Granskning av informationssäkerhet

Rapport

Helsingborgs stad

KPMG AB

2024-10-31

Antal sidor 22

Helsingborgs stad
Granskning av informationssäkerhet

2024-10-31

Innehållsförteckning

1 Sammanfattning

KPMG har av Stadsrevisionen och de förtroendevalda revisorerna i Helsingborgs stad fått i uppdrag att granska stadens arbete med informationssäkerhet.

Syftet med granskningen har varit att översiktligt bedöma om kommunstyrelsen har en ändamålsenlig och tillräcklig styrning och kontroll av informationssäkerhetsarbetet.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen delvis har en ändamålsenlig styrning och kontroll av informationssäkerhets-arbetet.

Kommunfullmäktige beslutade 2019 att uppdra till kommunstyrelsen att analysera behov och genomföra åtgärder i syfte att stärka stadens informations- och cybersäkerhetsarbete. Kommunstyrelsen i sin tur beslutade om ett antal uppdrag till förvaltningen att verkställa. Vi kan konstatera att kommunstyrelsen vid flera gånger erhållit återrapportering av uppdraget. Av rapportering framgår att det främst är tekniska säkerhetsåtgärder som har verkställts utifrån uppdraget och att det finns behov av förbättringar inom ett antal områden som är väsentliga för ett systematiskt informationssäkerhetsarbete. Vår granskning visar bland annat att uppdrag att revidera och upprätta styrande dokument inom området inte har verkställts.

Staden har en informationssäkerhetspolicy som beskriver ansvaret och ger övergripande inriktning av informationssäkerhetsarbetet. Den är dock föråldrad och har inte aktualiserats av kommunstyrelsen i enlighet med det ansvar som policyn reglerar, att granska policyn årligen och revidera vid behov. Någon revidering har inte gjorts sedan 2012. Enligt uppgift förväntas beslut om ny policy fattas inom kort.

Det saknas i nuläget kompletterande styrdokument i form av riktlinjer, anvisningar och instruktioner som konkretiserar policyns viljeriktning och krav på hur arbetet ska bedrivas. Vi bedömer att detta skapar en otydlighet i förhållande till den ansvarsfördelning som policyn reglerar och hur målen och de utgångspunkter som nuvarande policy ställer krav på ska uppnås.

Vi ser det som positivt att staden implementerat ett system som kan bidra med struktur för ett ledningssystem för informationssäkerhet, LIS och stöd i väsentliga processer i det arbete som ska genomföras. Samtidigt konstaterar vi att grunderna i ett LIS i nuläget saknas i brist på styrande dokument som tydliggjort ledningens viljeriktning med informationssäkerhetsarbetet.

Vi har därtill identifierat ytterligare områden som behöver stärkas för att staden ska ha ett systematiskt informationssäkerhetsarbete. Bland annat behöver riskanalyser på övergripande nivå genomföras så att styrelsen och stadsledningen har ett underlag för att prioritera vilka säkerhetsåtgärder som det finns behov av för att skydda staden. Det behöver även etableras ett mer systematiskt arbete med informationsklassning och riskanalyser för informationstillgångar där resultatet av sådana kommuniceras till berörda ansvariga för etablering av åtgärder i förhållande till hur skyddsvärd informationen är. Vi konstaterar att de mål och tillhörande handlingsplaner som säkerhetsfunktioner i staden upprättat har identifierat väsentliga förbättringsåtgärder.

Trots den redovisning av åtgärder som gjorts till kommunstyrelsen så uppfattar vi inte att styrelsen har haft en tillräcklig intern kontroll över informationssäkerheten i enlighet med deras övergripande ansvar. Vi ser det som en risk då granskningen visar att arbetet i nuläget är bristfälligt och i behov av en stärkt styrning vilket inte i tillräcklig grad har beaktats av kommunstyrelsen.

Under 2025 väntas nya lagkrav inom området och vi ser det som särskilt väsentligt att styrelsen informerar sig om vad detta innebär för staden. Detta så att erforderliga beslut och förbättringar kan genomföras i syfte att uppnå efterlevnad av cybersäkerhetslagen när den träder i kraft.

Nedan redovisas våra samlade bedömningar av respektive revisionsfråga.

Revisionsfråga	Bedömning
Finns aktuella styrande och vägledande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas?	Delvis
Finns beslutade informationssäkerhetsmål? Finns tillhörande handlingsplaner?	Ja Ja
Finns en ändamålsenlig organisation för informationssäkerhetsarbetet och är den etablerad?	Delvis
Har kommunstyrelsen tillsett att det finns en tillräcklig säkerhetskultur?	Delvis
Finns dokumenterade riskanalyser där informationssäkerhetsrisker beaktats?	Delvis
Har styrelsen under 2024 initierat ärende med bedömning över anpassningsbehov för att uppnå kraven i NIS2?	Nej
Har kommunstyrelsen säkerställt en tillräcklig förmåga att upptäcka och hantera informations- och it-säkerhetsincidenter?	Delvis
Finns en dokumenterad uppföljning av informationssäkerhetsarbetet?	Delvis
Har uppföljningen rapporterats så att styrelsen har tillräckliga underlag för att besluta om åtgärder?	Delvis

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

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen att:

- Besluta om styrande dokument som ska ingå i ett ledningssystem för informationssäkerhet som skapar förutsättningar för en ändamålsenlig styrning och kontroll av informationssäkerhetsarbetet.
- Säkerställa att stadens organisation och funktioner för informationssäkerhetsarbetet är anpassade efter omfattning och behov i enlighet med nuvarande (eller kommande) policys kravställning.
- Säkerställa att det linjebaserade ansvaret för förvaltningschefer, i form av informationsägare, är känt och uppbärs i hela organisationen.
- Utvärdera om det finns behov av kompletterande utbildning inom informationssäkerhet som målgruppsanpassas i förhållande till olika funktioners roller och tillhörande informationshantering.
- Säkerställa tillräckliga riskhanteringsrutiner på både övergripande nivå samt för informationstillgångar i staden och tillse att åtgärder vidtas för att hantera identifierade risker och sårbarheter.
- Fortsatt följa utvecklingen av NIS2-direktivet och den svenska tillämpningen i Cybersäkerhetslagen för anpassning enligt de krav som styrelsen, nämnder och förvaltningarna behöver efterleva.
- Upprätta och etablera stadsövergripande incidenthanteringsrutiner för alla verksamheter att följa. Samt tillse att eskaleringsvägar anges i rutinerna tillsammans med krav om uppföljning och analys av inträffade incidenter för att säkerställa att dessa utgår grund för beslut om förbättringsåtgärder.
- Säkerställa att minst årlig uppföljning av informationssäkerhetsarbetet genomförs och dokumenteras samt rapporteras till ledning och styrelsen.
- Överväga om det finns samordningsvinster med en mer utvecklad koncernsamverkan inom informationssäkerhet samt tillse att goda exempel och erfarenheter tillvaratas från respektive verksamhet oavsett den bedrivs av förvaltningarna eller bolagen.

