Granskning av informationssäkerhet

Rapport

Leksands kommun och Leksandsbostäder AB

KPMG AB

2024-03-27

Antal sidor 25

Antal bilagor 1

Leksands kommun och Leksandsbostäder AB
Granskning av informationssäkerhet

2024-03-27

Innehållsförteckning

1 Sammanfattning

KPMG har av Leksands kommuns revisorer samt lekmannarevisorer i Leksandsbostäder AB fått i uppdrag att granska kommunens och bolagets informationssäkerhetsarbete.

Syftet med granskningen har varit att bedöma om kommunstyrelsen och bolagsstyrelsen säkerställt att det finns ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen och bolagsstyrelsen delvis säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Kommunstyrelsen har antagit en principiell grund med mål och inriktning för ett systematiskt informationssäkerhetsarbete. Vi bedömer att det finns en organisatorisk struktur för arbetet, men vi ser en risk i att organisationen inte motsvarar den kravbild som anges av de styrande dokumenten, och som är nödvändig för att kunna möta aktuella cyberhot och risker. Kommunen uttrycker ambitioner om att likrikta informationssäkerhetsarbetet ytterligare. Vi vill understryka betydelsen att arbetet i dag är personbundet i stora delar, enligt vår bedömning.

Vi ser även ett behov av att bolagsstyrelsen säkerställer att Leksandsbostäder AB:s organisation för informationssäkerhet är ändamålsenlig. Bolaget har antagit kommunens styrande dokument för informationssäkerhet, och omfattas därigenom av samma kravbild. För att upprätthålla ett systematiskt informationssäkerhetsarbete är det av vikt att organisationen är tillräcklig för att motsvara omfattningen på arbetet.

I det följande redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Revisionsfråga	**Bedömning: Delvis (Kommunen)** **Bedömning: Delvis (Bolaget)**	**Rekommendationer**
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ska ställas och hur arbetet ska bedrivas?	Vår bedömning är att kommunstyrelsen delvis säkerställt att det finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas. Leksandsbostäder AB har antagit kommunens informationssäkerhetspolicy och styrande dokument.	**Kommunstyrelsen** Tillse att ansvar för nyckelfunktioner avseende informationssäkerhetsarbetet harmoniserar i styrande dokument. Säkerställa att linjeansvaret för informationssäkerhet är etablerat. Utvärdera om informationssäkerhetssamordnarens tjänsteutrymme är tillräckligt för att motsvara behov och kravställd säkerhetsnivå.

		Utvärdera om verksamheternas organisering för informationssäkerhetsarbete är tillräckligt för att motsvara kravställd säkerhetsnivå. **Bolagsstyrelsen** Utvärdera om bolagets organisering för informationssäkerhetsarbete är tillräckligt för att motsvara ett ändamålsenligt informationssäkerhetsarbete.
Revisionsfråga	**Bedömning: Nej (Kommunen)** **Bedömning: Nej (Bolaget)**	**Rekommendationer**
Finns ett systematiskt arbete med riskanalyser och informationsklassning och vidtas säkerhetsåtgärder som ett resultat av dessa bedömningar?	Vår bedömning är att arbetet med riskanalyser inte är systematiskt, men att arbetet med informationsklassningar är systematiskt. Det gäller såväl kommunen som Leksandsbostäder AB. Vår bedömning är att it-säkerhetsåtgärder inte vidtagits som ett resultat av riskanalys och informationsklassningar.	**Kommunstyrelsen** Säkerställa att riskanalys genomförs för kommunens samlade it-miljö. Säkerställa att it-säkerhetsåtgärder vidtas utifrån genomförda riskanalyser och informationsklassningar. **Bolagsstyrelsen** Säkerställa att riskanalys genomförs där informationssäkerhetsrisker beaktas och följs av åtgärder.
Revisionsfråga	**Bedömning: Nej (Kommunen)** **Bedömning: Nej (Bolaget)**	**Rekommendationer**
Har särskilda riskanalyser genomförts för informationstillgångar inom sociala sektorn, exempelvis vid nyttjandet av välfärdsteknik?	Riskanalys med avseende på informationstillgångar har inte genomförts för den välfärdsteknik som används.	Säkerställa att riskanalyser genomförs för välfärdsteknik.

Revisionsfråga	**Bedömning: Delvis (Kommunen)** **Bedömning: Delvis (Bolaget)**	**Rekommendationer**
Har styrelser tillsett att det finns en tillräcklig säkerhetskultur?	Vår bedömning är att kommunstyrelsen och bolagsstyrelsen delvis har tillsett att det finns en tillräcklig säkerhetskultur.	**Kommunstyrelsen** Följa upp deltagande i informationssäkerhetsutbildningar för att säkerställa deltagandet bland medarbetare och förtroendevalda Tillse fördjupad utbildning inom informationssäkerhet för berörda funktioner.
Revisionsfråga	**Bedömning: Ja (Kommunen)** **Bedömning: Ja (Bolaget)**	**Rekommendationer**
Finns etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljö?	Vår bedömning är att det finns en etablerad övervakning för att upptäcka hot om intrång och andra säkerhetsincidenter i it-miljön.	Ingen lämnad rekommendation.
Revisionsfråga	**Bedömning: Ja (Kommunen)** **Bedömning: Ja (Bolaget)**	**Rekommendationer**
Finns etablerade incidenthanteringsrutiner och inkluderar dessa uppföljning av inträffade incidenter?	Vår bedömning är att det finns etablerade incidenthanteringsrutiner och att dessa inkluderar uppföljning av inträffade incidenter.	**Kommunstyrelsen** Inkludera eskaleringsvägar till andra parter, exempelvis bolag som har tjänster från kommunen, i incidenthanteringsrutinen. Förtydliga hur externa leverantörer omfattas av incidenthanteringsrutinerna. **Bolagsstyrelsen** Säkerställa en incidenthanteringsrutin.

