# Granskning av IT-säkerhet

Rapport

Malmö stad

KPMG AB

2025-01-17

Antal sidor 26

**Malmö stad**
Granskning av IT-säkerhet
2025-01-17

# Innehållsförteckning

# 1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Malmö stad fått i uppdrag att granska stadens IT-säkerhet. Syftet med granskningen har varit att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad.

**Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen delvis har säkerställt en tillräcklig IT-säkerhet för Malmö stad.**

Vi baserar vår bedömning på att kommunstyrelsen genom styrande dokument har etablerat en styrning av IT-säkerhetsarbetet. Vi bedömer däremot att de inte säkerställt en tillräcklig uppföljning och kontroll av arbetet i enlighet med beslutade Riktlinjer för informationssäkerhet. Utbildningsinsatser har genomförts för användare i staden men vi bedömer att dessa inte varit tillräckliga för att etablera kunskap och medvetenhet om de IT-säkerhetshot som riktas mot användare. I granskningen har ett test genomförts och utifrån resultatet i testet bedömer vi att personalsäkerheten är bristfällig och konstaterar att medarbetarnas användning av IT-system är förenat med risker.

**Vår samlade bedömning utifrån granskningens syfte är att servicenämnden delvis har säkerställt en tillräcklig IT-säkerhet för Malmö stad.**

Vi baserar vår bedömning på att det finns beslutade säkerhetsnivåer avseende IT-säkerhetsåtgärder och att arbetet i hög grad genomförts enligt fastställda nivåer. Incidenter förekommer och tekniska skyddsåtgärder har etablerats så att hot som riktas till användare ska identifieras samt stoppas. Vi bedömer att incidenter som sker hanteras enligt dokumenterade rutiner med en tydlig ansvarsfördelning. Vi ser dock behov av att nuvarande kommunikationsplan vid kritiska incidenter utvecklas med tydliggörande av eskaleringsvägar till representanter i övriga förvaltningar för att säkerställa att kommunikationsvägar möjliggör en effektiv hantering av incidenter. Vi bedömer att nämnden inte har säkerställt en tillräcklig uppföljning och kontroll av arbetet i enlighet med beslutade Riktlinjer för informationssäkerhet.

På nästa sida presenteras våra bedömningar av respektive revisionsfråga.

| Revisionsfråga: | Finns styrdokument för arbetet med IT-säkerhet och säkerställs att dessa efterlevs? |
|---|---|
| Kommunstyrelsen | **Delvis**<br>Kommunstyrelsen har i enlighet med beslutat reglemente fastställt *Riktlinjer för informationssäkerhet*. Vi ser dock behov av att styrdokument på policynivå anpassas för att följa ISO27000-serien då nuvarande Trygghet- och säkerhetspolicy saknar väsentliga delar.<br><br>*Riktlinjer för informationssäkerhet* ställer krav på årlig kontroll och rapportering av efterlevnaden av riktlinjerna. Detta har inte genomförts i enlighet med regleringen vilket vi bedömer som en brist. |
| Servicenämnden | **Delvis**<br>Servicenämnden har enligt reglementet inte ansvar för att besluta om styrdokument inom IT-säkerhet. Vi kan konstatera att *Anvisningar för IT-säkerhet* har beslutats inom förvaltningen i enlighet med reglering i *Riktlinjer för informationssäkerhet*.<br><br>*Riktlinjer för informationssäkerhet* ställer krav på årlig kontroll och rapportering av efterlevnaden av riktlinjerna. Detta har inte genomförts i enlighet med regleringen vilket vi bedömer som en brist. |

| Revisionsfråga: | Förekommer och hanteras IT-säkerhetsincidenter kopplade till medarbetares användning av IT-system? |
|---|---|
| Kommunstyrelsen | **Delvis**<br>Kommunstyrelsen har genom *Riktlinjer för informationssäkerhet* beslutat om krav på utbildning inom informationssäkerhet. Utbildnings- och informationsinsatser har genomförts som riktats till samtliga stadens medarbetare men vi bedömer att dessa inte varit tillräckliga. En del i granskningen har varit ett test avseende användarnas medvetenhet om hot och risker inom IT-säkerhet. Vi bedömer utifrån resultatet att personalsäkerheten är bristfällig och konstaterar att medarbetarnas användning av IT-system är förenat med risker. Kompletterande utbildningsinsatser behöver riktas på övergripande nivå till användare av stadens IT-system då brister identifierades i samtliga verksamheter. |
| Servicenämnden | **I allt väsentligt**<br>Incidenter förekommer och hanteras i allt väsentligt i ett tekniskt perspektiv. Vi bedömer att relevanta skyddsåtgärder etablerats kopplat till medarbetare användning av IT-system. |

| Revisionsfråga: | Finns ett arbetssätt för att upptäcka och hantera IT-säkerhetsincidenter? |
|---|---|
| Servicenämnden | **I allt väsentligt**<br>Vi bedömer att det finns både etablerade arbetssätt och tekniska verktyg för att förebygga, förhindra, upptäcka och hantera IT-säkerhetsincidenter. |

| Revisionsfråga: | Är roller och ansvarsfördelning tydlig inom IT-organisationen vid IT-säkerhetsincidenter? |
|---|---|
| Servicenämnden | **Ja**<br>Det finns tydligt dokumenterad ansvarsfördelning och upprättade rutiner och processer för hur incidenter ska hanteras. Vi bedömer därtill att arbetet genomförs i enlighet med dessa.<br><br>Vi bedömer att nuvarande kommunikationsplan vid kritiska incidenter kan utvecklas med tydliggörande av eskaleringsvägar till representanter i övriga förvaltningar för att säkerställa att kommunikationsvägar möjliggör en effektiv hantering av incidenter. |

| Revisionsfråga: | Genomförs en systematisk uppföljning och rapportering av arbetet med IT-säkerhet? |
|---|---|
| Kommunstyrelsen | **Delvis**<br>Stadskontoret har enligt *Riktlinjer för informationssäkerhet* i ansvar att följa upp stadens arbete med informationssäkerhet och rapportera om resultatet till stadens ledningsgrupp och kommunstyrelsen. *Anvisning för informationshantering och säkerhetsprocesser* reglerar att årlig uppföljning och rapportering ska göras enligt beslutad rutin. Rutinen saknas och det saknas därigenom tydliggörande av hur denna rapportering ska genomföras.<br><br>Viss rapportering av uppföljning har gjorts till stadens ledningsgrupp men det saknas samlad årlig uppföljning och rapportering till kommunstyrelsen i enlighet med kraven vilket vi ser som en brist. |
| Servicenämnden | **Delvis**<br>Det saknas samlad årlig uppföljning och rapportering till servicenämnden i enlighet beskrivning i *Riktlinjer för informationssäkerhet* och *Anvisning för informationshantering och säkerhetsprocesser*. Samtidigt konstaterar vi att det saknas tydlighet från kommunstyrelsen och stadskontoret avseende hur denna uppföljning och rapportering förväntas genomföras.<br><br>Vi konstaterar att säkerhetsuppföljning i hög grad har genomförts i enlighet med kravställning i *Anvisning för informationshantering och säkerhetsprocesser* samt att resultatet i vissa delar har rapporterats internt inom förvaltningen.<br><br>Vi konstaterar att nuvarande utvärdering och uppföljning ger goda förutsättningar för att löpande anpassa IT-säkerhetsnivåer utifrån de hot, risker och sårbarheter som identifieras. Det behöver dock säkerställas att servicenämnden informeras om väsentliga delar så att tillräckliga förutsättningar finns för nämnden att upprätthålla sitt ansvar i enlighet med reglementet. Det bör även beaktas att kommunstyrelsen behöver hållas informerad om väsentliga delar av IT-säkerheten. |

*För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.*

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Bereda förslag till en informationssäkerhetspolicy eller motsvarande vars innehåll motsvarar de krav som ställs enligt ISO 27000-serien.
- Tillse att uppföljning och rapportering av informationssäkerhetsarbetet sker i enlighet med beslut i *Riktlinjer för informationssäkerhet* samt att kontroll av efterlevnad av riktlinjerna etableras.
- Tillse att rutin för uppföljning av det stadsövergripande informationssäkerhetsarbetet upprättas och etableras i enlighet med *Anvisning för informationshantering och säkerhetsprocesser*.
- Tillse att utbildning och information om IT-säkerhetshot och risker genomförs i hela organisationen för att stärka kunskap och medvetenhet hos användare. Därtill behöver genomförandegraden följas upp och åtgärder vidtas vid bristande genomförande.

