REGIONREVISORERNA

Rapport nr 13/2025

Omhändertagande av CERT-rekommendationer

Innehållsförteckning

1. Sammanfattning och rekommendationer

Revisionskontoret har granskat it-säkerhetsarbetet i regionens nätverksmiljö med fokus på hantering av rekommendationer om skyddsåtgärder. Syftet med granskningen är att bedöma om akutsjukhusnämnden och fastighets- och servicenämnden har en tillräcklig styrning och kontroll för att säkerställa att CERT:s identifierade it-relaterade risker åtgärdas i tid. Detta för att minimera eller eliminera potentiella hot mot regionens digitala informationsmiljö.

Revisionsfråga	**Svar**	**Motiv för bedömning**
1a. Har akutsjukhusnämnden säkerställt att rekommendationer från CERT åtgärdas effektivt och strukturerat på Danderyds sjukhus?	Delvis	Rekommendationerna från CERT har åtgärdats men det saknas tydliga processer för hanteringen.
1b. Har fastighets- och servicenämnden säkerställt att rekommendationer från CERT åtgärdas effektivt och strukturerat?	Delvis	Rekommendationerna från CERT åtgärdas effektivt men det saknas tydliga processer för hanteringen.
2a. Har akutsjukhusnämnden säkerställt att åtgärder efter rekommendationer från CERT följs upp strukturerat på Danderyds sjukhus?	Nej	Rekommendationerna är få men det görs ingen strukturerad uppföljning.
2b. Har fastighets- och servicenämnden säkerställt att åtgärder efter rekommendationer från CERT följs upp strukturerat?	Ja	Rekommendationer från CERT registreras i serviceförvaltningens ärendehanteringssystem vilket innebär att rekommendationerna följs upp strukturerat.

Revisionskontorets samlade bedömning är att akutsjukhusnämnden behöver stärka sin styrning och kontroll för att säkerställa att CERT:s identifierade IT-relaterade risker åtgärdas i tid. Revisionskontoret bedömer vidare att fastighets- och servicenämnden bör stärka sina processer kopplade till meddelanden från CERT. Revisionskontoret noterar att brister i processer kan komma att lösas i och med implementeringen av den nya riktlinjen för informationssäkerhet och dataskydd.

Rekommendationer

Revisionskontoret bedömer att akutsjukhusnämnden bör:

- utveckla kontrollen över de system som används samt säkerställa att samtliga system har en systemägare

Revisionskontoret bedömer att fastighets- och servicenämnden bör:

- informera nämnder och bolag om säkerhetsincidenter som rör dessas informationstillgångar och tjänster de nyttjar.

2. Utgångspunkter för granskningen

2.1. Bakgrund

Revisorerna beslutade i sin revisionsplan för år 2025 att granska it-säkerhetsarbetet i regionens nätverk med fokus på sårbarheter i och attacker mot regionens nätverksmiljö. I regionstyrelsens förvaltning finns Region Stockholm CERT (Computer Emergency Response Team) som är regionens gemensamma funktion för att förebygga och hantera it- och cybersäkerhetsincidenter. En del av funktionens uppdrag är att varna regionens nämnder och bolag om sårbarheter och brister som kan behöva åtgärdas för att inte utnyttjas och orsaka skada.

Region Stockholms organisering av it är komplex. Nämnder och bolag ansvarar för informationssäkerheten för all information, analog och digital, inom sin verksamhet. Förvaltning av system och applikationer hanteras dock ofta av serviceförvaltningen, andra nämnder eller externa leverantörer. System och applikationer kan vara regiongemensamma med en uppbyggd förvaltningsstruktur och tydligt definierade ansvar men även lokala system och applikationer där roller och ansvar för förvaltning och ägarskapen kan vara mer otydlig eller saknas helt. Det innebär att det finns risk för att styrelser och nämnder inte säkerställer att rekommendationer från CERT omhändertas och åtgärdas.

2.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om akutsjukhusnämnden och fastighets- och servicenämnden har en tillräcklig styrning och kontroll för att säkerställa att CERT:s identifierade it-relaterade risker åtgärdas i tid, för att minimera eller eliminera potentiella hot mot regionens digitala informationsmiljö. För att uppfylla syftet ska följande revisionsfrågor besvaras:

Har akutsjukhusnämnden och fastighets- och servicenämnden

1. säkerställt att meddelanden från CERT åtgärdas effektivt och strukturerat?
2. säkerställt att åtgärder efter meddelanden från CERT följs upp strukturerat?