Revisionsfråga	Bedömning: I allt väsentligt (Kommunen) Bedömning: Nej (Bolaget)	Rekommendationer
Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelsen med regelbundenhet?	Vår bedömning är att det i allt väsentligt finns en etablerad uppföljning av arbetet som rapporteras till kommunstyrelsen med regelbundenhet. Vår bedömning är att det inte finns en etablerad uppföljning av informations-säkerhetsarbetet som rapporteras till bolagsstyrelsen med regelbundenhet.	**Bolagsstyrelsen** Tillse uppföljning av bolagets informationssäkerhetsarbete.

2 Bakgrund

KPMG har av Leksands kommuns förtroendevalda revisorer samt lekmannarevisorer i Leksandsbostäder AB fått i uppdrag att genomföra en granskning av kommunens och bolagets informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2023.

På uppdrag av revisorerna genomförde KPMG under 2020 en förstudie av informationssäkerhetsarbetet i kommunen. Förstudien visade att det fanns risk för att arbetet inte nådde den grad av systematik som krävs för att säkerheten ska vara tillräcklig. Bland annat saknades tydliggörande riktlinjer, utbildning hade inte genomförts samt att informationsklassning och riskbedömning inte genomförts i tillräcklig grad så att säkerhetsåtgärder kunnat vidtas för att skydda den information som hanterades.

Under 2021 genomfördes på uppdrag av lekmannarevisorerna en förstudie av Leksandsbostäder AB:s informationssäkerhets- och dataskyddsarbete. Förstudien visade att det fanns behov av förbättringar avseende styrning, ansvar och att etablera utbildning och kunskap i syfte att förhindra att incidenter sker. Granskaren rekommenderade att en fördjupad granskning skulle genomföras inom två år för att följa upp att förbättringsåtgärder vidtagits.

Sedan förstudierna genomfördes har behov av ett systematiskt och riskbaserat arbete ökat då omvärldsläge med höjd beredskap innebär en ökad risk för angrepp i form av cyberhot och intrång. Därtill så har den digitalisering som pågår i offentliga verksamheter lett till att alltmer information hanteras digitalt och verksamheter är beroende av fungerande informations- och kommunikationsteknik för att upprätthålla verksamheters kontinuitet.

Utvecklingen och den förändrade användningen av ny teknik innebär också att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för kommunen och kommunala bolag.

Det är således väsentligt att kommunen och bolag bedriver ett systematiskt och ändamålsenligt informationssäkerhetsarbete där hot och risker analyseras löpande. Med anledning av ovanstående drar kommunens revisorer och lekmannarevisorer slutsatsen i sin riskanalys, att arbetet med informationssäkerhet behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen syftar till att bedöma om kommunstyrelsen och bolagsstyrelsen säkerställt att det finns ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Granskningen har omfattat följande revisionsfrågor:

— Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?

— Finns ett systematiskt arbete med riskanalyser och informationsklassning och vidtas säkerhetsåtgärder som ett resultat av dessa bedömningar?

— Har särskilda riskanalyser genomförts för informationstillgångar inom sociala sektorn, exempelvis vid nyttjade av välfärdsteknik?

— Har styrelser tillsett att det finns en tillräcklig säkerhetskultur?

— Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljö?

— Finns etablerade incidenthanteringsrutiner och inkluderar dessa uppföljning av inträffade incidenter?

— Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelserna med regelbundenhet?

2.2 Avgränsning

Granskningen omfattar en granskning av kommunstyrelsens övergripande ansvar för informationssäkerhet samt ansvar för de informationstillgångar som hanteras i verksamheterna.

Granskningen omfattar en granskning av bolagsstyrelsens övergripande ansvar för informationssäkerhet samt ansvar för de informationstillgångar som hanteras i verksamheten.

Granskningen omfattar både administrativ säkerhet och tekniska säkerhetsåtgärder.

Granskningen avgränsas till revisionsfrågorna. För revisionsfrågan ”Har särskilda riskanalyser genomförts för informationstillgångar inom sociala sektorn, exempelvis vid nyttjade av välfärdsteknik?” avgränsas välfärdsteknik till att omfatta tillsynskameror, läkemedelsautomater och kommunikationsverktyg etc. Trygghetslarm omfattas inte.