2 Bakgrund

Helsingborgs stad hanterar stora mängder känslig information och verksamheternas arbete med informationssäkerhet är avgörande för en säker hantering av personuppgifter och verksamhetskritisk information. Det är centralt i en organisation att informationen som hanteras alltid är korrekt, tillgänglig och skyddad från obehörig åtkomst. Informationssäkerhet brukar delas in i två delar: administrativ säkerhet och teknisk säkerhet. Skydd av data förknippas oftast med olika tekniska skydd såsom brandväggar, kryptering och liknande men den administrativa säkerheten är minst lika viktig och avser bland annat avser ändamålsenliga policys, rutiner och instruktioner samt hur anställda ska hantera information och behörigheter i olika it-system.

Kommunfullmäktige har 2009 beslutat om en informationssäkerhetspolicy. Enligt denna så har kommunstyrelsen det övergripande ansvaret för informationssäkerheten. Kommunstyrelsen har också det övergripande ansvaret för att den interna kontrollen fungerar tillfredsställande och för att informationssäkerhetspolicyn årligen granskas och vid behov revideras. Varje nämnd och bolag är ansvarig för informationssäkerheten inom sitt verksamhetsområde.

Brister i arbetet med informationssäkerhet kan bland annat öka riskerna för att information förloras, att känsliga personuppgifter kommer i orätta händer eller att informationens korrekthet inte kan garanteras. Det är därför av vikt att organisationer säkerställer ett systematiskt informationssäkerhetsarbete. Staden anger själva i sin risk-och sårbarhetsanalys för 2023–2026, att ett av de mest prioriterade områdena är att staden behöver säkerställa att informations-och cybersäkerheten utvecklas i takt med de tekniska språng som staden genomgår.

2.1 Inledning

Helsingborgs stad har verksamhet som uppnår kriterierna för att omfattas av NIS-direktivet som tillämpas genom svensk Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Den verksamhet som omfattas tillhörande stadens ansvar är kommunal hälso- och sjukvård. Dricksvattenförsörjning, energi och hamnverksamhet är andra sektorer som omfattas som i staden bedrivs i bolagsform.

Denna granskning har inkluderat bolag som står under lagkraven vilka är: Norra Skånes Vatten och Avlopp AB, Helsingborgs Hamn AB och Öresundskraft AB. Granskningen har även omfattat bolagen Nordvästra Skånes Renhållnings AB samt Helsingborgs Arena och Scen AB vilka inte står under ovan nämnda lagkrav. Detsamma gäller för majoriteten av stadens verksamheter, vilka i nuläget inte omfattas av ovan lagkrav, dock kan andra lagstiftningar som är verksamhetsanknutna ställa vissa krav på informationssäkerhet och sekretesshantering.

I kommande lagförslag föreslås offentlig förvaltning som en sektor som omfattas av ny lagstiftning genom Cybersäkerhetslagen som förväntas träda i kraft 1 januari 2025, se mer i avsnitt 3.5. Nuvarande tolkning av lagförslag är att samtliga verksamheter i staden och flertalet bolag kommer att omfattas av den nya lagstiftningen.

Resultatet av granskningarna har presenterats i separata rapporter för staden respektive bolagen. I denna rapport ges i slutet endast en översiktlig och samlad bild av koncernens nuläge.

2.2 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att översiktligt bedöma om staden har en ändamålsenlig och tillräcklig styrning och kontroll av informationssäkerhetsarbetet.

Granskningen har omfattat följande revisionsfrågor:

- Finns aktuella styrande och vägledande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet och är den etablerad?
- Finns dokumenterade riskanalyser där informationssäkerhetsrisker beaktats?
- Finns beslutade informationssäkerhetsmål och tillhörande handlingsplaner?
- Har styrelsen tillsett att det finns en tillräcklig säkerhetskultur?
- Har styrelsen säkerställt en tillräcklig förmåga att upptäcka och hantera informations- och it-säkerhetsincidenter?
- Finns en dokumenterad uppföljning av informationssäkerhetsarbetet?
- Har uppföljningen rapporterats så att styrelsen har tillräckliga underlag för att besluta om åtgärder?
- Har styrelsen under 2024 initierat ärende med bedömning över anpassningsbehov för att uppnå kraven i NIS2?

Granskningen har avgränsats till kommunstyrelsen.

2.3 Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för granskningens analyser, slutsatser och bedömningar. Dessa är bland annat:

- Kommunallagen (2017:725) - kap 6:6
- MSB:s metodstöd och rekommendationer avseende ledningssystem för informationssäkerhet
- Tillämpbara interna regelverk och policys

För de verksamheter som staden har identifierat som samhällsviktig tjänst utgörs även revisionskriterier enligt nedan:

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet)

- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2021:9) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (NIS-direktivet)
- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster
- Av ansvarig tillsynsmyndighet fastställda föreskrifter inom området

2.4 Metod

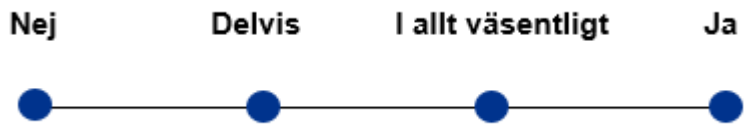
Granskningen har genomförts genom dokumentstudier och intervjuer.

Dokumentstudier har inkluderat reglemente för kommunstyrelsen, informationssäkerhetspolicy, rutiner och mallar samt underlag i form av redovisning av uppdrag, protokollsutdrag, presentationer samt processbeskrivningar.

Intervjuer har genomförts med biträdande stadsdirektör, digitaliseringsdirektör, informationssäkerhetsstrateg samt enhetschef digitaliseringsavdelningen.

Avstämning har genomförts med utvecklingsdirektör och säkerhetschef för genomgång av rapportens iakttagelser och samtidig faktakontroll.

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



Rapporten är faktakontrollerad av berörda intervjupersoner.

