SUNDHEDS-
OG ÆLDREMINISTERIET

Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Sundhedsministeren

Statsrevisorerne Sekretariatet
Folketinget Christiansborg
1240 København K
ministersvar@ft.dk

Dato: 5. marts 2018
Enhed: SUNDOK
Sagsbeh.: DEPMAHA
Sagsnr.: 1702738
Dok. nr.: 550072

Sundhedsministerens redegørelse til Statsrevisorerne vedr. Rigsrevisionens beretning nr. 04/2017 om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata

Statsrevisorerne har den 22. november 2017 fremsendt deres beretning nr. 04/2017 om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata.

Jeg vil indledningsvist gerne kvittere for, at beretningen sætter fokus på en helt central sikkerhedsdagsorden. Det øget trusselsniveau mod sundhedssektoren understreger, at modstandsdygtighed og styrket sikkerhed er afgørende for, at sundhedsvæsenet kan opretholde sin funktionalitet og beskytte borgernes sundhedsoplysninger. Det er et emne, som er højt prioriteret i Sundheds- og Ældreministeriet.

Jeg har indhentet udtalelser på baggrund af beretningen fra regionsrådet i hhv. Region Syddanmark, Region Midtjylland og Region Hovedstaden, *jf. §18, stk. 3 i lov om revisionen af statens regnskaber mv.* Udtalelserne er vedlagt denne redegørelse som bilag.

Rigsrevisionens beretning og statsrevisorernes bemærkninger
Rigsrevisionen vurderer, at de 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata ikke er tilfredsstillende. Det betyder, at der er risiko for, at følsomme og fortrolige persondata kommer i hænderne på uvedkommende eller ikke er pålidelige og tilgængelige, når der er brug for dem. På den baggrund er det Rigsrevisionens vurdering, at de grundlæggende tiltag mod hackerangreb og beskyttelse af adgangen til it-systemer og sundhedsdata bør prioriteres højt i alle landets regioner.

Rigsrevisionen bemærker i øvrigt, at de 3 regioner har oplyst, at de efterfølgende har iværksat konkrete initiativer i forhold til de undersøgte områder, der imødekommer flere af Rigsrevisionens kritikpunkter.

Statsrevisorerne er enig i Rigsrevisionens konklusioner og bemærker:

- At grundlæggende sikringstiltag mod hackerangreb ikke i tilstrækkelig grad er implementeret i nogen af de 3 regioner. Særligt kritisk er det, at 27.000 medarbejdere i Region Syddanmark har lokaleadministratorrettigheder, da det øger risikoen for hackerangreb.
- At styring og kontrol af medarbejdere med privilegerede rettigheder er mangelfulde i alle 3 regioner, herunder at der er utilstrækkelig begrænsning af mulighed for at tilgå internettet, når der logges på med privilegerende rettigheder.

- At Region Syddanmark og Region Hovedstaden har passwords til system- og servicekonto, der ikke har været skiftet i lang tid.
- At alle 3 regioners logningstiltag er mangelfulde, hvilket gør det vanskeligt at opdage og opklare hackerangreb og misbrug af rettigheder. Region Midtjylland har ikke implementeret nogen af de undersøgte logningstiltag, selv om regionen har udarbejdet en politik for området.

Regionernes bemærkninger og tiltag
Sundheds- og Ældreministeriet har indhentet udtalelser fra regionsrådet i hhv. Region Syddanmark, Region Midtjylland og Region Hovedstaden. Udtalelserne, som fremsendt til Sundheds- og Ældreministeriet, er vedlagt i sin hele form som bilag. Nedenfor indgår regionernes bemærkninger og tiltag til beretningens kritikpunkter.

Region Syddanmark
Regionsrådet i Region Syddanmark oplyser i udtalelsen, at: "Region Syddanmark har forholdt sig til Rigsrevisionens kritikpunkter og har etableret en række indsatser med henblik på, at i mødekomme Rigsrevisionens kritik."

Ad kritik vedr. politik for it-sikkerhed på udvalgte områder
Til kritikken om, at Region Syddanmark ikke har udarbejdet en politik, retningslinjer og procedurer på området oplyser regionsrådet: "Udformning af generelle retningslinjer afsluttes i juni 2018. Aktuelt er de første 6 ud af 15 i proces."