2.3 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

— Kommunallagens 6 kap. 6 § (Kommunstyrelsen)

— Kommunallagen 6 kap. 6 § (Leksandbostäder AB)

— Tillämpbara interna regelverk, policys och beslut

— MSB:s metodstöd och rekommendationer avseende Ledningssystem för informationssäkerhet och it-säkerhetsåtgärder

— Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där detta är tillämpbart

2.4 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

- Informationssäkerhetspolicy
- Riktlinjer för informationssäkerhet i Leksands kommun
- Rutiner för hantering av informationssäkerhetsincidenter

Intervjuer har genomförts med:

- It-chef
- It-säkerhetsansvarig
- Kommundirektör
- Informationssäkerhetssamordnare
- VD – Leksandbostäder
- Ordförande – Leksandbostäder
- Vice ordförande – Leksandsbostäder
- Kommunstyrelsens presidium
- Sektorchef - *Samhällsutveckling*
- Sektorchef - *Utbildningssektorn*
- Sektorchef – *Sociala sektorn*
- Systemförvaltare
- Systemförvaltare
- Systemförvaltare
- Pedagogisk utvecklingsledare och lärare
- Verksamhetschef hälso- och sjukvård

Samtliga intervjuade har getts möjligheten att faktakontrollera rapporten.

3 Resultat av granskningen

3.1 Organisation och styrning av informationssäkerhet

3.1.1 Ledningssystem för informationssäkerhet (LIS)

En kommuns eller ett bolags verksamhet kan identifieras som samhällsviktiga och står därav under kraven i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, även kallat NIS-direktivet. I lagen ställs krav på att verksamheter som är identifierade som samhällsviktiga ska ha ett etablerat ledningssystem för informationssäkerhet, ett så kallat LIS.

3.1.2 Styrande dokument inom informationssäkerhet

Kommunfullmäktige har antagit en informationssäkerhetspolicy[1] som gäller för kommunens samtliga verksamheter. Av policyn framgår att den inte gäller för de kommunala bolagen, undantaget sammanhang som avser hantering av gemensamma informationstillgångar eller i situationer med särskilda behov av samordning. Leksandsbostäder AB har inte fastställt någon informationssäkerhetspolicy men uttrycker i intervju att de i nuläget utgår från kommunens policy och har för avsikt att formellt anta en egen sådan. I samband med faktakontroll av granskningen framförs att bolagsstyrelsen antog kommunens informationssäkerhetspolicy i december 2023, samt att bolagets ledningsgrupp därefter antagit kommunens riktlinje för informationssäkerhet.

Enligt policyn ska arbetet med informationssäkerhet vara systematiskt och bygga på standardserien SS-ISO/IEC 27000. Policyn redovisar även mål för och uppföljning av arbetet. Former för arbetet konkretiseras ytterligare i Riktlinjer för informationssäkerhet i Leksand kommun[2]. Här beskrivs hur arbetet ska bedrivas för att vara systematiskt på både strategiskt och operativt plan. Till exempel anger bägge dokumenten att både riskanalys och informationsklassningar är väsentliga moment som bidrar till att identifiera och vidta ändamålsenliga säkerhetsåtgärder i syfte att skydda både enskilda system och it-infrastrukturen.

3.1.3 Ansvarsfördelning informationssäkerhet

Enligt kommunstyrelsens reglemente[3] har styrelsen ansvar för informationsfrågor, säkerhetsfrågor och it-system. Informationssäkerhetspolicyn och riktlinjen innehåller däremot överlappande uppgifter avseende vilket organ som har det yttersta ansvaret för informationssäkerheten. Policyn anger att kommunfullmäktige, kommunstyrelse och utskott har det yttersta ansvaret på respektive nivå medan riktlinjen framhåller kommunstyrelsen som ytterst ansvarig.

[1] Informationssäkerhetspolicy, antagen av kommunfullmäktige, 2018-10-16 §12
[2] Riktlinjer för informationssäkerhet i Leksand kommun, beslutad av kommunstyrelsen 2022-03-11
[3] Beslutad av kommunfullmäktige 2020-12-10

I policyn befästs också att informationssäkerhet är del av det ordinarie verksamhetsansvaret och att verksamhetsansvariga på alla nivåer är ansvariga inom respektive verksamhetsområde.

Policyn anger vidare att kommunens informationssäkerhetssamordnare har övergripande ansvar för att leda, samordna och följa upp informationssäkerhetsarbetet. Informationssäkerhetssamordnaren tillhör enheten administrativ service som är placerad inom kommunstyrelseförvaltningen och sektor verksamhetsstöd. Funktionen hörde tidigare till it-avdelningen, men lyftes ut för att kunna anta en mer utpräglat styrande roll. Detta uttrycks i intervjuer vara angeläget då informationssäkerhetssamordnaren ska driva kommunens samlade informationssäkerhetsarbete genom att stötta och samordna det operativa arbetet som sker inom verksamheterna.

Informationssäkerhetssamordnaren har sitt uppdrag på 50 procent av en heltidstjänst. Bland intervjuade verksamhetsföreträdare råder delade meningar om tjänsteutrymmet motsvarar befintligt stödbehov. Flera intervjuade anser att informationssäkerhets-samordnarens stöd är avgörande då de funktioner som utför det verksamhetsnära informationssäkerhetsarbetet inte besitter tillräcklig kapacitet och kompetens för att på egen hand tillse ett systematiskt informationssäkerhetsarbete.

Som vi nämnt tidigare i rapporten ingår informationssäkerhet i det ordinarie linjeansvaret. I intervju förklaras det innebära att sektorchefer har ett strategiskt ansvar för sektorns informationssäkerhetsarbete och i regel även är systemägare. Det operativa arbetet utförs däremot av systemförvaltare, medarbetare som ansvarar för förvaltning av enskilda verksamhetssystem. Rollerna ”systemägare” och ”systemförvaltare” definieras av de styrande dokumenten där ansvar kravställs i form av punktvisa åtaganden för det respektive it-system.