3 Resultat av granskningen

3.1 Styrande dokument och strategier

Vi har i granskningen tagit del av Helsingborgs Stads Informationssäkerhetspolicy.[1] Policyn är beslutad av kommunfullmäktige 2009. Policyn beskriver den övergripande styrningen av stadens informationssäkerhet. Bland annat framgår att arbetet ska utgå från relevanta lagar, förordningar, föreskrifter samt egna interna krav och avtal med externa parter. Vi kan konstatera genom dokumentgranskning att policyn i delar hänvisar till föråldrade ramverk men att den i vissa delar går att tillämpa för den övergripande viljeriktningen trots dess ålder.

Av policyn framgår att kommunstyrelsen är ansvarig för att den interna kontrollen av informationssäkerhetsarbetet fungerar samt att policyn granskas årligen och revideras vid behov. Någon revidering har inte gjorts sedan 2012. Intervjuade lyfter att ny policy är ute på remiss vid tid för granskningen och att en förhoppning är att den ska beslutas innan årsskiftet.

Nu gällande policy reglerar att stadsdirektören, på delegation av kommunstyrelsen, fastställer kommunövergripande anvisningar. Vi har i granskningen inte tagit del av några ytterligare styrdokument utöver policyn. Enligt intervjuade saknas dessa och planen är att upprätta riktlinjer efter att policyn beslutats. Vissa rutiner och mallar har vi tagit del av som uppges vara stödjande i olika moment.

Vi har i granskningen delgetts ett uppdrag från kommunfullmäktige[2] till kommunstyrelsen att återkomma med beskrivning av nuläget av den administrativa, beteendemässiga och tekniska säkerheten. Analysen skulle enligt uppdraget leda till att relevanta åtgärder med syfte att bygga en smart och uppkopplad stad med god cybersäkerhetsförmåga skulle vidtas.

I kommunstyrelsens protokoll daterat 7 juni 2021 ingick en återrapportering av uppdraget. I tillhörande tjänsteskrivelse beskrevs nuläget där ett identifierat utvecklingsområde avsåg ledningen och styrningen av informationssäkerhetsarbetet med hänvisning till att policydokument var föråldrade. Dessa uppgavs vara i behov av en grundlig revision för att motsvara aktuell hotbild och de säkerhetsutmaningar som gällde vid tiden. En annan del som det uppgavs finnas behov av var att tydliggöra ambitionsnivå, ansvar och roller. Som nämnts ovan så har ännu inga uppdaterade styrande dokument beslutats.

I kommunstyrelsens protokoll daterat 2024-05-07 redovisas uppdraget avseende stadens arbete med informations- och cybersäkerhet, IT-arkitektur, stadsnät och säkerhetsoperationscenter. I redovisningen saknas uppgift om status för revision av styrande dokument.

Vi har i granskningen fått uppgift om att staden beslutat om Digitala principer. Detta som ett resultat av stadsrevisionens tidigare granskning av stadens digitaliseringsarbete där brister identifierades avseende styrning av arbetet. Intervjuade

[1] Beslutat av kommunfullmäktige 2009-12-16.
[2] Kommunfullmäktige, 18-19 juni 2019, KF § 88

beskriver att principerna även inkluderar vissa krav som berör informationssäkerhet, bland annat ingår principen att skydda personliga integriteten samt principen att beakta informationens skyddsvärde i hela kedjan. Dessa principer lyfts som en avgörande faktor för en hållbar digitalisering där it-miljön kan vara robust och säker. De digitala principerna gäller för hela staden och har beslutats av Digirådet.

3.1.1 Ledningssystem för informationssäkerhet

I tidigare nämnt uppdrag för att stärka stadens informations- och cybersäkerhetsarbete beslutade kommunstyrelsen att:

- uppdra åt avdelningen för strategisk samhällsutveckling att införa ett ledningssystem för informationssäkerhet (LIS).

Vid redovisning av uppdraget till kommunstyrelsen 2024-05-07 framgår att ”*Ett nytt systemstöd (LIS) för att organisera informationssäkerhet och dataskyddsarbetet är infört.*”

I tjänsteskrivelse till ärendet beskrivs att det digitala verktyget avser att bidra med ett enhetligt och systematiskt arbetssätt för riskhantering och kontroll samt även utgöra en gemensam samlingsplats för dokumentation. Systemet har integrerade processer och kravkatalog för att stödja verksamheter att etablera ett systematiskt informationssäkerhetsarbete i enlighet med standarderna ISO27001 och 27002.

Vi har tagit del av exempel från systemet och hur en nämnd påbörjat arbetet med stöd av funktionerna som finns. Merparten av förvaltningarna har påbörjat arbetet i verksamhetssystemet och planen är att samtliga ska nyttja systemet inom kort.

3.1.2 Mål och handlingsplaner

I informationssäkerhetspolicyn anges det övergripande målet med informationssäkerheten vara

”att skapa kontinuitet i verksamheten genom att skydda och säkerställa informationstillgångarna så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt”

Utöver det övergripande målet finns ytterligare fyra mål i policyn med beskrivningar över hur målen ska kunna nås. Dessa mål har brutits ned i konkretiserande aktiviteter som ska genomföras för att nå måluppfyllelse.

Ovan nämnda uppdrag från kommunfullmäktige till kommunstyrelsen resulterade i ett stort antal förslag på prioriterade åtgärder. En av dessa var att upprätta en handlingsplan med prioriterade åtgärder för åren 2021–2023. Planen skulle ange strategiska prioriteringar och aktiviteter i syfte att kontinuerligt öka stadens förmåga på cybersäkerhetsområdet. Vi har inte tagit del av någon sådan handlingsplan.

På uppdrag av stadsledningsförvaltningens tidigare förvaltningschef har representanter för digitaliseringsavdelningen, enheten trygghet och säkerhet och stadsjuridiska enheten tagit fram en handlingsplan för systematiskt säkerhetsarbete 2024. Handlingsplanen är upprättad 2024-03-20 och inkluderar mål, aktiviteter, konsekvenser om arbetet inte genomförs samt behov av resurser för genomförande. Det framgår inte

av handlingsplanen i vilket forum handlingsplanen godkänts eller om den presenterats för kommunstyrelsen.

3.1.3 Bedömning

Vår bedömning är att det delvis finns styrande och vägledande dokument som delvis tydliggör ansvar, krav och hur arbetet ska bedrivas.

Staden har en informationssäkerhetspolicy som beskriver ansvaret och ger övergripande inriktning av informationssäkerhetsarbetet. Den är dock föråldrad och har inte aktualiserats av kommunstyrelsen i enlighet med det ansvar som policyn reglerar, att granska policyn årligen och revidera vid behov. Någon revidering har inte gjorts sedan 2012. Staden följer därmed inte den rekommendation som MSB har avseende att policydokument inom området inte ska vara äldre än tre till fem år. I nuläget saknas reglering av ansvar för it-säkerheten vilket vi rekommenderar att policyn ska inkludera. Enligt uppgift förväntas en ny policy beslutas inom kort.

