Granskning av informationssäkerhet

Rapport

Region Jönköpings län

KPMG AB

2023-12-13

Antal sidor 24

Region Jönköpings län
Granskning av informationssäkerhet

2023-12-13

Innehållsförteckning

1 Sammanfattning

KPMG har av Region Jönköpings läns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av regionens arbete för att upprätthålla en god informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Syftet med granskningen har varit att bedöma om regionstyrelsen och nämnden för folkhälsa och sjukvård har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen och nämnd för folkhälsa och sjukvård i allt väsentligt säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Region Jönköpings län bedriver ett systematiskt arbete med informationssäkerhet där processer, säkerhetsåtgärder och mål utgår från identifierade risker och hot. Pågående arbete och även teknisk förmåga utvärderas löpande, vilket främjar proaktivitet och bidrar till ett kontinuerligt arbete med utveckling och förbättringar. Vid tid för granskningen pågår implementering av ett ledningssystem för informationssäkerhet vilket försvårar vår möjlighet att uttala oss om dess ändamålsenlighet. Det finns en regelbunden och dokumenterad uppföljning av informationssäkerhetsarbetet som rapporteras till regionstyrelsen i enlighet med styrande dokument. I nuläget saknas dock rapportering till nämnden för folkhälsa och sjukvård och vi anser att former för rapportering behöver tydliggöras utifrån nämndens verksamhetsansvar.

I det följande presenteras våra bedömningar och rekommendationer.

Revisionsfråga	Bedömning: I allt väsentligt	Rekommendationer
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?	Vår bedömning är att det finns styrande dokument som tydliggör ansvar, krav och former för informationssäkerhetsarbetet men att de styrande dokumenten inte implementerats fullt ut. Vi ser behov av att de styrande dokumenten kompletteras avseende ansvar för nämnder samt det it-säkerhetsansvar som är fördelat i praktiken.	**Regionstyrelsen** Säkerställa att ledningssystemet för informationssäkerhet implementeras i regionens organisation. Säkerställa att nuvarande styrdokument kompletteras avseende ansvar för nämnder samt it-säkerhetsarbetet. **Nämnden för folkhälsa och sjukvård** Säkerställa att ledningssystemet för informationssäkerhet implementeras i samtliga verksamheter.

Revisionsfråga	Bedömning: I allt väsentligt	Rekommendationer
Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?	Vi bedömer att det i allt väsentligt finns en ändamålsenlig organisation för informationssäkerhetsarbetet. Utifrån nuvarande arbetsbelastning ser vi risk för att implementeringsarbetet för ledningssystemet för informationssäkerhet inom hälso- och sjukvårdsverksamheterna inte kommer att kunna prioriteras tillräckligt. Det behöver därigenom säkerställas att det i samband med implementering och efterföljande efterlevnad av krav finns en organisation för genomförande av arbetet inom samtliga verksamheter.	**Nämnden för folkhälsa och sjukvård** Genom dialog med regionstyrelsen tillse att personella resurser finns tillgängliga för implementerings-processen av LIS inom verksamheterna.
Revisionsfråga	**Bedömning: Ja**	**Rekommendationer**
Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?	Vår bedömning är att det finns beslutade informations-säkerhetsmål med tillhörande handlingsplaner.	Inga rekommendationer.
Revisionsfråga	**Bedömning: Ja**	**Rekommendationer**
Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?	Vår bedömning är att regionstyrelsen och nämnden för folkhälsa och sjukvård tillsett en tillräcklig säkerhetskultur.	Inga rekommendationer.
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Finns ett systematiskt arbete med riskanalyser och informationsklassning?	Vår bedömning är att Region Jönköpings län delvis bedriver ett systematiskt arbete med informationsklassning och riskanalyser.	**Regionstyrelsen och nämnden för folkhälsa och sjukvård** Säkerställa att samtliga av de system som nyttjas genomgår informationsklassning samt riskanalys.

Revisionsfråga	Bedömning: Ja	Rekommendationer
Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?	Vi bedömer att regionstyrelsen vidtagit erforderliga tekniska säkerhetsåtgärder i syfte att skydda it-miljön mot aktuella hot och risker.	Inga rekommendationer.
Revisionsfråga	**Bedömning: Ja**	**Rekommendationer**
Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön?	Vi bedömer att det finns en etablerad övervakning i syfte att upptäcka hot om intrång och andra säkerhetsincidenter i it-miljön.	Inga rekommendationer.
Revisionsfråga	**Bedömning: Ja**	**Rekommendationer**
Finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?	Vår bedömning är att det finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp. Rutinerna inkluderar även tydliga eskaleringsvägar.	Inga rekommendationer.
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?	Vi bedömer att det delvis saknas dokumenterade reserv- och återgångsrutiner.	**Regionstyrelsen och nämnden för folkhälsa och sjukvård** Säkerställa att reserv- och återgångsrutiner vid störning eller avbrott upprättas.
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Finns en etablerad uppföljning av informations- och it-säkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?	Vi bedömer att det finns en etablerad uppföljning av informations- och it-säkerhetsarbetet. Det sker en regelbunden rapportering till regionstyrelsen i enlighet med styrande dokument. Vi anser däremot att det finns behov av att tydliggöra vilken rapportering av uppföljningen som ska göras till nämnden för folkhälsa och sjukvård. Detta utifrån nämndens verksamhetsansvar.	**Regionstyrelsen** Tydliggöra i styrande dokument hur former för rapportering till nämnder ska ske. **Nämnden för folkhälsa och sjukvård** Att nämnden utifrån sitt verksamhetsansvar tillser att de erhåller en rapportering av uppföljning för informationssäkerheten.

2 Bakgrund

KPMG har av Region Jönköpings läns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av regionens arbete för att upprätthålla en god informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete.

Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, konfidentiell och spårbar. Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Utvecklingen och den förändrade användningen av ny teknik innebär också att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Den digitala utvecklingen måste följas av ett anpassat och balanserat säkerhetsarbete för att säkerställa att de system och digitala tjänster som nyttjas för informationshantering och lagring inte är exponerade och tillgängliga för cyberhot och angrepp. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för regionen. Det är således väsentligt att regionen har en tillräcklig intern styrning och kontroll av sitt it-säkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

Med anledning av ovanstående drar regionens revisorer slutsatsen i sin riskanalys, att arbetet med informations- och it-säkerhet behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen har syftat till att bedöma om regionstyrelsen och nämnden för folkhälsa och sjukvård har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
- Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?
- Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?

— Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön?

— Finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?

— Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?

— Finns en etablerad uppföljning av informations- och it-säkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?

Granskningen har omfattat regionstyrelsens övergripande ansvar för informationssäkerhet samt regionstyrelsen och nämnden för folkhälsa och sjukvårds verksamhetsansvar för informationstillgångar som hanteras av nämnden.

Granskningen har avsett år 2023.