Utifrån resultatet av vår granskning rekommenderar vi servicenämnden att:

- Tillse att uppföljning och rapportering sker i enlighet med beslut i *Riktlinjer för informationssäkerhet* samt att kontroll av efterlevnad av riktlinjer etableras. Uppföljning och rapportering behöver genomföras dels utifrån nämndens ansvar för egen informationssäkerhet, dels specifikt i relation till nämndens ansvar för kommungemensam IT och tillhörande IT-säkerhet.
- Tillse att rutinerna för incidenthantering kompletteras med datering, beslutsinstans samt ansvarig för revidering för att säkerställa dess aktualitet och förankring.
- Komplettera kommunikationsplan vid kritiska incidenter med tydliggjorda eskaleringsvägar och mottagare av information hos samtliga förvaltningar/verksamheter.

# 2 Bakgrund

Stadsrevisionen bedömde 2020 utifrån genomförd fördjupad granskning av kommunens IT-säkerhet att kommunstyrelsen och servicenämnden endast delvis säkerställde en tillräcklig IT-säkerhet.

Kommunstyrelsen och servicenämnden har efter genomförd granskning vidtagit ett antal åtgärder utifrån revisionens slutsatser.

Serviceförvaltningen genomförde en egen granskning av stadens IT-säkerhet under 2021. Även denna granskning påvisade att staden fortsatt hade ett stort antal brister IT-miljön. Under 2021 genomfördes även en omorganisation av stadens IT-organisation. Här fick servicenämnden överta ett antal verksamheter och servicenämnden fick även ansvar över kommungemensam IT. Inom ramen för ansvaret får nämnden leda, utveckla och samordna stadsgemensamma frågor avseende exempelvis IT, digitalisering och digital infrastruktur. Kommunstyrelsen ansvarar övergripande för styrdokument inom IT.

Stadsrevisionen önskar mot ovan bakgrund att granska stadens IT-säkerhet. Detta då revisionen uppfattar att det finns en fortsatt risk för brister inom IT-säkerheten.

## 2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad.

Granskningen har omfattat följande revisionsfrågor:

- Finns styrdokument för arbetet med IT-säkerhet och säkerställs att dessa efterlevs?
- Finns ett arbetssätt för att upptäcka och hantera IT-säkerhetsincidenter?
- Är roller och ansvarsfördelning tydlig inom IT-organisationen vid it-säkerhetsincidenter?
- Förekommer och hanteras IT-säkerhetsincidenter kopplade till medarbetares användning av IT-system?
- Genomförs en systematisk uppföljning och rapportering av arbetet med IT-säkerhet?

Granskningen avser kommunstyrelsen och servicenämnden och berör arbetet med stadens IT-säkerhet under 2024.

Med tillräcklig IT-säkerhet avses i denna granskning att den bedrivs i enlighet med lagstiftning, föreskrifter och kommunfullmäktiges beslut.

## 2.2 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- 6 kap. 6 § kommunallagen (2017:725)
- Reglemente för kommunstyrelsen och servicenämnden
- Reglemente för intern kontroll
- Trygghets- och säkerhetspolicy för Malmö stad
- Malmö stads riktlinjer för informationssäkerhet och underliggande styrdokument
- Riktlinjer för IT- och Digitalisering
- Utvecklingsplan för IT och digitalisering 2024
- ISO 27001 och 27002. Detta med hänvisning till att fastställda interna styrdokument ställer krav på att arbetet bedrivs i enlighet med denna standard för informationssäkerhet.

## 2.3 Metod

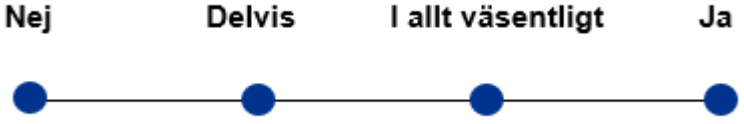
Granskningen har genomförts genom dokumentstudier, intervjuer och ett test av användarnas säkerhetsmedvetenhet.

Dokumentstudier har inkluderat styrande dokument inom informationssäkerhet som ingår i stadens ledningssystem för informationssäkerhet. Vi har även granskat specifika anvisningar inom IT-säkerhet och incidenthanteringsrutiner. Utöver dessa har vi även fått underlag för uppföljning i form av mätningar och kontrollmoment samt exempel på incidentrapporter.

Intervjuer har genomförts med två informationssäkerhetssamordnare med övergripande samordningsansvar för stadens informationssäkerhetsarbete, enhetschef infrastruktur, processledare infrastruktur, tjänsteägare datacenter och Incident Manager.

I samband med testet har systemförvaltare för systemet Platina samt utvalda funktioner inom IT-och digitalisering varit involverade.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.




Rapporten är faktakontrollerad av intervjupersoner som deltagit granskningen.

# 3 Inledning

## 3.1 Begreppsdefinition

I ett systematiskt informationssäkerhetsarbete ingår fyra områden av säkerhetsåtgärder. Dessa är:

1. Organisatorisk säkerhet (ibland benämnd administrativ säkerhet)
2. Teknisk säkerhet (it-säkerhet och cybersäkerhet)
3. Personalrelaterad säkerhet
4. Fysisk säkerhet

Då IT-säkerheten är en del i det övergripande informationssäkerhetsarbetet och har ett beroende till övriga områden så används både informationssäkerhet och IT-säkerhet som begrepp i rapporten. Detta för att kunna återge en helhetsbild av arbetet i Malmö stad. Granskningen har dock ett fokus på arbetet avseende IT-säkerhet och incidenthantering avseende IT-säkerhetshändelser.

# 4 Resultat av granskningen

## 4.1 Ansvarsfördelning

Av Kommunfullmäktiges *Reglemente för styrelsen och övriga nämnder* (beslutat 2024-08-29, gällande från 2024-10-01) framgår att kommunstyrelsen har ansvaret för beslut om riktlinjer för kommunens gemensamma IT. Följande uppgifter undantas enligt reglementet från kommunstyrelsen, vilka i stället ankommer på servicenämnden; leda, utveckla och samordna kommunens gemensamma IT- och digitaliseringsfrågor, informationssystem och digitala infrastruktur.

## 4.2 Styrdokument IT-säkerhet

Ett av kraven i ISO 27000-standarden är att högsta ledningen tydligt ska visa ledarskap och åtagande i fråga om ledningssystemet för informationssäkerhet. Detta ska göras genom att säkerställa att informationssäkerhetspolicy och informationssäkerhetsmål är upprättade och förenliga med organisationens strategiska inriktning. Enligt standarden ska informationssäkerhetspolicyn finnas i dokumenterad form, vara anpassad till organisationens syfte och innefatta ett åtagande att uppfylla tillämpliga krav relaterade till informationssäkerhet.

IT-säkerhet är en del av informationssäkerheten vilket innebär att övergripande styrdokument inom informationssäkerhet även bör inkludera reglering av IT-säkerhetsområdet.

Vi har i granskningen tagit del av styrande dokument i form av policy, riktlinjer och anvisningar. I *Anvisning för informationshantering och säkerhetsprocesser* (beslutad av Enhetschef Säkerhet och beredskap, 2022-11-01) vilken presenteras mer i avsnitt 4.2.2, finns nedan bild och en bilaga som beskriver hierarki av styrande dokument för

informationssäkerhet som gäller inom Malmö stad. Dessa ska enligt nämnd anvisning utgöra Malmö stads Ledningssystem för informationssäkerhet, LIS.