2.3. Avgränsningar och ansvarig nämnd

Granskningen avser ansvarspröva fastighets- och servicenämnden och akutsjukhusnämndens hantering av rekommendationer som skickas till verksamheterna via Region Stockholms CERT. För akutsjukhusnämnden har Danderyds sjukhus granskats.

2.4. Revisionskriterier

Revisionskriterierna utgör de bedömningsgrunder som bildar underlag för granskningens analyser, slutsatser och bedömningar. Revisionskriterier för denna granskning är:

- **Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174)**

  Lagen är den svenska implementeringen av NIS-direktivet (EU 2016/1148) och ställer krav på att samhällsviktiga aktörer, som sjukhus, bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete samt rapporterar allvarliga IT-incidenter till berörda myndigheter (till exempel MSB).

- **Kommunallag (2017:725) 6 kapitlet**
  Varje nämnd i kommunen eller regionen ansvarar för att verksamheten inom sitt område följer fullmäktiges mål och riktlinjer samt gällande lagar och regler.
- **Policy verksamhetsskydd (RS 2020-0147)**
  Arbetsprocesser och egendom såsom lokaler, infrastruktur, utrustning och information ska värderas och skyddas. Skyddet ska dimensioneras utifrån aktuell hotbild och anpassas till skyddsvärde, riskacceptans och lagkrav. Skyddsåtgärder ska förebygga att informationstillgångar röjs, ändras, görs otillgängliga eller förstörs.
- **Riktlinjer för informationssäkerhet (RS 2020-0148)**
  Riktlinjerna konkretiserar Region Stockholms policy för verksamhetsskydd och är styrande för skyddet av informationstillgångar som hanteras vid Region Stockholms samtliga nämnder och bolag. Riktlinjen tydliggör nämnder och bolags ansvar att medverka i de regionövergripande processer som etablerats för att hantera händelser och sårbarheter, till exempel CERT. En ny riktlinje beslutades i regionfullmäktige den 9 december, 2025, men har inte legat till grund för den här granskningen.

2.5. Metod och kvalitetssäkring

Granskningen är genomförd med dokumentstudier, dels av de styrande dokument som ligger till grund för ansvarsutkrävande, dels lokala dokument som syftar till lag- och regelefterlevnad i verksamheterna så som process- och rutinbeskrivningar för hantering av meddelanden från CERT.

Intervjuer har genomförts med CERT-funktionen, informationssäkerhetssamordnare och incidentmanagers inom respektive förvaltning samt med it-chef och av it-chef utpekade tjänstepersoner.

Källan i iakttagelseavsnitten är intervjuer om inget annat anges specifikt.

Granskningen genomförs av Lisa Höglund (projektledare) och Maria Lingner vid revisionskontoret.

Ett utkast av rapporten har stämts av med intervjupersoner och ledningen för Danderyds sjukhus och serviceförvaltningen. Intern kvalitetssäkring har gjorts av enhetschef Joakim Söderberg och revisionsdirektör Rickard Norberg.

3. Ansvar och förutsättningar

3.1. Förutsättningar

Region Stockholm valde att centralisera delar av it-verksamheten till en regiongemensam intern it-leverantör, SLL IT (sedermera serviceförvaltningen), omkring 2010. Stora delar av teknik och teknisk kompetens flyttades till SLL IT som hade uppdrag att leverera it-tjänster till regionens övriga verksamheter.[1] Idag är stora delar av regionens it centraliserad och även majoriteten av lokala it-system är kopplade till tjänsteöverenskommelser med serviceförvaltningen för att möjliggöra installation i den centraliserade it-miljön.