2.2 Ansvarig nämnd/styrelse

Granskningen har avsett regionstyrelsen och nämnden för folkhälsa och sjukvård.

2.3 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

— Kommunallagens 6 kap. 6 §

— Tillämpbara interna regelverk, policys och beslut

— MSB:s metodstöd och rekommendationer avseende Ledningssystem för informationssäkerhet och it-säkerhetsåtgärder

— Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där detta är tillämpbart (svensk lagstiftning utifrån NIS-direktivet)

2.4 Metod

Granskningen har genomförts genom intervjuer samt genom dokumentstudier. Dokumentanalysen har bland annat omfattat övergripande styrdokument fastställda av regionfullmäktige, regionstyrelsen och regiondirektören i Region Jönköpings län. Exempel på styrande dokument är reglemente för styrelse och nämnd, Informationssäkerhetspolicy med tillhörande riktlinjer som även omfattar anvisningar för informationssäkerhetsarbetet.

Intervjuer har genomförts regiondirektör, informationssäkerhetsansvarig, informationssäkerhetschef, specialist på informationssäkerhetssektionen, it-säkerhetschef, hälso- och sjukvårdsdirektör, verksamhetsutvecklare tillika informationssäkerhetssamordnare inom hälso- och sjukvård.

Intervjuer har även skett med regionstyrelsens presidium samt med nämnden för folkhälsa och sjukvårds presidium.

Rapporten är faktakontrollerad av samtliga medverkande.

3 Resultat av granskningen

3.1 Styrning och organisering av informationssäkerhetsarbetet

3.1.1 Ledningssystem för informationssäkerhet (LIS)

Alla regioner har verksamhet som är identifierad som samhällsviktig och står under kraven i lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, även kallad NIS-direktivet. I lagen ställs krav på att verksamheter som är identifierade som samhällsviktiga ska ha ett etablerat ledningssystem för informationssäkerhet, ett så kallat LIS. Region Jönköping omfattas av NIS-direktivet med anledning av hälso- och sjukvårdsverksamheten.

Regionen har ett dokument *Allmänt om ledningssystemet för informationssäkerhet och dataskydd*[1] som beskriver regionens LIS. Grunden i LIS utgörs av *Region Jönköpings läns informationssäkerhetspolicy*[2]. I den framgår att informationssäkerhetsarbetet ska bedrivas på ett systematiskt och riskbaserat sätt i enlighet med standardserien SS-ISO/IEC 27 000. Vidare framgår att målet med informationssäkerhetsarbetet ska vara att information ska skyddas så att den är tillgänglig för behöriga personer och tjänster när den behövs. Policyn konkretiseras i ett flertal dokument som presenteras i rapporten under de tematiska avsnitt som dokumenten berörs av.

Region Jönköpings län påbörjade implementering av ledningssystemet under 2022. Omfattningen av ledningssystemet baseras på analyser av behov och påverkansfaktorer för informationssäkerhetsarbetet. Vi har tagit del av processbeskrivningar, rollbeskrivningar samt styrande dokument som visar ledningssystemets struktur.

Vid tiden för granskningen var implementeringen av ledningssystemet i slutfasen. Att integrera ledningssystemet i verksamheternas dagliga arbete ses av flera centrala funktioner som den största utmaningen. Flera intervjuade uttrycker att det är avgörande att identifiera nyckelpersoner som kan bära implementeringen ut i kärnverksamheterna. Detta understryks vara särskilt viktigt inom hälso- och sjukvården där personella resurser för informationssäkerhetsarbetet redan i dag beskrivs som begränsade. Både de funktioner som arbetar med implementeringen av ledningssystemet och företrädare för hälso- och sjukvården konstaterar att det krävs tydlig central samordning och strukturerade utbildningsinsatser för att förankra ledningssystemet.

Från hälso- och sjukvården understryks vikten av anpassade utbildningar då medarbetarnas arbetsuppgifter omfattar allt från patientkontakt till administrativt arbete, varför olika personalgrupper behöver beakta informationssäkerhet ur olika aspekter.

Som en parallell process till införandet av ledningssystemet delges vi att det även pågår en genomlysning av styrande dokument, i syfte att säkerställa att lednings-systemet följer NIS-direktivets krav. Även om inte detta arbete är genomfört så ingår i

[1] 2023-03-10
[2] 2020-04-07

granskningen bedömningar utifrån NIS-direktivet då detta utgör ett av granskningens revisionskriterier.

3.1.2 Regionstyrelsens övergripande ansvar för informationssäkerhet

Av informationssäkerhetspolicyn framgår att regionstyrelsen har det övergripande ansvaret för informationssäkerheten. Ansvaret för informationssäkerheten på verksamhetsnivå följer det delegerade verksamhetsansvaret. Av policyn framgår även att regiondirektören i sin roll som regionstyrelsens verkställande tjänsteperson fastställer de verksamhetsövergripande riktlinjerna för informationssäkerhet.

Inom Region Jönköpings län är kanslidirektören övergripande informationssäkerhetsansvarig med ansvar att tillse att en organisation för informationssäkerhetsarbetet finns på plats som möter verksamhetens krav och behov.

Utöver detta finns en informationssäkerhetschef som har ett övergripande ansvar för samordning och uppföljning av informationssäkerheten. Däribland ingår att ge rådgivande insatser, ansvara för utbildning och information inom området, fastställa metod för informationsklassning och riskanalys, granska efterlevnaden av styrande dokument för informationssäkerhet samt att rapportera status på informationssäkerheten minst årligen och vid behov till regiondirektören. Informationssäkerhetschef är också chef för informationssäkerhets- och juridiksektionen som är del av Region Jönköpings läns regionledningskontor.

Det saknas reglering av ansvar för det övergripande it-säkerhetsarbetet i nuvarande policy och övriga styrdokument för informationssäkerhet. Däremot finns ett tydligt dokument[3] med roll- och ansvarsbeskrivningar för funktioner inom It-centrum. Regionens it-avdelning benämns It-centrum och består vid tiden för granskningen av cirka 220 medarbetare uppdelade på tre enheter: ledningsstöd, utveckling och förvaltning samt drift och support. Avdelningen leds av en it-direktör som har det övergripande verksamhetsansvaret.

I It-centrums ledningsstab finns en it-säkerhetschef tillika chefsarkitekt vars primära uppdrag är att handha den övergripande säkerhetsarkitekturen för regionens it-miljö. Rollen kan jämföras med rollen och ansvaret för informationssäkerhetschef men avseende it-säkerhetsarbetet och de tekniska säkerhetsåtgärder som är en del av informationssäkerhetsarbetet.

