Ledningens genomgång Informationssäkerhet

Stockholms Hamnar 2024

2023-12-04

Fastställande av Ledningens genomgång

Ledningens genomgång informationssäkerhet fastställs i sin helhet för verksamhetsåret 2024

Föredragande: Frida Carlbring, informationssäkerhetssamordnare

Stockholm 2023-12-04

Magdalena Bosson

Elektroniskt undertecknad av Magdalena Bosson
Datum: 2023.12.04 19:44:32 +01'00'

Magdalena Bosson, VD

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

2022 och 2023 upprättade Stockholms Hamnar en årlig handlingsplan för informationssäkerhet- och dataskyddsarbete. Handlingsplanen syftade till att förtydliga hur arbetet under verksamhetsåret skulle stärka förmågan på dessa områden. Handlingsplanen redogör de aktiviteter och dess tidpunkt för genomförande likt Ledningens genomgång.

Under året 2023 har löpande inventering och informationsklassning genomförts i verksamheten. För att säkerställa kritiska system och informationsmängder har en intern prioriteringsordning gjorts för genomförandet. Informationssäkerhetssamordnaren håller fortsatt ihop de initiala informationsklassningarna, men ett större ansvar läggs på informationsägare att följa upp åtgärdsplaner och implementering.

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 2023-10-13. Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

Stockholms Hamnar har under 2023 fastställt en lokal tillämpningsanvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom den egna verksamheten. Den lokala tillämpningsanvisningen skall revideras årligen.

2.3 Ny lagstiftning

2.3.1.1 NIS 2 och CER-direktivet

Den 14 december 2022 beslutades direktiven om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2) och om kritiska entiteters motståndskraft (CER). Direktiven ska börja tillämpas den 18 oktober 2024. Den 23 februari 2023 fattade regeringen beslut om att ge en särskild utredare i uppdrag att föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS 2-direktivet och CER-direktivet ska kunna genomföras. Uppdraget ska redovisas senast 23 februari 2024.

Medan NIS-direktivet inriktar sig på skydd av informationssystem tar CER-direktivet sikte på samhällsviktig verksamhet. En identifierad sektor är transporter och således ska verksamheten omhänderta dessa krav.

Vad gäller NIS-direktivet är det i dag tydligt att kraven på IT-säkerhet för viktiga funktioner ytterligare kommer skärpas. Eftersom CER-direktivet är nytt kommer detta att behöva bevakas under inledningen av 2024 för att sedan omhändertas när kravbilden blivit tydlig.

3 Resultatet från egen uppföljning (VoR och IKP)

Stockholms Hamnar har under 2023 följt upp de kontrollaktiviteter som redovisades i VoR 2023.

- Inventering och informationsklassning sker löpande i verksamheten, för att säkerställa kritiska system och informationsmängder har en intern prioriteringsordning gjorts för genomförandet. ISAM håller fortsatt ihop de initiala informationsklassningarna, men ett större ansvar läggs på informationsägare att följa upp åtgärdsplaner och implementering.

- Hur hantering av behörigheter vid anställning och avslut av finns beskrivet i lokal tillämpningsanvisning. Åtkomst till Stockholms Hamnars olika system, gruppdiskar och samarbetsytor samt övriga informationstillgångar ska styras utifrån principerna om behov och minsta möjliga behörighet. Behörighet ska endast tilldelas när det krävs för att kunna utföra sina arbetsuppgifter.

- Lokal tillämpningsanvisning (hanteringsanvisning) finns upprättad och är fastställd av VD 2023-05-29.

- Generella rutiner för övergripande incidenthantering kopplat till informationssäkerhet- och dataskydd är reviderade.

- Kraven på informationssäkerhet inom upphandlingsförfarande av nya system har förtydligats.

4 Resultat från revisioner och tillsyn

Stockholms stads revisionskontor genomförde under våren 2023 en kartläggning av Stockholms Hamnars informationssäkerhetsarbete kopplat till NIS-direktivet. I kartläggningen framkom det att arbetet bedrivs löpande men att det kvarstår åtgärder som behövs för att säkerställa efterlevnad av bestämmelserna i lagen.

Stockholms Hamnar har identifierat de delar av verksamheten som är samhällsviktiga och omfattas av NIS-direktivet. Informationstillgångar har identifierats och klassats och beroenden till andra system, tjänster, nätverk och leverantörer har kartlagts.

Verksamhetens informationssäkerhetsarbete utgår från regelbundna riskanalyser. För de delar av verksamheten som omfattas av NIS-direktivet genomförs särskilda riskanalyser minst en gång per år. Åtgärdsplaner upprättas direkt och följs upp halvårsvis.

Stockholms Hamnar har upprättat rutiner för rapportering och hantering av incidenter, inklusive NIS-incidenter. Uppföljning av inträffade incidenter sker regelbundet. Inga NIS-incidenter har hittills inträffat.

Revisionskontoret bedömde att Stockholms Hamnar bör utveckla sitt informationssäkerhetsarbete genom att fastställa en övergripande kontinuitetsplan som beskriver verksamhetens arbete för att säkerställa och upprätthålla kontinuitet i verksamheten.

Under hösten 2023 har Transportstyrelsen genomfört en tillsyn av verksamhetens efterlevnad av säkerhetsskyddslagen. Säkerhetsskyddsarbetet omfattar även informationssäkerhet kopplad till säkerhetsskyddsklassificerade uppgifter. Transportstyrelsens initiala bedömning är att Stockholms Hamnar uppfyller kraven på informationssäkerhet.

5 Förbättringar som föreslås för Stockholms Hamnars informationssäkerhetsarbete

5.1 Prioritering av åtgärder 2024

Stockholms Hamnar ska under 2024:

- Fortsätta att genomföra informationsklassningar med fokus på att klassa de verksamhetsprocesser som innehåller stora volymer, känslig information och/eller särskilt skyddsvärda personuppgifter.
- Genomföra utbildningar för ledningsgrupp, chefer och medarbetare.
- Ta fram separata incidenthanteringsrutiner för verksamhetskritiska system med hjälp av Objektledare-IT.
- Ta fram rutiner för kontroll av behörigheter, i första hand för verksamhetskritiska system.

- Genomlysning av de system som omfattas av NIS-direktivet, kommande NIS 2.
- Genomföra risk- och sårbarhetsanalys kopplat till NIS/NIS 2.
- Ta fram kontinuitetsplaner koppat till system som omfattas av NIS-direktivet .

5.2 Prioritering av åtgärder 2025

- Följa upp och revidera genomförda informationsklassningar.
- Följa upp systemspecifika incidenthanteringsrutiner.
- Genomföra stickprover av tilldelade behörigheter.
- Öva kontinuitetsplaner kopplat till NIS-direktivet.

5.3 Prioritering av åtgärder 2026

- Upprätta och öva systemspecifika kontinuitetsplaner.
- Följa upp att Informationsägare omhändertagit handlingsplaner från klassning.