Vi har i flera intervjuer fått bilden av att ansvar för informationssäkerhetsarbetet är otydligt för såväl verksamhetsansvariga som systemägare och systemförvaltare, liksom att det varierar hur insatta verksamhetsansvariga är i det pågående informationssäkerhetsarbetet. Även bland systemförvaltare uppfattar vi att det föreligger en variation i kunskapsnivå. Huruvida systemförvaltarna uppfattar sig ha fått information om vilka arbetsuppgifter som förväntas utföras, samt vilket utrymme som finns för att lägga tid på det då de flesta systemförvaltare har sitt uppdrag vid sidan av eller som del av annan tjänst. Kommunen uppges ha arbetat med systematisk informationssäkerhet sedan 2021 och systemförvaltarmodellen som kanal för arbetet är en förhållandevis ny struktur. Detta förklaras vara anledning till att arbetet och utövande av ansvar inte är fullt ut enhetligt.

Vidare ser vi att det förekommer olika uppgifter om systemförvaltarfunktionernas roller. Systemförvaltare tillskrivs olika ansvar i policyn respektive riktlinjen medan systemägare, enligt den powerpoint som används på kommunens systemförvaltarträffar, ”ansvarar för informationssäkerheten”.

Ansvarsfördelning inom Leksandbostäder AB

Kommunfullmäktige har beslutat om ägardirektiv[4] för Leksandsbostäder AB. Ägardirektivet saknar reglering av krav avseende informationssäkerhet.

Som vi skrivit tidigare har bolaget antagit kommunens informationssäkerhetspolicy, därmed även den ansvarsfördelning som beskrivs i den. Därvid är bolagets vd i egenskap av verksamhetsansvarig även ansvarig för informationssäkerheten i bolaget. Övriga roller för arbetet beskrivs muntligen där det framgår att bolaget har en verksamhetsutvecklare som fungerar som kontaktperson till kommunens informationssäkerhetssamordnare, samt utsedda systemförvaltare.

Bolaget har ett avtal med kommunen som innebär att bolaget köper fullständigt stöd av informationssäkerhetssamordnaren. Avtal finns också för drift och support av it-verksamhet vilket innebär att bolaget är del av den kommungemensamma it-miljön.

3.1.4 Ansvarsfördelning it-säkerhet

Enligt informationssäkerhetspolicyn har it-chef ett ansvar för att samordna arbetet med it-säkerhet och säkerställa att it-miljön lever upp till gällande krav.

It-chef leder it-avdelningen som finns inom sektor verksamhetsstöd och service, som utgörs av två enheter: en utvecklingsenhet respektive en supportenhet. Då granskningen genomfördes bestod avdelningen av 12 medarbetare varav en utsetts till it-säkerhetsansvarig. Vi har inte tagit del av några dokument som reglerar it-avdelningens verksamhet eller ansvar för enskilda funktioner. I intervju framgår att it-säkerhetsansvarig ansvarar för it-säkerhetsarbete kopplat till både infrastruktur och användarsäkerhet.

3.1.5 Bedömning

Vår bedömning är att kommunstyrelsen delvis säkerställt att det finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas.

Vi bedömer att det inom Leksandsbostäder AB delvis finns styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas.

Vi konstaterar att kommunfullmäktige antagit styrande dokument som ger inriktning och struktur för informationssäkerhetsarbetet i kommunen. Vi ser dock en risk att nuvarande formuleringar avseende ansvarsfördelning kan bidra till en otydlighet då de inte är samstämmiga.

Vi anser att kommunstyrelsen behöver utvärdera om informationssäkerhetssamordnarens tjänsteutrymme är tillräckligt för att möta det stödbehov som förmedlas. Det är nödvändigt för att uppfylla de säkerhetsnivåer som kravställs av styrande dokument samt för att kommunen ska kunna möta aktuella hot och risker. Vår uppfattning är att arbetssätt hos nyckelfunktioner är personbundet och baseras på den enskildas kunskaper och engagemang. I nuläget fullföljs inte linjeansvaret så som styrande dokument kravställer. Det arbete som utförs av enskilda

[4] Daterad 2013-06-10

funktioner bidrar i delar till informationssäkerhet men har inte tillräcklig systematik för att säkerställa ett enhetligt och fullständigt informationssäkerhetsarbete. I de fall linjeansvaret brister och om informationssäkerhetssamordnaren inte har utrymme att ta ett helhetsgrepp ser vi en risk i att informationssäkerheten blir fragmentiserad.

Gällande Leksandsbostäder AB ser vi det som en fördel att bolagets och antagit kommunens informationssäkerhetspolicy och riktlinje för informationssäkerhet. Detta då bolaget är integrerat i kommunens it-miljö och har stöd av funktioner i kommunen. Vår bedömning är att bolagsstyrelsens behöver utvärdera om bolagets informationssäkerhetsorganisation motsvarar kravställningen som anges av de styrande dokumenten.

3.2 Informationssäkerhetsarbetet i praktiken

3.2.1 Riskbedömning och informationsklassning

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, framgår att leverantör av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Utifrån detta har MSB rekommendationer avseende säkerhetsåtgärder i syfte att öka skyddet mot angrepp eller minimera eventuell skada. Rekommendationerna omfattar bland annat säkerhetsuppdateringar, säkerhetskopiering samt förmågan att upptäcka säkerhetshändelser.

