Region Hovedstaden

Center for IT og Medicoteknologi

Sektion for Informationssikkerhed

Bidrag til ministerredegørelse for Rigsrevisionens beretning om regionernes beskyttelse af sundhedsdata mod cyberangreb

Dato: 14. marts 2025

Rigsrevisionen offentliggjorde deres beretning om regionernes beskyttelse af sundhedsdata mod cyberangreb den 20. januar 2025.

I beretningen konkluderer Rigsrevisionen, at Region Hovedstaden lever tilfredsstillende op til langt de fleste af Rigsrevisionens vurderingskriterier i forhold til at beskytte sundhedsdata mod cyberangreb.

Rigsrevisionen vurderer dog, at Region Hovedstaden kun delvist lever op til følgende vurderingskriterier:

- Region Hovedstaden har et tilstrækkeligt overblik over it-systemer med sundhedsdata, men der foretages ikke en systematisk vurdering af, hvor kritiske it-systemerne er for driften.
- Region Hovedstaden har et større antal enheder, såsom PC'er, mobiltelefoner og tablets med adgang til sundhedsdata, som ikke er sikkerhedsopdateret.

Dertil vurderer Rigsrevisionen, at Region Hovedstaden ikke lever op til følgende vurderingskriterier:

- Region Hovedstaden har ikke implementeret et såkaldt multifaktorlogin ved ekstern adgang til kritiske it-systemer, og dermed lever regionen ikke op til dette kontrolområde.
- Region Hovedstaden har ikke i tilstrækkelig grad foretaget en såkaldt segmentering af de kritiske it-systemer.

Region Hovedstadens bemærkninger

Region Hovedstaden er positive overfor, at Rigsrevisionen har taget initiativ til at undersøge regionernes beskyttelse af sundhedsdata mod cyberangreb og er grundlæggende enig i Rigsrevisionens fund og konklusioner. Hertil er regionen tryg ved, at Rigsrevisionens konklusioner er i overensstemmelse med de opmærksomhedspunkter, som Region Hovedstaden har fokus på i arbejdet med regionens cybersikkerhed. Det bestyrker, at Region Hovedstaden har rette prioritering og allokering af ressourcer til området.

Region Hovedstaden bemærker, at undersøgelsen viser, at regionen efterlever størstedelen af Rigsrevisionens vurderingskriterier tilfredsstillende, herun-

der en række vigtige områder, der beskytter regionen mod cyberangreb. Eksempelvis har regionen en ensartet og robust sikkerhedsinfrastruktur, der proaktivt forhindrer trusler gennem let og ensartet udrulning af sikkerhedsopdateringer. Dertil er regionen særligt tilfredse med, at undersøgelsen viser, at Region Hovedstadens cyberberedskab lever op til samtlige vurderingskriterier vedrørende beredskab. Det afspejler regionens fokus på ikke udelukkende at undgå ulovlig indtrængen i regionens systemer, men i høj grad også at forberede sig på at håndtere potentielle hændelser og angreb.

Generelt er forebyggelse af cyberangreb omkostningstungt og omfattende, og selvom der tages de nødvendige tiltag for at sikre sig, vil truslen fra cyberangreb være en grundpræmis i en digitaliseret sundhedssektor. Derfor er et stærkt cyberberedskab afgørende for at kunne beskytte sundhedsdata og forhindre, at hospitalsvæsnet sættes ud af drift ved angreb.

Region Hovedstaden bemærker derudover, at Rigsrevisionens fund overordnet ligger i tråd med regionens fokus for det videre strategiske arbejde med cyber- og informationssikkerhed i Region Hovedstaden. Regionen lancerede i 2024 en strategi for cyber- og informationssikkerhed 2024-2027, og indsatsområderne i strategien imødekommer - foruden kommende lovgivningsmæssige krav på området - de fleste af de områder, som Rigsrevisionen udpeger som genstand for modning. I regionens arbejde med cyber- og informationssikkerhed er der anlagt en risikobaseret tilgang, der afvejer sandsynligheden og risikoen ved et cyberangreb med de økonomiske hensyn og den sikkerhed, der opnås ved tiltaget. Således sikres det, at regionen opnår mest mulig sikkerhed for de ressourcer, der er allokeret til området.