Region Stockholms mål är att i första hand kommunicera digitalt, både internt och externt, i de situationer där det är lämpligt.[2] Det är därför en prioriterad fråga att stärka Region Stockholms digitala resiliens, det vill säga förmågan att hantera och anpassa sig till digitala hot, störningar och förändringar.[3]

Mot bakgrund av ökade krav på robusthet och it-säkerhet lyfter Regionfullmäktige i Region Stockholms budget för 2025, att samtliga it-tjänster som inte redan är gemensamma ska utvecklas till att bli det. En samordning av de gemensamma stödtjänsterna ska öka robustheten, stärka säkerheten och ge ekonomiska skalfördelar. Att tjänsterna ska vara gemensamma betyder att nämnder och bolag inte ska använda någon annan leverantör eller bedriva dem i egen regi. Tjänsterna ska köpas av fastighets- och servicenämnden.[4]

3.2. Ansvar och roller

Ansvaret för informationssäkerheten är kopplat till verksamhetsansvaret i alla led. Det betyder att varje nämnd eller bolag och varje medarbetare som är ansvarig för en verksamhet också har ansvaret för informationssäkerheten i verksamheten. Samtliga nämnder och bolag ansvarar också för att det finns processer och rutiner för att hantera händelser och sårbarheter som kan utgöra ett hot mot Region Stockholms informationstillgångar inom respektive nämnds och bolags ansvarsområde. Nämnder och bolag ska också medverka i de regionövergripande processer som etablerats i detta syfte.[5]

3.2.1. Regionstyrelsen

Regionstyrelsen ska leda och samordna it- och digitaliseringsverksamhet samt frågor om informationssäkerhet och integritetsskydd.[6] Det innebär bland annat att ansvara för uppsikt över nämndernas och bolagens arbete med informationssäkerhet samt för

[1] Exv: Överenskommelse SLL IT, DSAB, Karolinska universitetssjukhuset, överförande av personal och budget (LS1201-0006-1)

[2] Region Stockholms policy för innovation och digitalisering

[3] Ansvar i ett fortsatt tufft läge, Budget 2025 för Region Stockholm (RS 2024-0217)

[4] Ansvar i ett fortsatt tufft läge, Budget 2025 för Region Stockholm (RS 2024-0217)

[5] Riktlinjer för informationssäkerhet (RS 2020-0148)

[6] Reglementen för regionstyrelsen och övriga nämnder (RS 2022-0762)

analys, ledning och samordning inom området.[7] Säkerhetsövervakning ska tillhandahållas av regionstyrelsen.[8]

3.2.2. **Fastighets- och servicenämnden**

Enligt reglementet[9] ska fastighets- och servicenämnden ansvara för moderna administrativa stödtjänster genom att mot ersättning tillhandahålla tjänster inom bland annat it. Serviceförvaltningen levererar drift och it-förvaltning av regionens infrastruktur samt arbete med klient- och användarstöd och gemensamma plattformar. De ansvarar för systemförvaltning (it), nätverk, servrar, lagring, datacenter, e-post, katalogtjänster och säkerhetslösningar för hela regionen.[10] Det åligger också serviceförvaltningen att livscykelhantera hårdvara och säkerställa att rätt säkerhetsnivåer upprätthålls för de tjänster som de tillhandahåller.

3.2.3. **Danderyds sjukhus**

I linje med Region Stockholms organisation av it består Danderyds sjukhus arbete med it-säkerhet huvudsakligen av att beställa och följa upp it-tjänster från serviceförvaltningen och andra externa leverantörer. Utöver de it-tjänster som Danderyds sjukhus beställer finns även lokala it-system där akutsjukhusnämnden ansvarar för drift och informationssäkerhet. För dessa system ska Danderyds sjukhus utse systemägare.[11] För samtliga system som används på sjukhuset ska akutsjukhusnämnden säkerställa en korrekt användning, rapportera incidenter, säkerställa att personal genomgår informationssäkerhetsutbildning och genomföra en årlig riskanalys för informationstillgångar.[12]

Danderyds sjukhus har sedan bildandet av SLL IT inte längre egen teknisk kompetens för drift och förvaltning av de system sjukhuset använder. Enligt intervjuer finns även ett stort antal system som ägs av verksamheterna, där samordnad insyn och kontroll saknas.

3.2.4. **Informationssäkerhetssamordnare**

Varje nämnd och bolag ska utse en informationssäkerhetssamordnare som har i uppgift att samordna och följa upp arbetet med informationssäkerhet inom den egna organisationen och rapportera allvarliga incidenter till ledningen.[13] När CERT-funktionen startades 2016 ombads nämnder och bolag att identifiera en kontaktperson för CERT-meddelanden och samtliga valde då att utse informationssäkerhetssamordnaren som kontaktperson.

