2023 års rapport till regionstyrelsen enligt ledningssystemet för informationssäkerhet (inkluderat dataskydd)

Rapporten är framtagen av Region Skånes CISO/Informationssäkerhetschef och avser perioden 2023-04-19 till 2024-04-19

Innehållsförteckning

1 Omvärld

Det är en dynamisk och föränderlig värld vi lever i som har kommit in i en mogen digitaliseringsålder innan det blev dags för nästa stora kliv in i artificiell intelligens- (AI) och automatiseringsålder. Medan informationssäkerheten tidigare handlade om att skydda informationen i våra digitaliserade enheter och verktyg såsom mobiltelefoner och bärbara datorer blir insatserna mycket högre när vi nu börjar anförtro våra liv till automatiseringen och AI.

Den framtiden är redan här, i form av självkörande bilar, robotar som levererar paket och framtidens hälsosystem som håller på att tas fram i syfte att behandla fler patienter och rädda fler liv. Informations-säkerheten är en viktig förutsättning för både nutid och framtid. God informationssäkerhet inom transport men framför allt inom hälsa- och sjukvårdssektorn har bevisats vara skillnaden på liv och död.

Arbetet med informationssäkerhetsområdet omfattar fyra delområden[i]:

1. Organisatoriskt skydd som omfattar ledningssystem, styrdokument, dataskydd, övergripande processer och verktygsstöd
2. Teknisk skydd, mot cyberattacker genom säkerhetstekniska åtgärder (IT-säkerhet)
3. Fysiskt skydd med skal- och brandskydd samt
4. Personrelaterat skydd som bland annat handlar om medvetandegörande- och utbildningsinsatser.

Det rådande omvärldsläget ställer höga krav på god informationssäkerhet speciellt med tanke på att i den senaste rapporten från ett av världens största försäkringsbolag Allianz, listas cyberattacker om den högsta risken för 2024[ii].

EU:s cybersäkerhetsbyrå (ENISA) skriver i sin rapport från 2023 att offentlig förvaltning, individer och hälso- och sjukvårdssektorer fortsätter att vara de primära målen för dataläckor och intrång. IBM i

sin rapport ”Cost of Data Breach” från 2023 skriver att hälsa- och sjukvårdssektorn ligger på topp det 13:de året i rad som mest utsatt sektor för cyber/dataintrång med genomsnittlig kostnad på ca 110 MSEK per incident följt av tvåan på listan, som är finanssektorn med cirka hälften av den summan.

Orsakerna kan vara fler men i grunden handlar det om att finanssektor skyddar ekonomiska medel medan hälsa- och sjukvårdssektorn skyddar medborgarnas hälsa och liv. En sådan attack bär med sig mycket större kostnader och konsekvenser och påverkar individer och invånare mycket djupare.

Som en åtgärd har EU-rådet i november 2022 antagit ett nytt direktiv för att påskynda säkerhetsåtgärder och höja EU- medlemsstaternas skyddsnivå när det gäller samhällskritisk infrastruktur. Det nya NIS-direktivet (NIS2) ska implementeras i svensk lag genom den nya Cybersäkerhetslagen.

Den kommande Cybersäkerhetslagen som träder i kraft 1 januari 2025 sätter krav på mer effektiv styrning och ledning av informationssäkerhetsområdet samt mer och högre specialistkompetens inom informationssäkerhetsområdet inkluderat dataskydd vilket innebär att det blir svårare och mer kostsamt att rekrytera. Därför är samordning av hela informationssäkerhetsområdet samt intern kompetensutveckling kombinerat med snabb och rörlig kompetensförsörjning inom och utanför Region Skåne av stor betydelse för det kommande arbetet inom området.

2 Region Skåne och informationssäkerhetsområdet

Mognaden behöver öka i snabbare takt inom Region Skåne avseende vad informationssäkerhetsområdet är samt vilka delområden det

består av[iii]. Omvärlden är i ständig rörelse och förändring vilket påverkar även informationssäkerheten där omvärldsläge, hotbild och hotaktörer förändras kontinuerligt i takt med utvecklingen.