3.2.2 Riskbedömning

Enligt Riktlinjer för informationssäkerhet ska risk- och sårbarhetsanalys genomföras för informationstillgångar som har ett lägsta skyddsvärde som innebär att de inte ska spridas till obehöriga. Systemägare ansvarar enligt riktlinjen för att riskanalys genomförs av systemförvaltare.

Av intervjuer framgår att arbetet med riskanalyser inte är systematiskt då varken riskanalys för den gemensamma it-miljön eller för enskilda informationstillgångar har genomförts. Kommunen genomförde under 2023 Infosäkkollen[5], vilket kan beskrivas som en självskattad nulägesanalys av informationssäkerhetsarbetet. Delgivet resultat visar bland annat att kommunen inte genomfört systematiska riskanalyser.

Inom den sociala sektorn uttrycks ambitioner om att implementera välfärdsteknik. Den enda välfärdsteknik som nyttjades då granskningen genomfördes var ett mindre antal läkemedelsrobotar som är placerade i respektive kunds hushåll. Roboten förser kunderna med färdiga läkemedelsdoser vid förprogrammerade tidpunkter. I systemet lagras personuppgifter om kunderna, vilket uppges vara den enda sorts information som systemet innehåller. Vi delges en riskanalys[6] som genomfördes inför implementeringen av robotarna, vilken konstateras sakna riskanalys ur ett informationshanteringsperspektiv. Intervjuad menar att dylik riskbedömning inte ansetts

[5] Ett verktyg från Myndigheten för samhällsskydd och beredskap som offentliga organisationer kan använda för att skatta sitt informationssäkerhetsarbete. Källa: www.msb.se
[6] Daterad 220923

motiverad sett till den mängd information som systemet innehåller, men att blir ett viktigt moment då annan välfärdsteknik införs.

Riskanalys inom Leksandbostäder AB

Bolaget har inkluderat it-säkerhet som ett kontrollmoment i bolagets internkontrollplan. Därutöver har ingen riskanalys med avseende på informationssäkerhet genomförts.

3.2.3 Informationsklassning

Informationssäkerhetspolicyn och Riktlinjer för informationssäkerhet stipulerar att samtliga it-system och informationstillgångar ska klassas med klassningsmodellen KLASSA[7]. Det ska genomföras i samband med upphandling av system och därefter periodiserat i syfte att tillse att klassningen är aktuell. Resultat från informationsklassningen ska generera en åtgärdsplan, vilken ska ligga till grund för till exempel kravställning mot systemleverantörer.

Vi har tagit del av resultat från cirka 15 klassningar samt ett antal åtgärdsplaner. I intervju beskrivs att klassningar tidigare genomfördes godtyckligt och sporadiskt, men att ett arbete gjorts med att strukturera och likrikta arbetssätt. Då granskningen genomfördes hade majoriteten av kommunens system klassats förhållandevis nyligen, enligt muntliga uppgifter. Undantag utgörs framför allt av system som inte innehåller känslig information.

Enligt de styrande dokumenten är det upp till systemägare att tillse att klassningar utförs av systemförvaltare. Vi har i intervjuer fått bild av att det förekommer variation i hur väl ansvar för detta är känt bland systemägarna. Flera klassningar har genomförts på initiativ av systemförvaltare utan att det förankrats hos systemägare. Vi uppfattar att de flesta systemförvaltare arbetar självständigt utan inblandning från systemägare, som i flera fall inte deltagit i klassningar.

Informationsklassning i Leksandbostäder AB

Vi har inom ramen för granskningen mottagit dokumentation som visar att de flesta av bolagets system har informationsklassats. Arbetet beskrivs ha skett i samverkan mellan informationssäkerhetssamordnare och systemförvaltare. Riskanalys konstateras däremot inte ha genomförts.

3.2.4 Bedömning

Vår bedömning är att arbetet med riskanalyser inte är systematiskt, men att arbetet med informationsklassningar är systematiskt. Det gäller såväl kommunen som Leksandsbostäder AB.

Både kommunen och bolaget har genomfört informationsklassningar för merparten av sina system och det finns tillhörande åtgärdsplaner. Vi ser att arbetet kan utvecklas genom att systemägarna i högre grad är involverade och tar del av resultatet vilket styrande dokument föreskriver.

[7] En modell för informationsklassning framtagen av Sveriges kommuner och regioner.

Vi konstaterar att riskanalyser inte har genomförts i enlighet med krav i styrande dokument och att arbetet med detta bör prioriteras i högre grad för att möta aktuella behov och risker.

Vår bedömning är att det inte genomförts särskilda riskanalyser för informationstillgångar inom den sociala sektorn.

Enligt vår bedömning bör utrustning och system inom ramen för välfärdsteknik riskbedömas på samma sätt som andra informationstillgångar.

3.3 It-säkerhetsarbetet

3.3.1 Etablerade it-säkerhetsåtgärder

Av informationssäkerhetspolicyn framgår att resultatet från informationsklassning ska ligga till grund för att tillse ett ändamålsenligt skydd för kommunens informationstillgångar.

Även om informationsklassningar har genomförts för ett stort antal av kommunens system kan vi utifrån intervjuuppgifter konstatera att implementerade it-säkerhetsåtgärder varken bygger på genomförd riskanalys eller resultat av informationsklassningar. Enligt intervjuer har klassningar tidigare inte genomförts tillräckligt systematiskt för att kunna utgöra grund för it-säkerhetsåtgärder. Resurser har även prioriterats till att reducera kommunens tekniska skuld där utbyte av föråldrad infrastruktur och system genomförts i stor omfattning, men där kvarstående arbete finns.