För det övergripande informationssäkerhetsarbetet finns tre konstellationer som är betydelsefulla för det strategiska arbetet. Detta då de identifierar viktiga frågor inom informations- och it-säkerhet respektive fattar vägledande beslut inom dessa frågor:

- Säkerhetskommittén, vars syfte är att hålla ihop samtliga säkerhetsfrågor inom organisationen. Kommittén utgörs av chefer för it-säkerhet, informationssäkerhet, beredskap respektive allmän säkerhet.
- Programstyrgruppen, som utgörs av regionledningen och tar övergripande strategiska beslut avseende prioriteringar och inriktning av digitalisering och it-

[3] Daterad 2023-10-31

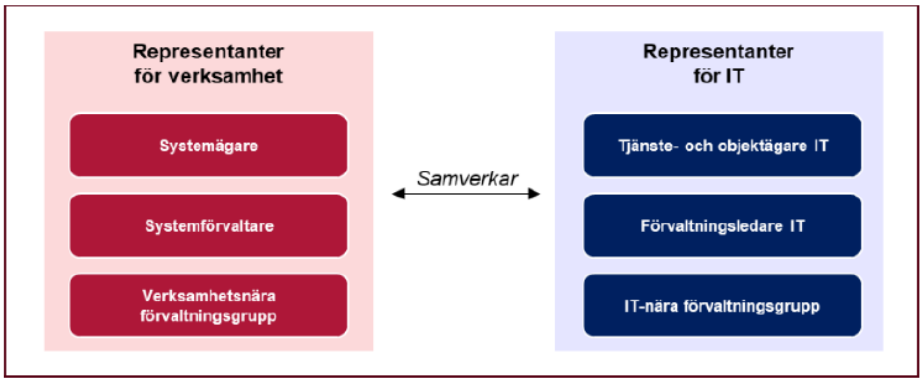
verksamhet. Programstyrgruppens ansvar regleras av riktlinjen för styrning av utveckling och förvaltning av IT-lösningar[4].

- För it-säkerhetsarbetet finns ett forum bestående av it-arkitekter som arbetar specifikt med it-säkerhetsutveckling.

Vid sidan av It-centrums linjeorganisation har Region Jönköpings län en beslutad modell för systemförvaltning[5] där informationssäkerhetsarbete hanteras inom ramen för förvaltningen av respektive system.

Enligt systemförvaltningsmodellen finns systemägare som har övergripande ansvar för ett system, systemförvaltare som är operativt ansvariga för systemet samt verksamhetsnära förvaltningsgrupper som består av verksamhetsrepresentanter för ett specifikt verksamhetsområde. Motsvarande funktioner från ett tekniskt perspektiv möts upp från funktioner inom It-centrum.

Bilden nedan visar rollerna i regionens systemförvaltningsmodell.



3.1.3 Styrelsens och nämndens verksamhetsansvar för informationssäkerhet och informationstillgångar

Som tidigare nämnts är den som är ansvarig för en verksamhet ägare till den information som skapas och hanteras inom den egna verksamheten och också ansvarig för informationssäkerheten inom verksamhetsområdet. Detta innebär att den ansvariga ska tillse att verksamhetens information hanteras i enlighet med gällande lagstiftning samt policy, riktlinjer och regler för informationssäkerhet.

Utifrån Region Jönköping läns organisationsmodell är det regiondirektören som ansvarar för informationssäkerheten avseende regionstyrelsens verksamhetsansvar. Hälso- och sjukvårdsdirektören har det övergripande ansvaret för informationssäkerhet inom nämnden för folkhälsa och sjukvårds verksamhetsområde. Genom dokumentstudier och intervjuer noterar vi att nämnden för folkhälsa och sjukvårds ansvar utifrån det verksamhetsansvar som anges i policyn för informationssäkerhet inte framgår tydligt. Enligt riktlinje för styrning av utveckling och förvaltning av it-lösningar[6] är hälso- och sjukvårdsdirektören systemägare för samtliga system som hälso- och

[4] Giltig från 2023-05-15
[5] Riktlinje styrning av utveckling och förvaltning av it-lösningar
[6] Ej daterad

sjukvården ansvarar för. Regiondirektören är systemägare för system som omfattar regionstyrelsens verksamhetsansvar.

Viktiga funktioner utöver detta till följd av det linjebaserade ansvaret är verksamhetschefer som i regel är informationsägare och därmed innehar ansvar för informationssäkerheten inom aktuell verksamhet. Vi uppfattar från intervjuer att såväl systemägarskap som informationsägarskap är känt hos berörda funktioner, och att ansvar axlas. Samtidigt är arbetsbelastningen på dessa funktioner enligt uppgift hög vilket innebär att informationssäkerhetsarbete ofta nedprioriteras.

En av de viktigaste informationssäkerhetsaspekterna inom hälso- och sjukvården är att säkerställa att obehöriga inte tar del av patientinformation. Ett sätt att kontrollera det är att göra loggkontroller genom att till exempel stickprovsgranska vilka patientjournaler som en anställd tagit del av. I intervjuer framförs att loggkontrollerna är tidskrävande och att det tidigare låg på respektive verksamhet att genomföra dem. För att avlasta verksamheterna har det inom hälso- och sjukvården etablerats en central logghantering. Än så länge görs loggning inom vissa verksamheter, arbete pågår dock med att stegvis koppla på samtliga verksamheter.

Intervjuade anger hälso- och sjukvårdens it-styrgrupper är betydelsefulla för it-säkerhetsarbetet. Styrgrupperna följer hälso- och sjukvårdens olika medicinska verksamhetsområden och har ett övergripande strategiskt perspektiv, gör prioriteringar samt bereder hälso- och sjukvårdens it-relaterade frågor till programstyrgruppen. Enligt riktlinjen är direktörerna för de olika medicinska specialiteterna ordförande för respektive styrgrupp.

Styrgrupperna, liksom it-kontaktpersoner som utsetts per verksamhet, beskrivs som de primära kontaktytorna för samverkan med informationssäkerhets- och juridiksektionen. Utöver den personella organiseringen finns dokumenterade överenskommelser om servicenivåer för det stöd som hälso- och sjukvården efterfrågar från It-centrum avseende drift och support för de system som nyttjas inom verksamheterna.

3.1.4 Bedömning

Vår bedömning är att det finns styrande dokument som tydliggör ansvar, krav och former för informationssäkerhetsarbetet. Vi bedömer dock att ansvaret ytterligare kan beskrivas i de styrande dokumenten.

Vi ser bland annat behov av att de styrande dokumenten tydliggör nämndernas ansvar utifrån det delegerade verksamhetsansvaret. Vi ser även behov av att tydliggöra det ansvar som i praktiken är fördelat avseende it-säkerhetsarbetet.

Vi konstaterar att Region Jönköpings län inte slutfört etableringen av ledningssystemet för informationssäkerhet och tillhörande styrdokument vilket innebär att dessa vid tid för granskningen inte implementerats fullt ut.