Ad kritik vedr. beskyttelse mod hackerangreb
Til kritikken om, at Region Syddanmark ikke har sikret, at ingen medarbejdere har lokaladministratorrettigheder oplyser regionsrådet: "Region Syddanmark udruller Windows 10 til alle PC'er i 2018. I den forbindelse fjernes lokale administratorrettigheder."

Ad kritik vedr. medarbejdere med privilegerede rettigheder
Til kritikken vedr. medarbejdere med privilegerede rettigheder og adgang til internettet oplyser regionsrådet: "Løsningen er udrullet til IT i 2017. Udbredes til resten af regionen i 2018."

Ad kritik vedr. system- og servicekonto med privilegerede rettigheder
Regionsrådet oplyser, at indsatsen her er gennemført.

Ad kritik vedr. logning af konto med privilegerede rettigheder
Regionsrådet oplyser, at indsatsen her er gennemført.

Endelig oplyser regionsrådet, at Region Syddanmark har taget Rigsrevisionens kritik til efterretning, og at regionen inden udgangen af 2018 har etableret de tilstrækkelige tiltag, der imødekommer kritikken.

Region Midtjylland
Regionsrådet i Region Midtjylland oplyser i udtalelsen, at Region Midtjylland arbejder "…til stadighed med at minimere risikoen for, at følsomme og fortrolige persondata kommer i hænderne på uvedkommende eller ikke er pålidelige og tilgængelige, når der er brug for dem."

Regionsrådet fremhæver, at arbejdet med informationssikkerhed i regionen sker i et

helheldsorienteret perspektiv og oplyser: ”Der er udarbejdet en ”Handleplan for Informationssikkerhed”, som er et flerårligt projekt med en lang række initiativer som adresserer forhold i lovgivning, politikker, analyser og revisionsrapporter. Flere af handleplanens initiativer adresserer opmærksomhederne i Rigsrevisionens beretning.”

I relation til de anførte bemærkninger i beretningen bemærker regionsrådet specifik til tre kritikpunkter:

Ad kritik vedr. grundlæggende sikringstiltag mod hackerangreb
Regionsrådet oplyser: ”Region Midtjylland har afsluttet migrering af ny platform ”Fælles It-platform” med udfasning af XP-enheder i Regionen. Dataudtræk pr. 8. januar 2018 viser, at der i en periode på 14 dage forud herfor er blevet registreret 983 aktive XP-enheder. Enhederne beskyttes med alternative sikkerhedsforanstaltninger.”

Med hensyn til kritikken vedrørende manglende begrænsning af download af programmer oplyser Regionsrådet: ”… at Region Midtjylland ikke har indført begrænset mulighed for download af programmer, men derimod har implementeret teknologi, som sikrer, at kun godkendte programmer afvikles.”

Ad kritik vedr. styring og kontrol af medarbejdere med privilegerede rettigheder
Regionrådet oplyser: ” Region Midtjylland har udbedret de anførte forhold omkring tilgang til internettet for privilegerede brugere herunder udarbejdet manglende politikker og implementeret kontrol af brugerrettigheder.”

Ad kritik vedr. logning af konto med privilegerede rettigheder
Regionsrådet oplyser: Region Midtjylland viderefører igangværende logningsprojekter som anført i Region Midtjyllands ”Handleplan for Informationssikkerhed”.”

Region Hovedstaden
Regionsrådet i Region Hovedstaden oplyser i udtalelsen, at Region Hovedstaden har kontinuerligt fokus på at forbedre og øge it-sikkerheden i takt med udviklingen i trusselsbilledet. Det fremhæves bl.a.: ”... Region Hovedstaden (har, red.) blandt andet implementeret systemer, der kan identificere kendte sikkerhedsrisici og minimere risiko for skadelig adfærd. Ligesom der sker monitorering af regionens internetforbindelse døgnet rundt.” Derudover bemærker regionsrådet, at regionen har: ”stort fokus på medarbejdernes awareness ift. angreb gennem løbende informationstiltag, kampagner m.m.”