Dataskydd är sedan 2022 del av ledningssystemet för informationssäkerhet och faller under det organisatoriska benet av informationssäkerhetsområdet. Därför kommer i fortsättningen området kallas för informationssäkerhetsområdet för att på ett enklare och tydligare sätt representera helhetsperspektivet.

En färdplan har tagits fram för 2024 för att göra det enklare för verksamheterna att samverka inom informationssäkerhetsområdet med fokus på processer, verktygsstöd som kompletterar processerna samt säkerhetstekniska verktyg för att göra verksamheten insats enklare och effektivare, bättre synliggörande av incidenter och risker samt bättre samverkan inom hela informationssäkerhetsområdet dvs både de organisatoriska, tekniska, fysiska och personrelaterade delar.

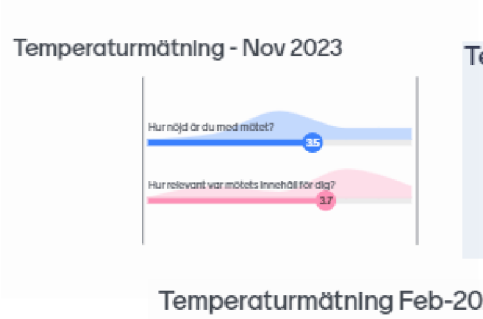
Planerna innehåller även aktiviteter och delaktiviteter som handlar om översyn av nuvarande organisation, strategi och mål, ett strukturerat arbetssätt att hantera inkomna ärenden och interna projekt på ett mer effektivt sätt, framtagning av en plan på utbildning och kompetenshöjning samt fortsatt arbete med att utveckla ledningssystemet för informationssäkerhet med att bland annat implementerad edataskyddsprocesser i ledningssystemet för informationssäkerhet.

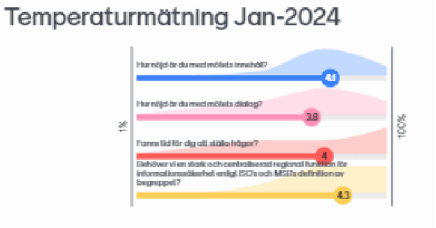
I denna rapport belyses det arbete som har skett samt vissa av de utmaningar som organisationen står inför och som kommer prägla det fortsatta arbetet. En redogörelse ges även kring några av de omvärldsfaktorer som är viktiga att ta med i beaktning för att säkerställa att Region Skåne står väl rustad inför nuvarande och kommande krav som ställs inom informationssäkerhetsområdet.

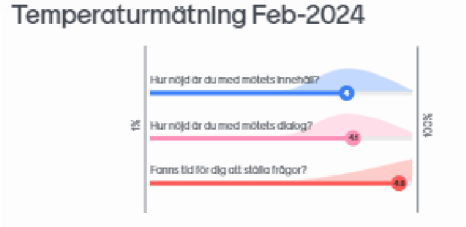
1. Informationssäkerhetsorganisation

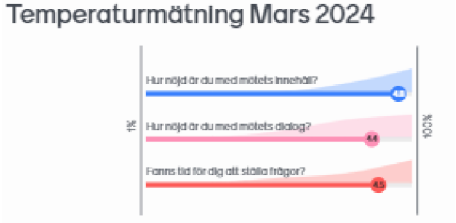
Region Skåne har en CISO/Informationssäkerhetschef (hädanefter CISO) som har i uppdrag att styra och leda ansvarsområdet inklusive övergripande ansvar för ledningssystemet för informationssäkerhet. Det finns även en informationssäkerhetsorganisation i syfte att samordna arbetet med informationssäkerhet. I den ingår samordnare för informationssäkerhet och dataskydd. CISO funktionen stöttas dessutom av olika enheter där den ena som finns på koncernkontoret jobbar med det organisatoriska delområdet och den andra enheten som står för det tekniska delområdet finns på förvaltningen Digitalisering IT och MT. Arbetet för att förtydliga ansvaret för fysiskt- och personrelaterat delområde kvarstår och är i sig en organisatorisk-, strukturell- och slutligen en säkerhetsrisk.

