Tjänsteställe, handläggare
Nämndadministration, Anneli Björkholm

Sammanträdesdatum
2022-06-01

FöredragningsPM
Dnr: 22RS4118

Organ
Regionstyrelsen

Årsrapport informationssäkerhet 2021

Förslag till beslut
Regionstyrelsen beslutar

att godkänna redovisningen i Årsrapport om informationssäkerhet 2021.

Sammanfattning
Årsrapporten om informationssäkerhet innehåller information om följande punkter:

1. riskanalyser som har gjorts av informationssäkerheten,
2. incidenter som har påverkat informationssäkerheten och som medfört eller hade kunnat medföra vårdskada,
3. uppföljningar som har gjorts, och
4. förbättringsåtgärder som har vidtagits.

Rapporten är framtagen för regionstyrelsen och den ska, utifrån punkterna ovan, redovisa hur informationssäkerhetsabetet har bedrivits inom Region Örebro län under året och vad som är fokusområden framöver.

Ärendebeskrivning
Information är en av Region Örebro läns (nedan regionen) viktigaste tillgångar. Det är även en förutsättning för en säker och effektiv verksamhet samt en förutsättning för digitaliseringen. Informationssäkerhet handlar om att skydda information på ett säkert sätt. Det gäller all slags information oavsett var den finns lagrad, exempelvis på papper, digitalt eller muntligt.

Regionen ska bedriva ett systematiskt informationssäkerhetsarbete med utgångspunkt enligt den svenska och internationella standarden för informationssäkerhet SS-ISO/IEC 27001:2017 (Ledningssystem för informationssäkerhet). I det systematiska informationssäkerhetsarbetet ska hot,

sårbarheter och risker identifieras samt säkerhetsåtgärder införas som reducerar dessa till en för regionen acceptabel nivå med hänsyn till konfidentialitet, riktighet och tillgänglighet.

Ledningens genomgång är också ett viktigt steg enligt standarden för informationssäkerhet (SS-ISO/IEC 27001:2017) samt ett krav utifrån Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter inom hälso- och sjukvården (HSLF-FS 2016:40).

Utifrån dessa krav har denna rapport tagits fram för Regionstyrelsen för att redovisa Region Örebro läns informationssäkerhetsarbete under 2021. Årsrapporten tar upp det arbete inom området informationssäkerhet som utförts i Region Örebro län med utgångspunkt från Regionkansliet och enheten för juridik och informationssäkerhet utifrån det som har rapporterats till regionens informationssäkerhetssamordnare. I årsrapporten beskrivs arbetet enligt nedanstående rubriker.

Granskningar och skyddsåtgärder

Informationsklassningar och riskanalyser

Informationsklassningar och riskanalyser genomförs men med varierande kvalité. Fler personer i verksamheterna behöver utbildas för att kunna genomföra riskanalyser och informationsklassningar av regionens informationstillgångar. Informationsklassningar och riskanalyser är grunden för det systematiska informationssäkerhetsarbetet. Detta är således något som måste bli en naturlig del av all informationshantering, exempelvis vid upphandlingar, inköp, drift och förvaltning av IT-stöd samt för hantering av information i verksamheternas processer.

Metoder, modeller och andra hjälpmedel i arbetet med riskanalyser och informationsklassningar behöver förenklas och struktureras ytterligare..

Uppföljningar

Enkätuppföljning Infosäkkollen

Ett regeringsuppdrag ställt till MSB (Myndigheten för samhällsskydd och beredskap) för att mäta framförallt förutsättningen för det systematiska informationssäkerhetsarbetet och i vilken utsträckning som det systematiska arbetet bedrivs. Resultatet av mätningen visar vilka åtgärder som behöver genomföras inom regionen.

Enkätuppföljning informationssäkerhetskultur inom regionen

En enkät primärt riktad till informationsägare i de olika förvaltningarna. Frågorna i enkäten handlade om grundläggande kunskaper om exempelvis informationssäkerhetspolicy, riktlinjer och rutiner gällande informationssäkerhet.

Syftet med enkätuppföljningen är att mäta kunskap och informationssäkerhetskulturen i regionen för de funktioner som är informationsägare.

Uppföljning av informationssäkerhetsarbetet i regionen (ISK)

Förvaltningarna har rapporterat för 2021. I rapporteringen framgår att vissa förvaltningar har avsatt resurser för sitt informationssäkerhetsarbete. För att öka kunskapen om roller och ansvar samt förståelsen för vad ett systematiskt informationssäkerhetsarbete är behövs informationsinsatser då ett systematiskt riskbaserat informationssäkerhetsarbete kräver kontinuerlig översyn och uppföljning för att motverka eventuellt nya uppkomna säkerhetsbrister.