Vi anser att ledningssystemet ger stöd för ett systematiskt informationssäkerhetsarbete i enlighet med rekommendationerna från Myndigheten för samhällsskydd och beredskap, MSB. För att ledningssystemet ska bli integrerat i den dagliga verksamhetsstyrningen bedömer vi det vara av vikt att implementeringen sker med tydlig central samordning och enligt den etablerade struktur för systemförvaltning som

redan finns inom Region Jönköpings län. Vår uppfattning är att verksamhetschefer är centrala funktioner i implementeringsarbetet, både i rollen som informationsägare och utifrån ansvaret att leda och fördela arbetsuppgifter, vilket avser resurssättning av informationssäkerhetsarbetet.

Vi bedömer att det i allt väsentligt finns en ändamålsenlig organisation för informationssäkerhetsarbetet.

Vår bedömning är att det i stora delar finns en ändamålsenlig organisation av informations- och it-säkerhetsarbetet och att organiseringen följer en röd tråd från strategisk till operativ nivå. Vi ser att det linjebaserade ansvaret för informationssäkerhet är tydligt förankrat och att det finns uttalade forum för samverkan och utveckling inom informationssäkerhetsfrågor.

Vi uppfattar att det inom hälso- och sjukvården redan i dag finns utmaningar att kunna prioritera informationssäkerhetsarbetet. Då informationssäkerhet i enlighet med styrande dokument följer verksamhetsansvaret är vår bedömning att det behöver säkerställas att organisation och funktioner för informationssäkerhetsarbetet inom hälso- och sjukvården anpassas i förhållande till ledningssystemets krav och de lagar och föreskrifter som verksamheten har att efterleva. Detta är särskilt väsentligt i implementeringsfasen då ledningssystemet ska utgöra grunden för ett systematiskt informationssäkerhetsarbete. Det är därtill väsentligt med anledning av att nämnden omfattas av NIS-direktivet samt andra lagkrav i syfte att säkerställa informationssäkerhet och skydd av patientuppgifter.

Vi saknar reglering av ansvar för det övergripande och strategiska it-säkerhetsarbetet i övergripande styrdokument, men uppfattar oaktat det att ansvaret är tydligt i regionen, enligt uppgifter från intervjuer. Vi bedömer att It-centrum i hög grad upprätthåller ansvaret och att det ansvaret ska tydliggöras i de styrande dokumenten. Vi konstaterar även att ansvaret är tydliggjort på intranätet. Region Jönköpings län har en systemförvaltarmodell som reglerar roller och ansvarsuppgifter per system. I de dokument som styr förvaltningsmodellen regleras ansvar för utförande av operativt informationssäkerhetsarbetet och vi bedömer att detta ansvar efterlevs i enlighet med beskrivningarna.

Vi bedömer att befintliga forum i form av programstyrgruppen och säkerhetskommittén tillsammans med It-centrums interna organisering utgör väl etablerade strukturer för att eskalera it-säkerhetsfrågor identifierade på verksamhetsnivå till rätt beslutsnivå. Forumen kanaliserar även strategiska behov till den operativa nivån. För att ytterligare tydliggöra uppdrag och mandat för dessa forum bör exempelvis säkerhetskommitténs roll och ansvar beskrivas vid revidering av befintliga styrdokument.

3.2 Informationssäkerhetsmål och handlingsplaner

Region Jönköpings län har antagit nio kortsiktiga mål samt åtta strategiska mål för informationssäkerhetsarbetet, vilka utmynnar i ett övergripande mål för det samlade informationssäkerhetsarbetet. Utifrån det övergripande målet har strategiska mål och kortsiktiga mål formulerats. De strategiska målen ska uppnås under 2024–2026 medan de kortsiktiga målen avser 2022–2023.

Ett exempel på ett kortsiktigt mål är att statistik om informationssäkerhetsincidenter ska tas fram och användas i förbättringssyfte. Kopplat till detta finns ett strategiskt mål om att statistiken ska återrapporteras och utvärderas.

Arbetet med samtliga mål samordnas av informationssäkerhetssektionen, och för att integrera dem i det löpande arbetet finns handlingsplaner med aktiviteter som ska genomföras för att uppnå respektive mål. Informationssäkerhetssektionen har även ett årshjul där väsentliga händelser och övergripande aktiviteter sammanställts. Årshjulet följs kontinuerligt och anses ge en bra översiktlig bild över sektionens löpande verksamhet.

3.2.1 Bedömning

Vår bedömning är att det finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner.

Enligt vår mening bidrar sättet på vilket strategiska mål bryts ned till kortsiktiga mål, handlingsplaner och årshjul till en tydlig målstyrning och systematik.

3.3 Informationsklassning och riskbedömning

MSB:s föreskrifter utifrån NIS-direktivet ställer krav på samhällsviktiga leverantörer att ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att klassa information med utgångspunkt i vilka konsekvenser som kan uppkomma vid brister i konfidentialitet, riktighet och tillgänglighet. Det finns även krav på att identifiera, analysera och värdera risker för organisationens information, nätverk och informationssystem.

Klassificering görs utifrån en fastställd klassningsmodell. Klassningsresultatet, tillsammans med genomförd riskbedömning, ger underlag för att välja säkerhetsåtgärder så att informationen inte får otillräckligt skydd eller överskyddas med höga kostnader som följd.

3.3.1 Informationsklassning och riskanalys

Region Jönköpings län har upprättat riktlinjer för informationsklassning och riskanalys[7]. Av riktlinjerna framgår att regionen använder Sveriges kommuner och regioners verktyg KLASSA. Riktlinjerna beskriver även processen för klassningsarbetet samt för värdering av de informationssäkerhetsrisker som identifierats i klassningen. Systemägaren ansvarar enligt riktlinjerna för att i samråd med verksamhetsansvarig,

[7] Riktlinje informationsklassning och riskanalys, informationssäkerhetschef, 2023-03-28

tillika informationsägare, besluta om informationsklassning. Vidare framgår av dokumentet att den som är ansvarig för förvaltningen av systemet också är ansvarig för att bedöma och bearbeta resultatet från klassningen.

Utöver detta finns ytterligare ett dokument benämnt informationsklassning och riskhantering[8]. Riskhanteringen ska enligt dokumentet bidra till att förbättra ledningssystemet och omfattar delarna förarbete, riskanalys och efterarbete. I efterarbetet ingår att ta fram en handlingsplan som beskriver om identifierade informationssäkerhetsrisker behöver åtgärdas eller om de kan accepteras. Utifrån detta tas sedan en åtgärdsplan fram för prioriterade informationssäkerhetsrisker. Informationsklassning, riskanalys och riskhantering ligger därmed till grund för de säkerhetsåtgärder som vidtas för att stärka skyddet av informationssystemen.