Genom redovisade svar från Infosäkkollen och muntlig redogörelse i intervjuer har vi fått en ingående beskrivning av de it-säkerhetsåtgärder som kommunen implementerat. Med hänsyn till att en alltför detaljerad redovisning kan exponera kommunen för säkerhetsrisker väljer vi att beskriva etablerade it-säkerhetsåtgärder översiktligt. Härvid konstaterar vi att det finns grundläggande säkerhetsåtgärder som nätverkssegmentering, klientskydd, backup-hantering och multifaktorsautentisering på flera betydande system.

För utvärdering av it-säkerhetsåtgärder uppges att kommunen avser att genomföra penetrationstester i samverkan med den externa leverantör som avtalats för övervakning av it-miljön (se rapportavsnitt *3.3.3 ”övervakning”*).

Etablerade it-säkerhetsåtgärder Leksandsbostäder AB

Bolaget ingår i kommunens gemensamma it-miljö och omfattas således av de etablerade it-säkerhetsåtgärderna som it-avdelningen vidtagit för kommunens it-miljö.

3.3.2 Bedömning

Vår bedömning är att it-säkerhetsåtgärder inte vidtagits som ett resultat av riskanalys och informationsklassningar.

It-säkerhetsåtgärder behöver vidtas i relation till behov hos de informationstillgångar som ska skyddas, varför kommunstyrelsen och bolaget behöver säkerställa att

riskanalys och informationsklassningar ligger till grund för de it-säkerhetsåtgärder som det finns behov av och att dessa etableras.

Vi konstaterar att it-resurser prioriterats till livscykelhantering. Vi ser positivt på att det har prioriterats då föråldrade system och produkter utgör en säkerhetsrisk.

3.3.3 Övervakning

Kommunen har tillsammans med Moras, Orsas och Älvdalens kommuner avtalat om en extern tjänsteleverantör, en så kallad SOC[8], för övervakning av it-miljön. Övervakning görs i syfte att detektera eventuella intrångsförsök och andra störningar.

För att kunna hantera eventuella störningar i ett akut skede köper kommunen dygnet runt-beredskap av Mora kommun. Oavsett när på dygnet som en händelse inträffar, går larm till Moras beredskapsfunktion som därefter kontaktar it-chef i Leksands kommun, enligt en muntligt beskriven men icke dokumenterad eskaleringskedja. Lösningen innebär vidare att den externa tjänsteleverantören har mandat att vid behov stänga ned servrar, system och användare för att skydda kommunens it-miljö.

Övervakning inom Leksandsbostäder AB

Övervakning och beredskap omfattar även Leksandsbostäder AB som del av kommunens gemensamma it-miljö.

3.3.4 Bedömning

Vår bedömning är att det finns en etablerad övervakning för att upptäcka hot om intrång och andra säkerhetsincidenter i it-miljön.

3.4 Säkerhetskultur

Enligt informationssäkerhetspolicyn har verksamhetsansvarig att tillse att medarbetare har kunskap om informationssäkerhet. Av intervjuer framgår att utbildning inte tillhandahållits inom verksamheterna, däremot samordnas en kommungemensam digital utbildning till samtliga anställda och förtroendevalda en gång om året. Deltagande följdes tidigare upp av informationssäkerhetssamordnaren, men det görs inte systematiskt längre. Den uppfattning som uttrycks är att deltagandet bland medarbetare är förhållandevis bra, men lägre bland förtroendevalda.

Utifrån intervjuer får vi bilden att den generella kunskapsnivån ökat inom kommunen, men att variationer kopplade till typ av arbetsuppgift förekommer där medarbetare med hög grad av datoranvändning beskrivs ha högre medvetenhet. Bland förtroendevalda beskrivs medvetenheten som genomgående låg.

Vi har tidigare i rapporten beskrivit ”systemägare” och ”systemförvaltare”, som är nyckelroller i informationssäkerhetsarbetet. Ingen anpassad utbildning har genomförts för dessa funktioner, vilket uttrycks vara ett behov för att ge samtliga systemägare och systemförvaltare samma förutsättningar och för att höja kunskapsnivån.

[8] ”Security operations center” (SOC) är en funktion som i realtid övervakar nätverk, applikationer etc som tillhör kommunens it-miljö.

Utbildning inom Leksandsbostäder AB

Anställda, men inte styrelseledamöter, uppges ha genomfört den årliga utbildningen, vilket följts upp av bolagsledningen. Kunskapen om informationssäkerhet beskrivs som låg inom bolaget då informationssäkerhet som arbetsfält är nytt inom bolaget.

3.4.1 Bedömning

Vår bedömning är att kommunstyrelsen och bolagsstyrelsen delvis har tillsett att det finns en tillräcklig säkerhetskultur.

Vi konstaterar att utbildning tillhandahålls regelbundet. För att säkerställa att den genomförs av anställda och förtroendevalda bedömer vi att deltagandet behöver följas upp. En bristande säkerhetskultur ökar risken för att information inte hanteras på ett ändamålsenligt sätt, och att kommunkoncernen i större utsträckning riskerar drabbas av incidenter.