Ett informationssäkerhetsråd där informationssäkerhetsorganisationen möts på månadsbasis har som uppdrag att stödja, samordna och följa upp Region Skånes informationssäkerhetsarbete. Enligt beslutade riktlinjer ska även respektive förvaltning ha en organisation som hanterar frågor om informationssäkerhet inklusive dataskydd. Förvaltningar ska enligt styrdokument avsätta tillräckligt med resurser för att arbetet ska kunna bedrivas effektivt. Storleken på organisationen avgörs utifrån förvaltningens storlek samt mängden och känsligheten av den information som hanteras. Det finns stora variationer idag avseende hur förvaltningarna möter upp de kraven för tillräckliga resurser för effektivt arbete. Informationssäkerhetsorganisationen har en koppling till Region Skånes ledning genom CISO funktionen.









CISO har sedan november 2023 bedrivit enkäter med samordnare inom informationssäkerhetsrådet i syfte att samla insikter och följa utvecklingen inom den dialog och samordning i rådets arbete. Resultaten i figuren ovan påvisar en kontinuerlig förbättring trots befintliga organisatoriska och strukturella brister.

2. Ledningssystem för informationssäkerhet (LIS)

Region Skånes ledningssystem för informationssäkerhet (LIS) är ett viktigt verktyg för effektiv styrning av informationssäkerheten. LIS utgår ifrån SS-ISO/IEC 27000 serien som bland annat motsvarar kraven utifrån ISO 27001 samt säkerhetsåtgärder i enlighet med kraven i ISO 27002. Det är samma ledningssystem som anvisas av både EU och svenska tillsynsmyndigheter och ger Region Skåne möjlighet att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

I enlighet med fastställda riktlinjer för informationssäkerhet ska informationssäkerhetsarbetet vara en integrerad del av organisationens samtliga processer och övergripande ledningsstruktur. Detta genom att informationssäkerhet beaktas i utformningen av samtliga processer, informationssystem och säkerhetsåtgärder inom Region Skåne.

I LIS finns ett stort antal styrdokument, bland annat riktlinjer instruktioner, anvisningar och mallar för att konkretisera hur informationssäkerhetsarbetet ska bedrivas. Trots en, i struktur genomarbetad ledningssystem, så är efterlevnaden av den och dess styrdokument relativt låg inom verksamheten. Även uppföljningen av styrdokument är långt ifrån tillfredställande.

Tydliggörande av begreppet informationssäkerhet och dess komponenter enligt internationella standarders och svenska tillsynsmyndigheternas definition, samt utvecklingen av regionens ledningssystem för informationssäkerhet och dataskydd är en förutsättning för att regionen ska öka mognadsgraden för regionens informationssäkerhetsarbete.

3. Revisioner

Under perioden har det genomförts:

- en uppföljning på tidigare revision av informationssäkerhet inom redovisningsrevision och
- två revisioner där den ena utvärderade informationssäkerhetsområdet med fokus på kollektivtrafiken och den andra fokuserade på patientdata.

Resultatet av uppföljningen visar att ”det återstår ett stort arbete innan regionens arbete med informationssäkerhet har uppnåtts. De centrala ekonomi- samt personalsystem (Raindance och Personec P) ingår inte bland de system som har klassificerats/riskanalyserats. Detta skapar en osäkerhet för graden av effektivitet i kontrollmiljön för de processer som stöds av dessa system. Utifrån rekommendationerna från föregående års granskning har endast ett fåtal åtgärdats.”

Enligt d etvå senaste revisioner är ledningssystemet för informationssäkerhet (LIS) ej etablerat i tillräcklig utsträckning vilket har genererat en bristfällig kännedom om gällande styrdokument och krav. Det finns behov för att uppdatera styrdokument som och även effektiva sätt att uppdatera dessa på en lämplig nivå inom organisationen.

