ASKERSUNDS KOMMUN 2023-01-26

Revisorerna

Till
Askersundsbostäder AB

För kännedom
Kommunfullmäktige

Granskning av informationssäkerhet i Askersundsbostäder AB

Bolagets lekmannarevisor har med stöd av KPMG granskat bolagsstyrelsens informationssäkerhetsarbete. Granskningens syfte har varit att bedöma om styrelsen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i bolaget.

Utifrån genomförd granskning är vår sammanfattande bedömning att styrelsen till viss del har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten inom bolaget.

Vår bedömning är att bolagsstyrelsen och VD behöver ta ett större ansvar för informationssäkerheten för att organisationen ska bedömas ändamålsenlig. Vi uppfattar att IT-ansvarig, som är extern konsult, har ett alltför stort ansvar i arbetet i relation till övriga linjechefer i verksamheten samt i förhållande till mandat och befogenheter. Vi vill dock poängtera att vi inte funnit några brister i utövandet och att det arbete som genomförts av funktionen har lagt en god grund för bolagets informations-säkerhetsarbete.

Det finns upprättade styrande dokument som i vissa delar tydliggör ansvar, kravställning och hur informationssäkerhetsarbetet ska bedrivas på övergripande nivå. Det saknas uppgift på att nuvarande dokument har beslutats av styrelsen så att de är formellt antagna. Informationssäkerhetspolicyn eller kompletterande riktlinjer bör även revideras med beskrivning av bolagsstyrelsens ansvar för informationssäkerhetsfrågorna.

I nuläget sker en viss kravställning på tekniska åtgärder utifrån riskbedömningar och klassningar. Dock saknar arbetet med riskanalys och klassning systematik och är därtill personberoende. Vi uppfattar att IT-säkerhetsåtgärder som IT-ansvarig bedömer att det finns behov av implementeras för de informationstillgångar som hanteras i bolagets system. Vår bedömning är att det finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.) där utveckling och införande av nya verktyg sker löpande för att säkerheten ska möta nya hot och risker. De implementerade säkerhetsåtgärderna har till viss del följts upp genom att regelbundet övervaka säkerhetshändelser och analysera dess konsekvenser för att kunna förbättra informationssäkerheten avseende den tekniska säkerheten.

I nuläget saknas i övrigt uppföljning av det informationssäkerhetsarbete som genomförs inom bolaget för övriga aspekter av informationssäkerheten i form av administrativ och organisatorisk säkerhet. Det finns incidenthanteringsrutiner men vi ser behov av att stärka kännedom om vad som är incidenter och hur dessa, om de sker, ska hanteras.

Utifrån vår bedömning och vår slutsats rekommenderar vi styrelsen för Askersundsbostäder att:

- Avseende styrande dokument för informationssäkerhet:
  - Revidera policy med beskrivning av bolagsstyrelsens ansvar.
  - Revidera policy med beskrivning av hur uppföljning av informationssäkerhetsarbetet ska genomföras.
  - Bedöma om det finns behov av kompletterande anvisningar för hur informationssäkerhetsarbetet ska genomföras inom bolaget, exempelvis utifrån MSB:s metodstöd.
  - Fatta beslut om de styrande dokument som ska utgöra styrning för bolagets informationssäkerhetsarbete och förankra dessa i verksamheten.
- Tillse att verksamhetsansvariga upprätthåller sitt linjeansvar för informationssäkerhet genom att ta ansvar och delta i aktiviteter i arbetet, främst avseende riskanalyser och informationsklassning.
- Etablera en regelbunden uppföljning av informationssäkerhetsarbetet, där efterlevnad av styrdokument ingår som en del.

Vi önskar att bolagsstyrelsen senast den 15 maj 2023 inkommer med svar på vilka åtgärder de ämnar vidta med anledning av vad som framkommit i granskningen.

Per-Olof Thulin
Lekmannarevisor