Vidare bedömer vi att särskild utbildning bör tillhandahållas systemförvaltare och systemägare som utsedda nyckelpersoner i informationssäkerhetsarbetet. Vi ser därigenom att fördjupad kunskap är en förutsättning för att kunna göra ett adekvat arbete.

3.5 Incidenthantering

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, framgår att leverantör av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förbygga och minimera verkningar av incidenter som påverkar närverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärder ska syfta till att säkerställa kontinuiteten i tjänsterna.

3.5.1 Rutiner för incidenthantering

Kommunen har en rutin för hantering av informationssäkerhetsincidenter[9] som redovisar innebörden av en incident, roller vid incidenthantering samt tillvägagångssätt vid anmälningar. Rutinen beskriver även hur incidenter ska dokumenteras och följas upp i förbättringssyfte. Analys av incidenter ska genomföras av informationssäkerhetssamordnaren som också ska rapportera allvarliga incidenter till kommundirektör och allmänna utskottet, enligt informationssäkerhetspolicyn.

De intervjuade konstaterar att informationssäkerhetsincidenter anmäls sporadiskt, vilket tros vara en följd av en bristande kunskap om incidenter.

Incidenthantering inom Leksandbostäder AB

Bolaget saknar interna incidenthanteringsrutiner. Det framgår inte av den kommungemensamma rutinen huruvida den omfattar bolaget. Rutinen förefaller inte heller vara känd inom bolaget. Till följd av en tidigare incident uppger intervjuade att medvetenheten om informationssäkerhetsincidenter höjts inom bolaget, liksom vetskapen om att it-avdelningen ska kontaktas vid incidenter.

[9] Ej daterad

3.5.2 Bedömning

Vår bedömning är att det finns etablerade incidenthanteringsrutiner och att dessa inkluderar uppföljning av inträffade incidenter.

Vi ser ett behov av att kommunstyrelsen och bolagsstyrelsen säkerställer att medarbetare och förtroendevalda har förståelse för innebörden av en informationssäkerhetsincident är och hur en sådan ska anmälas. Detta i syfte att minska risken för att incidenter inträffar, samt att inträffade incidenter hanteras ändamålsenligt.

Som del i den kommungemensamma it-miljön anser vi att incidenthanteringsrutinen även bör omfatta Leksandsbostäder AB.

3.6 Uppföljning och återrapportering

Av 6 kap. 6 § Kommunallagen (2017:725) framgår att nämnderna inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten. De ska även se till att den interna kontrollen är tillräcklig och att verksamheten beskrivs på ett i övergripande tillfredställande sätt.

Vidare framgår av MSB:s metodstöd att för att ledningen på en strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i kommunen behöver det ske en kommunövergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning. Resultatet från ledningens genomgång ska dokumenteras och bevaras.

3.6.1 Uppföljning i praktiken

Enligt informationssäkerhetspolicyn ska uppföljning genomföras av informationssäkerhetssamordnare årligen och rapporteras till kommundirektör och allmänna utskottet. Uppföljning har genomförts i enlighet med policyn.

Som exempel på det har vi tagit del av en lägesrapport[10] som upprättas en gång per halvår av informationssäkerhetssamordnaren. Dokumentet beskriver genomförda aktiviteter och status för informationssäkerhetsarbetet samt kommande åtgärder. De intervjuade framför att det finns behov av att stärka uppföljningen mot kommunstyrelsen utöver lägesrapporten som kommuniceras skriftligt.

Återrapportering av pågående arbete uppges även ske i samband med delårs- och årsredovisning. Informationssäkerhetssamordnaren har även en stående punkt på kommunledningens sammanträden där aktuella frågor lyfts.

Uppföljning inom Leksandbostäder AB

Ingen uppföljning av informationssäkerhetsarbetet har genomförts och rapporterats till bolagsledningen eller till bolagsstyrelsen.

[10] Lägesrapport över kommunens GDPR och informationssäkerhetsarbete, daterad 2023-10-04

3.6.2 Bedömning

Vår bedömning är att det i allt väsentligt finns en etablerad uppföljning av informationssäkerhetsarbetet som rapporteras till kommunstyrelsen med regelbundenhet.

Vår bedömning är att det inte finns en etablerad uppföljning av informationssäkerhetsarbetet som rapporteras till bolagsstyrelsen med regelbundenhet.

Mot bakgrund av det förhöjda säkerhetsläget med ökad risk för cyberhot och intrång är det viktigt att styrelserna är informerade om aktuella hot och risker samt kommunkoncernens förmåga att skydda sig mot dessa. Detta så att sårbarheter kan identifieras och åtgärder för att stärka informations- och it-säkerheten beslutas.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelsen och bolagsstyrelsen säkerställt att det finns ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen och bolagsstyrelsen delvis säkerställt att ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Kommunstyrelsen har i informationssäkerhetspolicyn antagit en principiell grund med mål och inriktning för ett systematiskt informationssäkerhetsarbete. Vi bedömer att det finns en organisatorisk struktur för arbetet, men vi ser en risk i att organisationen inte genomför arbetet i enlighet med den kravbild som anges av de styrande dokumenten, och som är nödvändig för att kunna möta aktuella cyberhot och risker. Kommunen uttrycker ambitioner om att likrikta informationssäkerhetsarbetet ytterligare. Vi vill understryka betydelsen av det då arbetet i dag är personbundet i stora delar och då linjeansvaret för informationssäkerhet inte är fullt ut etablerat.