Nuvarande organisation och funktioner föreslås utvärderas för att identifiera om de är anpassade i förhållande till ledningssystemets omfattning och krav på hur informationssäkerhetsarbetet ska

bedrivas. Påbörjade aktiviteter på Koncernkontoret under andra halvan av 2023 har haft som mål att delvis titta på de konsolideringsmöjligheter i projektet för konsolidering inom bland annat informationssäkerhetsområdet och om befintlig organisation och resurser är lämpliga i förhållande till ledningssystemets omfattning. Slutsatsen var att nuvarande organisation och funktioner inte är lämpliga för omfattning och krav avseende effektiv hantering av informationssäkerhetsarbetet och ledningssystemet för informationssäkerhet.

Regionstyrelsen uppsiktsplikt ska starka den interna kontrollen över efterlevnad av styrande dokument.

Region Skånes medarbetare behöver genomföra de obligatoriska utbildningarna som finns tillgängliga samt deltagarantalet behöver följas upp.

Nuvarande rutiner för incidenthantering behöver kompletteras med tydlig beskrivning avseende ansvar, processer och eskaleringsvägar i händelse av olika incidenttyper samt att rutinerna etableras i organisationen samt att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov på regionsövergripande nivå.

4. Förvaltningsspecifika slutsatser

Flera förvaltningar uttrycker fortsatt behov av stöd från regionsövergripande enhet(er) för att kunna utveckla och utföra ett fullgott arbete inom de processer som informationssäkerhets- och dataskyddsarbetet kräver. Utmaningar inom organisationen kopplat till befintliga arbetsprocesser och resurssättning kvarstår.

Utan en säkerställd kompetensförsörjning på såväl förvaltningarna som inom de regionsövergripande enheter kvarstår regionen på fortsatt låg mognadsnivå. Detta tillsammans med viktiga faktorer i form av exempelvis effektiva processer och verktygsstöd på taktisk

nivå kombinerat med resurssättning med rätt kompetens påverkar i stor grad tidsgången som krävs för att utföra aktiviteter, uppdrag och projekt.

En utveckling av ledningssystemet syftar bland annat till att förtydliga styrningen och ledningen av arbetet med informationssäkerhet och dataskydd och att tydligare definiera processer samt roller och ansvar.

Många av de svårigheter som uppgetts kopplat till process och verktygsstöd kommer sannolikt kunna, åtminstone delvis, åtgärdas genom Region Skånes införande av ett olika stödsystem för informationsklassificering, riskhantering, incidenthantering och ärendehantering. Detta kommer möjliggöra och förenkla utveckling av relevanta processer inom informationssäkerhet samt möjliggöra en tydligare spårbarhet och utökade möjligheter till uppföljning.

Tekniska lösningar kopplade till tekniska säkerhetsåtgärder är under utveckling eller redan tagna i drift, vilket delvis ökar mognadsgraden för den tekniska delen av informationssäkerheten. För att på ett fullgott sätt kunna nyttja de tekniska lösningarna krävs en samordning av dessa samt att de rapporter och annat utfall som dessa lösningar producerar, tas till vara, analyseras och presenteras till områdesansvarig chef, dvs. CISO, organisationen för informationssäkerhet samt andra viktiga nyckelroller för en 360 graders perspektiv inom området.

5. Förbättringsåtgärder

Efter genomförda revisioner och i dialog med verksamheten samt verksamhetens samordnare har ett antal förbättringsområden identifierats. Det arbete har resulterat i en s.k. ”Roadmap 2024” eller en färdplan av aktiviteter där även de kortsiktiga mål som beslutas av Regionstyrelsen har inkluderats eller omfattas.

Arbete och aktiviteter pågår inom fler målområden:

- Översyn av organisation, strategi och mål i syfte att ta fram en organisation som effektivt kan arbeta med alla aspekter inom informationssäkerhetsområdet samt uppdatera de befintliga eller utveckla nya strategier och mål. Även roller och ansvar inom informationsägarebeslutet som definierar informationsägarens ansvar för informationstillgångar håller på att förtydligas och uppdateras. Då konsolideringsrapporten saknade organisatoriskt förslag har CISO i slutet av 2023 presenterat för beställare av konsolideringsuppdraget ett förslag på organisation av informationssäkerhetsfunktionen med resurser och funktioner som är anpassade till Region Skånes storlek i syfte att bedriva ett effektivt informationssäkerhetsarbete och även underhålla ledningssystemet för informationssäkerhet i sin helhet.