### 4.2.1 Policy

*Trygghet och säkerhetspolicy för Malmö stad* (antagen av kommunfullmäktige 2017-05-24) ska visa stadens inriktning för trygghets- och säkerhetsarbetet och vara ett stöd i arbetet på alla nivåer i organisationen. Policyn är det övergripande styrdokumentet för informationssäkerhet i staden.

Vi noterar genom dokumentgranskning att informationssäkerhet eller IT-säkerhet inte omnämns specifikt i detta dokument. Vi noterar även att policyn inte har reviderats i enlighet med krav i dokumentet. Detta ska göras minst var fjärde år eller oftare vid behov. Kommunstyrelsen ansvarar för framtagande och revidering av policyn.

Enligt intervjuade ser stadskontoret i nuläget över behovet av, och eventuell utformning av policy för säkerhetsområdet vilket även ska inkludera informationssäkerheten.

### 4.2.2 Riktlinjer för informationssäkerhet med tillhörande anvisningar

I enlighet med reglementets ansvarsfördelning har kommunstyrelsen beslutat om *Malmö stads riktlinjer för informationssäkerhet* (beslutat av kommunstyrelsen 2022-06-07). Syftet med riktlinjerna uppges vara att på strategisk nivå fastställa ansvar, målsättning och arbetssätt för informationssäkerhet och sätta ramarna för hur allt arbete med informationssäkerhet ska bedrivas.

I dokumentet regleras att innehållet i riktlinjen och underliggande anvisningar, regler och rutiner baseras på standarden för informationssäkerhet SS-ISO/IEC 27000-serien.

Vad gäller IT-säkerhet har riktlinjen ett teknikavsnitt av vilket det framgår krav på att beakta informationssäkerhetsperspektivet för all IT under hela livscykeln samt att alla informationssystem ska ha en dokumenterad ägare som ansvarar för att säkerställa skydd av informationen.

Riktlinjerna anger att mer detaljerade krav, beskrivningar och vägledning som förklarar hur stadens verksamheter ska implementera innehållet i riktlinjen ska finnas i anvisningar, regler och rutiner. Stadsdirektören har enligt riktlinjerna rätt att delegera fastställande av underliggande dokument till enhetschef Säkerhet och beredskap samt avdelningschef inom IT- och Digitaliseringsavdelningen (härefter ITD). Vi kan genom dokumentgranskning se att detta har efterlevts för de underlag vi tagit del av.

Vi har i granskningen tagit del av *Anvisning för personalsäkerhet* (beslutad av Enhetschef Säkerhet och beredskap, 2022-11-01), *Anvisning för informationshantering och säkerhetsprocesser* (beslutad av Enhetschef Säkerhet och beredskap, 2022-11-01) samt *Anvisning IT-säkerhet* (beslutad av Avdelningschef It- och Digitaliseringsavdelningen, 2022-11-01). Samtliga erhållna anvisningar hänvisar till säkerhetsåtgärder som ISO 27002 ställer krav på.

#### *4.2.2.1 Efterlevnad*

Efterlevnaden av riktlinjen ska, enligt dokumentet, följas upp löpande och sammanställas av stadskontoret årligen med återkoppling till stadens ledningsgrupp och kommunstyrelsen. Varje nämnd har ansvar för sin informationssäkerhet och motsvarande uppföljning av efterlevnaden av riktlinjen ska göras årligen och rapporteras till den egna förvaltningsledningen och nämnden.

Vi har i granskningen inte erhållit någon dokumentation som visar att uppföljning av efterlevnaden har gjorts där denna har rapporterats till stadens ledningsgrupp, förvaltningsledningen, kommunstyrelsen eller servicenämnden. Uppföljning av informationssäkerhetsarbetet på en mer övergripande nivå har rapporterats till stadens ledningsgrupp, vilket beskrivs i avsnitt 4.5 Uppföljning och rapportering.

Intervjuade har beskrivit att informationssäkerhetsarbetet bedrivs med utgångspunkt från de beslutade styrdokumenten. De IT-säkerhetsåtgärder som staden arbetar med uppges i hög grad vara samstämmiga med krav enligt ISO 27002 även om inte ITD stämmer av alla åtgärder mot dessa kontinuerligt. Åtgärder utgår från praxis och högt ställda krav inom IT-säkerhet och uppfattningen från intervjuade är att dessa därigenom motsvarar eller överträffar åtgärder som *Anvisning för IT-säkerhet* ställer som krav. Intervjuade menar därigenom att efterlevnad av dokumenten finns i hög grad även om det inte dokumenterats.

### 4.2.3 Övriga riktlinjer och planer med bäring på granskningsområdet

#### *4.2.3.1 Riktlinjer för IT och Digitalisering*

*Riktlinjer för IT och digitalisering* (kommunfullmäktige, 2021-03-31 § 100) syftar till att säkerställa att området IT och digitalisering fungerar som en helhet. Riktlinjerna beskriver definition av kommungemensam IT samt den ansvarsfördelning som gäller mellan kommunstyrelsen, servicenämnden och övriga nämnder. Det finns även beskrivning av förvaltningarnas ansvar.

Av riktlinjerna framgår att servicenämnden ansvarar för att årligen till kommunstyrelsen bereda ärende om antagande av plan för kommungemensam IT. Serviceförvaltningen ansvarar för att ta fram planen som ska inkludera behov som kommunicerats från samtliga förvaltningar och sedan sammanställts på aggregerad nivå av ITD.

#### *4.2.3.2 Utvecklingsplan kommungemensam IT och Digitalisering*

Vi har tagit del av *Utvecklingsplan kommungemensam IT och Digitalisering 2024* (godkänd av servicenämnden 2023-06-20 samt beslutad av kommunstyrelsen 2023-

10-18). Av planen för 2024 framgår att arbetet med att stärka säkerheten runt stadens digitala infrastruktur och cybersäkerhetsförmåga ska fortsätta.

Vi har tagit del av *Utvecklingsplan för kommungemensam IT och Digitalisering 2025* (godkänd av servicenämnden 2024-06-18 samt beslutad av kommunstyrelsen 2024-08-14) av vilken det framgår att IT- och cybersäkerhet har en framträdande roll i utvecklingsplanen. För att genomföra arbetet enligt de behov som planen identifierat krävs utökad ram. Detta ska enligt underlaget äskas separat i nämndens budgetskrivelse.

I samband med beslut i kommunstyrelsen framgår av ärendet att servicenämnden i sin budgetskrivelse 2025 begär medel om totalt 21 miljoner kronor för finansiering av genomförande av 2025 års utvecklingsplan, varav 16 miljoner kronor avser insatser inom IT-säkerhet och fem miljoner kronor övriga insatser i utvecklingsplanen.

### 4.2.4 Bedömning

**Vår bedömning är att kommunstyrelsen i allt väsentligt har beslutat om styrdokument för arbetet med IT-säkerhet men att det inte har säkerställts att dessa efterlevs.**

I enlighet med det av kommunfullmäktige beslutade reglementet för kommunstyrelsen och övriga nämnder har kommunstyrelsen beslutat om Riktlinjer för informationssäkerhet. Riktlinjerna inkluderar även IT-säkerhet på övergripande nivå. Kompletterande anvisningar har beslutats inom stadskontoret i enlighet med den i Riktlinjer för informationssäkerhet fastställda delegationen.

Riktlinjer för informationssäkerhet anger att styrande dokument ska följa informationssäkerhetsstandarden ISO 27000-serien vilket vi konstaterar att Riktlinjer för informationssäkerhet och kompletterande anvisningar gör. Vi noterar dock att Trygghets- och säkerhetspolicyn i nuvarande form inte når upp till kraven enligt standarden och ser positivt på det arbete som pågår med att upprätta ett nytt policydokument vilket bör anpassas för att nå upp till kraven enligt standarden.

Riktlinjer för informationssäkerhet ställer krav på årlig kontroll av efterlevnaden av riktlinjerna med rapportering till förvaltningsledning och kommunstyrelsen. Detta har inte genomförts i enlighet med beslutad rutin vilket vi bedömer är en brist.