[7] Riktlinjer för informationssäkerhet (RS 2020-0148)

[8] Ansvar i ett fortsatt tufft läge, Budget 2025 för Region Stockholm (RS 2024-0217)

[9] Reglementen för regionstyrelsen och övriga nämnder (RS 2022-0762)

[10] Regionrevisorernas rapport 3/2021 Strategisk styrning av it och digitalisering

[11] Riktlinjer för informationssäkerhet (RS 2020-0148)

[12] Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174)

[13] Riktlinjer för informationssäkerhet (RS 2020-0148)

3.3. CERT (Computer Emergency Response Team)

Region Stockholm CERT, är en övergripande funktion inom regionledningskontoret med uppdrag att stödja Region Stockholms verksamheter med att upptäcka och hantera it-säkerhetsrelaterade hot och händelser. Verksamhetens mål är att minska omfattningen och skadeverkan av it-säkerhetsrelaterade hot och störningar. CERT:s verksamhet är indelad i flera delar, där de delar som granskningen omfattar är bevakning av sårbarheter och avvikelser.

3.3.1. Identifiering av sårbarheter och avvikelser

Identifiering av sårbarheter och avvikelser sker genom:

- Säkerhetsövervakning – it-säkerhetsloggar övervakas och analyseras. Vid bekräftad störning görs en bedömning av vilken åtgärd som är lämplig och hur akut en åtgärd är.
- Sårbarhetsbevakning – CERT genomför regelbunden sårbarhetsscanning. Om en ny hög/kritisk sårbarhet upptäcks så kompletteras scanningsrapporten med information till berörda informationssäkerhetssamordnare, där det framkommer att det är viktigt att åtgärder genomförs. CERT utför även fördjupade analyser vid behov till exempel i form av penetrationstester.

3.3.2. Kommunikation och stöd kring sårbarheter och avvikelser

I de fall säkerhetsövervakning och sårbarhetsscanning resulterar i identifiering av avvikelser och sårbarheter kommuniceras resultatet genom ett CERT-meddelande med rekommendationer till berörda nämnder och bolag. Rekommendationerna är inte ett krav på åtgärd men fungerar som ett instrument för att minska risk för verksamhetsstörningar och stärka regelefterlevnad. Initialt var informationssäkerhetssamordnare mottagare av kommunikation från CERT men det har förändrats över tid och CERT använder nu flera olika kanaler för kommunikation.

Avvikelser
Avvikelser identifieras via säkerhetsövervakningen. För att bekräfta en störning kan CERT-funktionen ta direktkontakt med en användare och dennes chef. Även rekommendationer om åtgärd kan gå den vägen. Bekräftade störningar kommuniceras huvudsakligen till incident manager-funktionen hos berörd nämnd/bolag. Kommunikationsvägen är dock inte konsekvent, för till exempel Danderyds sjukhus går CERT-meddelandet istället till informationssäkerhetssamordnaren. CERT informerar ibland även informationssäkerhetssamordnare om pågående störningar. För system som förvaltas av serviceförvaltningen men berör en annan nämnd eller bolag varierar det också vem som får CERT-meddelandet och information om störningen.

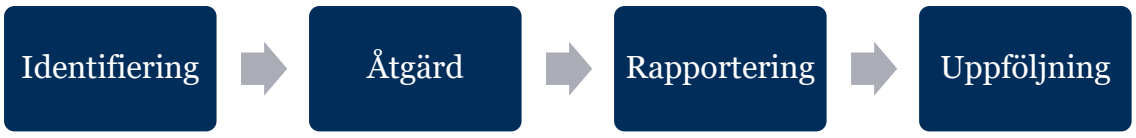
Sårbarheter
Den kontinuerliga sårbarhetsscanningen kommuniceras regelbundet till informationssäkerhetssamordnare vid nämnder och bolag. Fördjupade analyser och tester och rekommendationer kopplat till dessa sker i samverkan med berörda ägare av system eller tjänster.

CERT har som rekommendation att en funktionsyta ska upprättas specifikt för kommunikation mellan CERT och nämnder och bolag. Att det finns en upprättad funktionsyta innebär dock inte att den faktiskt används. Det framkommer inte av rekommendationen vilka roller som bör ha tillgång till informationen.