- Verktygsstöd och stödsystem för att effektivisera arbetet med ärenden och projekt i syfte att minska ledtider vid rådgivning och hjälp till verksamheten samt möjlighet för effektivare hantering av aktiviteter och delaktiviteter som bedrivs som projekt.

- Utveckling & samordning av Incidenthanteringsprocessen där olika typer av incidenter, med ursprung inom olika delområden hanteras på olika sätt. Aktiviteten ämnar analysera nuläget samt föreslå anpassningar i syfte att samköra och synliggöra samtliga incidenter kopplade till informationssäkerhetsområdet (tex. cybersäkerhetsincidenter, personuppgiftsincidenter, incidenter kopplade till personrelaterade säkerhetsbrister osv.) CISO med stöd av informationssäkerhetsorganisationen kommer under 2024 att göra en översyn av processen för hanteringen av informationssäkerhetsincidenter samt berörda styrdokument. Översynen består av en analys av styrning av incidenthantering inom nuvarande ledningssystemet för informationssäkerhet samt en GAP-analys av incidenthanteringsprocessen, som sker under 2024 som ska definiera gapen mellan befintligt styrdokument ”Instruktion för hantering av informationssäkerhetshändelser och incidenter” och de incidenthanteringsprocesser som andra

delar av regionen använder sig av. Efter genomförd analys ska nuvarande rutiner för hantering av informationssäkerhetsincidenter anpassas till en enhetlig regionsgemensam process som definierar ansvar, processer, eskaleringsvägar, lärdomar och förbättringsbehov

- Utveckling av Informationsklassificering vilket inkluderar enhetligt systematiskt arbetssätt för informationsklassificeringar vilket på sikt medför bra beslutsunderlag för att undvika upprepande arbete genom ett verktygs- och systemstöd samt kategorisering av informationstyper.

- Utveckling av Riskbedömningsprocessen vilket omfattar införande av stödsystem för riskhantering kommer att genomföras. Stödsystemet kommer att medföra ett förändrat arbetssätt där man utgår från informationen i stället för system som därmed också kräver en omställning i verksamheten med ett mer aktivt informationsägarskap.

- Utveckling av Säker Upphandling i syfte att ta fram ett regionsövergripande kravbibliotek som har täckning för hela informationssäkerhetsområdet, samt integrera informationssäkerheten så tidigt som möjligt i den befintliga upphandlingsprocessen.

- Översyn av styrdokument och ledningssystemets struktur som ska se till att identifiera dokumenten och dess ägare samt ge förslag på reviderad dokumentstruktur och integration av delkomponenterna – organisatorisk-, fysisk-, teknisk, och personrelaterad komponent under samma ledningssystem.

- Översyn av utbildningar och behov för kompetenshöjning i syfte att höja mognaden samt förbättra och förstärka säkerhetskulturen i Region Skåne. En grundutbildning är sedan tidigare framtagen och revideras vid behov, men ytterligare aktiviteter behöver genomföras. Översyn av utbildningar och behov för nödvändiga

kompetenshöjningar kommer att göras i samband med utveckling av området informationssäkerhet. Målet är att inventera, utvärdera, utveckla, samordna och vid behov konsolidera befintliga och/eller framtida utbildningar. Därefter ska en regionsövergripande utbildning planeras och implementeras i syfte att oka riskmedvetenhet. Utbildningen kommer omfatta informationssäkerhetsområdet och alla fyra delområden. Förutsättningen för valet av plattform för utbildningen är att det ska kontinuerligt gå att följa upp deltagarantalet

- Intern uppföljningsprocess för ledningssystemet för informationssäkerhet behöver tas fram vilket omfattar även efterlevnaden av de styrande dokument. Uppföljningen ska minst årligen genomföras av informationssäkerhetsspecialister ihop med informationssäkerhetssamordnare. Uppföljningen planeras att kompletteras eller kombineras med årlig intern kontroll.

---

[i] Vad är informationssäkerhet? (informationssakerhet.se)
[ii] https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2024-cyber-incidents.html
[iii] Vad är informationssäkerhet? (informationssakerhet.se)