Region Hovedstadens initiativer

Initiativerne i regionens strategi for cyber- og informationssikkerhed imødekommer overvejende Rigsrevisionens konklusioner. Dertil er iværksat en række opfølgende indsatser, som skal imødekomme de vurderingskriterier, hvor Region Hovedstaden finder behov for yderligere fokus for at sikre regionens sundhedsdata mod cyberangreb.

For de områder, hvor Rigsrevisionen vurderer, at Region Hovedstaden delvist efterlever vurderingskriterierne, gælder det:

- Region Hovedstaden er enig i Rigsrevisionens vurdering af, at regionen ikke foretager en systematisk vurdering af, hvilke it-systemer der er mest driftskritiske, og dermed kun delvist lever op til vurderingskriteriet om at sikre et tilstrækkeligt overblik over it-systemer med sundhedsdata. Denne problemstilling indgår som et selvstændigt indsatsområde i regionens strategi for cyber- og informationssikkerhed 2024-2027 og forventes at være etableret ultimo 2025. Konkret forventer regionen at have færdiggjort en simpel metode og model til klassificering af it-porteføljen efter kritikalitet i Q2 2025. Regionen forventer ligeledes

at have fuldendt kortlægning af de 20 mest kritiske systemer indenfor hver af regionens domæner samt de samfundskritiske NIS2 tjenester inden udgangen af Q4 2025.

- Region Hovedstaden er uenig i Rigsrevisionens vurdering af, at regionen ikke har sikkerhedsopdateret enheder såsom PC'er, mobiltelefoner og tablets. Rigsrevisionens vurdering baserer sig på, om enheder kører på de nyeste versioner af styresystemet (fx iOS på apple-produkter). Region Hovedstaden vurderer dog, at så længe det pågældende styresystem sikkerhedsopdateres på enhederne, anses det som sikkert, selvom der eksisterer en nyere version af styresystemet. Regionen bemærker, at Region Hovedstaden har en proces for opdatering af operativsystemer, indtil udstyr ikke længere modtager sikkerhedsopdateringer og herefter udfasning. Der er desuden et hensyn til regionens ressourcer i udskiftning af udstyr.

For de områder, hvor Rigsrevisionen vurderer, at Region Hovedstaden ikke efterlever vurderingskriterierne, gælder det:

- Region Hovedstaden er enig i Rigsrevisionens vurdering af, at regionen ikke har tilstrækkeligt multifaktorlogin ved ekstern adgang til kritiske it-systemer. Regionen har i august 2024 påbegyndt et projekt vedrørende multifaktorautentifikation på regionens firewalls samt styringsplatformen hertil. Det betyder, at alle brugere i regionen samt den eksterne leverandør skal bruge multifaktorlogin for at logge på regionens firewalls, hvilket imødekommer en delmængde af Rigsrevisionens vurderingskriterium. Hertil arbejder Region Hovedstaden løbende på en udbygning af multifaktorautentifikation ved ekstern adgang til kritiske it-systemer. Region Hovedstaden har igangsat en indsats, der skal imødekomme dette vurderingskriterium senest ultimo 2026.

- Region Hovedstaden er enig i Rigsrevisionens vurdering af, at regionen ikke foretager tilstrækkelig segmentering af regionens netværk. Segmentering af regionens netværk indgår som et selvstændigt indsatsområde i regionens strategi for cyber- og informationssikkerhed 2024-2027. I regi af indsatsområdet i strategien er segmentering af regionens netværk for nuværende testet på Amager- og Bornholms Hospital med henblik på at udrulle segmenteringen på regionens øvrige hospitaler, hvilket forventes i mål i Q3 2026.

Regionen bemærker, at Region Hovedstaden er den eneste region med to vurderingskriterier, som Rigsrevisionen ikke vurderer at være tilfredsstillende. Dette skal blandt andet ses i lyset af Region Hovedstadens omfang og kompleksitet på it-området samt regionens størrelse. Vurderingen ændrer ikke på regionens overordnede prioritering, og at patienterne fortsat kan føle sig

trygge ved, at sundhedsdata og hospitalsdriften generelt er tilstrækkeligt beskyttet mod cyberangreb i regionen.

Rigsrevisionens konklusioner vil indgå som en vigtig del af det videre arbejde med cyber- og informationssikkerhed i regionen og supplerer strategien for cyber- og informationssikkerhed 2024-2027.