arbetsplats i hemmet”.”

Några väsentliga delar i anvisningen är att endast utrustning som tillhandahålls av Malmö stad får nyttjas vid mobil användning och distansarbete. Tjänst som tillhandahålls för att ansluta till stadens IT-miljö, så kallad, remote access, ska nyttjas men får inte användas för att ansluta en mobil enhet (telefon/platta). Det framkommer vidare att lagring ska ske på plats som arbetsgivaren beslutat.

3.5.1 Sammanträden och distansarbete

Vid kommunfullmäktiges sammanträde 2020-03-19 beslutades att ledamöter i nämnder och utskott ska få delta vid respektive nämnds eller utskottssammanträden på distans.

Bakgrunden till beslutet var Corona-pandemin och att iaktta försiktighet för smittspridning och ändå genomföra möten med deltagande från valda ledamöter. Beslutet tidsbegränsades att gälla till och med den 31 augusti 2020. En förlängning av beslutet fattades av kommunstyrelsen 2020-08-14. Beslutet gäller så länge Folkhälsomyndigheten kvarstår med rekommendation att hålla digitala möten som en åtgärd för att undvika smittspridning av covid-19.

I beslutet i mars fick kommunstyrelsen i uppdrag att utforma tillämpningsanvisningar för sammanträden på distans. Kommunstyrelsen beslutade vid sammanträde 2020-04-15 om dessa tillämpningsanvisningar.

Det framgår av anvisningarna att ledamöter endast får använda utrustning som tillhandahålls av Malmö stad. Vidare att gällande integritetslagstiftning ska tillämpas vid all behandling av personuppgifter samt att ordförande ska erinra samtliga ledamöter om vikten av att inte nämna enskildas personuppgifter eller sekretessbelagda uppgifter under mötets gång.

Detta anses särskilt viktigt vid behandlingen av ärenden som omfattas av sekretess. Ordförande har i ansvar att avbryta och stoppa enskild ledamot som bryter mot detta för att upprätthålla informationssäkerheten.

För distansmöten så fanns redan en befintlig tjänst som kunde nyttjas då Teams ingår i Office365. Kommunikatörerna gjorde en stor insats för att informera om användning av tjänsterna så att detta skulle kunna komma igång. Bedömningen som gjordes av IT-enheten på stadskontoret avseende risker förknippade med användning av tjänsten var att de säkerhetslösningar som tillhandahålls via Microsoft håller en hög säkerhetsnivå och kan användas för distansmöten.

Som följd av Corona-pandemin och många medarbetare började arbeta på distans gick en allmän information ut via intranätet. Vad gäller informationssäkerhet så fokuserades informationen på hemarbete och att inte koppla upp sig via osäkra wifi-nätverk och vara försiktig med att arbeta med sekretessbelagd information i offentliga miljöer.

Det fanns också en instruktion om hur medarbetare skulle koppla upp sig mot IT-miljön. Förstahandsvalet skulle enligt informationen vara att använda arbetsgivarens utrustning, det vill säga telefonens uppkoppling och sin arbetsdator. Enligt uppgifter i intervjuer fanns dock möjlighet att koppla upp sig med privat utrustning. Denna registreras i sådana fall innan åtkomst kan ske. Enligt uppgift kan upp till fem enheter registreras per användare och ansluta till stadens IT-miljö.

Enligt intervjupersoner så upprättades inga riskanalyser för dessa nya arbetssätt och tjänster. Det uppges bero på att möjlighet att arbeta på distans har funnits under lång tid i Malmö stad och att det finns ett regelverk i riktlinjer för informationssäkerhet.

Däremot var det en enorm ökning av användandet. Det innebar även att fler system tillgängliggjordes för distansarbete. Förvaltningar uppmanades följa de processer som finns beskrivna med risk- och sårbarhetsanalyser för respektive system vilket gjordes i en anpassad utsträckning pga. tidspress.

Det genomfördes inte någon övergripande risk- och sårbarhetsanalys för informations- och IT-säkerhet i samband med Corona-pandemin. Krisledningsgruppen har efterfrågat information om hur många som anslutit sig via distans men inga frågeställningar kring hur detta går till eller vilka säkerhetsåtgärder som krävs för att upprätthålla informationssäkerheten.