Det saknas i nuläget kompletterande styrdokument i form av riktlinjer, anvisningar och instruktioner som konkretiserar policyns viljeriktning och krav på hur arbetet ska bedrivas. Vi bedömer att detta skapar en otydlighet i förhållande till den ansvarsfördelning som policyn reglerar och hur målen och de utgångspunkter som nuvarande policy ställer krav på ska uppnås.

Vi ser det som positivt att staden implementerat ett stödsystem med en struktur för ett ledningssystem för informationssäkerhet, LIS. Samtidigt konstaterar vi att grunderna i ett LIS i nuläget saknas i brist på styrande dokument som tydliggjort ledningens viljeriktning med informationssäkerhetsarbetet. Policyn är på en alltför övergripande nivå för att utgöra styrning för hela informationssäkerhetsarbetet för samtliga styrelser och nämnder och därigenom är vår bedömning att stadens LIS behöver kompletteras.

Vi bedömer att det finns beslutade informationssäkerhetsmål samt tillhörande handlingsplaner.

Informationssäkerhetspolicyn innehåller mål med övergripande utgångspunkter för hur dessa ska nås som kan ses som vägledande för arbetet. Det finns en dokumenterad handlingsplan för 2024 med prioriterade åtgärder för att stärka informationssäkerheten.

Vi tolkar därtill att uppdrag från kommunfullmäktige 2019 och efterföljande beslut från kommunstyrelsen till förvaltningen i hög grad kan uppfattas ha utgjort handlingsplan för att stärka informations- och cybersäkerheten fram till nu. Vi kan dock konstatera att det främst är tekniska säkerhetsåtgärder som har verkställts utifrån uppdraget. Det bedöms dock inte vara tillräckligt då vi i vår granskning konstaterar väsentliga brister i den organisatoriska säkerheten, där vi i tidigare bedömning redan konstaterat att det saknas ett ledningssystem och tillräckliga styrdokument för att uppnå ett systematiskt informationssäkerhetsarbete. Vi ser det som väsentligt att kommunstyrelsen tar del av handlingsplanen och tillser en regelbunden uppföljning av densamma för att följa arbetets utveckling.

3.2 Organisation, roller och säkerhetskultur

3.2.1 Ansvarsfördelning

I kommunstyrelsens reglemente[3] framgår som övergripande uppgifter ansvar att leda, utveckla och samordna arbetet med stadens verksamhetsskydd inklusive informationssäkerhet. Samt även ansvar för drift och underhåll av kommunens digitala system och verksamhetssystem.

Informationssäkerhetspolicyn beskriver följande ansvar i organisationen.

- Kommunfullmäktige beslutar om policyn.
- Kommunstyrelsen har det övergripande ansvaret för att den interna kontrollen fungerar tillfredställande.
- Stadsdirektören fastställer, på delegation av kommunstyrelsen, kommunövergripande anvisningar.
- Varje nämnd är ansvarig för informationssäkerheten inom sitt/sina verksamhetsområden.
- Respektive förvaltningschef ansvarar för att informationssäkerhetsarbetet bedrivs i linje med fastställd informationssäkerhetspolicy.
- Chefer på alla nivåer ansvarar för att informationssäkerheten efterlevs enligt gällande policy och anvisningar inom sitt respektive ansvarsområde.
- Varje medarbetare ansvarar för att tillämpa gällande policy och anvisningar samt vara uppmärksam på och rapportera händelser som kan påverka säkerheten.

Samordning av informationssäkerhetsarbetet ska enligt policyn göras inom Stadsledningsförvaltningens enhet för Trygghet och säkerhet. I deras uppgift ingår att utvärdera informationssäkerhetsarbetet, ge råd samt föreslå åtgärder.

I intervju har vi fått beskrivet att det inom avdelningen finns säkerhetsstrateger varav en av dessa har uppgift att samordna och leda informationssäkerhetsarbetet. I intervju beskrivs att nuvarande bemanning inte är tillräcklig för att etablera arbetssätt samt stödja förvaltningarna i deras arbete utifrån de behov som finns. Intervjuade beskriver att beslut har fattats att anställa en CISO[4] som kan ha det stadsövergripande ansvaret för helheten inom informationssäkerhet.

Intervjuade beskriver att Helsingborgs stad har valt att i hög grad integrera informationssäkerhetsarbetet i arbetet med civil beredskap och processerna för Risk- och sårbarhetsanalys och kontinuitetshantering. Sedan fyra år finns ett nätverk för säkerhetssamordnare där samtliga förvaltningar och bolag har representanter med. Enligt muntliga uppgifter diskuteras även informationssäkerhetsfrågor när nätverket träffas.

[3] Beslutat av kommunfullmäktige 2022-10-25, reviderat 2022-11-23
[4] Chief Information Security Officer

Av intervjuer framgår att det linjebaserade ansvaret för informationssäkerhet är känt, men att det varierar hur aktivt informationssäkerhetsarbetet är mellan förvaltningarna. I nuläget saknas dock en samlad bild över nuläget som baseras på uppföljning av arbetet inom respektive förvaltning. Viktiga roller i förvaltningarnas arbete beskrivs av intervjuade vara utsedda informationssäkerhetssamordnare samt att systemförvaltare finns utsedda för alla verksamhetskritiska system.

I de styrande dokumenten framgår inte ansvar för teknisk it-säkerhet. Vi uppfattar dock från intervjuade att digitaliseringsavdelningen har detta ansvar och är en nyckelfunktion i arbetet vad gäller tekniska säkerhetsåtgärder. Av redovisningen till kommunstyrelsen 2024 lyfts tillgång till kompetens som en utmanande faktor. Dels är tjänsten it-säkerhetsansvarig vakant då det är en svårrekryterad kompetens med stor konkurrens. Därtill uppges det finnas behov av kompetens och resurser för att kunna göra analyser och bedömningar av hot och risker med stöd av nya tekniska implementationer som gjorts i enlighet med uppdrag från kommunstyrelsen 2021.

I intervju framkommer att det pågår en organisationsförändring inom digitaliseringsavdelningen som digitaliseringsdirektören initierat. I den nya organisationen ska nya team bildas. En beskrivning av organisationen som vi tagit del av visar att ett dedikerat team ska ansvara för säkerhet och klient. Ett annat team ska ansvara för ekonomi och kvalitet, där ska bland annat uppföljning och kontroll genomföras. En ledningsgrupp ska även formeras där varje team är representerat.