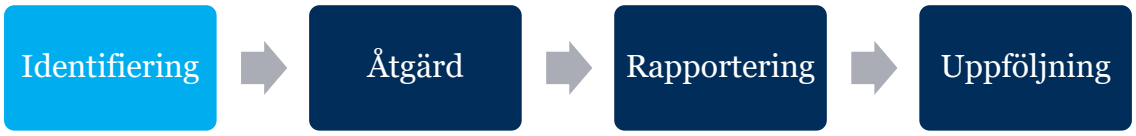
CERT-funktionen tillhandahåller även fördjupat stöd till nämnder och bolag kopplade till pågående incidenter och sårbarheter.

4. Processen

En leverantör av samhällsviktiga tjänster ska ha interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser avseende informationshantering i nätverk och informationssystem.[14]



4.1. Identifiering av sårbarhet eller avvikelse



En leverantör av samhällsviktiga tjänster ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att identifiera, analysera och värdera risker för organisationens information, nätverk och informationssystem.[15]

CERT identifierar en incident eller en sårbarhet och meddelar berörd part. I avsnitten nedan beskrivs mottagarna av CERT:s identifierade sårbarheter och avvikelser.

4.1.1. Danderyds sjukhus

Resultatet från CERT:s planerade, fördjupade analyser kommuniceras direkt till systemägaren/systemförvaltaren, som också informerats inför den fördjupade analysen. I enstaka fall tar CERT direktkontakt med användare och användares chef för att utreda om en avvikelse är en faktisk störning eller ej. Övrig information från CERT går till informationssäkerhetssamordnaren, antingen direkt eller via en utpekad funktionsyta. Det är oklart vem mer än informationssäkerhetssamordnaren som har tillgång till funktionsytan och om någon annan agerar på inkommande meddelanden. I undantagsfall där informationssäkerhetssamordnartjänsten varit vakant har rekommendationer från CERT i stället gått till en av personerna inom incident manager-funktionen. Utöver de regelbundna sårbarhetsrapporterna och ibland information om ärenden som pågår på serviceförvaltning får Danderyds sjukhus endast ett mindre antal meddelanden per år från CERT.

[14] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)

[15] Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174)

4.1.2. **Serviceförvaltningen**

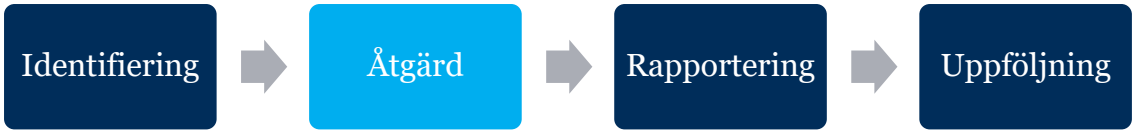
På serviceförvaltningen tar informationssäkerhetssamordnaren regelbundet emot sårbarhetsrapporter från CERT.

Vid mer akuta ärenden kontaktas incident management-funktionen. CERT lägger även in ärenden i serviceförvaltningens ärendehanteringssystem vilket skapar förutsättningar för spårbarhet.

Resultatet från planerade, fördjupade analyser kommuniceras direkt till systemägaren/systemförvaltaren, som också informerats inför den fördjupade analysen.

Serviceförvaltningen och dess underleverantörer genomför kontinuerliga kontroller av servrar. Hanteringen av dessa är dock inte en del av den här granskningen.

4.2. Åtgärd av sårbarhet eller avvikelse



En leverantör av samhällsviktiga tjänster ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att utifrån genomförd informationsklassning och riskbedömning införa ändamålsenliga och proportionerliga säkerhetsåtgärder.[16]

4.2.1. **Danderyds sjukhus**

Danderyds sjukhus saknar processbeskrivning för hur incidenter ska hanteras både från CERT och relaterat till andra it-incidenter. Det finns planer på att ta fram en process för incidenthantering på sjukhuset men det prioriteras inte i nuläget.

Merparten av resultaten från de sårbarhetsscanningarna som genomförs av CERT berör system och tjänster som Danderyds sjukhus köper av serviceförvaltningen vilket innebär att Danderyds sjukhus inte har teknisk rådighet. Dessa tjänster regleras genom tjänsteöverenskommelser. Övriga rekommendationer som berör Danderyds sjukhus medför exempelvis att identifiera och inhämta utrustning när CERT bedömer att den behöver genomgå fördjupad teknisk analys. Ärendena hanteras i dessa fall likartat som andra incidenter. Åtgärder som inte omfattas av tjänsteöverenskommelsen hanteras genom att Danderyds sjukhus lägger en beställning till serviceförvaltningen om åtgärd.

