Ledningens genomgång Informationssäkerhet

Stockholms Hamnar 2025

2024-11-26

Fastställande av Ledningens genomgång

Ledningens genomgång informationssäkerhet fastställs i sin helhet för verksamhetsåret 2025

Föredragande: Frida Carlbring, informationssäkerhetssamordnare

Stockholm 2024-11-29

Magdalena Bosson

Magdalena Bosson, VD

Elektroniskt undertecknad av Magdalena Bosson
Datum: 2024.11.29 08:09:07 +01'00'

1 Sammanfattning

Med ledningens genomgång avses att ledningen ser över verksamhetens systematiska informationssäkerhetsarbete och dess styrning för att säkerställa dess fortsatta inriktning och omfattning. Stockholms Hamnar skall bedriva ett systematiskt och riskbaserat informationssäkerhets- och dataskyddsarbete. Detta innebär att bolaget tar de steg som behövs för att identifiera vilken information som är viktig och sedan införa säkerhetsåtgärder för att skydda den. Arbetsroller kopplat till arbetet med informationssäkerhet- och dataskydd samt aktiviteter har identifierats för att arbetet ska bli en naturlig del av verksamheten.

Informationssäkerhetssamordnaren och dataskyddsombudet samverkar med varandra då både rutiner och åtgärder för områdena går samman.

2 Underlag för ledningens genomgång

2.1 Status för åtgärder från ledningens tidigare genomgångar

Stockholms Hamnar har under 2024 följt upp de kontrollaktiviteter som redovisades i Ledningens genomgång för informationssäkerhet 2024.

- Löpande inventering och informationsklassning har genomförts i verksamheten. Den interna prioriteringsordning som gjordes under 2023 har följts upp för att säkerställa kritiska informationsmängder klassas först. Informationssäkerhetssamordnaren har fortsatt att hålla i de initiala informationsklassningarna. Arbetet med att ett större ansvar läggs på informationsägare att följa upp åtgärdsplaner och implementering pågår och kommer att följas upp vidare.
- Styrelsen och ledningsgruppen har deltagit i ett digitalt informationsmöte för att få grundläggande kunskaper i nuvarande NIS och kommande NIS2 samt CER-direktivet.
- Informationssäkerhetssamordnare och objektledare IT har genomfört en bolagsövergripande föreläsning om informations- och IT-säkerhet. Föreläsningen genomfördes fysiskt men spelades även in för möjligheten att se den i efterhand.
- Objektledare-IT har inom förvaltningsobjekten påbörjat arbetet med att skapa en incidenthanteringsprocess. Ett forum har etablerats för att analysera inträffade incidenter och hur dessa skall omhändertas.
- Verksamheten har påbörjat arbetet med att se över användaradministrationen. Detta genom att förankra ett arbetssätt i hela förvaltningsorganisationen, aktiviteten finns i alla förvaltningsplaner för 2025. Vidare kommer verksamheten arbeta med driftsättning av ett IAM system (identity access management) i syfte att få en centraliserad administration av användare, behörigheter och rättigheter.

- Verksamheten har under våren 2024 driftsatt den outsourcade miljön för de mest verksamhetskritiska systemen som upphandlades under 2023.
- Verksamheten har bevakat rapporteringen om hur NIS2-direktivet utvecklas, både genom omvärldsbevakning och genom deltagande i MSBs konferens om cybersäkerhet. Verksamheten har också svarat på en internremiss till Stadshus AB som varit remissinstans för betänkandet (SOU 2024:64)
- Arbetet med identifierade NIS-system har fortsatt enligt etablerat arbetssätt.
- Verksamheten har reviderat sin riskanalys för de system som omfattas av NIS-direktivet och har även tagit fram en mer utvecklad mall för att dokumentera detta arbete.
- IT-enheten har tagit fram en kontinuitetsplan som ännu inte har testats för NIS-systemen. Denna innehåller information om vad som skall prioriteras, hur det skall genomföras, informeras och var resurserna skall hämtas ifrån.