**Vår bedömning är att servicenämnden inte har beslutat om styrdokument för arbetet med IT-säkerhet vilket vi bedömer är korrekt i relation till fastställt reglemente och reglering i Riktlinjer för informationssäkerhet. Vi bedömer att nämnden inte har säkerställt att styrande dokument efterlevs.**

Enligt det av kommunfullmäktige beslutade reglementet för kommunstyrelsen och övriga nämnder ingår inte i servicenämndens ansvar att besluta om styrande dokument för it-säkerhet. Beslut om anvisningar kan enligt Riktlinjer för informationssäkerhet delegeras från stadsdirektören till andra chefsbefattningar. Vi kan konstatera att anvisningar för IT-säkerhet har beslutats i enlighet med den i Riktlinjer för informationssäkerhet fastställda delegationen.

Riktlinjer för informationssäkerhet ställer krav på årlig kontroll av efterlevnaden av riktlinjerna med rapportering till förvaltningsledning och nämnden. Detta har inte genomförts i enlighet med beslutad rutin vilket vi bedömer är en brist.

## 4.3 Arbetssätt och ansvar vid IT-säkerhetsincidenter

Enligt *Riktlinjer för informationssäkerhet* är definitionen för en incident ”*En oförutsedd händelse som får en oönskad effekt i form av skada för individ eller verksamhet*”.

Mål enligt ISO 27001 avseende informationssäkerhetsincidenter är att säkerställa ett konsekvent och effektivt tillvägagångssätt för hantering av informationssäkerhets-incidenter inklusive kommunikation kring säkerhetshändelser och svagheter.

I *Anvisning för informationshantering och säkerhetsprocesser* framgår att det ska finnas en centralt framtagen mall, rutin och ett kommungemensamt IT-stöd för inrapportering av informationssäkerhets- och personuppgiftsincidenter. Av anvisningen framgår att IT-relaterade incidenter ska rapporteras till IT-support via e-post, telefon eller på det sätt som IT-support anger.

### 4.3.1 Incidenthanteringsrutiner

Vi har i granskningen erhållit tre rutiner enligt nedan.

1. *Beskrivning av incidentprocess* beskriver på övergripande nivå varför staden har en incidentprocess samt hur den fungerar och förvaltas. Av dokumentet framgår att det är upprättat inom serviceförvaltningen. Underlaget saknar uppgift om fastställande, datering samt ansvarig för rutinen.
2. *Hantering av säkerhetsincident* (daterad 2024-08-30, version 1.0) beskriver ITD:s hantering av IT-säkerhetsincidenter. Rutinen innehåller sex steg i en modell. Modellen omfattar hanteringen från det förebyggande arbetet för att hindra att incidenter sker till hur incidenter ska följas upp och utgöra grund i förbättringsarbetet. Enligt dokumentet är beställare/uppdragsgivare samt författare namngivna funktioner inom IT- och Digitaliseringsavdelningen.
3. *Bedömning och hantering av Major incident* är en fördjupad beskrivning över hantering av kritiska incidenter. Rutinen beskriver roller, ansvarsfördelning och process för arbetet. Rutinen beskriver även involvering av funktioner utanför ITD samt hur kommunikationen ska ske till centrala funktioner och förvaltningarna. Underlaget saknar uppgift om fastställande, datering samt ansvarig för rutinen.

### 4.3.2 Verktyg för hantering av IT-säkerhetsincidenter

I rutinen *Hantering av säkerhetsincident* beskrivs hur staden som del i sitt förebyggande arbete skapat förutsättningar för att upptäcka säkerhetsincidenter. Bland annat beskrivs olika tekniska implementeringar som ger stöd i att upptäcka avvikelser som kan ge indikation på säkerhetsincidenter samt hur analyser och bedömningar från olika källor och omvärldsbevakning kan skapa en nulägesbild över händelser eller avvikelser i IT-miljön.

Intervjuade beskriver att flera väsentligt säkerhetshöjande åtgärder har vidtagits i Malmö stad med start under 2022. Därtill lyfts åtgärder som ingått i beslutad *Utvecklingsplan för IT och Digitalisering 2024.* Dessa åtgärder har möjliggjorts dels genom ramtilldelning för nämnden, dels genom överföring av resurser från kommunstyrelsen till servicenämnden. Vi har bland annat genom protokollsgranskning noterat att kommunstyrelsen vid sammanträdet 2024-04-10 beslutat att överföra 3 miljoner kronor från kommunstyrelsens medel till förfogande till servicenämnden för genomförande av *Utvecklingsplanen för kommungemensam IT och digitalisering 2024*.

Genom utvecklingsplanen samt andra underlag som vi tagit del av i ärenden till kommunstyrelsen och servicenämnden beskrivs ett antal åtgärder som vidtagits i syfte att stärka IT-säkerheten. En av dessa åtgärder har varit införande av en så kallad SOC-tjänst (Security Operations Center), en tjänst med både tekniska implementationer och bemanning av it-säkerhetsspecialister som löpande analyserar och agerar på it-säkerhetshändelser. Arbete med säkrare autentiseringsmetoder samt uppgradering och investeringar i infrastrukturen är andra exempel på åtgärder. Dessa har, enligt intervjuade, sammanvägt lett till en minskning av antal incidenter som rapporterats till servicedesk inom ITD.

### 4.3.3 Arbetssätt och ansvar för hantering av incidenter

Incidenter hanteras på olika sätt beroende på typ av incident. Mindre incidenter som har en liten inverkan på verksamheten hanteras inom ordinarie supportorganisation. Kritiska incidenter har en särskild hantering och dessa rutiner träder in när minst ett av följande kriterier uppfylls:

- Stor verksamhetspåverkan
- Felet drabbar många
- Normal hantering anses vara otillräcklig

Enligt processkarta för hantering av så kallad Major Incident som vi tagit del av kan incidenter identifieras och inrapporteras på flera olika sätt, dels genom teknisk övervakning dels genom kommunikationskanaler i form av telefon, e-post eller portal. Det har identifierats ett förbättringsområde att förenkla inrapportering via serviceportalen. Detta då nuvarande inrapportering enligt intervjuade kan uppfattas som svår för användare som inte har IT-kompetens.

Efter rapportering görs en initial bedömning av incidenterna. Denna bedömning ligger sedan till grund för den prioritering och fortsatta utredning och analys som bedöms behövas.

Av de incidenthanteringsrutiner som presenterats ovan, framgår ett antal roller vilka har tilldelade ansvar för hantering av IT-säkerhetsincidenter. En nyckelroll är Incident Manager som ansvarar för att säkerställa att incidenter hanteras på ett effektivt och konsekvent sätt. Rollen har ansvar och uppgifter både i det förebyggande arbetet och en särskild roll vid pågående incidenter. I det förebyggande arbetet lyfts bland annat upprättande av rutiner, utbildning samt ansvar att leda och koordinera incidenthanteringsteamet. Vid hantering av pågående incidenter har Incident Manager ett utökat mandat, exempelvis avseende arbetsledning och beslutsfattande för att

möjliggöra beslut som leder fram till att kunna återgå till normaldrift så snart som möjligt.

I *Hantering av säkerhetsincident* beskrivs ytterligare roller som är väsentliga i incidenthanteringen. Här ingår exempelvis koordinatorer, IT-tekniker och IT-specialister. Det finns även ett antal roller och funktioner som ingår i incidenthanteringsprocessen för information, kommunikation och samordning. Enligt *Hantering av säkerhetsincident* är ledningsgruppen inom ITD en av mottagarna av information när kritiska incidenter sker.

Intervjuade bekräftar samstämmigt att de rutiner som finns efterlevs och att stadens incidenthantering fungerar effektivt och utifrån tydliga roller och ansvar. Däremot lyfts som risk att det i Malmö stad även finns andra rapporteringsvägar för incidenter som inte är IT-säkerhetsincidenter. Exempelvis informationssäkerhets- eller personuppgiftsincidenter vilket försämrar möjligheten att få en samlad bild av informationssäkerhetsrelaterade incidenter.