Det framkommer vid intervjuer att vissa incidenter som initieras av CERT och berör Danderyds sjukhus kan lösas av serviceförvaltningen utan att Danderyds sjukhus får kännedom om incidenten.

Trots avsaknaden av en tydlig process uppger såväl incident manager som informationssäkerhetssamordnare att ärenden som inkommer från CERT omhändertas snabbt.

[16] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)

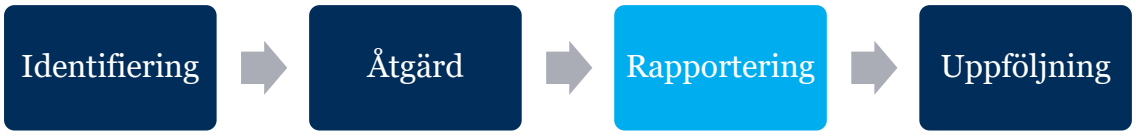
4.2.2. **Serviceförvaltningen**

Serviceförvaltningen har en processbeskrivning för incidenthantering. Processen särskiljer inte rekommendationer från CERT från övriga incidenter. Däremot så innehåller rekommendationer från CERT mer information om till exempel prioritering och åtgärdsförslag än incidenter som identifierats via andra källor. Det gör att det går att bortse från vissa steg i den övergripande processen och att hanteringen i stället kan gå direkt till åtgärd. Processbeskrivningen innebär också att servicedesk-funktionen har en viktig roll i såväl felsökning som verifiering av lösning och återkoppling till användare. Servicedesk medverkar inte i CERT-ärenden.

Det finns en kompletterande rutin för säkerhetsincidenter[17] (en händelse som påverkar eller riskerar att påverka säkerheten i en organisation, ett system eller en process) som beskriver vad en incident manager ska göra vid en säkerhetsincident. Rutinen beskriver huvudsakligen hur interaktionen med CERT ska fungera i det inledande skedet och vilka berörda som ska informeras.

Vilka åtgärder som genomförs beror på vilken typ av incident det rör sig om. Det kan till exempel handla om att hämta in en påverkad dator eller att uppdatera en applikation till den senaste versionen.

4.3. Rapportering av sårbarhet eller avvikelse



”Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller. Rapporteringen ska göras till den myndighet som regeringen bestämmer”[18], i det här fallet MSB.

Incidenter ska enligt MSB:s föreskrifter[19] rapporteras till MSB inom sex timmar med bland annat beskrivning av störningen och vilken samhällsviktig tjänst som berörs. Inom 24 timmar ska rapporteringen kompletteras med information om vilka åtgärder som vidtas för att minimera konsekvenserna av incidenten. Inom fyra veckor ska rapportören informera om vilka åtgärder som vidtagits och ska vidtas för att förebygga och hantera liknande incidenter.

Enligt nuvarande lagstiftning är endast utförare av samhällskritisk verksamhet rapporteringsskyldiga till myndighet. Det innebär att andra delar av samma organisation inte omfattas av rapporteringsskyldighet.

[17] IM rutin för säkerhetsincidenter (KB0015463)

[18] Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174)

[19] Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9)

4.3.1. **Danderyds sjukhus**

Som leverantör av samhällsviktiga tjänster ska Danderyds sjukhus rapportera till myndigheter om de incidenter som har betydande påverkan på verksamheten. Sjukhuset rapporterar till MSB i de fall störningen gör att ett prioriterat system inte kan användas. Det är incident manager-funktionen som hanterar rapportering till myndigheter, i samråd med informationssäkerhetssamordnaren och berörda chefer.

Informationssäkerhetssamordnaren ska ha möjlighet att rapportera större avvikelser till högsta ledningen[20]. Fram till avbolagiseringen rapporterade informationssäkerhetssamordnaren till sjukhusets ledning en gång per år. År 2025 fanns planering för liknande rapportering till ledningen för Danderyds sjukhus men rapporteringen ställdes in på grund av sjukdom. Ett ärende om informationssäkerhet ska upp till akutsjukhusnämnden i mars 2026.