Enligt riktlinjen för styrning av utveckling och förvaltning av it-lösningar ska samtliga system ha en förvaltningsplan som omfattar åtgärder och utvecklingsaktiviteter, vilken ska revideras årligen. Enligt intervjuuppgifter finns informationsklassning som aktivitet i samtliga förvaltningsplaner och om den inte genomförs under ett år följer den med till nästkommande år. Detta anses understryka kravet på att klassningar ska genomföras även för befintliga system.

Klassningsarbetet involverar medarbetare från It-centrum, systemägare, representanter från berörd verksamhet samt funktioner från informationssäkerhetssektionen. Som stöd för arbetet finns mallar som tagits fram av informationssäkerhetssektionen. Utifrån resultatet av informationsklassning och riskanalys genereras en handlingsplan som It-centrum använder för att ta fram adekvata it-tekniska säkerhetsåtgärder för systemet.

Från genomförda intervjuer får vi bilden att informationsklassningar och riskanalyser genomförs i enlighet med riktlinjerna och att det är ett obligatoriskt moment som genomförs inför upphandling som del i en strukturerad införandeprocess. Däremot uppfattar vi att detta arbete i regel initieras av medarbetare från It-centrum då informationsägare uppges ha svårt att avsätta resurser. Ett av Region Jönköpings läns mål med informationssäkerhetsarbetet för 2023 är att 50 procent av ej klassificerade system ska klassas. Intervjuade anger att målet inte har uppnåtts. Av Region Jönköpings läns cirka 700 system uppges endast en mindre del informationsklassats, främst på grund av resursbrist inom informationsägarens verksamhet.

3.3.1.1 Styrelsens och nämndens arbete med riskanalys, informationsklassning och åtgärdsplaner

Inom både regionstyrelsens verksamhetsområde samt hälso- och sjukvården har de mest verksamhetskritiska systemen genomgått klassning och riskanalys. Det totala antalet system förklaras vara stort och merparten av de system som inte genomgått klassificering uppges vara mindre system.

Vår uppfattning från genomförda intervjuer är att hälso- och sjukvården inte informationsklassat befintliga system regelmässigt då verksamheterna har svårt att avsätta tid för det. Mot bakgrund av det konstaterar intervjuade att hälso- och

[8] Informationsklassning och riskhantering, 2023-03-28

sjukvården behöver prioritera vilka system som ur säkerhetssynpunkt är mest angelägna att informationsklassa.

Granskningen har inte visat att hälso- och sjukvården eller regionstyrelsen gjort någon samlad riskbedömning där prioritering gjorts av hur kritiska systemen är eller vilka informationstillgångar som har störst skyddsbehov.

3.3.2 Bedömning

Vår bedömning är att Region Jönköpings län delvis bedriver ett systematiskt arbete med informationsklassning och riskanalyser i enlighet med styrande dokument och det som anges i MSB:s metodstöd.

Vi anser att informationsklassning och riskanalys behöver genomföras för befintliga system för att regionen ska uppnå ett fullgott systematiskt klassningsarbete.

Vidare kan vi konstatera att initiativ och ansvar tas av It-centrum för att tillse att informationsklassningar genomförs med anledning av verksamhetschefers arbetsbelastning. Med anledning av detta är vår bedömning att det finns behov av en ansvarsförskjutning från det tekniska perspektivet för att säkerställa att även organisatoriska säkerhetsåtgärder inkluderas i arbetet. Detta i enlighet med ansvarsfördelningen som finns i styrande dokument.

Vi vill påtala betydelsen av att information i befintliga system skyddas med ändamålsenliga säkerhetsåtgärder. För att säkerställa att hälso- och sjukvårdens mest kritiska informationstillgångar och system skyddas av erforderliga säkerhetsåtgärder anser vi att en konsekvensanalys behöver genomföras som kan ligga till grund för prioritering av vilka system som initialt är mest angelägna att riskbedöma och informationsklassa.

3.4 Säkerhetskultur

Som ett av Region Jönköpings läns informationssäkerhetsmål för arbetet under 2023 anges att 50 procent av medarbetarna ska ha genomgått utbildning i informationssäkerhet. Syftet med utbildningarna är att skapa en god informationssäkerhetskultur. Utbildningarna ska utvärderas under 2024–2026.

På regionens intranät finns ett antal olika utbildningar tillgängliga för regionens medarbetare vilka samordnas av informationssäkerhetssektionen. Basen är en introduktionsutbildning i informationssäkerhet. Därtill finns olika målgruppsanpassade utbildningar så som informationssäkerhet kopplat till patientsäkerhet för vårdpersonal liksom utbildning anpassad för förtroendevalda. Intervjupersoner uppger att utbildningsutbudet är varierande i syfte att nå samtliga medarbetare inom regionens olika verksamheter. Uppföljning av deltagande medarbetare sker på verksamhetsnivå medan informationssäkerhetssektionen sammanställer statistik över genomförda utbildningar på regionövergripande nivå.

Utöver regelrätta utbildningar brukar aktualitetsbaserad information om exempelvis pågående virusattacker publiceras på intranätet. I syfte att träna

säkerhetsmedvetenheten hos anställda har informationssäkerhetssektionen även skickat ut fiktiva nätfiskemeddelanden via e-post.

Den sammantagna uppfattningen hos de intervjuade är att den generella medvetandenivån har ökat, både till följd av utbildningar och som konsekvens av ökade omvärldshot.

Av riktlinjerna för informationsklassning och riskanalys framgår även att regionen ska tillhandahålla utbildning i processen och i verktyget KLASSA. Exempelvis genomförde regionen en utbildning i detta för förvaltningsledare under tiden för genomförandet av granskningen.

3.4.1 Bedömning

Vår bedömning är att regionstyrelsen och nämnden för folkhälsa och sjukvård tillsett en tillräcklig säkerhetskultur.

Utbildningsinsatser bidrar till att öka kunskap och medvetenhet hos medarbetare och förtroendevalda, vilket i sin tur kan leda till att risken för att incidenter inträffar minskar. Enligt vår bedömning bidrar målgruppsanpassade utbildningar till att ytterligare främja ändamålsenligheten och öka relevansen i utbildningsmaterialet.

3.5 IT-säkerhet

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Utifrån detta har MSB rekommendationer avseende säkerhetsåtgärder i syfte att öka skyddet mot angrepp eller minimera eventuell skada. Rekommendationerna omfattar bland annat säkerhetsuppdateringar, säkerhetskopiering samt förmågan att upptäcka säkerhetshändelser.

3.5.1 Riskanalys och omvärldsbevakning

Vi har tagit del av en ingående redogörelse för It-centrums strukturella arbete med it-tekniska säkerhetsåtgärder för såväl den gemensamma infrastrukturen som för enskilda system. Intervjuade anger att genomförda prioriteringar och analyser är grundande i en långtgående systematik. Bland annat bygger vidtagna åtgärder på utvärdering av digital mognad, lagkrav och förordningar, tester av motståndskraft i form av sårbarhetsscanningar och penetrationstester samt riskanalyser där krav på säkerhetsnivåer identifierats.