En säkerhetsgrupp har etablerats med representanter från avdelningen för Trygghet och säkerhet, Digitaliseringsavdelningen samt avdelningen för juridik.

3.2.2 Säkerhetsmedvetenhet

I informationssäkerhetspolicyn anges att verksamheten kontinuerligt ska arbeta med att informera och utbilda anställda i informationssäkerhet.

Av underlag vi tagit del av framgår att en grundläggande informationssäkerhets-utbildning finns tillgänglig i stadens lärplattform *Learns*. Det är en utbildning som Myndigheten för samhällsskydd och beredskap tillhandahåller kostnadsfritt som heter DISA. Vi har inte erhållit någon dokumenterad uppföljning av genomförandegraden av DISA i stadens verksamheter men enligt muntliga uppgifter är genomförandegraden låg.

Staden har även kompletterat denna med digital utbildning som skickas via e-post. Av redovisningen till kommunstyrelsen, som vi beskrivit tidigare i rapporten, framgår att stadens samtliga medarbetare sedan 2022 genomfört utbildning i cybersäkerhet med fokus på att göra medarbetarna medvetna kring risker. Utbildningen är indelad i olika teman där uppföljning kan göras på varje temaområde.

Av material som vi tagit del av kring utbildningen framgår att det finns möjlighet att få uppföljning per förvaltning, vilken ombesörjs av säkerhetsstrateg. I presentation av uppföljning av alla som fått utskick från oktober 2024 framgår att olika många anställda i staden varit mottagare av de olika modulerna. Av de som erhållit utskick så har modulerna genomförts av som lägst 66 % av mottagarna och som högst av 92 % av mottagarna. I genomsnitt är genomförandegraden (oaktat antal mottagare) 78 %.

En del i utbildningen har varit olika simuleringar av fejkade mejl vilket varit ett sätt att kombinera utbildning med tester. Detta i syfte att medvetandegöra användare på sådana hot eller risker som skulle kunna användas av hotaktörer. Uppföljning över hur många som ”klickat” och därmed inte identifierat risken eller att det kunde varit ett potentiellt hot har minskat med tiden som utbildningen och testerna genomförts. Den senaste månaden klickade 2,8 % av mottagarna av de 26371 fejkade mejl som skickades. Motsvarande uppföljning totalt för de senaste två åren visar på en klickfrekvens om 3,7 %.

3.2.3 Bedömning

Vår bedömning är att det delvis finns en ändamålsenlig och etablerad organisation för informationssäkerhetsarbetet.

Vi bedömer att den dokumenterade ansvarsfördelning som finns i policyn är känd och delvis etablerad i organisationen. I nuläget regleras inte digitaliseringsavdelningens ansvar i informationssäkerhetsarbetet varpå vi rekommenderar att detta dokumenteras.

Vi ser en risk att nuvarande funktioner och resurser i arbetet inte är anpassad efter de behov och den omfattning som staden har i sitt informationssäkerhetsarbete. Detta blir särskilt väsentligt att utvärdera i förhållande till förväntade krav i ny lagstiftning inom området som förväntas träda i kraft under 2025.

Vi bedömer att styrelsen delvis tillsett en tillräcklig säkerhetskultur.

Vi baserar vår bedömning på att utbildningar inom informationssäkerhet har genomförts och även följts upp. Vi kan konstatera att genomförandegraden är alltför låg för vissa utbildningar medan andra har en högre genomförandegrad där även förbättring i medvetenhet och kunskap kan noteras.

Mot bakgrund av att staden inom kort kan stå för nya lagkrav genom Cybersäkerhetslagen ser vi det som väsentligt att utvärdera om det finns ytterligare behov av målgruppsanpassade utbildningar i förhållande till de informationstillgångar som hanteras inom stadens olika verksamheter. Det är även av vikt att beakta behov hos förtroendevalda som också hanterar information och är användare i stadens it-miljö.

3.3 Riskhantering informationssäkerhet

3.3.1 Kommunövergripande riskhantering

Av policyn framgår att riskanalyser (innefattande hot- och sårbarhetsanalyser) ska genomföras regelbundet för kritiska kommunala funktioner (tjänster).

Av den senaste Risk-och sårbarhetsanalysen (RSA) för Helsingborgs Stad för åren 2023–2026 kan vi notera att den i hög grad har inkluderat risker inom området. Utifrån identifierade risker har även en bedömning gjorts att stadens samhällsviktiga verksamheter har ett kritiskt beroende till it och informationssystem.

Resultatet av risk- och sårbarhetsanalysen visade att staden har behov av att prioritera åtgärder kopplat till:

- informations- och cybersäkerhet samt säkerhets- och verksamhetsskydd
- elektroniska kommunikationer och redundant samband
- kontinuitetshantering

Intervjuade uppger att staden behöver utveckla arbetet med riskhantering. I det stödsystem som implementeras för informationssäkerhet så finns visst stöd för riskanalyser och riskhantering men arbetet har inte kommit i gång vid tid för granskningen. Baserat på intervjuer konstaterar vi att det inte genomförts någon kommunövergripande riskanalys specifikt för informationssäkerhetsrisker som ett sätt att avgöra vilka säkerhetsåtgärder som staden har behov av.

Som beskrivits tidigare så har staden gjort ett strategiskt val att inkludera informationssäkerhetsarbetet inom ramen för processerna kopplat till civil beredskap och framhåller därigenom att de uppfattar att stadens risk- och sårbarhetsanalys på ett heltäckande sätt beaktar informationssäkerhetsriskerna.

3.3.2 Informationsklassning och riskanalyser för stadens informationstillgångar

Informationssäkerhetspolicyn reglerar att stadens informationstillgångar fortlöpande identifieras, klassificeras och relevanta hot värderas och hanteras.

Vi har fått muntliga uppgifter om att informationsklassning och riskanalyser har genomförts. Vi har även tagit del av stödjande mallar och instruktion för genomförandet av dessa aktiviteter.

Vi har dock inte erhållit underlag som visar hur stor andel av stadens informationstillgångar som i nuläget har klassats och riskanalyserats. Intervjuade uppger en uppskattning att ca 40–50 % av tillgångarna är klassade. Detta görs numer i stödsystemet för informationssäkerhet vilket ses som positivt då material och underlag finns samlat och även kan följas upp. De bedömningar som görs kan användas både internt för kravställning av säkerhetsåtgärder men även i relation till externa leverantörer.