4.3.2. **Serviceförvaltningen**

Serviceförvaltningen är inte rapporteringsskyldiga till myndighet enligt MSB:s föreskrifter om rapportering för samhällsviktiga tjänster. Om en incident inträffar i serviceförvaltningens tjänsteutbud är det den nämnd/bolag som serviceförvaltningen levererar tjänster till som ska rapportera.

För den interna rapporteringen inom fastighets- och servicenämnden har revisionskontoret vid upprepade tillfällen efterfrågat information men inte erhållit något. Vid genomgång av protokoll från fastighets- och servicenämnden syns inga spår av rapportering kopplad till informationssäkerhet.

4.4. Uppföljning av sårbarhet eller avvikelse

En leverantör av samhällsviktiga tjänster ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att följa upp och utvärdera säkerhetsåtgärder i syfte att vid behov anpassa skyddet av informationen.[21]

CERT-teamet gör inte någon uppföljning av vilka åtgärder som vidtas baserat på den information som teamet skickar eller vilka effekter åtgärderna ger.

4.4.1. **Danderyds sjukhus**

Uppföljning av sårbarheter sker genom att informationssäkerhetssamordnaren jämför veckorapporterna från CERT med föregående veckas. Om en sårbarhet åtgärdats bör den ha försvunnit från listan till nästa veckorapport. I övrigt görs ingen uppföljning av

[20] Riktlinjer för informationssäkerhet (RS 2020-0148)
[21] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)

om identifierade sårbarheter har åtgärdats. Enligt intervjuer på grund av att det inte efterfrågats.

Danderyd sjukhus har begränsade förutsättningar att genomföra en samlad uppföljning av aktiviteter som sker till följd av meddelanden och rekommendationer från CERT då kommunikationen sker till olika intressenter inom sjukhuset samt att vissa incidenter blir lösta på serviceförvaltningen utan sjukhusets kännedom.

4.4.2. **Serviceförvaltningen**

Uppföljning av sårbarheter sker genom att informationssäkerhetssamordnaren jämför regelbundna sårbarhetsrapporterna från CERT med föregående rapport. För incidenter som hanteras i serviceförvaltningens ärendehanteringssystem skickar systemet automatiskt en påminnelse om att ett ärende inte är avslutat.

5. Bedömning

5.1. Danderyds sjukhus

Revisionskontoret konstaterar att Danderyds sjukhus får ett fåtal meddelanden från CERT utöver de regelbundna sårbarhetsrapporterna. I granskningen har det inte framkommit tecken på att förekommande fall inte hanterats.

Danderyds sjukhus har en incident manager-funktion som är kontaktbar dygnet runt vilket innebär beredskap för att hantera allvarliga incidenter. CERT-funktionens primära kontaktyta är dock informationssäkerhetssamordnaren som är en enskild individ som jobbar kontorstider. Danderyds sjukhus har skapat en funktionsyta för informationssäkerhet men det finns otydligheter kring vilka som har tillgång till ytan och om någon annan än informationssäkerhetssamordnaren agerar på information som kommer in. Revisionskontoret ser en risk för personberoende kopplat till den CERT-information som går via informationssäkerhetssamordnaren.

Danderyds sjukhus saknar dokumenterade processer och rutiner för it-incidenthantering. Mot bakgrund av att CERT-meddelanden är sällsynta men kan vara akuta bedömer revisionskontoret att en tydlig process för hantering av dessa meddelanden är att rekommendera. Revisionskontoret noterar att avsaknaden av sådana processer sannolikt kommer att åtgärdas genom implementeringen av den nya *Riktlinjen för informationssäkerhet och dataskydd*[22], som beslutades av Regionfullmäktige den 9 december 2025. Riktlinjen föreskriver att regiongemensamma processer för informationssäkerhet och dataskydd ska införas i verksamheterna.