I ovan nämnd rutin *Bedömning och hantering av Major Incident* beskrivs hur kommunikation i samband med kritiska incidenter ska fungera. För incidenten utsedd kriskommunikatör ska exempelvis ansvara för kommunikation enligt en kommunikationsplan. I beskrivningar ingår bland annat kommunikationskanaler samt frekvens för kommunikation till olika målgrupper. I detta ingår även eskalering till Tjänsteperson i Beredskap som i sin tur har mandat att initiera stadsövergripande krisledning.

Ett förbättringsområde som lyfts i intervjuer är kommunikation till de olika förvaltningarna. Då Malmö stad har ett decentraliserat IT-ansvar där även förvaltningarna själva har ansvar för vissa informationssystem och applikationer finns en utmaning i att veta vem eller vilka som behöver kontaktas vid incidenter. I vissa fall uppges det finnas ett beroende av att Incident Manager känner till ”rätt” personer och kan ta direktkontakt för informationsinhämtning eller spridning.

### 4.3.4 Incidentrapporter och uppföljning av incidenter

Vi har tagit del av exempel på dokumenterade incidentrapporter. Dessa redogör för en summering av inträffad incident, tidslinje för hantering samt åtgärder och förbättringsförslag för att inte incidenter ska inträffa på nytt.

De incidentrapporter vi fått del av verifierar att hantering av dessa incidenter har skett i enlighet med rutinerna *Hantering av säkerhetsincident* samt *Bedömning och hantering av Major Incident*. Incident Manager har signerat de rapporter vi tagit del av men en av incidentrapporterna saknar signering av avdelningschef, vilket är ett avsteg från rutinen.

Vi kan genom incidentrapport från en tidigare inträffad incident konstatera att genomförd analys och uppföljning av incidenten identifierat behov av ny rutin och process för hantering av säkerhetsincidenter. Vi har kunnat konstatera att den rutin vi tagit del av i granskningen som benämns *Hantering av säkerhetsincident*, har uppdaterats enligt de behov som föranleddes av denna analys.

Vi har tagit del av underlag för rapportering till Säkerhetsråd inom ITD. Vi har inte i styrande dokument eller rutiner tagit del av beskrivning av forumet eller vilka som deltar i detta. Enligt intervjuade består säkerhetsrådet av enhetschef med ansvar för infrastruktur, enhetschef utveckling, enhetschef leverans och sektionschef i leveransenheten (särskilt ansvar för strategi kring säkerhet). I början av 2025 kommer enligt uppgift enhetschef infrastruktur att ersättas i rådet av sektionschef infrastruktur.

Av rapportering vid säkerhetsrådets möte i september 2024 framgår redovisning av antal händelser som de tekniska verktygen identifierat. En kategorisering har gjorts enligt prioriteringsskalan *låg*, *medium* och *hög*. Enligt rapportering som avsåg augusti 2024 fanns ett fåtal händelser med *hög* prioritet och ingen av dessa bedömdes som kritiska. 92 % av händelserna hade prioriteringen *låg*.

### 4.3.5 Bedömning

**Vår samlade bedömning är att det inom servicenämnden finns arbetssätt för att upptäcka och hantera IT-säkerhetsincidenter samt att roller och ansvarsfördelning för hantering av dessa är tydliga inom IT- och Digitaliseringsavdelningen.**

Vi baserar vår bedömning på att det dels finns dokumenterade rutiner och tillhörande underlag som dels tydliggör ansvar dels beskriver processer för hantering av incidenter, både i ett förebyggande syfte och i akuta situationer. Därtill finns tekniska verktyg och tjänster för att upptäcka, hindra och även hantera incidenter i tidiga skeden för att på så sätt minska konsekvensen av de hot som riktas mot staden.

Vi bedömer att nuvarande kommunikationsplan vid kritiska incidenter kan utvecklas med tydliggörande av eskaleringsvägar till representanter i övriga förvaltningar för att säkerställa att kommunikationsvägar möjliggör en effektiv hantering av incidenter.

## 4.4 Användarrelaterade incidenter

I *Riktlinjer för informationssäkerhet* framgår att alla medarbetare ska ha tillräckliga kunskaper om informationssäkerhet i förhållande till sin roll och sina arbetsuppgifter. De ska vara säkerhetsmedvetna och ha god kännedom om de hot och risker som finns och hur de kan skydda sig mot dem. Varje anställd har en skyldighet att rapportera informationsrelaterade brister och incidenter.

Alla anställda ska få utbildning inom informationssäkerhet anpassad utifrån den roll man har och den information man hanterar.

*Anvisning för personalsäkerhet* beskriver kraven mer detaljerat. I anvisningen är kraven utformade med grund i säkerhetsåtgärder enligt ISO 27002. Bland annat framgår av anvisningen att:

- Det ska finnas ett kommungemensamt LMS-verktyg (Learning management system) där stadskontoret tillhandahåller en basutbildning avseende informationssäkerhet till alla anställda.
- Alla anställda ska varje år genomgå den kommungemensamma basutbildningen i informationssäkerhet.

- Stadskontoret ska tillhandahålla en kommungemensam så kallad awareness-utbildning inom informationssäkerhet.
- Alla anställda ska varje år genomgå den kommungemensamma awareness-utbildningen i informationssäkerhet.

I intervjuer framkommer att alla medarbetare ska genomföra basutbildningen DISA (Digital informationssäkerhet för alla är en digital utbildning som tillhandahålls av Myndigheten för samhällsskydd och beredskap. Den är kostnadsfri och tillgänglig via deras hemsida). Det finns dock vid tidpunkten för granskningen inget sätt att följa upp att så sker.

Det pågår ett arbete för att etablera ett LMS-verktyg vilket förväntas ge bättre förutsättningar till uppföljning av genomförandegraden. Planen från stadskontoret är även att, tillsammans med informationssäkerhetsorganisationen Malmö stad, anpassa utbildningen i den mån det går och komplettera med andra utbildningar eller insatser när behov finns.

Det beskrivs finnas olikheter mellan förvaltningarna med avseende på hur de erbjuder introduktion och utbildning inom informationssäkerhet. Däremot uppges att de centrala informationssäkerhetssamordnarna inom stadskontoret utbildar förvaltningarnas informationssäkerhets- och dataskyddssamordnare på samma sätt oavsett förvaltning. Bland annat har nyligen en platsutbildning i risk, incident och kontinuitet genomförts av utbildningsledare från Svenska institutet för standarder (SIS).

Utöver dessa utbildningsinsatser har medvetenhetskampanjer med artiklar publicerats på intranätet. Det har även gjorts riktade insatser till chefer och medarbetare under den nationella informationssäkerhetsmånaden som infaller årligen i oktober.

Malmö stad har enligt muntliga uppgifter haft incidenter som orsakats av oaktsamhet från enskilda användare. De har dock kunnat hanteras skyndsamt och utan allvarlig påverkan på information eller verksamhet. Den SOC som finns tillgänglig dygnet runt avhjälper hot tidigt genom de automatiska åtgärder som finns integrerade.

Andra åtgärder för att minska risken för användarrelaterade incidenter har varit att mejl från externa avsändare innehåller en gul varning högst upp i mejlet för att uppmana mottagaren till vaksamhet. Enligt uppgift i intervju kan ITD se att antal klick på länkar med mera har minskat. Uppfattningen från intervjuade är att en majoritet av inkomna phising-mejl filtreras tack vare de tekniska implementationer som finns. Det finns även information på intranätet om hur medarbetare kan agera om de misstänker att de erhållit phising-mejl, bland annat kan detta rapporteras direkt i e-postklienten som skräppost. Det förekommer även att medarbetare kontaktar servicedesken för säkerhets skull.