Det har dock framkommit att resultatet av genomförda analyser inte kommuniceras till digitaliseringsavdelningen, varpå de inte har några underlag för att anpassa de tekniska säkerhetsåtgärderna i förhållande till hur skyddsvärd informationen är som

hanteras i stadens olika system. Funktioner på digitaliseringsavdelningen har inte heller behörighet och åtkomst till de informationsklassningar och riskanalyser som förvaltningarna dokumenterad i stödsystemet. Detta uppges bero på att åtkomsthanteringen inte medger tillgång till andras uppgifter.

3.3.3 Bedömning

Vår bedömning är att det delvis finns dokumenterade riskanalyser som beaktar informationssäkerhetsrisker.

Vi baserar vår bedömning på att informationssäkerhetsrisker beaktas i stadens övergripande risk- och sårbarhetsanalys 2023–2026 vilket vi ser som positivt. Vanligen är denna riskbedömning på en övergripande nivå och vi anser därför att denna bör kompletteras med en stadsövergripande riskanalys som beskriver de informationssäkerhetsrisker som staden skulle kunna utsättas för.

Det är därtill väsentligt att informationsklassning och riskanalyser genomförs för samtliga verksamhetskritiska informationstillgångar samt att resultatet kommuniceras eller delges ansvariga för de olika säkerhetsåtgärderna (organisatoriska, tekniska, personrelaterade samt fysiska) så att dessa kan vidtas för att skydda tillgångarna.

Utan dessa bedömningar finns risk för att vissa informationstillgångar har bristande skydd som utgör sårbarhet för staden eller att vissa informationstillgångar har för högt skydd vilket skulle kunna vara kostnadsdrivande.

3.4 NIS2-direktivet, ny lagstiftning inom området

3.4.1 Cybersäkerhetslagen förväntas träda i kraft under 2025

Medlemsländer i EU, däribland Sverige, har sedan 2018 haft EU-direktivet NIS[5] att följa. Den svenska tillämpningen av direktivet regleras i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Direktivet syftade till att öka säkerheten i nätverk och informationssystem inom samhällsviktiga verksamheter, där konsekvenser vid it-bortfall skulle kunna leda till allvarliga konsekvenser med samhällsstörningar som följd. I den lagstiftning som gällt sedan 2019 fanns endast sju sektorer som omfattades av kraven. NSR AB har inte verksamhet som omfattats av NIS-regleringen.

2022 beslutade EU-parlamentet om ett nytt direktiv, benämnt NIS2, med förstärkta krav och en utökning av verksamheter och sektorer som ska omfattas av lagen för att ytterligare stärka säkerheten och även samordningen inom området. I Sverige har en utredning på uppdrag av regeringen genomförts som ska ligga till grund för nytt lagförslag i form av Cybersäkerhetslagen. Lagen förväntas träda i kraft under 2025.

Av utredning och lagförslag framgår ett antal förändringar mot det första NIS-direktivet, exempelvis de nedan som Sveriges kommuner och regioner, SKR, lyfter som väsentliga för kommuner och kommunala bolag:

[5] NIS står för ”The Directive on Security of Network and Information Systems”

- NIS2 ställer tydligare krav på riskanalyser och säkerhetskrav, men också på ledningens deltagande i cybersäkerhetsarbetet.
- NIS2 innebär också att hela verksamheten kommer att omfattas av lagstiftningen.
- NIS2 omfattar betydligt fler aktörer än nuvarande lagstiftning (NIS), antalet sektorer ökar från sju till 18.
- En av de nya sektorerna är offentlig förvaltning, vilket innebär att kommuner och regioner kommer att omfattas av lagstiftningen.
- NIS2 innebär också att en administrativ sanktionsavgift införs, för offentlig förvaltning föreslås den ligga på minst 5.000 kr och som mest 10. 000 000 kr.

Vi har i granskningen haft i uppdrag att efterfråga och bedöma om bolaget har genomfört analys eller annan bedömning över hur nuvarande informationssäkerhet står sig i relation till de förväntade förstärkta kraven. Detta som ett sätt, att i tid innan lagen träder i kraft, ha förutsättningar att vidta åtgärder om det finns områden där bolaget identifierar förbättringsbehov utifrån stärkta krav.

Vi har i de underlag vi tagit del av i granskningen inte kunnat identifiera något ärende eller uppdrag från styrelsen om anpassningar eller analyser i förhållande till förstärkta krav och ny lagstiftning inom informationssäkerhet. I redovisning av uppdrag från stadsledningsförvaltningen till kommunstyrelsen 2024 ingick dock information till styrelsen att ”*ytterligare arbete kommer att krävas för att höja säkerhetsnivån och för att följa den nya cybersäkerhetslagen som träder i kraft 1 januari 2025. Den nya cybersäkerhetslagen kommer innebära avsevärt högre krav för det kommunala informationssäkerhetsarbetet”.*

Kommunstyrelses beslut var att godkänna redovisningen. Inga beslut om uppdrag eller åtgärder fattades enligt protokollsutdraget.

I tidigare nämnd handlingsplan finns beskrivning om krav på anpassningar för att möta nya lagkrav. Intervjuade uppger även att det inom digitaliseringsavdelningen har påbörjats vissa analyser i syfte att kartlägga nya krav och behov utifrån lagförslaget.

3.4.2 Bedömning

Vi bedömer att styrelsen inte initierat ärende med bedömning över anpassningsbehov för att uppnå kraven i NIS2-direktivet.

Vi kan dock se av återrapporterat uppdrag till kommunstyrelsen att tjänstepersoner informerat styrelsen om att det kommer innebära nya förutsättningar och krav på stadens arbete. Det har även tagits andra initiativ och finns dokumenterat som prioriterad åtgärd i handlingsplan 2024 som upprättats av tjänstepersoner inom stadsledningsförvaltningen.

Vi ser det som väsentligt att kommunstyrelsen tillser att de när den svenska lagstiftningen beslutats får information om de nya kraven och på vilka sätt styrelsen och staden i stort påverkas av dessa.

3.5 Incidenthanteringsrutiner

Av föreskrift (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster går att utläsa att en leverantör ska ha interna regler och arbetssätt för att kunna upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser. Därtill ska leverantören efter avslutad incidenthantering identifiera grundorsaker till att incidenter och avvikelser inträffat samt vidta åtgärder för att förhindra att liknande incidenter och avvikelser inträffar på nytt.

3.5.1 Rutiner och arbetssätt för att hantera incidenter inom staden

För att inte exponera staden för it-säkerhetsrisker har vi valt att inte ge någon ingående beskrivning av funktioner och it-säkerhetsåtgärder som implementerats i syfte att stärka stadens förmåga att avvärja intrångsförsök och andra cyberhot.