Av särskild betydelse uppfattar vi att mognadsmodellerna är. Mognadsmodellerna bygger på ISO 27000, ISO 9000 samt lagkrav och föreskrifter, däribland säkerhetslagar. Modellerna utgörs av kontrollområden som utvärderar olika säkerhetsaspekter och ligger till grund för framtagandet av en it-säkerhetsplan. Planen innehåller aktiviteter och åtgärder på ett övergripande plan i syfte att upprätthålla och stärka it-säkerheten.

Ett område som pekas ut som särskilt komplicerat ur säkerhetsmässig synvinkel är medicinskteknisk utrustning. Produkterna ligger ofta i teknisk framkant och är efterfrågade av hälso- och sjukvården då de möjliggör förbättrade behandlingsmetoder. Dock uppges att det finns viss problematik med att integrera produkterna i befintlig it-miljö på grund av att deras uppsättning kan innebära sårbarheter för regionens it-miljö. Om sådana risker identifieras initieras en diskussion mellan It-centrum och berörd verksamhet avseende vilken lösning som minimerar eller eliminerar sårbarheterna. Utöver detta är produkterna ofta molnbaserade, vilket medför en säkerhetsrisk då flera leverantörer har säte utomlands. Regionen har i detta avseende en riktlinje för hantering av molntjänster[9] vars syfte är att ge vägledning inför att en molntjänst ska införskaffas.

Mot bakgrund av att alltför detaljerade uppgifter kan riskera att avslöja känsliga uppgifter redogör vi endast översiktligt för ett urval av säkerhetsåtgärder som It-centrum, utifrån genomförda analyser, vidtagit för att tillse en säker it-miljö:

- Inloggning med SITHS-kort för att minska risken för otillbörlig åtkomst till information
- Regelbunden installation av säkerhetsuppdateringar
- Uppgradering av centrala komponenter
- Nätverkssegmentering
- Lösning för säkerhetskopiering
- Implementering av skyddsåtgärder prioriteras utifrån ett arkitekturperspektiv indelade i olika nivåer

3.5.2 Övervakning och säkerhetsloggar

It-centrum har ett team, så kallat ”SOC” (Security operations center), som utför löpande övervakning över it-miljön. Teamet utgörs av fyra it-säkerhetsanalytiker och en teamleader.

På sättet som teamets arbetsuppgifter beskrivs konstaterar vi att det både utförs ett operativt dagligt arbete med att genomsöka komponenter för att detektera intrångsförsök, samt ett mer strategiskt säkerhetsarbete. Härvid genomförs återkommande sårbarhetsscanningar för att upptäcka svaga punkter och hot i syfte att utveckla det långsiktiga sårbarhetsskyddet. Arbetet återrapporteras veckovis till it-säkerhetschef, och oftare om situationen är mer akut.

[9] Riktlinje hantering av molntjänster, giltig från 2021-06-24

3.5.3 Bedömning

Vi bedömer att regionstyrelsen vidtagit erforderliga tekniska säkerhetsåtgärder i syfte att skydda it-miljön mot aktuella hot och risker.

Etablerade säkerhetsåtgärder är, enligt vår bedömning, i linje med MSB:s rekommendationer för ett starkt cyberförsvar, och utvärderas regelbundet för att fastställa att de fungerar ändamålsenligt. Tillvägagångssättet följer en strukturerad process där säkerhets- och sårbarhetsrisker analyseras löpande och ur flera aspekter, vilket enligt vår bedömning ökar sannolikheten att identifiera såväl inre sårbarheter som yttre risker.

Vi bedömer att det genomförts systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder för att upptäcka eventuella brister, genom exempelvis penetrationstester och regelbunden sårbarhetsskanning.

Av företrädare för hälso- och sjukvården såväl som för It-centrum uppfattar vi att det finns olika synsätt kring nyttjandet av produkter inom medicinsk teknik. Vi anser att tydliga riktlinjer avseende säkerhetskrav som externa produkter och tjänster ska uppfylla skapar tydlighet. Med utgångspunkt i befintlig riktlinje bedömer vi att överväganden om sådana produkter behöver utgå från riskanalyser som beaktar både patientsäkerhets- och it-säkerhetsperspektiv, och att befintlig riktlinje revideras med avseende på detta.

Vi bedömer att det finns en etablerad övervakning i syfte att upptäcka hot om intrång och andra säkerhetsincidenter i it-miljön.

Vår bild är att det finns en robust struktur för att arbeta med övervakning ur både ett löpande och ett proaktivt perspektiv för att reducera risker och hot som Region Jönköpings län kan utsättas för.

3.6 Incidenthanteringsrutiner

Region Jönköpings län har ett antal styrande dokument som reglerar incidenthantering. Både riktlinje för incidenthantering[10] samt riktlinje för övervakning, mätning, analys och utvärdering[11] anger att incidenter ska användas i verksamhetsförbättrande syfte. Där förtydligas bland annat att informationssäkerhets- respektive it-incidenter ska tas om hand och utredas av berörd verksamhet, samt analyseras och följas upp enligt särskilda rutiner. Riktlinjen för incidenthantering förklarar vad som avses med begreppen informationssäkerhetsincident och it-säkerhetsincident. Den anger även att incidenter ska anmälas via Region Jönköpings läns gemensamma avvikelsehanteringssystem. Systemet nås via intranätet och har en särskild kategori för informations- och it-säkerhetsincidenter. Vi uppfattar emellertid att it-säkerhetsincidenter oftast kanaliseras via aktuellt systems systemförvaltare medan informationssäkerhetsincidenter anmäls genom avvikelsehanteringssystemet.

[10] Incidenthantering och ständiga förbättringar, 2023-05-05
[11] Övervakning, mätning, analys och utvärdering, 2023-05-05

I enlighet med de styrande dokumenten uppges att informationssäkerhetsincidenter samordnas av informationssäkerhetssektionen medan It-centrum samordnar it-säkerhetsincidenter. Vi får intryck av att beskrivningar av incidenter har målgruppsanpassats i informations- och utbildningsmaterial utifrån regionens olika kärnverksamheter i syfte att konkretisera risker som kan uppstå inom respektive verksamhet.

3.6.1 Hantering och dokumentation av informationssäkerhetsincidenter

Av riktlinje för incidenthantering framgår att berörd verksamhet ansvarar för att utreda och dokumentera incidenter, samt vidta åtgärder i både ett direkt och ett mer långsiktigt perspektiv.

De flesta av regionens samtliga informationssäkerhetsanmälningar uppges röra patientnära hälso- och sjukvårdsverksamhet. Dessa anmälningar vidarebefordras av informationssäkerhetssektionen till avvikelsesamordnare inom hälso- och sjukvården där dessa hanteras med hälso- och sjukvårdens systematik för avvikelsehantering. Det innebär dels att incidenten hanteras ur ett omedelbart perspektiv med utredning och eventuellt påföljande åtgärd, dels att den analyseras med ett proaktivt synsätt som del i ett strukturerat arbete med ständiga förbättringar.