Samtliga nämnder och bolag har ansvar för informationssäkerheten inom sin verksamhet. I intervjuer framkommer att Danderyds sjukhus har bristande kontroll över de it-system som används i sjukhusets verksamheter. Förutom att det saknas en samlad bild av vilka system som används framkommer det att flertalet lokalt inköpta system saknar såväl systemägare som systemförvaltning. Revisionskontoret bedömer att detta riskerar att försena och försvåra omhändertagandet av rekommendationer från CERT. I och med att Danderyds sjukhus köper infrastruktur och drift från serviceförvaltningen finns begränsningar i sjukhusets rådighet över och insyn i den miljö där säkerhetsrisker kan identifieras av CERT-funktionen. I intervjuer med serviceförvaltningen framkommer att det förekommer att serviceförvaltningen åtgärdar incidenter som skickas via CERT och berör Danderyds sjukhus utan att sjukhuset informeras. Vidare framkommer i intervjuer att CERT kommunicerar direkt med systemägare för att utföra riktade tester mot enskilda system där resultatet redovisas till systemägaren utan information till informationssäkerhetssamordnaren eller den lokala it-avdelningen. CERT uppger även att de i vissa fall kontaktar medarbetare på Danderyds sjukhus direkt. Sammantaget ser revisionskontoret en risk att det är svårt för akutsjukhusnämnden att få en samlad bild över statusen på informationssäkerheten på sjukhuset.

Revisionskontoret bedömer att akutsjukhusnämnden bör:

Utveckla kontrollen över de system som används samt säkerställa att samtliga system har en systemägare

5.2. Serviceförvaltningen

I granskningen har det inte framkommit tecken på att serviceförvaltningen inte hanterar de incidenter som identifierats.

Även på serviceförvaltningen konstaterar revisionskontoret ett personberoende relaterat till rollen informationssäkerhetssamordnare.

Serviceförvaltningen har en dokumenterad process för incidenthantering med en kompletterande rutin för allvarliga säkerhetsincidenter. Revisionskontoret menar att processbeskrivningen inte är tillräcklig vid en incident som upptäckts av CERT eftersom de första stegen redan utförts av CERT och de sista stegen saknar mottagare. Den kompletterande rutinen beskriver huvudsakligen hur kommunikationen kring en incident ska se ut och att framtagandet av en åtgärdsplan ska initieras men saknar steg om genomförande, verifiering och avslut. Revisionskontorets bedömning är att process och rutinbeskrivningarna inte är tillräckliga för en effektiv hantering av incidenter identifierade av CERT. Revisionskontoret konstaterar att brister i processer kan komma att lösas i och med den nya riktlinjen.

Revisionskontoret bedömer att fastighets- och servicenämnden bör:

- informera nämnder och bolag om säkerhetsincidenter som rör dessas informationstillgångar och de tjänster de nyttjar.

Vad gör regionrevisorerna?

Regionrevisorerna granskar den verksamhet som bedrivs av regionens nämnder och bolagsstyrelser. Revisionsuppdraget är det största inom kommunal verksamhet.

Att vara revisor är ett förtroendeuppdrag vars syfte är att med oberoende, saklighet och integritet främja, granska och bedöma verksamheten. Den övergripande uppgiften för revisorerna är att granska hur nämnder och styrelser tar sitt ansvar. De förtroendevalda revisorerna är fullmäktiges och ytterst medborgarnas instrument för den demokratiska kontrollen. De har därmed en viktig funktion i den lokala självstyrelsen.

Ledamöter i nämnder och styrelser ansvarar inför fullmäktige för hur de själva, anställda och uppdragstagare genomför verksamheten. I ansvaret ingår att genomföra en ändamålsenlig verksamhet utifrån fullmäktiges mål, beslut och riktlinjer samt de föreskrifter som gäller för verksamheten, på ett ekonomiskt tillfredsställande sätt och med en tillräcklig intern kontroll samt att upprätta rättvisande räkenskaper.

I årsrapporter för nämnder och styrelser sammanfattar revisionskontoret den granskning som genomförts under det gångna året. Verksamhetsrevisionen redovisas löpande i projektrapporter. Publikationerna finns på www.regionstockholm.se. Det går även att prenumerera på regionrevisorernas nyhetsbrev genom att anmäla intresse via e-postmeddelande till regionrevisorerna.rev@regionstockholm.se.

Postadress: Box 22230, 104 22 Stockholm
Besöksadress: Hantverkargatan 25 b (T-bana Rådhuset)
Telefon: 08-737 25 00
E-post: regionrevisorerna.rev@regionstockholm.se
Hemsida: www.regionstockholm.se

Region Stockholm