I tidigare beskriven redovisning av uppdrag för att stärka informationssäkerhetsarbetet i staden så framgår flertalet tekniska förstärkningar varav flera av dessa berör incidenthantering och stadens förmåga att upptäcka och hantera sådana. Av de åtgärder som återrapporteras så har staden gjort förstärkningar både i infrastruktur, som servrar och nätverk, men även tekniska verktyg för övervakning av säkerhetshändelser. Intervjuade beskriver att de investeringar som kommunstyrelsen gett förutsättningar för att vidta genom resursförstärkningar, inneburit väsentlig skillnad i robusthet och säkerhet. Antal störningar och incidenter har kraftigt minskat sedan nya implementeringar.

Utifrån intervjuer får vi bild av att staden har flera väsentliga funktioner på plats, och att it-säkerhetsåtgärder implementerats i avsikt att leva upp till NIS-direktivet och kommande Cybersäkerhetslag avseende de tekniska säkerhetsåtgärderna som kravställs.

Vi har även tagit del av det kravbibliotek som ingår i det nya stödsystemet som är implementerat, vilket inkluderar bedömningar av de säkerhetsåtgärder som ingår utifrån lagkrav och föreskrifter. Vi ser därför att det finns underlag för att anpassa kommande behov av åtgärder, om verksamheterna i högre grad genomför informationsklassningar och även hittar vägar att kommunicera detta till ansvariga på digitaliseringsavdelningen.

Gällande hanteringen av inträffade incidenter uppger intervjuade att staden har dokumenterade rutiner. Vi har i granskningen tagit del av de rutiner som digitaliseringsavdelningen utgår från i sin incidenthantering. Dessa baseras på allvarlighetsgrad för incidenter där olika angreppssätt följer som baseras på en initial bedömning över hur allvarlig incidenten är.

Denna bedömning ska enligt uppgift göras av servicedesk som är mottagare vid anmälan. Incidentrapporter skrivs av utsedd incident manager. De interna rutinerna som digitaliseringsavdelningen utgår från i incidenthanteringen uppges väl förankrade och tydliga.

Däremot så framkommer i intervjuer att det inte är lika tydligt hur incidenter ska eskaleras vidare från digitaliseringsavdelningen när behov av det finns. Som exempel lyfts att det inneburit att eskalering skett brett för att inte riskera att någon mottagare

missas. Det saknas även eskaleringsvägar till andra berörda funktioner inom SLF, exempelvis säkerhetschef, säkerhetsstrateg eller stadsdirektör/biträdande stadsdirektör. I slutfasen av granskningen inkom uppgifter att nuvarande incidenthanteringsrutiner hade tydliggjorts vad gäller rapportering av personuppgiftsincident samt rapportering till informationssäkerhetsfunktionen.

Det uppges därtill finnas vissa otydligheter när eskalering ska hanteras inom stadsledningsförvaltningens interna krisledning eller när den stadsövergripande krisledningen ska aktiveras.

Enligt uppgift sker endast en analys och genomgång av inträffade incidenter om det skett en större incident där krisledningsgruppen varit aktiverad.

3.5.2 Bedömning

Vi bedömer att styrelsen delvis säkerställt en tillräcklig förmåga att upptäcka och hantera informations- och it-säkerhetsincidenter.

Vår bedömning baseras på att kommunstyrelsen gett förvaltningen i uppdrag att vidta åtgärder i syfte att säkerställa stadens förmåga och it-säkerhet. Åtgärderna följer i stora delar de rekommendationer som anges av regulatoriska ramverk som är aktuella för staden och vi bedömer att staden i ett tekniskt perspektiv har skyddsmekanismer på plats.

För att ytterligare stärka hanteringen vid incidenter ser vi behov av stadsövergripande incidenthanteringsrutiner som är beslutade och kommunicerade som tydligt beskriver ansvar och eskaleringsvägar för it- och informationssäkerhetsincidenter. Eskaleringsvägar bör tydliggöras dels inom stadsledningsförvaltningen, i förhållande till andra förvaltningar, dels i relation till myndigheter där lagkrav finns på rapportering inom vissa tidsramar. Det är därtill väsentligt att inträffade incidenter analyseras och utgör en del i förbättringsarbetet där åtgärder vidtas för att minimera risken att liknande incidenter inträffar på nytt.

3.6 Uppföljning och rapportering

De uppdrag som kommunstyrelsen beslutat om till förvaltningen har återrapporterats vid flera tillfällen. Vid denna information har en samlad bild av vidtagna åtgärder i syfte att förbättra informationssäkerheten avlämnats.

Vi har därtill tagit del av underlag i form av nulägesbeskrivning och önskad målbild inom informationssäkerhetsarbetet som enligt intervjuade har presenterats till stadsdirektör och ytterligare tre direktörer i staden.

Det saknas i dock i nuläget en samlad uppföljning som beskriver stadens informations-säkerhetsarbete. I avsaknad av samlad uppföljning av arbetet har aktiviteten ”Ledningens genomgång” eller motsvarande inte genomförts, med undantag för ovan information.

3.6.1 Rapportering

Vi kan genom protokollsgranskning bekräfta att rapportering utifrån lämnat uppdrag till förvaltningen avseende stadens arbete med informations- och cybersäkerhet, IT-arkitektur, stadsnät och säkerhetsoperationscenter har gjorts till kommunstyrelsen. Som vi skrivit tidigare så beslutade kommunstyrelsen att godkänna redovisningen. Beslutet har inte följts av några ytterligare uppdrag eller åtgärder för att utveckla informationssäkerhetsarbetet.

3.6.2 Bedömning

Vi bedömer att det delvis finns en dokumenterad uppföljning av informationssäkerhetsarbetet och att rapportering delvis har gjorts.

Vi konstaterar att det finns dokumenterade underlag som påtalar att det finns brister och behov av förbättringar i stadens informationssäkerhetsarbete. Bland annat genom återrapportering av de uppdrag som kommunstyrelsen gett till förvaltningen som återrapporterats under året.

Det har dock inte gjorts någon årlig uppföljning i samlad form och den rapportering som gjorts till styrelsen har inte avsett utvärdering av informationssäkerhetsarbetet i förhållande till interna eller externa krav. Då vi i granskningen identifierat ett antal brister avseende stadens arbete för att uppnå ett systematiskt informationssäkerhetsarbete bedömer vi att kommunstyrelsen hade haft behov av kompletterande uppföljning för att få en helhetsbild.

Vi anser att det är av vikt att arbetet med informationssäkerhet följs upp minst årligen samt att det finns en tydlig struktur för löpande återrapportering till både ledning och styrelsen. Insikt i arbetet ger underlag för att ytterligare besluta om nödvändiga åtgärder för att stärka stadens informationssäkerhet om behov av detta identifieras. Detta i syfte att skydda staden mot risker, både interna vid bristande informationshantering eller i form av cyberhot, vilket kan utsätta staden för både ekonomisk skada och förtroendeskada om information förstörs eller röjs till obehöriga.