Informationssäkerhetssektionens del i incidenthanteringen inom hälso- och sjukvården beskrivs vara att sammanställa incidentanmälningar på aggregerad nivå. För de incidenter som sektionen handlägger uppges att eskaleringsvägar etablerats som del i ett internt organisationsträd. Till exempel finns en personuppgiftsansvarig som hanterar personuppgiftsincidenter. Vi har tagit del av en kvartalsrapport för informationssäkerhet[12] som författats av informationssäkerhetssektionen där antal anmälda incidenter sammanställts.

Av riktlinjen framgår att incidenter ska analyseras enligt en särskild rutin för statistik, uppföljning och analys. Det framgår emellertid inte vilken funktion som ansvarar för analysen, eller hur den ska presenteras eller följas upp.

3.6.2 Hantering och dokumentation av it-säkerhetsincidenter

Vi har fått en muntlig redogörelse för processen vid it-säkerhetsincidenter. Enligt redogörelsen samordnas incidenter i ett initialt skede av It-centrums incidentkoordinator, som har till uppgift att löpande bevaka anmälningsflödet. Anmälningarna utreds och dokumenteras i ett digitalt verktyg som också uppges innehålla It-centrums interna incidenthanteringsrutin. Rutinen beskrivs förtydliga hur incidenter ska värderas, hanteras och eskaleras vid behov. För incidenter med akut och allvarlig påverkan finns särskilda rutiner som involverar regionens beredskapsfunktion, vilken finns att tillgå dygnet runt. För dessa incidenter, som kan innebära en hög påverkan på verksamheten, finns särskilda rutiner upprättade som bland annat omfattar kortare eskaleringsvägar.

Ansvarig för incidenthantering är driftchef, som därigenom ansvarar för att incidenter analyseras både vecko- och månadsvis. Detta är en åtgärd för att effektivisera det

[12] Ej daterad

kortsiktiga incidenthanteringsarbetet, samt för att tillse att strategiska åtgärder vidtas för återkommande problem och behov. I de fall en incident rör ett verksamhetssystem deltar även systemförvaltare från berörd verksamhet i efteranalysen.

Därtill uppges att årliga externrevisioner utifrån ISO 9000 av incidenthanteringsarbetet genomförs, vilket beskrivs vara av vikt som del i det strategiska utvecklingsarbetet.

3.6.3 Reserv- och återgångsrutiner

It-centrum har upprättat en krisplan som beskriver hur It-centrum ska agera och arbeta i händelse av en större krissituation. Planen går enligt uppgift i linje med regionens övergripande beredskapsstruktur för samordnings- och kommunikationsvägar, och syftar till att kunna upprätthålla avdelningens övergripande funktionalitet.

Enligt intervjuade finns ett stort antal tekniska reserv- och återgångsrutiner vid avbrott och andra verksamhetsbortfall. Däremot saknas rutiner för händelser där it-miljön utsätts för intrång eller hot, vilket därmed ses som ett prioriterat arbete att ta fram sådana rutiner.

Regionen har enligt intervjuade inte förutsättningar för att kontinuitetsplanera för samtliga regionens 700 system. Arbetet inriktas därför mot system vars bortfall har stor påverkan på verksamheten. Enheter som bedriver verksamhet som identifierats som samhällsviktig, samt där genomförda informationsklassningar och riskanalyser visar på hög risk, är prioriterade i arbetet. För dessa ska risk- och sårbarhetsanalyser genomföras som grund för kontinuitetsplaner. I intervjuer uppges att risk- och sårbarhetsanalyser är under framtagande.

Avseende reserv- och återgångsrutiner för den administrativa aspekten har informationssäkerhetssektionen tillsammans med representanter från regionens verksamheter påbörjat ett motsvarande arbete. I det fallet uppges det handla om att gå igenom verksamhetskritiska dokument och ta ställning till hur dessa ska säkerställas.

Inom hälso- och sjukvården uppges det pågå arbete med att ta fram reservrutiner baserade på olika störningsscenarier. Svårigheten upplevs vara att hitta rätt avvägning mellan att ha reservrutiner som är tillräckligt omfattande men samtidigt operativa i syfte att utgöra ett fullgott stöd.

3.6.4 Bedömning

Vår bedömning är att det finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp. Rutinerna inkluderar även tydliga eskaleringsvägar.

Det finns tydliga eskaleringsvägar beskrivna i det verktyg som används vid anmälan av en incident och vi anser att både informationssäkerhetsincidenter och it-säkerhetsincidenter hanteras inom etablerade organisationsstrukturer och med en systematik som utgår från ett förbättringsperspektiv.

Vi bedömer att det delvis saknas dokumenterade reserv- och återgångsrutiner.

Vi konstaterar att det både inom It-centrum och informationssäkerhetssektionen pågår arbete med att utforma rutiner för händelser som intrång och hot. Vi bedömer att det är ett nödvändigt arbete för att stärka organisationens robusthet vid störningar och avbrott. Att säkerställa att verksamheten kan fortsätta vid avbrott är särskilt viktigt för verksamhet inom folkhälsa och sjukvård.

3.7 Uppföljning och återrapportering

3.7.1 Uppföljning

Av de styrande dokumenten framgår att uppföljning av informationssäkerhetsarbetet ska göras med ambitionen att utvärdera effekten av ledningssystemet och bidra till förbättring av arbetet. Riktlinjen Övervakning, mätning, analys och utvärdering anger hur utvärderingen ska gå till, bland annat genom intern kontroll av verksamheternas systematiska informationssäkerhetsarbete. I riktlinjen för incidenthantering och ständiga förbättringar ges konkret förslag på hur verksamheterna kan arbeta med uppföljning av det operativa informationssäkerhetsarbetet. Vi har inte erhållit något material som visar att verksamheterna arbetar enligt föreslagen modell.

Vi har tagit del av informationssäkerhetssektionens handlingsplan[13] för uppföljning av det övergripande arbetet. Av planen framgår vilka områden som ska följas upp samt vem som är ansvarig för genomförandet. Planen omfattar även uppföljning av de antagna informationssäkerhetsmålen.

Vi har därtill tagit del av en kvartalsrapport[14] som sammanställs av informationssäkerhetssektionen. Rapporten är tematiskt indelad och åskådliggör bland annat statistik avseende genomförda klassningar, utbildningar och informationsklassning. Rapporten utgör det underlag med vilket informationssäkerhetschef återrapporterar arbetet till kanslidirektör. Det beskrivs också utgöra grund för Ledningens genomgång, som vi redovisar nedan. Kvartalsrapporten svarar inte mot handlingsplanen och den omfattar inte uppföljning av informationssäkerhetsmålen i enlighet med handlingsplanen.