Förbättringsåtgärder

KLASSA
SKR har under 2021 tagit fram ett webbaserat verktyg för informationsklassning och riskanalys, KLASSA, för att stödja Kommuner och regioner i informationssäkerhetsarbetet med möjlighet att genomföra en informationsklassning och riskanalys kopplat till IT-stöd, enskilda dokument och processer. Regionens informationssäkerhetssamordnare har varit delaktig arbetet tillsammans med Kommuner och regioner och har därmed haft möjlighet att påverka hur klassningsverktyget på ett lämpligt sätt ska kunna stötta verksamheterna i sitt arbete med informationsklassning och riskanalyser.

Utbildningsinsatser
De utbildningar som ges regelbundet har delvis genomförts digitalt. Informationsinsatser kopplade till informationssäkerhetsarbetet har främst skett i digitalform.

Incidenter/avvikelser

Granskade och stoppade intrång via internet via regionens intrångsskydd ”IPS”.
Under januari hade regionen under ett dygn ca 7000 så kallade attackers och ca 21.000 malware. Motsvarande siffror under ett dygn december är ca 1.100.000 attackers och ca 100.000 malware. Det visar en mycket tydligt ökad aktivitet. Det mesta av denna trafik genereras säkerligen av automatiska genomsökningar efter sårbarheter, men en

del är också manuellt initierade attackförsök.

Samlad bild från regionens E-postfilter
Fram till början av november användes tjänsten Hosted Email Security från Trend, men har under november succesivt bytts ut till tjänsten Exchange Oneline Protection från Microsoft. Totalt under perioden 2020-11-01 – 2021-11-01 har det till alla regionens domäner adresserats 72.842.744 mail. Av totalen har 64.382.322 mail blockerats, mestadels av de algoritmer som tjänsten sätter och hanterar, men också av de regler som regionen kan påverka. Av de 52 miljoner blockerade mailen framgår att 128 identifierades som Advanced Threats och 52 identifierades som Ransomware.

Personuppgiftsincidenter

Under 2021 registrerades 202 misstänkta personuppgiftsincidenter av verksamheten i avvikelsesystemet Platina. Av dessa anmäldes 2 vidare till IMY.

Exempel på fokusområden för 2022 Region Örebro län

Det systematiska informationssäkerhetsarbetet
Arbetet med informationsklassningar och riskanalyser grundläggande för det systematiska informationssäkerhetsarbetet samt vid upphandlingar, inköp, drift och förvaltning av IT-stöd. En viktig del är att få Ledningssystem för informationssäkerhet (LIS) på plats. Ett grundläggande förslag finns framtaget och presenterat för informationssäkerhetsrådet. Ledningssystemet ska vara vägledande i de olika faserna i det systematiska informationssäkerhetsarbetet samt innehålla de ”verktyg” som behövs för att bedriva arbetet. De styrande dokumenten ses löpande över för att uppdateras och utgör bas för innehållet i ledningssystemet.

NIS-direktivet och NIS-lagstiftningen
Utifrån NIS-lagstiftningen har således hälso- och sjukvården och folktandvården ett särskilt krav på sig att bedriva ett systematiskt informationssäkerhetsarbete. Däri ingå att kartlägga vilka system/tjänster/infrastruktur etc. som är av särskild vikt för att vårdgivaren ska kunna leverera den samhällsviktiga tjänsten hälso- och sjukvård och tandvård. För att kunna leva upp till kraven i NIS-lagstiftningen behöver hälso- och sjukvården beskriva vilka krav som ställs på respektive vårdsystem för att kunna upprätthålla det samhällsviktiga uppdraget. Detta arbete behöver ske tillsammans med Regionservice IT. Det här arbetet behöver prioriteras.

FVIS (Framtidens vårdinformationssystem)

Stödja VISUS-arbetet i informationssäkerhet- och juridikfrågor.

Konsekvenser för miljö-, barn- och jämställdhetsperspektiven

Beslutet väntas inte få några konsekvenser för miljö-, barn- eller jämställdhetsperspektiven.

Ekonomiska konsekvenser

Det finns i dagsläget inga ekonomiska konsekvenser.

Beslutsunderlag

FöredragningsPM till regionstyrelsen 2022-06-01.
Årsrapport informationssäkerhet 2021.

Rickard Simonsson
Regiondirektör

Skickas till:

Regionkansliet Enheten för Juridik-och Informationssäkerhet