3.7 Informationssäkerhet i de kommunala bolagen i koncernen

Som beskrivits i inledningen så har stadsrevisionen uppdragit till KPMG att göra granskning av informationssäkerheten i Helsingborgs stad och utvalda bolag i koncernen. De bolag som ingår i avgränsningen har varit Nordvästra Skånes Vatten och Avlopp AB, Helsingborgs Hamn AB, Öresundskraft AB, Nordvästra Skånes Renhållnings AB och Helsingborg Arena och Scen AB.

I granskningen inkluderas inte moderbolaget Helsingborgs Stads Förvaltning AB avseende eget informationssäkerhetsarbete. Utifrån beslutat ägardirektiv kan vi inte heller se att moderbolaget har något ansvar eller uppgift för att samordna eller följa upp dotterbolagens informationssäkerhetsarbete. Däremot framgår av ägardirektivet att moderbolaget ska säkerställa bolagens efterlevnad av och samverkan inom civil beredskap. Vi kan utifrån det se att även informationssäkerhet kan beröras då den stadsövergripande risk- och sårbarhetsanalysen med tillhörande kontinuitetsplanering identifierat kritiska beroenden till it och informationssystem samt risker inom området.

Flertalet bolag bedriver även samhällsviktig verksamhet där övriga verksamheter har ett mycket stort kritiskt beroende av dessa, exempelvis el, dricksvatten och avlopp.

Genom vår dokumentgranskning och våra genomförda intervjuer så får vi bilden att det i nuläget saknas etablerad struktur för koncernsamverkan gällande informationssäkerhet. Intervjuade från bolagen uppger att staden respektive varje bolag bedriver informationssäkerhetsarbetet var för sig. Däremot framhålls i intervjuer att det finns ett nätverk för säkerhetsarbetet, vilket nämnts tidigare i rapporten, där både förvaltningar och bolag är representerade. Dock råder delade meningar i hur hög utsträckning informationssäkerhet diskuteras inom ramen för nätverket.

Den samverkan som i nuläget har identifierats är Helsingborg Arena och Scen AB som har avtal med stadens digitaliseringsavdelning som leverantör av it-tjänster där de tekniska aspekterna omhändertas samt även att de i vissa frågor har en samordning med stadens strateg med ansvar för informationssäkerhetsfrågor.

Resultatet av respektive bolags granskningar presenteras i separata rapporter och vi ger nedan en översiktlig summering av våra iakttagelser från granskningarna.

- Intervjuade beskriver även att ägardialogen i mars 2024 med samtliga bolag hade följande tema som diskuterades: *Specifika händelser i omvärlden/säkerhetsläget med påverkan för verksamheten – specifikt bolagets förmåga att hantera insideraktiviteter, incidenter inom cybersäkerhet och IT-säkerhet*
- Staden som ägare har varken i bolagsstyrningsdokumentet eller ägardirektiv beslutat om krav på bolagens informationssäkerhetsarbete.
- De bolag som står under NIS-direktivets krav har ett mer systematiskt informationssäkerhetsarbete än övriga bolag och vi vill särskilt framhålla goda riskhanteringsrutiner med etablerade processer för att fånga risker på olika nivåer.
- Flera av bolagen har beslutat om policy och tillhörande riktlinjer och rutiner för det arbete som kravställs. Vi har i granskningarna gjort bedömningen att styrande dokument för de flesta revisionsobjekten är i behov av vissa justeringar och tydliggöranden.
- Styrelserna är i alltför låg utsträckning involverade i styrning och uppföljning med undantag för styrelsen i Öresundskraft AB. Det blir väsentligt att se över detta i förhållande till att nya lagkrav förväntas ställa högre krav på styrelsernas involvering i informationssäkerhetsfrågorna.
- De flesta styrelserna har erhållit information från bolagets företrädare om nya lagkrav utifrån NIS2-direktivet. Endast ett fåtal av styrelserna har själva initierat ärende för att få information om anpassning av arbetet eller behov av åtgärder i förhållande till ny lagstiftning. Från verksamheterna har vissa analyser och bedömningar påbörjats samt även i vissa fall anpassningar av tekniska åtgärder.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att översiktligt bedöma om Helsingborgs stad har en ändamålsenlig och tillräcklig styrning och kontroll av informationssäkerhetsarbetet.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen delvis har en ändamålsenlig styrning och kontroll av informationssäkerhetsarbetet.

Utifrån våra iakttagelser och bedömningar rekommenderar vi kommunstyrelsen att:

- Besluta om styrande dokument som ska ingå i ett ledningssystem för informationssäkerhet som skapar förutsättningar för en ändamålsenlig styrning och kontroll av informationssäkerhetsarbetet.
- Säkerställa att stadens organisation och funktioner för informationssäkerhetsarbetet är anpassade efter omfattning och behov i enlighet med nuvarande (eller kommande) policys kravställning.
- Säkerställa att det linjebaserade ansvaret för förvaltningschefer, i form av informationsägare, är känt och uppbärs i hela organisationen.
- Utvärdera om det finns behov av kompletterande utbildning inom informationssäkerhet som målgruppsanpassas i förhållande till olika funktioners roller och tillhörande informationshantering.
- Säkerställa tillräckliga riskhanteringsrutiner på både övergripande nivå samt för informationstillgångar i staden och tillse att åtgärder vidtas för att hantera identifierade risker och sårbarheter.
- Fortsatt följa utvecklingen av NIS2-direktivet och den svenska tillämpningen i Cybersäkerhetslagen för anpassning enligt de krav som styrelsen, nämnder och förvaltningarna behöver efterleva.
- Upprätta och etablera stadsövergripande incidenthanteringsrutiner för alla verksamheter att följa. Samt tillse att eskaleringsvägar anges i rutinerna tillsammans med krav om uppföljning och analys av inträffade incidenter för att säkerställa att dessa utgår grund för beslut om förbättringsåtgärder.
- Säkerställa att minst årlig uppföljning av informationssäkerhetsarbetet genomförs och dokumenteras samt rapporteras till ledning och styrelsen.
- Överväga om det finns samordningsvinster med en mer utvecklad koncernsamverkan inom informationssäkerhet samt tillse att goda exempel och erfarenheter tillvaratas från respektive verksamhet oavsett den bedrivs av förvaltningarna eller bolagen.

Datum som ovan

KPMG AB