### 4.4.1 Test av användarnas kunskap och medvetenhet

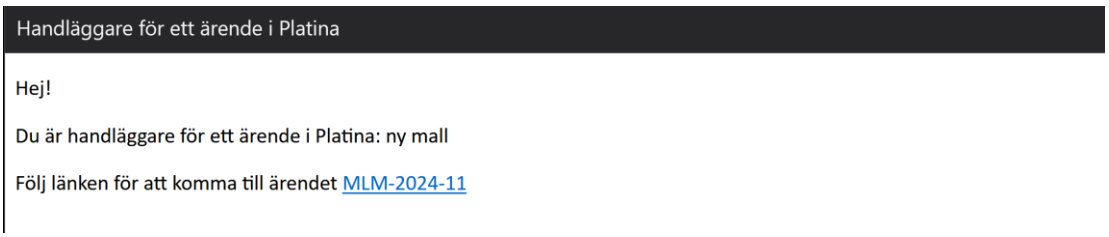
Som del i granskningen har Stadsrevisionen efterfrågat ett test av medarbetares användning av IT-system. Enligt projektplan för granskningen skulle detta riktas mot ett i Malmö stads övergripande IT-system för hantering av dokumentation.

Testet har utgjorts av en simulerad phising-attack, på svenska benämnt *nätfiske*. Totalt skickades 3500 mejl till användare av systemet. Dessa användare var organiserade inom samtliga förvaltningar och inte specifikt kommunstyrelsens eller servicenämndens verksamheter.

Det är inledningsvis viktigt att poängtera att syftet inte var att testa stadens tekniska IT-säkerhet. För att kunna genomföra testet behövde vissa tekniska skyddsåtgärder som är etablerade i staden kopplas bort. Bland annat gjordes en teknisk anpassning för att godkänna det stora utskick av mejl som testet innebar samt att den domän som mejlet kom från ”vitlistades”. Det är sannolikt att de tekniska skyddsåtgärder som staden har i annat fall skulle ha stoppat mejlutskicket och medarbetarnas medvetenhet hade då inte kunnat testas enligt tänkt metod.

Testet var utformat för att få användarna att tro att de hade fått ett dokument delat till sig. Den avsändare som nyttjades var administratorplatina@malmo.email. Praxis vid genomförande av sådana test är att ge mottagarna 72 timmar att agera.

Det mejl som mottagarna fick var utformat enligt nedan:


Handläggare för ett ärende i Platina

Hej!

Du är handläggare för ett ärende i Platina: ny mall

Följ länken för att komma till ärendet MLM-2024-11

De som klickade på länken i mejlet kom till en sida för att logga in med sin mejladress vilket sedan ledde till en ny sida där användaren uppmanades att ange sitt lösenord för att därefter få tillgång till dokumentet.

Målvärde vid phisingattacker liknande den som genomfördes inom ramen för denna granskning är att färre än 5 % av användarna klickar på länkar och sedan lämnar sina inloggningsuppgifter. Målvärdet baseras på att medvetandehöjande åtgärder och utbildning har genomförts inom verksamheten. Detta kan därigenom ses som ett riktmärke för Malmö stad som enligt uppgift i granskningen har erbjudit utbildnings- och informationsinsatser till sina medarbetare.

Resultatet i testet indikerar att det finns behov av ytterligare insatser för att öka användarnas medvetenhet om hot och risker vid användning av informationssystem. Detta då resultatet inte var i linje med ovan nämnt målvärde då en högre andel än 5 % av de som mottog mejlet klickade på länken och lämnade sina uppgifter. En detaljerad rapport över resultatet har överlämnats till säkerhetsfunktioner inom staden. I denna rapport ges endast en övergripande bild med hänvisning till att alltför detaljerade uppgifter kan vara känsliga att offentliggöra.

Även om det primära målet i detta test var att samla in autentiseringsuppgifter, är det viktigt att betona att bara att klicka på länken i mejlet utan att inloggningsuppgifter lämnas utgör betydande risker. I mer avancerade scenarier av liknande hot mot användare kan klickande på länkar potentiellt utlösa andra skadliga effekter och hot.

Det är viktigt att notera att vi i testet inte samlade in de faktiska lösenorden och att ingen validering av korrekta lösenord genomfördes. Detta tillvägagångssätt säkerställde att testet skulle fungera samtidigt som integriteten hos känsliga data skyddades.

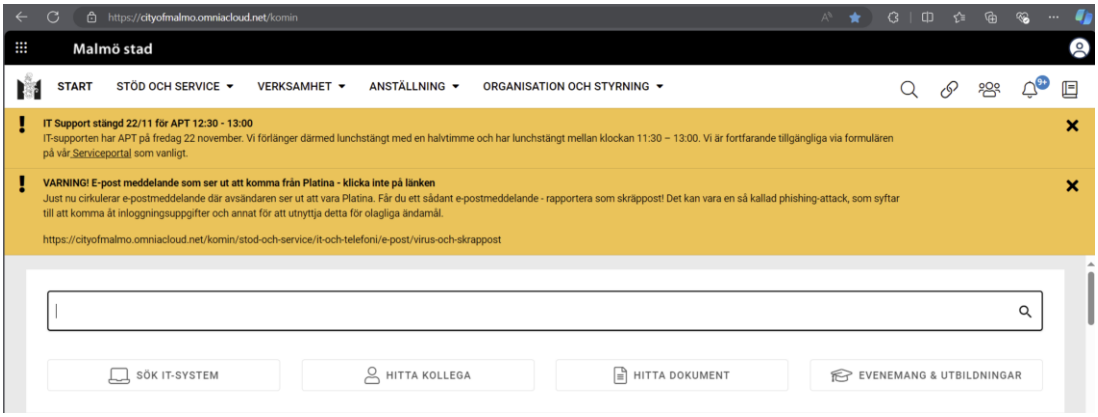
Som det sista steget i testet omdirigerades de som angett sina uppgifter till en sida med meddelandet "*Filen kan inte nås. Filen du försöker komma åt har flyttats eller tagits bort*."

### 4.4.2 Hantering av hot om säkerhetshändelse orsakad av användare

Som vi nämnt tidigare så var tanken att testet skulle vara aktivt i 72 timmar. Vi fick dock signaler redan efter 27 timmar att det fanns starka önskemål från stadens IT-funktioner att avbryta testet. Detta motiverades med att testet hade en allvarlig påverkan på stadens supportfunktion och även uppfattades som ett intrång på IT-säkerheten. Efter samråd med teknisk testledare och acceptans från Stadsrevisionen avbröts testet.

Vi har efter testets genomförande efterfrågat underlag över hur användarna reagerade och rapporterade till supportfunktioner. Vi har tagit del av en kommunikationstråd för ”superanvändare” av Platina, det system som mejlet uppgavs gälla. Där har flera av dessa reagerat och uppmanat till uppmärksamhet samt varnat andra användare om risk för phising. I denna kommunikation hänvisades även användare som klickat på länken att ta kontakt med IT-support eller anmäla säkerhetsincident genom Service-portalen.

Därtill efterfrågades att en varning skulle publiceras i ett bredare perspektiv för att nå fler vilket föranledde att nedan varning publicerades på Malmö stads intranät.




Vi har inte fått några dokumenterade underlag över incidenthanteringen men en skriftlig redogörelse. Av den framgår att både ITD:s incidentprocess och stadens incidentprocess initierades i samband med testet. I ett inledande skede informerades tjänsteperson i beredskap som i sin tur aktiverade kriskommunikatör.

Supportorganisationen inom ITD påbörjade hanteringen i enlighet med de rutiner som vi beskrivit tidigare i rapporten. Incidenten kategoriserades och åtgärder vidtogs i enlighet med de rutiner som finns.

Representanter från ITD framhåller att, det faktum att de på grund av omständigheter kring testets genomförande och i detta specifika fall, inte kunde aktivera åtgärder och stoppa de falska mejlen innebar att händelsen eskalerade. Detta riskerade även att leda till en svårförklarlig och kostsam krishantering som inte varit nödvändig i skarpt läge. I en sådan situation är uppfattningen från ITD att phisingmejlen kunde ha stoppats inom en timme och hotet varit avvärjt.