De frågor som i övrigt har inkommit i samband med vårens distansarbete har främst gällt lagring i molnet, hur information kan krypteras och allmänt kring användande av tjänster, exempelvis Teams. För dessa frågor har inte funnits några beslut över hantering utan svar har varit upp till den som får frågan att besvara.

3.5.2 IT-säkerhetslösningar för distansarbete

IT-service upptäckte snabbt att befintlig brandvägg inte hade kapacitet för den ökade belastningen på nätet vilket påskyndande beslutet att avropa en ny brandvägg utifrån avtal. Aktivitet fanns dokumenterad i tjänsteplanen för 2020 men fick tidigareläggas.

På tre veckor löstes kapacitetsbristen genom en ny accesslösning in till stadens IT-miljö som låg utanför brandväggen, en hemarbetsplatsplattform, Citrix ADC. Via den kommer användarna till inloggningssidan till IT-miljön och kan utifrån åtkomsthanteringen få tillgång till verksamhetssystem och lokala lagringsytor.

Molntjänsterna är öppna vilket innebär att användare kan ladda ner dokument till en privat dator eller registrera en privat telefon och komma åt både privata dokument och dokument som tillhör Malmö stad. I riktlinjer för informationssäkerhet finns dock anvisningar över hur information ska hanteras.

Åtkomst till förvaltningarnas verksamhetssystem på distans är dels beroende på tilldelad AD-behörighet. Det är systemägaren för verksamhetssystemen som avgör om det ska finnas tillgång till dessa via distans eller inte. De behöver göra en egen bedömning över vad som kan öppnas upp mot andra klienter och vad medarbetare får komma åt utanför brandväggen.

Ett fåtal verksamheter valde att gå ifrån att ha spärrar för distansuppkoppling mot verksamhetssystemen. Vid de tillfällena krävdes en beställning av ”change” för att genomföra denna ändring. När verksamheter rådfrågar IT om vad som är lämpligt att ha åtkomst till via distans så ska det bygga på den klassificering som har gjorts för informationen. Så det är avgörande att denna är gjord med rätt riskbedömning för att hanteringen sedan ska bli korrekt. Det är inte tillåtet att ta del av journalsystem via distanslösningen.

3.5.3 Penetrationstest av system för åtkomst på distans

I granskningen har penetrationstest genomförts för att identifiera eventuella sårbarheter i stadens system för fjärråtkomst där inloggning sker mot Malmö stads IT-miljö. Exempelvis vid hemarbete eller sammanträden på distans. Avgränsningen har varit att identifiera risker för intrång via de system som staden använder för fjärranslutning. Testet har inte omfattat vidare åtkomst till förvaltningarnas verksamhetssystem efter att åtkomst till IT-miljön har skett.

Ett penetrationstest är en metod för att utvärdera säkerheten i en applikation eller ett system genom att simulera ett angrepp från en motståndare. Syftet med detta är att beskriva de sårbarheter som har påträffats, bedöma risken för dessa och ge rekommendation om åtgärder för att öka säkerheten. Penetrationstestet har genomförts genom s.k. grey-box metodik i enlighet med OWASP Testing Guide v.4.0 och har inkluderat testfall för alla kända sårbarheter som drabbar webapplikationer och system för fjärråtkomst.

En sårbarhet är en defekt eller en svaghet i ett systems design, implementation eller funktion och användning som kan exploateras för att kringgå systemets säkerhetspolicy. KPMG tillämpar en förenklad klassificeringsmetod baserad på CVSS (Common Vulnerability Scoring System) för att bedöma sårbarheter. Syftet med klassificeringen är att påvisa hur allvarlig en påträffad sårbarhet är så att prioritering kan göras.

Sårbarheterna klassificeras i fyra nivåer där KPMG rekommenderar att sårbarheter i nivåerna medel och hög bör åtgärdas.