Vi ser även ett behov av att bolagsstyrelsen säkerställer att Leksandsbostäder AB:s organisation för informationssäkerhet är ändamålsenlig. Bolaget har antagit kommunens styrande dokument för informationssäkerhet, och omfattas därigenom av samma kravbild. För att upprätthålla ett systematiskt informationssäkerhetsarbete är det av vikt att organisationen är tillräcklig för att motsvara omfattningen på arbetet.

I det följande redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Tillse att ansvar för nyckelfunktioner avseende informationssäkerhetsarbetet harmoniserar i styrande dokument
- Säkerställa att linjeansvaret för informationssäkerhet är etablerat
- Utvärdera om informationssäkerhetssamordnarens tjänsteutrymme är tillräckligt för att motsvara behov och kravställd säkerhetsnivå
- Utvärdera om verksamheternas organisering för informationssäkerhetsarbete är tillräckligt för att motsvara kravställd säkerhetsnivå
- Säkerställa att riskanalys genomförs för kommunens samlade it-miljö
- Säkerställa att riskanalyser genomförs för välfärdsteknik
- Säkerställa att it-säkerhetsåtgärder vidtas utifrån genomförda riskanalyser och informationsklassningar
- Följa upp deltagande i informationssäkerhetsutbildningar för att säkerställa deltagandet bland medarbetare och förtroendevalda
- Tillse fördjupad utbildning inom informationssäkerhet för berörda funktioner

- Inkludera eskaleringsvägar till andra parter, exempelvis bolag som har tjänster från kommunen, i incidenthanteringsrutinen
- Förtydliga hur externa leverantörer omfattas av incidenthanteringsrutinerna

Utifrån resultatet av vår granskning rekommenderar vi styrelsen för Leksandsbostäder AB att:

- Utvärdera om bolagets organisering för informationssäkerhetsarbete är tillräckligt för att motsvara ett ändamålsenligt informationssäkerhetsarbete
- Säkerställa att riskanalys genomförs där informationssäkerhetsrisker beaktas och följs av åtgärder
- Säkerställa en incidenthanteringsrutin
- Tillse uppföljning av bolagets informationssäkerhetsarbete

Leksands kommun och Leksandsbostäder AB
Granskning av informationssäkerhet

2024-03-27

Datum som ovan
KPMG AB

Linnéa Grönvold
Certifierad kommunal yrkesrevisor och kundansvarig

Jenny Thörn
Verksamhetsrevisor

Sofie Ernerudh
Verksamhetsrevisor

Sofia Gunnarsson
Verksamhetsrevisor

5 Bilaga A

Som revisionskriterium i granskningen utgår vi från MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete och säkerhetsåtgärder med fokus på nedanstående områden.

Standard och krav

Metodstödet bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien och då främst på SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och kontroller samt ser över styrdokumenten med jämna mellanrum.

Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare om vilka krav som ställs i arbetet. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer.

Ansvar och organisation

Metodstödet beskriver hur ansvaret för arbetet med informationssäkerhet bör fördelas i organisationen samt tydliggör betydelsen av ledningens förståelse och engagemang i informationssäkerhetsarbetet för att det ska lyckas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten. Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Utbildning och kommunikation

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som implementeras.

Riskanalys och informationsklassning

Genom en riskanalys ska verksamheten identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Risker och potentiella händelser som kan leda till negativa konsekvenser beskrivs och bedöms sedan avseende sannolikheten att de inträffar samt potentiella konsekvenser.

Metodstödet anger vidare att informationsklassning är en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver. Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it-tjänster. De identifierade behoven av säkerhetsåtgärder bör dokumenteras i en åtgärdsplan. It-säkerhetsåtgärder rent tekniskt kan vara en del men klassningen kan även ha identifierat behov av kompletterande risk- och konsekvensanalyser, förbättrade rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Skyddsåtgärder

Informationstillgångar består av information och resurser som används för att hantera information. Själva informationen är den primära tillgången som ska klassas. Resurser som används för att hantera informationen, till exempel it-system och fysiska tillgångar, samt rutiner i verksamheten ska sedan utformas enligt skyddsnivåer som matchar klassningens resultat. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

I MSB:s föreskrift för säkerhetsåtgärder i informationssystem framgår att systemägaren behöver ha en dialog med berörda informationsägare inom organisationens olika verksamheter för att införa de säkerhetsåtgärder som ger rätt nivå av skydd för informationssystemet. Behovet av säkerhetsåtgärder identifieras utifrån de informationsklassningar och riskbedömningar som informationsägaren har genomfört, samt systemägarens egna riskbedömningar för informationssystemet.

MSB:s metodstöd beskriver att övervakning anger status för ett system, en process eller en aktivitet. Övervakning sker ofta kontinuerligt genom exempelvis att loggar i ett it-system övervakas och avvikelser automatiskt rapporteras. Övervakning och mätning görs för att bedöma om implementerade säkerhetsåtgärder har avsedd verkan och fungerar tillfredsställande.

Uppföljning och förbättringsarbete

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i organisationen behöver det ske en övergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning.

Resultatet från ledningens genomgång ska dokumenteras och bevaras.

Interna styrdokument

Enligt MSB bör ledningen se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan ledningen ge vägledning till chefer och övriga medarbetare över de krav och förhållningssätt som gäller i informationssäkerhetsarbetet.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.