### 4.4.3 Bedömning

**Vår bedömning är att IT-säkerhetsincidenter kopplade till medarbetares användning av IT-system förekommer och att kommunstyrelsen delvis säkerställt att dessa hanteras.**

Kommunstyrelsen har genom *Riktlinjer för informationssäkerhet* beslutat om krav på utbildning inom informationssäkerhet. Utbildnings- och informationsinsatser har genomförts som riktats till samtliga stadens medarbetare men vi bedömer att dessa inte varit tillräckliga. Vi bedömer att det saknas uppföljning av genomförandegrad för obligatorisk grundutbildning och det har inte säkerställts genom uppföljning eller kontroll hur nya medarbetare får del av information om informationssäkerhet i samband med introduktionen.

En del i granskningen har varit ett test avseende användarnas medvetenhet om hot och risker inom IT-säkerhet. Vi bedömer utifrån resultatet att personalsäkerheten är bristfällig och konstaterar att medarbetarnas användning av IT-system är förenat med risker. Kompletterande utbildningsinsatser behöver genomföras för användare av stadens IT-system då brister identifierades i samtliga verksamheter.

**Vår bedömning är att IT-säkerhetsincidenter kopplade till medarbetares användning av IT-system förekommer och att servicenämnden i allt väsentligt säkerställt att dessa hanteras.**

Incidenter förekommer och vi bedömer att tekniska skyddsåtgärder har etablerats så att hot som riktas till användare kan stoppas eller hanteras innan de leder till allvarliga konsekvenser.

## 4.5 Uppföljning och rapportering

### 4.5.1 Krav enligt styrande dokument

I avsnitt 4.2.2.1 har vi redogjort för uppföljning i form av krav på kontroll av efterlevnaden av *Riktlinjer för informationssäkerhet* med tillhörande rapportering, vilken gäller både kommunstyrelsen och servicenämnden.

I kommunstyrelsens övergripande ansvar för arbetet med informationssäkerhet ingår enligt *Riktlinjer för informationssäkerhet* att följa upp stadens arbete med informationssäkerhet och rapportera resultatet till stadens ledningsgrupp och kommunstyrelsen. Vad gäller nämndernas ansvar framgår att den av förvaltningsledningen utsedda informationssäkerhetssamordnaren ansvarar för uppföljning av förvaltningens interna informationssäkerhetsarbete samt rapportering till förvaltningsledningen.

Av *Anvisning för informationshantering och säkerhetsprocesser* framgår att Malmö stads arbete med informationssäkerhet årligen ska följas upp enligt stadsövergripande rutin. Av dokumentet framgår dock att rutinen inte är upprättad. Intervjuade bekräftar att rutinen saknas.

Genom protokollsgranskning för servicenämnden och kommunstyrelsen kan vi konstatera att samlad uppföljning och tillhörande rapportering av informationssäkerhetsarbetet respektive IT-säkerhetsarbetet enligt ovan reglering saknas. Detta bekräftas även i intervjuer och framhålls som ett förbättringsområde.

Utöver den årliga uppföljningen anges i ovan nämnda anvisning att säkerhetsuppföljning ska genomföras vid behov. Anvisningen beskriver att uppföljning kan bestå av flera olika moment och tillvägagångssätt såsom utvärdering av processer, genomlysning av upprättad dokumentation samt att den använda tekniken kontrolleras utifrån ett säkerhetsperspektiv. Exempelvis kan sårbarhetsanalyser och penetrationstester göras.

I enlighet med *Anvisning för informationshantering och säkerhetsprocesser* har säkerhetsuppföljning gjorts på flera sätt för att utvärdera och verifiera befintliga skydd och IT-säkerhet. Revisioner av IT-säkerheten har genomförts inom ITD. Här ingår bland annat SOC-revision (en tredjepartsrevision som syftar till att göra en efterlevnadskontroll för tjänster som tillhandahålls av externa leverantörer) och CIS Controls (ett ramverk med fastställda kontrollområden inom it-säkerhet där regelbunden uppföljning identifierar sårbarheter och förbättringsområden). I det sistnämnda ingår 18 punkter som visar mognadsgrad samt åtgärder för att höja säkerheten årligen. Det har även gjorts GAP-analyser. Den senaste analysen utgår från en jämförelse av nuläget i förhållande till krav i ny lagstiftning genom NIS2-direktivet (*The Directive on security of network and information systems* är ett EU-direktiv där den svenska regleringen tillämpas i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. 2022 beslutade EU-parlamentet om nytt direktiv, kallat NIS2. Detta förväntas träda i kraft 2025 genom Cybersäkerhetslagen).

ITD gör även regelbundet sårbarhetsanalyser och penetrationstester för att utvärdera skyddsnivåer i förhållande till sårbarheter. Intervjuade beskriver att ledningsgrupp inom ITD träffas veckovis där säkerhetsfrågor är ett stående inslag.

### 4.5.2 Cybersäkerhetskollen

Analyser och uppföljning av stadens arbete har gjorts genom verktyg som tillhandahålls av Myndigheten för samhällsskydd och beredskap (MSB). Mätningen har etablerats som ett sätt för myndigheten att få en lägesbild över arbetet på nationell nivå. Verktyget heter Cybersäkerhetskollen och har delar både för informationssäkerhet och IT-säkerhet (före 2024 hette verktyget Infosäkkollen men består nu av två delar, Infosäkkollen och IT-säkkollen och har därefter bytt namn till Cybersäkerhetskollen). I denna uppföljning gör verksamheter en självskattning av sitt informationssäkerhetsarbete i relation till ISO 27001 och ISO 27002.

### *Infosäkkollen*

Enligt intervjuade har mätningen i staden varit ett viktigt moment för att inkludera hela organisationen i uppföljning av informationssäkerhetsarbetet. Tillvägagångssättet i Infosäkkollen har varit att respektive förvaltning har gjort en egen mätning och stadskontoret har gjort en övergripande för hela staden.

Vi har tagit del av utdrag från protokoll fört vid stadskontorets ledningsgruppsmöte i april 2024 (2024-04-02) där resultatet av mätningen 2023 presenterades tillsammans med redogörelse av prioriterade områden för att höja mognadsgraden. Resultatet har även presenterats på stadens ledningsgrupp vid möte 2024-04-12. 2024 års resultat presenterades för stadskontorets ledningsgrupp 2024-11-19 då även stadsdirektören närvarade. Anteckningar från mötet visar att medvetenhet och utbildning är ett planerat fokus framåt.

### *IT-säkkollen*

Mätningen IT-säkkollen har genomförts av ITD åren 2023 och 2024. Mätningen avser etablerade IT-säkerhetsåtgärder och bedömning sker enligt en skala från 1 till 4 där graden av skydd beskrivs enligt följande: 1=Inget skydd, 2=Bristfälligt skydd, 3=Visst skydd och 4=Adekvat skydd.

Resultatet i IT-säkkollen har förbättrats mellan de två mätningar som genomförts av ITD. Det kvarstår vissa åtgärder för att höja värdet i mätningen. Intervjuade beskriver dock att mätningen inte är helt tillämpbar och inte tillräckligt nyanserad för att ge ett tillförlitligt resultat. MSB ska enligt uppgift justera metoden till mättillfället 2025.

Resultatet i IT-säkkollen har, enligt material vi tagit del, av presenterats på säkerhetsrådet inom ITD i september 2024 (2024-09-27).

## 4.5.3 Intern kontroll

I *Reglemente för intern kontroll* (beslutat av kommunfullmäktige 2016-12-20) framgår att nämnder årligen ska besluta om intern kontrollplan som beskriver prioriterade åtgärder och granskningar utifrån dokumenterade riskanalyser.

Samtliga verksamheter ska enligt *Malmö stads handbok för intern kontroll* (fastställd av stadskontoret, version 3, reviderad oktober 2020) genomföra riskanalyser som är heltäckande och speglar verksamhetens delar. I handboken beskrivs arbetssätt och moment för internkontrollarbetet. I avsnittet för riskanalys framgår att informationssäkerhetsrisker är en riskkategori att beakta i arbetet med riskanalys och identifiering av kontrollområden.