Sårbarhetsklassificering	Beskrivning
Hög	En framgångsrik exploatering av en sårbarhet i denna nivå kan resultera i avsevärd skada för systemet. Sårbarheten är vanligtvis enkel att exploatera, är fjärråtkomlig och kan användas för att kompromettera hela systemet.
Medel	En framgångsrik exploatering av en sårbarhet i denna nivå kan resultera i måttlig skada för systemet. Sårbarheten är vanligtvis enkel att exploatera, medger åtkomst till känslig information om systemet och kan användas för att vidare exploatera systemet.
Låg	En angripare kan insamla information om systemet som kan användas för att exploatera kända sårbarheter(portar, tjänster och versioner för installerad mjukvara).
Ingen	Det föreligger liten eller ingen risk mot systemet.

Sårbarheter har genom penetrationstestet identifierats inom klassificeringarna medel och låg. Granskningsresultatet redovisas inte vidare i denna rapport utan i en enskild bilaga som delges utsedda personer inom staden då informationen är säkerhetsklassad och måste hanteras enligt gällande rutiner för detta.

3.5.4 Bedömning

Det finns inte någon dokumenterad risk- och sårbarhetsanalys där risker i samband med förändrade arbetssätt och nyttjande av nya tekniska lösningar för distansuppkoppling genomförts.

För nämndssammanträden på distans via Teams gjordes en bedömning att tjänsten hade tillräcklig IT-säkerhet. Därtill beslutade kommunstyrelsen om tillämpningsanvisningar för att säkerställa informationssäkerheten, främst gällande sekretessbelagd information och hantering av personuppgifter.

I samband med förändringar som behövde ske skyndsamt så kan vi ha en förståelse för att det inte fanns tid att genomföra omfattande risk- och sårbarhetsanalyser. Men vi anser att det borde ha skett en dialog där juridiska och säkerhetsmässiga bedömningar gjorts och skriftligt dokumenterats i beslut som fattats kring användning, inloggning, och hantering av information i de tjänster och system som nyttjas via distans. Det borde därtill ha tagits fram anvisningar på samma sätt som kommunstyrelsen gjorde för nämndssammanträden på distans som hade kommunicerats till stadens medarbetare för att säkerställa informationssäkerheten.

Med den låga medvetenhet som påvisats i granskningen tillsammans med ökning av identitetsstölder finns goda underlag för att ansvariga för säkerheten borde iakttagit en större försiktighet i implementeringen av nya lösningar samt varit extra tydliga med var och ens ansvar i samband med distansarbete och möten på distans.

Utifrån genomfört penetrationstest är vår bedömning att den tekniska säkerhetsrisken i form av hot mot stadens IT-miljö vid distansarbete via de system som finns för fjärranslutning är låg.

Det saknas kontinuitetsplan för den övergripande IT-driften och nätverk vilken skulle påverka funktionaliteten av distanslösningar vid avbrott eller störning.

3.6 Uppföljning och rapportering

Enligt MSB:s metodstöd för ett systematiskt informationssäkerhetsarbete som vi beskrivit inledningsvis i rapporten så är ledningens förståelse för och engagemang i informationssäkerhet 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.

I ett ledningssystem för informationssäkerhet är en årlig rapportering till ledningen en avgörande punkt för att följa upp det arbete som skett inom informationssäkerhet samt få beslut om prioriteringar och åtgärder för att förbättra arbetet under kommande år.

I rapporten för nulägesanalys för informationssäkerhet från 2019 finns följande beskrivning av uppföljning och rapportering. ”I tidigare granskningar från år 2015 och 2017 samt stadsrevisionens granskning från 2018 framgår att det inte genomförs någon heltäckande dokumenterad uppföljning av Malmö stads informationssäkerhet och att rapportering och uppföljning av området saknas helt hos samtliga nämnder.” Resultatet i nulägesanalysen 2019 visar ingen förändring av detta.

De centrala informationssäkerhetssamordnarna har efter genomförd nulägesanalys presenterat resultatet för stadskontorets ledningsgrupp. Ledningsgruppen ansåg att analysen borde redovisas till alla förvaltningar tillsammans med respektive informationssäkerhetssamordnare. Sedan dess har fyra möten skett med förvaltningar under 2020 där samordnare, samordnarens chef och någon mer representant från förvaltningen deltagit. Presentation har inte getts till ledningsgrupp eller ansvarig nämnd för förvaltningen.

Enligt riktlinje för informationssäkerhet ska de utsedda informationssäkerhetssamordnarna rapportera om arbetet till förvaltningschef.