Arbetet med dataskydd har breddats för att nå ut i verksamheten genom att utse dataskyddshandläggare. Dataskyddshandläggarna ska vara en länk mellan informationssäkerhetssamordnaren och dataskyddsombudet till chefer och medarbetare i verksamheten. Gruppen har haft fyra möten med teman under året för att sprida information och kunskap inom dataskydd och informationssäkerhet ut på avdelningarna. Dataskyddshanläggarna också har ett ansvar att fånga upp och vägleda medarbetare inom dataskydd. Denna grupp har tillsammans utvärderat var i verksamheten vi behöver omhänderta och fånga upp arbetet med dataskydd samt informationssäkerhet.

2.2 Faktorer som påverkar Stockholms Hamnars ledningssystem för informationssäkerhet

Stockholms stads informationssäkerhetsarbete regleras i en riktlinje som är en bilaga till stadens Kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören, dessa har senast reviderats 2024-11-13. Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

Stockholms Hamnar har en lokal tillämpningsanvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom den egna verksamheten. Den lokala tillämpningsanvisningen skall revideras under 2025.

2.3 Ny lagstiftning

2.3.1 NIS2-direktivet

NIS2-direktivet är en EU-reglering som ska förbättra cybersäkerheten i medlemsstaterna. NIS2-direktivet ersätter det tidigare NIS-direktivet.

Syftet med NIS2-direktivet är att öka motståndskraften mot cybersäkerhetsrisker genom att ställa krav på en hög gemensam cybersäkerhetsnivå för nätverks- och informationssystem inom hela EU. Det handlar om att verksamheter som ansvarar för

viktiga samhällsfunktioner ska ha ett systematiskt informationssäkerhetsarbete som leder fram till att lämpliga riskhanteringsåtgärder vidtas. I Sverige kommer NIS2 införas genom en ny lag, cybersäkerhetslagen, som väntas träda i kraft under augusti 2025.

NIS2 ställer skärpta krav på organisatoriska, tekniska och driftrelaterade säkerhetsåtgärder. Bland annat ställs krav på att verksamheter ska göra riskanalyser och vidta säkerhetsåtgärder för att skydda IT-system och nätverk. Ledningens engagemang i cybersäkerhetsarbetet ska genom det nya direktivet öka.

2.4 Genomförd tillsyn - NIS

20 mars 2024 genomförde Transportstyrelsen en tillsyn enligt lagen (2018:1147) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Tillsynen omfattade 6-11§§ i Transportstyrelsens föreskrifter och allmänna råd (TSFS 2022:14), om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn.

Transportstyrelsens syfte med tillsynen är att kontrollera att verksamheten bedrivs i enlighet med gällande förordningar, föreskrifter och av organisationen fastställda anvisningar och rutiner.

3 Förbättringar som föreslås för Stockholms Hamnars informationssäkerhetsarbete

3.1 Prioritering av åtgärder 2025

- Uppföljning av registerförteckningar åligger chefer vilket behöver förtydligas med arbetssätt hur detta ska tas om hand.
- En tydligare processkartläggning behöver tas fram för att tydliggöra hur personuppgifter och informationsmängder behandlas i verksamheten.
- Fortsatt arbete med nuvarande NIS och förberedelse för kommande NIS2. Detta genomförs med interna resurser men förstärks av extern expertis.
- Utbildning av styrelse och ledningsgrupp.
- Utbildning för medarbetare inom inköp och upphandling.
- Följa upp och revidera genomförda informationsklassningar.
- Följa upp systemspecifika incidenthanteringsrutiner.
- Genomföra stickprov av tilldelade behörigheter.
- Stresstest och övning av kontinuitetsplaner kopplat till NIS-direktivet.

3.2 Prioritering av åtgärder 2026

- Fortsätta förbättra, öva och testa systemspecifika kontinuitetsplaner.
- Följa upp att Informationsägare omhändertagit handlingsplaner från klassning.

3.3 Prioriteringar av åtgärder 2027

- Införa riskbaserat och systematiskt informationssäkerhetsarbete.