Tjänsteställe, handläggare
Juridik och Informationssäkerhet, Anneli Björkholm

Datum
2024-04-22

Beteckning
24RS2465

Er beteckning

Sammanfattning, årsrapport 2023

Region Örebro län (regionen) ska utöva ett systematiskt informationssäkerhetsarbete med stöd av den svenska och internationella standarden ISO 27000 för informationssäkerhet och cybersäkerhet samt dataskydd.

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 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 regionens informationssäkerhetsarbete under 2023. Årsrapporten tar upp det informationssäkerhetsarbete som skett (och är pågående) i regionen. I årsrapporten beskrivs arbetet enligt nedanstående rubriker.

Granskningar och skyddsåtgärder

Informationsklassningar och riskanalyser
Fler personer 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.

Uppföljningar

Myndigheten för samhällsskydd och beredskaps (MSB) Infosäkkollen
Ett regeringsuppdrag ställdes till MSB år 2021 för att mäta framför allt förutsättningen för det systematiska informationssäkerhetsarbetet och i vilken utsträckning som det systematiska arbetet bedrivs i regioner och kommuner. Mätningen skicks ut till regioner vart annat år, där 2023 års resultatet redovisas i denna rapport. Resultatet av uppföljningen visar en ökad nivå på det systematiska informationssäkerhetsarbetet.

Uppföljning av verksamheternas angivna förbättrande åtgärder
Sammanfattningsvis så finns det en ökad kunskap och medvetenhet. Introduktionen av nya medarbetare innehåller information om var rutiner och riktlinjer finns. Flertalet av medarbetarna har genomgått e-learningutbildning för informationssäkerhet som finns i regionens utbildningsportal PingPong. Vissa verksamheter arbetar aktivt med att uppdatera kunskapen hos medarbetare genom att uppmana att gå utbildningen vartannat år. Det är tydligt att riktlinjer och rutiner för hur digitala möten ska genomföras har fått ett stort genomslag och att medvetenheten för säkra digitala möten generellt är hög i samtliga verksamheter. Informationsklassning och riskanalyser vid upphandling av it-stöd har ökat.

Uppföljning av informationssäkerhetsarbetet i regionen (ISK)
I förvaltningarnas rapportering för år 2023 framgår att informationsklassning och riskanalys genomförs särskilt vid upphandling av it-stöd. Arbetet med informationssäkerhet pågår kontinuerligt. Staben administration, juridik och säkerhet har uppdraget att verka för att arbete görs i de olika delar av organisationen som berörs. De nationella systemen som regionen ansluter sig till informationklassas via Inera respektive e-hälsomyndigheten.

Regionkansliet arbetar löpande med informationssäkerhetsfrågor i samarbete med förvaltningarna.

Förbättringsåtgärder

Ett verktyg för informationsklassning och riskanalys
Sveriges Kommuner och Regioner (SKR) har tagit fram ett webbaserat verktyg för informationsklassning och riskanalys, (KLASSA). Verktyget ska stödja kommuner och regioner i informationssäkerhetsarbetet med att genomföra en informations-klassning och riskanalys kopplat till it-stöd och processer. Regionens informations-säkerhetssamordnare har varit delaktiga i arbetet tillsammans med andra kommuner och regioner.

Utbildningsinsatser
Utbildningar inom informationssäkerhet genomförs löpande inom regionen. Vissa utbildningsinsatser är återkommande exempelvis för chefer och ST-läkare, andra planeras in utifrån förfrågan eller vid behov.

Incidenter/avvikelser

Granskade och stoppade intrång via internet via regionens intrångsskydd ”IPS”
Regionens intrångsskydd (IPS = Intrusion Prevention System) arbetar utifrån två huvudprinciper, det stoppar trafik utifrån avsändar-/destinationsadress och det analyserar övrig trafik efter ”signaturer” (det vill säga kännetecken) som tyder på skadligt beteende. Regionen har ett abonnemang och det kommer fortlöpande information till regionen om svartlistade adresser och intrångs-signaturer som är förknippade med it-brottslighet och skadlig mjukvara. Den första sortens trafik (från/till svartlistade adresser) har ökat och ligger på en högre nivå än tidigare. Nivån låg på 320 miljoner blockerade requests under år 2022. Nivån för år 2023 låg på 785 miljoner blockerade requests det vill säga cirka 2,2 miljoner per dag (mer än en fördubbling jämfört med år 2022).