Intervjupersoner beskriver att rapportering, om den görs, sker till närmaste chef. Det är dock oklart vad eller om det sker något med den informationen i en fortsatt rapportering till ledningsgrupp eller till politiken. Ingen av intervjupersonerna har haft någon rapportering till dessa forum och det sker ingen uppföljning till styrelse eller nämnder specifikt för deras ansvarsområden eller generellt för IT-säkerheten. Då det upplevs finnas en avsaknad av etablerade rapporteringsvägar för informationssäkerhet och IT-säkerhet anses området bli eftersatt då inget forum finns att lyfta behov i.

3.6.1 Intern kontroll

För intern kontroll finns tydliggjord rapportering vilket framgår i handbok framtagen som stöd i stadens arbete med intern kontroll. För de kontrollmål som beslutas i internkontrollplanen för 2020 har beslut om internkontrollplan fattats samt

återrapportering av granskningar skett till både kommunstyrelsen och servicenämnden.

Kommunstyrelsens internkontroll 2020

Röjande av sekretess ingår i kommunstyrelsens internkontrollplan för 2020 och är ett stadsövergripande kontrollmål vilket innebär att även servicenämnden omfattas.

Risk beskrivs gälla att handlingar som innehåller typiskt sett sekretessbelagd information kommer obehörig till del på grund av bristande kunskap i hur den här typen av information ska hanteras, oavsett digitalt format eller pappersform, vilket kan leda till allvarliga konsekvenser för Malmö stad som organisation, andra organisationer eller den enskilde.

I uppföljning av kommunstyrelsens interna kontroll för tertial 2, 2020 anges att kontrollmålet har granskats genom en enkät till 400 chefer. Resultatet av enkäten visar att det råder en viss osäkerhet kring hur sekretessbelagda uppgifter ska hanteras. Utifrån enkäten har djupintervjuer med nyckelpersoner genomförts vilket visar att dessa ibland är osäkra, men att de upplever att det finns ett gott stöd att hämta i den juridiska kompetens som finns på stadskontoret. Rekommenderad åtgärd utifrån granskningen är att genomföra en informationsinsats till stadskontorets chefer och medarbetare och att informationssäkerhet bör ingå som ett obligatoriskt introduktionsblock för stadskontorets nya medarbetare.

Servicenämndens internkontroll 2020

I servicenämndens internkontrollplan för 2020 finns förutom kontrollmålet för sekretess även mål för Informationssäkerhet där risken är att beslutade riktlinjer och anvisningar för informationssäkerhet inte efterlevs.

I uppföljning av servicenämndens interna kontroll för tertial 2, 2020, framkommer flera punkter och åtgärder kopplat till kontrollmålet om sekretess som rör informationssäkerhet. Dels att det pågår ett arbete med att revidera styrdokument för informationssäkerhet dels att det bör ske en inventering av vilka uppgifter som berör förvaltningen och sedan klassificera den enligt klassificeringsmodell för bedömning av skydds- och kravnivå som finns i riktlinje för informationssäkerhet.

Det framgår även av uppföljningen att granskningen visar att cheferna har behov av utbildning. Både utbildning i vad som förväntas av dem som chefer i förhållande till sekretess och informationshantering. Ett förbättringsförslag är att chefer genomför DISA-utbildningen (datorstödd informationssäkerhetsutbildning för användare) som erbjuds via Myndigheten för samhällsskydd och beredskap.

Genom proaktiva, löpande möten med avdelningarna ska man säkerställa att riktlinjerna och anvisningarna blir tydliga för avdelningarna och att de därmed efterlevs i högre grad.

3.6.2 Bedömning

Vår bedömning är att kommunstyrelsen och servicenämnden inte har säkerställt en tillräcklig rapportering av stadens informations- och IT-säkerhetsarbete. Det finns inga återkommande eller planerade rapporteringstillfällen där dessa frågor finns på kommunstyrelsens eller servicenämndens agenda. De centralt utsedda

informationssäkerhetssamordnarna inom stadskontoret har i uppdrag att samordna hela stadens arbete men den uppföljning som har gjorts i form av genomförda nulägesanalyser har endast återrapporterats inom tjänstepersonsorganisationen. Detsamma gäller inom servicenämndens ansvarsområde där rapportering sker till ansvarig chef men det är inte tydligt hur denna rapportering tas vidare till ansvariga för information och informationssystem. Kommunstyrelsen och övriga nämnder är ytterst ansvariga som informationsägare och bör därför säkerställa att de har tillräcklig kännedom om hot och risker för dessa för att bedöma behov av åtgärder och resurser.