Nämnderna ska med grund i sin riskanalys bedöma och besluta om det finns informationssäkerhetsrisker som ska ingå i planen för kontroller under året. Det kan även finnas kommunövergripande risker som nämnderna får krav på att inkludera i sina internkontrollplaner. En sådan risk är ”otillåten tillgång till information och lokaler” vilken inkluderats både under 2023 och 2024 under riskkategorin informationssäkerhet. Uppföljning av intern kontroll i samband med delårsrapportering visade att inga större avvikelser funnits inom vare sig kommunstyrelsen eller servicenämnden.

Genom dokumentgranskning av internkontrollplaner för kommunstyrelsen och servicenämnden kan vi konstatera att IT-säkerhet inte har inkluderats som kontrollområde.

### 4.5.4 Rapportering till kommunstyrelsen

Kommunstyrelsen beslutade vid sammanträdet 2024-02-07 om ett nämndinitiativ (STK-2024-347) där stadskontoret fick ett antal uppdrag i syfte att höja den civila beredskapen i Malmö. Bland annat skulle stadskontoret i samråd med serviceförvaltningen genomföra en översyn av stadens arbete med cybersäkerhet och återrapportera detta till kommunstyrelsen. Vid kommunstyrelsens sammanträde 2024-03-06 besvarades nämndinitiativet.

I den tjänsteskrivelse (G-Tjänsteskrivelse KSAU 240304 Besvarande av nämndinitiativ från Helena Nanne (M) och Håkan Fäldt (M) om att höja den civila beredskapen i Malmö) som vi tagit del av i ärendet framgår att stadskontoret anser att det redan idag sker ett systematiskt utvecklingsarbete av Malmö stads informations- och cybersäkerhetsarbete. Vidare beskrivs att staden har etablerade arbetssätt för att identifiera risker och hot samt att det görs regelbundna genomlysningar och riskanalyser som ligger till grund för planering och löpande investeringar inom området för att säkerställa adekvata skyddsnivåer.

Kommunstyrelsen beslutade att nämndinitiativet gällande översyn av cybersäkerheten skulle anses besvarad med hänvisning till den redovisning som tjänsteskrivelsen redogjort för.

Vi har inte noterat ytterligare ärenden med avseende på uppföljning och rapportering av IT-säkerhet vid styrelsens sammanträden under 2024.

### 4.5.5 Rapportering till servicenämnden

Servicenämndens Årsanalys 2023 (godkänd av Servicenämnden 2024-02-15) innehåller övergripande beskrivning av IT-säkerhet utifrån det av kommunfullmäktige beslutade målet *”Malmö stad ska verka för att öka tryggheten bland Malmöborna och för att brottsligheten ska minska”*. I Årsanalys 2023 framgår Servicenämndens särskilda ansvar för arbetet med ökad IT-säkerhet.

Enligt årsanalysen har arbetet utifrån målet gått enligt plan. Bland annat genom förstärkningar i infrastrukturen för ökad IT-säkerhet tillsammans med etablering av stärkt övervakning och incidenthantering tack vare SOC, vilken vi beskrivit tidigare i rapporten.

Utöver de ärenden vi lyft tidigare i rapporten har vi endast noterat ytterligare ett ärende på servicenämnden med avseende på IT-säkerhet under 2024. Vid sammanträdet 2024-01-30 fanns en informationspunkt om IT-säkerhet. Av protokollet framgår inte vilken typ av information som delgetts nämnden och inga beslut fattades i ärendet.

### 4.5.6 Bedömning

**Vår bedömning är att det delvis genomförs en systematisk uppföljning av IT-säkerhetsarbetet men att den rapportering som gjorts till kommunstyrelsen inte är tillräcklig.**

Kommunstyrelsen har enligt *Riktlinjer för informationssäkerhet* i ansvar att följa upp stadens arbete med informationssäkerhet och rapportera resultatet till stadens ledningsgrupp och kommunstyrelsen. Viss rapportering av uppföljning på en övergripande nivå har gjorts till stadens ledningsgrupp och kommunstyrelsen. Vi bedömer dock att den rapportering som gjorts inte är tillräcklig för att motsvara den samlade årliga uppföljning och rapportering som behöver göras för att kommunstyrelsen ska ha tillräckligt med information och insyn i arbetet.

*Anvisning för informationshantering och säkerhetsprocesser* reglerar att årlig uppföljning och rapportering ska göras enligt beslutad rutin. Rutinen saknas och det finns därigenom i nuläget inget tydliggörande över hur denna rapportering ska genomföras.

**Vår bedömning är att det delvis genomförs en systematisk uppföljning av arbetet med IT-säkerhet men att den rapportering som gjorts till servicenämnden inte är tillräcklig.**

Det har inte gjorts någon samlad årlig uppföljning och rapportering till servicenämnden i enlighet beskrivning i *Riktlinjer för informationssäkerhet* och *Anvisning för informationshantering och säkerhetsprocesser*. Samtidigt konstaterar vi att det saknas tydlighet från kommunstyrelsen och stadskontoret för hur denna uppföljning och rapportering förväntas genomföras då rutinen saknas.

Vi bedömer att säkerhetsuppföljning i hög grad har genomförts i enlighet med kravställning i *Anvisning för informationshantering och säkerhetsprocesser* samt att resultatet i vissa delar har rapporterats inom förvaltningen men inte till nämnden.

Vi bedömer att nuvarande uppföljning ger goda förutsättningar för att löpande anpassa IT-säkerhetsnivåer utifrån de hot, risker och sårbarheter som identifieras. Det behöver dock säkerställas att servicenämnden informeras om väsentliga delar så att tillräckliga förutsättningar finns för nämnden att upprätthålla sitt ansvar i enlighet med reglementet. Vi bedömer att den rapportering som gjorts inte är tillräcklig för att motsvara den samlade årliga uppföljning och rapportering som behöver göras för att servicenämnden ska ha tillräckligt med information och insyn i arbetet.

Utöver rapportering till nämnden bör även IT-säkerhetsarbetet inkluderas i den årliga rapporteringen till kommunstyrelsen då det är en väsentlig del i Malmö stads samlade informationssäkerhetsarbete.

# 5 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad.

**Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen delvis har säkerställt en tillräcklig IT-säkerhet för Malmö stad.**

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Bereda förslag till en informationssäkerhetspolicy eller motsvarande vars innehåll motsvarar de krav som ställs enligt ISO 27000-serien.
- Tillse att uppföljning och rapportering av informationssäkerhetsarbetet sker i enlighet med beslut i *Riktlinjer för informationssäkerhet* samt att kontroll av efterlevnad av riktlinjerna etableras.
- Tillse att rutin för uppföljning av det stadsövergripande informationssäkerhetsarbetet upprättas och etableras i enlighet med *Anvisning för informationshantering och säkerhetsprocesser*.
- Tillse att utbildning och information om IT-säkerhetshot och risker genomförs i hela organisationen för att stärka kunskap och medvetenhet hos användare. Därtill behöver genomförandegraden följas upp och åtgärder vidtas vid bristande genomförande.

**Vår samlade bedömning utifrån granskningens syfte är att servicenämnden delvis har säkerställt en tillräcklig IT-säkerhet för Malmö stad.**

Utifrån resultatet av vår granskning rekommenderar vi servicenämnden att:

- Tillse att uppföljning och rapportering sker i enlighet med beslut i *Riktlinjer för informationssäkerhet* samt att kontroll av efterlevnad av riktlinjer etableras. Uppföljning och rapportering behöver genomföras dels utifrån nämndens ansvar för egen informationssäkerhet, dels specifikt i relation till nämndens ansvar för kommungemensam IT och tillhörande IT-säkerhet.
- Tillse att rutinerna för incidenthantering kompletteras med datering, beslutsinstans samt ansvarig för revidering för att säkerställa dess aktualitet och förankring.
- Komplettera kommunikationsplan vid kritiska incidenter med tydliggjorda eskaleringsvägar och mottagare av information hos samtliga förvaltningar/verksamheter.

Datum som ovan

KPMG AB

Veronica Hedlund Lundgren

*Certifierad kommunal yrkesrevisor*

Jenny Thörn

*Verksamhetsrevisor*