Ingen rapportering som avser informationssäkerhet har lämnats till nämnden för folkhälsa och sjukvård. Genom dokumentgranskning har vi inte kunnat notera några krav på uppföljning och rapportering till nämnderna och det tydliggörs inte vidare vad *verksamhet* som benämns i Riktlinje för övervakning, mätning, analys avser i förhållande till styrelser och nämnder. Därmed saknas uppföljning från nämndens sida av det informationssäkerhetsarbete som sker inom de verksamheter som nämnden ansvarar för. Intervjuade beskriver att informationssäkerhetsarbetet följs upp och kontrolleras i de processer som genomförs av informationssäkerhets- och juridiksektionen på regionledningskontoret, samt rapporteras till regionstyrelsen i enlighet med de styrande dokumenten.

[13] Ej daterad
[14] Kvartalrapportering informationssäkerhet Q2

It-centrum är certifierat mot standarden ISO 9000 som avser ledningssystem för kvalitet. Med anledning av certifieringen är it-verksamheten föremål för en årsutvärdering mot de 153 kontroller som utvärderingen omfattar. Det är bland annat den utifrån den utvärderingen som it-säkerhetsplanen upprättas.

3.7.2 Ledningens genomgång och annan rapportering till regionstyrelse

Enligt informationssäkerhetspolicyn ska regiondirektören rapportera till regionstyrelsen vid behov och minst årligen om status på informationssäkerheten. Enligt metodstödet från Myndigheten för samhällsskydd och beredskap kallas detta ”ledningens genomgång” och är en av de aktiviteter som redovisas i handlingsplanen för uppföljning, som nämns ovan.

Granskningen har visat att det sker regelbunden rapporteringen till regionstyrelsen och regionledningen, och att systematiken både grundas i styrande dokument och i ökat intresse från förtroendevalda.

Informationssäkerhetschefen återrapporterar en gång per termin till regionstyrelsen och regionledningen. Informations- och it-säkerhetsfrågor uppges även ingå då säkerhetskommittén rapporterar till ledningens genomgång avseende generella säkerhetsfrågor. Den rapporteringen lämnas till regionstyrelsen en gång per år.

Utöver den strukturerade återrapporteringen sker uppföljning vid behov till regionledning och regionstyrelse. Från flera intervjuade framförs att säkerhetsfrågor ur allmänt perspektiv rönt stort intresse bland förtroendevalda under 2023, varför säkerhetskommittén besökt regionstyrelsen vid ett par tillfällen.

3.7.3 Bedömning

Vi bedömer att det finns en etablerad uppföljning av informations- och it-säkerhetsarbetet.

Vår bedömning är att arbetet rapporteras regelbundet till regionledning och regionstyrelse, och att uppföljningen genomförs i enlighet med styrande dokument och MSB:s rekommendationer för ett systematiskt informationssäkerhetsarbete.

Vi anser att det finns behov av att tydliggöra vilken rapportering av uppföljningen som ska göras till nämnden för folkhälsa och sjukvård. Detta utifrån nämndens verksamhetsansvar.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om regionstyrelsen och nämnden för folkhälsa och sjukvård har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen och nämnden för folkhälsa och sjukvård i allt väsentligt säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Region Jönköpings län har ett upprättat ledningssystem för informationssäkerhet som beskriver former för arbetet och hur ansvaret är fördelat. Det finns i delar ansvar som behöver tydliggöras i de styrande dokumenten och vi konstaterar att ledningssystemet ännu inte implementerats fullt ut i hela verksamheten. Vi bedömer att det finns en ändamålsenlig organisation för arbetet där roller och ansvar är fördelat och upprätthålls.

Det finns behov av att stärka systematiken vad gäller arbetet med informations-klassning och riskanalys. Dessa aktiviteter behöver genomföras för befintliga system för att regionen ska ha tillräckliga underlag för att besluta och införa de säkerhetsåtgärder som det finns behov av. Därtill behövs, i enlighet med styrande dokument, en utvidgning av ansvar där både teknisk och organisatorisk säkerhet beaktas. Detta då klassningar i dagsläget initieras ur ett tekniskt perspektiv, och det därigenom finns risk för att risker och behov av åtgärder inom organisatorisk säkerhet missas.

It-säkerhetsarbetet följer en strukturerad process där säkerhets- och sårbarhetsrisker analyseras löpande och ur flera aspekter. För att upptäcka eventuella brister genomförs systematiska uppföljningar och kontroller av vidtagna åtgärder. Dock saknas reserv- och återgångsrutiner för hälso- och sjukvårdens system, vilket vi ser som nödvändigt för en verksamhet med samhällskritisk karaktär.

Vi ser att det finns en löpande uppföljning av informations- och it-säkerhet och att detta rapporteras i enlighet med styrande dokument. Det uppföljningsarbete som genomförs är ändamålsenligt i syfte att utgöra grund för det fortsatta informationssäkerhetsarbetet men vi ser behov av att tydliggöra krav och former för rapportering till nämnden för folkhälsa och sjukvård i enlighet med deras verksamhetsansvar.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen utifrån sitt samordningsansvar samt verksamhetsansvar att:

- Säkerställa att ledningssystemet för informationssäkerhet implementeras i regionens organisation.
- Säkerställa att det i styrande dokument tydliggörs nämndernas ansvar för informationssäkerhetsarbetet.
- Säkerställa att nuvarande styrdokument kompletteras med ansvar för it-säkerhetsarbetet.

- Säkerställa att ansvar avseende informationsklassningar och riskanalyser inte enbart omfattar det tekniska perspektivet utan även omfattar organisatorisk säkerhet.
- Säkerställa att samtliga system som nyttjas inom Region Jönköpings län genomgår informationsklassning samt riskanalys.
- Säkerställa att rutiner för reserv- och återgångsrutiner vid störning eller avbrott upprättas.
- Tydliggöra i styrande dokument hur former för rapportering till nämnder ska ske.

Utifrån resultatet av vår granskning rekommenderar vi nämnden för folkhälsa och sjukvård att:

- Säkerställa att ledningssystemet för informationssäkerhet implementeras i samtliga verksamheter.
- Genom dialog med regionstyrelsen tillse att personella resurser finns tillgängliga för implementeringsprocessen av LIS inom verksamheterna.
- Säkerställa att samtliga system som nyttjas inom nämnden genomgår informationsklassning samt riskanalys.
- Följa upp att rutiner för reserv- och återgångsrutiner vid störning eller avbrott upprättas för de system som nämnden ansvarar för.
- Tillse att de erhåller en rapportering av uppföljning för informationssäkerheten.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Sofie Ernerudh
Verksamhetsrevisor

Ida Larsson
Verksamhetsrevisor

Veronica Hedlund Lundgren
Certifierad kommunal yrkesrevisor
Kundansvarig

dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.