De kontrollmål som finns internkontrollplan för 2020 har följts upp och rapporterats av både kommunstyrelsen och servicenämnden för tertial 2, 2020. Dessa kontrollmål är dock inte tillräckliga för att följa upp vare sig stadens informationssäkerhetsarbete eller upprättad IT-säkerhet. Vår bedömning är därför att ytterligare uppföljning behöver ske för arbetet och att den interna kontrollen kommande år bör kompletteras med ytterligare kontrollmål utifrån de brister som påvisats i nulägesanalys för informationssäkerhet men även i denna granskning. Bland annat bör det genomföras en kontroll av åtkomst- och behörighetshantering i förvaltningarna för att säkerställa att rutiner finns som följs och att hanteringen fungerar vid förändringar av roller/ansvar samt vid avslut av anställningar.

4 Slutsats och rekommendationer

4.1 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och servicenämnden endast till viss del säkerställer en tillräcklig IT-säkerhet. Ett antal viktiga förbättringsområden har identifierats.

Det saknas konkreta former avseende organisation och ansvar för att säkerställa ett strukturerat arbete med stadens IT-säkerhet. I nuläget finns inte en övergripande helhetsbild över säkerhetshot och behov av säkerhetslösningar för att avgöra vad som behöver prioriteras utifrån riskbedömning av eventuella sårbarheter. Detta medför en risk att inte tillräckliga åtgärder vidtagits för att skydda stadens IT-miljö mot obehörigt intrång. Detta kan försvåra förutsättningar för ett systematiskt arbete och en tillräcklig uppföljning av vidtagna säkerhetsåtgärder.

Kommunstyrelsen ska enligt reglementet ansvara för att leda, strategiskt utveckla och samordna stadens gemensamma digitaliserings- och IT-frågor, informationssystem, digital infrastruktur och telekom. Vår bedömning är att kommunstyrelsen utifrån sitt ansvar endast till viss del har säkerställt att arbetet med IT-säkerhet är tillräcklig. Vi baserar bland annat vår bedömning på följande iakttagelser:

- Det finns inte en ändamålsenlig organisation med tydlig ansvarsfördelning för att styra IT-säkerhetsarbetet. Det sker i nuläget inte ett sammanhållet och strukturerat arbete med frågorna där helheten för stadens IT-miljö och IT-komponenter ingår. Det saknas dokumenterade uppdragsbeskrivningar för var och ens ansvar och mandatet är otydligt mellan stadskontoret och förvaltningarna.
- Det finns endast till viss del styrdokument som styr arbetet. Dessa finns i form av Riktlinjer och anvisningar för informationssäkerhet. Det saknas policys som anger den politiska viljeriktningen och mål med arbetet där ansvaret är tydliggjort. Därtill saknas styrande dokument för IT-säkerhet. Efterlevnaden av beslutade styrdokument beskrivs som bristfällig och ett flertal exempel har framkommit där riktlinjen inte följs.
- Det yttersta ansvaret för informationssäkerheten finns hos respektive nämnd. Detta innebär att kommunstyrelsen genom sin uppsiktsplikt behöver säkerställa att nämndernas arbete sker i enlighet med gällande lagar och beslutade riktlinjer. Vår bedömning är att nuvarande kontrollmål för intern kontroll inte är tillräckligt för att följa upp nämndernas arbete med informationssäkerhet och att detta sker i enlighet med beslutade riktlinjer.
- Vår bedömning är att den otydliga organiseringen och att inte det finns ett sammanhållet arbete för IT-säkerhet kan utgöra en risk för åtgärder inte vidtas för sårbarheter med högst säkerhetsrisk då det inte finns någon övergripande bild av sårbarheter eller en tydliggjord prioritering.