Samlad bild från regionens E-postfilter
Regionen använder ett e-postfilter från Exchange Online Protection från Microsoft. Det är en extern tjänst utanför regionens datahallar som kontrollerar mejlflödet innan mejl släpps in i regionens miljö.

Totalt under år 2023 har det till alla regionens domäner adresserats drygt 14 miljoner e-post. Av totalen har cirka 7,3 miljoner e-postleveranser blockerats, det mesta har klassats som spam sedan kommer blockering på grund av förfalskade avsändar-adresser (spoofing) högt i statistiken. Under större delen av året följer inflödet av spam samma veckovisa mönster där det egentligen inte sticker ut några värden sett över året. Däremot märks en ökande trend av inkommande e-post av alla kategorier, inte minst av e-post klassat som nätfiske (phishing).

Personuppgiftsincidenter
Under 2023 har det registrerats 272 personuppgiftsincidenter i Platina, av dessa är det 28 incidenter som anmälts vidare till Integritetsskyddsmyndigheten, IMY. Det som är återkommande är kallelse/brev/läkarintyg som skickas till fel patient och dokumentation av patientuppgifter i fel journal.

Exempel på fokusområden för 2024 Region Örebro län

Det systematiska informationssäkerhetsarbetet

Arbetet med informationsklassningar och riskanalyser är grundläggande för det systematiska informationssäkerhetsarbetet samt vid upphandlingar, inköp, drift och förvaltning av IT-stöd. Ledningssystem för informationssäkerhet (LIS) som är känd i verksamheterna som ”Processen för det systematiska informationssäkerhetsarbetet” är ett stöd och vägledning då kompetensen för att genomföra de principer och arbetssätten ofta efterfrågas.

Processen upplevs som ett bra stöd och är väl känd i de förvaltningar som har avsatt resurser som arbetar med informationssäkerhetsarbetet. Informationsinsatser kommer fortsatt att genomföras för det systematiska informationssäkerhetsarbetet.

NIS-lagstiftningen
Ett NIS2 direktiv kom under år 2022 och ska implementeras i svensk lag under år 2024. Genom NIS2 direktivet omfattas hela regionen, inte bara hälso- och sjukvården och folktandvården. Ytterligare krav kommer således att ställas gällande kontinuitet för det systematiska och riskbaserade arbetet.

Parallellt med detta kommer också det så kallade CER-direktivet som ska implementeras på ett samordnat sätt med NIS2-direktivet. CER-direktivet ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet

Framtidens vårdinformationssystem
Under år 2022 startades en ny informationssäkerhetsgrupp där alla regioner som ska införa det nya vårdinformationsystemet ingår. Informationssäkerhetssamordnare ingår i gruppen. Gruppen har fortsatt arbetat aktivt under år 2023 med informations- och it-säkerhetsfrågor.

Ett arbete inom regionen har pågått under år 2023 med att genomföra informations-klassning, riskanalyser, konsekvensbedömning (DPIA) samt kontinuitetsplanering kopplat till det nya vårdinformationssystemet, Cosmic. Cosmic består av många olika funktioner, så detta arbete kommer även att pågå under år 2024.

Upphandling och kravställning
Informationsklassning och riskanalys ska alltid ske inför en upphandling eller anskaffning då kraven för den informationsmängd som ska hanteras är specifik. Regionservice Upphandlingsavdelning samt Regionservice Medicinsk teknik har kontinuerliga dialoger med verksamheterna i samband med upphandlingar och avtalsförvaltning gällande informationsklassning och riskanalyser i samband med de upphandlingar som sker vi dem. Detta har gett ett bra resultat vilket MSB:s infosäkkollen påvisar.

Arbetet gällande generell kravställning kopplat till informationssäkerhet vid upphandling och anskaffning inom regionen sker fortsatt under år 2024.