- IT-enheten på stadskontoret har i sitt uppdrag för kommungemensam IT investerat i nya tekniska lösningar och säkerhetsfunktioner i nätverk, datacenter, klienter och tjänster.
- Utifrån genomfört penetrationstest är vår bedömning att den tekniska säkerhetsrisken i form av hot mot stadens IT-miljö vid distansarbete via de system som finns för fjärranslutning är låg. Det saknas en dokumenterad riskanalys inför implementering av system och tjänster samt förändrade arbetssätt. En riskbedömning gjordes för nämndsammanträden på distans och beslut fattades om åtgärder och hantering för att upprätthålla informationssäkerheten.
- Säkerheten överlag är beroende på hur användarna säkerställer sitt ansvar i informationshanteringen. Medvetenheten bedöms som låg i stadens verksamheter med risk för att incidenter sker som inte upptäcks och kan skada stadens informationstillgångar och förtroende från medborgarna.
- Det saknas till stor del dokumenterade kontinuitetsplaner för verksamhetskritiska system.
- Det finns till viss del rutiner för incidenthantering genom beskrivning i riktlinjer för informationssäkerhet och dokumenterad rutin inom IT-service. Det behöver dock säkerställas att dessa är kända och följs av samtliga verksamheter. Det sker i nuläget ingen övergripande dokumentation av inträffade incidenter. Centrala funktioner som informationssäkerhetssamordnare och IT-säkerhetsarkitekter tar inte del av inträffade incidenter i nuvarande hantering för att kunna vara delaktiga för att åtgärder vidtas för att dessa inte ska inträffa igen.
- Det sker inte en tillräcklig rapportering av stadens informations- och IT-säkerhetsarbete till kommunstyrelsen. Det finns inga återkommande eller planerade rapporteringstillfällen där dessa frågor finns på kommunstyrelsens agenda. Ansvariga i arbetet rapporterar till närmaste chef men upplever det otydligt hur informationen hanteras vidare.

Enligt servicenämndens reglemente ansvarar nämnden för förvaltning och support för Malmö stads IT-miljö och IT-infrastruktur. Vår bedömning är att servicenämnden endast till viss del har säkerställt att IT-säkerheten är tillräcklig utifrån följande iakttagelser:

- Det finns inte tilldelade resurser inom nämndens ansvar så att IT-service kan vidta nödvändiga åtgärder för att upprätthålla säkerhet för nätverk och drift. I nuläget tas beslut om resurser och genomförande av stadskontorets ledningsgrupp för IT.
- IT-service på serviceförvaltningen har i sitt uppdrag för kommungemensam IT investerat i nya tekniska lösningar och säkerhetsfunktioner i nätverk och datacenter, klienter och tjänster.
- Det genomförs inte tillräckliga risk- och sårbarhetsanalyser för nätverk och drift. Då förvaltningarna är beroende av kommunens IT-verksamhet, bedömer vi

bristen på styrdokumentation inom drift och teknik som en risk vad avser kontinuitets- och avbrottshantering.

- Det saknas tillräckliga funktioner för övervakning av aktivitet i nätverk och system för att upptäcka intrångsförsök och i tid stoppa dessa.
- Det sker inte en tillräcklig rapportering av förvaltningens IT-säkerhetsarbete till servicenämnden. Det finns inga återkommande eller planerade rapporteringstillfällen där ansvariga i arbetet bjuds in. Rapportering sker från ansvariga funktioner inom IT-service till närmaste chef men det finns en upplevelse att det är otydligt hur informationen hanteras vidare.

4.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Etablera en organisation med tydligt ansvar och mandat för stadens informations- och IT-säkerhetsarbete
- Ta fram policy för informationssäkerhet eller revidera befintlig Trygg- och säkerhetspolicy så att informationssäkerhet är inkluderat. Samt komplettera denna med de riktlinjer och anvisningar som behövs för att styra arbetet
- Ge nämnder och förvaltningar i uppdrag att kartlägga samtliga informationssystem och tjänster och dokumentera dessa i förteckning för att säkerställa att det finns en komplett förteckning som är uppdaterad och kan fungera som informationskälla i hanteringen av IT-säkerhetsåtgärder
- Säkerställa att det genomförs risk- och konsekvensanalyser för verksamhetskritiska informationssystem och att det finns tillhörande kontinuitetsplaner för dessa
- Säkerställa att metod för klassning finns som är tillämpbar för dagens informationssystem och tjänstehantering och att klassning genomförs både på system och information som hanteras i förvaltningarna
- Säkerställa att nyanställda samt befintliga medarbetare får information och utbildning i ansvaret för informationssäkerhet och IT-användning
- Besluta om stadsövergripande rutin för incidenthantering och rapportering där ansvar och eskaleringsvägar finns tydliggjorda samt kommunicera denna till verksamheterna. Det behöver även säkerställas att en uppföljning sker av inträffade incidenter så att detta kan beaktas i förbättringsarbetet
- Säkerställa genom intern kontroll att det sker ett tillräckligt arbete med informationssäkerhet i förvaltningarna där efterlevnad av beslutad riktlinje och anvisningar för informationssäkerhet finns
- Skapa struktur för enhetlig uppföljning av informationssäkerhet inklusive IT-säkerhet och etablera rapporteringsvägar till ledning och styrelse

Utifrån vår bedömning och slutsats rekommenderar vi servicenämnden att:

- Utifrån ansvar i reglementet säkerställa att det finns en tilldelad budget för förvaltning av IT-miljö och IT-infrastruktur så att IT-säkerhetsåtgärder vid behov kan vidtas för systemdrift och nätverk
- Upprätta risk- och sårbarhetsanalyser för nätverk och drift med tillhörande handlingsplaner för åtgärder för att nå önskad nivå av IT-säkerhet
- Upprätta styrdokument avseende drift och teknik med tillhörande kontinuitetsplaner för att det ska finnas reserv- återgång- och återställningsrutiner i händelse av störning eller avbrott och en prioritering av verksamhetskritiska system kan göras
- Säkerställa att förvaltningsspecifik rutin för incidenthantering inkluderar information till berörda funktioner med ansvar för informationssäkerhet, IT-säkerhet och ansvar för driftsäkerhet

2020-11-18

KPMG AB

Jenny Thörn

Kommunal revisor

Sara Linge

Granskningsledare och certifierad kommunal revisor

Bilaga 1 Intervjupersoner

- IT-chef
- Informationssäkerhetssamordnare centralt utsedda, placerade på stadskontoret
- IT-säkerhetsarkitekter
- Infrastrukturarkitekt
- Tjänsteägare stadskontoret
- Chef nätdrift IT-service
- Tekniskt ansvarig operativ drift nätverk IT-service
- Utvecklingsansvarig IT-service
- Incident manager IT-service
- IT-samordnare/Informationssäkerhetssamordnare serviceförvaltningen
- IT-samordnare serviceförvaltningen
- IT-sekreterare serviceförvaltningen
- IT- handläggare serviceförvaltningen
- Systemförvaltare serviceförvaltningen

Bilaga 2 Dokumentgranskning

Titel	Fastställd	Ansvarig
Trygghet- och säkerhetspolicy	2017	Stadskontoret
IT-strategi	2007	Kommunfullmäktige
Riktlinjer och anvisningar för informationssäkerhet	2019	Kommunstyrelsen
Reglemente kommunstyrelsen	2019	Kommunfullmäktige
Reglemente servicenämnden	2018	Kommunfullmäktige
Reglemente för intern kontroll	2016	Kommunfullmäktige
Internkontrollplan samt uppföljning av intern kontroll kommunstyrelsen	2020	Kommunstyrelsen
Internkontrollplan samt uppföljning av intern kontroll servicenämnden	2020	Servicenämnden/ Kommunstyrelsen
Nulägesanalys informationssäkerhet	2019	Stadskontoret
Rutiner och blankett för informationsklassning	2019	Stadskontoret
Tjänsteplan	2019	Stadskontoret IT-enheten
Tjänsteplan	2020	Stadskontoret IT-enheten
Utvecklingsplan	2020	Stadskontoret IT-enheten
Projektbeskrivningar	2017–2020	Stadskontoret IT-enheten
Riskanalyser implementering Office 365 och tillhörande tjänster	2017	Stadskontoret IT-styrning