Regionsrådet gør desuden opmærksom på, at idet Region Hovedstaden skal løse opgaven på sikkerhedsområdet for de midler, der er til rådighed for området, er regionen meget fokuseret på, at få prioriteret rigtigt, således at de får mest mulig sikkerhed for midlerne.

I relation til de anførte bemærkninger i beretningen bemærker regionsrådet specifik til tre kritikpunkter:

Ad kritik vedr., at Region Hovedstaden ikke har sikret, at medarbejdere med privilegerede rettigheder ikke kan gå på nettet, når de er logget på med deres privilegerede rettigheder.

Regionsrådet oplyser: ”Region Hovedstaden har siden Rigsrevisionens it-revision den 5. januar 2017 arbejdet med en løsning der sikrer, at medarbejderne med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder. Denne løsning forventes færdig implementeret i første kvartal af 2018.”

Ad kritik vedr., at Region Hovedstaden ikke har sikret, at alle system- og servicekonto har autogenererede passwords og at dette er systemunderstøttet.
Regionsrådet oplyser: ”Region Hovedstaden kan tilføje, at de system- og servicekonti, der ikke havde systemunderstøttede autogenerede passwords, på tidspunktet for it-revisionen, var til ældre systemer, der fik passwords, inden regionen fik indført et system til at autogenerere passwords. Region Hovedstaden har efterfølgende imødekommet Rigsrevisionens kritik og indført systemunderstøttelse ift. at sikre, at passwords til konti med privilegerede rettigheder følger god praksis. Der udestår dog endnu nogle få gamle konti, hvor det ikke har været muligt at ændre passwords. En række af disse vil blive lukket ned i 2018, og for de øvrige vil rettighederne blive bragt ned til et niveau, så de ikke er privilegerede. Dette arbejde forventes at kunne gøres færdigt i første kvartal af 2018.”

Ad kritik vedr., at Region Hovedstaden ikke logger, når brugere med privilegerede rettigheder starter programmer, men kun, at de logger af og på.
Regionsrådet oplyser: ”Region Hovedstaden har desuden igangsat en proces ift. at få etableret logning, når medarbejdere med privilegerede rettigheder starter programmer. Det er dog en både kompliceret, dyr og omfattende proces, som det vil tage tid at få allokeret, implementeret og gennemført. Logningsløsningen vil endvidere være omkostningstung at etablere. Systemet er under indkøb og første fase af implementeringen vil være færdig med udgangen af 2018.”

Med hensyn til det forhold, at Rigsrevisionen vurderer, at Region Hovedstaden kun delvist har sikret, at regionen modtager sikkerhedsopdateringer fra producenterne af relevante produkter oplyser regionsrådet ”… regionen kan hente sikkerhedsopdateringer fra relevante producenter og der er indført faste patchprocedurer for servere og computere.” Ydereligere gør regionsrådet opmærksom på, at regionen har afviklet en betydelig del af sine XP-computere. Antallet af XP-computere er fra primo 2016 til ultimo 2017 reduceret fra 3500 til ca. 320. Dertil oplyser regionsrådet: ” Region Hovedstaden er i proces med at sikre de resterende XP-computere bag firewalls, indtil de kan opgraderes eller erstattes af nyere løsninger.”

Endelig gør regionsrådet opmærksom på, at Rigsrevisionens beretning også påpeger andre punkter, hvor regionen kun delvist opfylder kravene. Hertil bemærker regionsrådet: ”Som det også fremgår af beretningen, så har Region Hovedstaden siden it-revisionen i januar 2017 dog iværksat en række tiltag for at imødekomme de øvrige kritikpunkter, som Rigsrevisionens beretning påpeger.”

Sundheds- og Ældreministeriets foranstaltninger og overvejelser

- *Overvejelser ift. beretningens indhold og konklusioner*

Rigsrevisionens beretning indeholder en alvorlige kritik af de 3 regioners beskyttelse af adgange til it-systemer og sundhedsdata, og jeg deler Rigsrevisionens vurdering af, at de grundlæggende tiltag mod hackerangreb og beskyttelse af adgangen til it-systemer og sundhedsdata bør prioriteres højt i alle landets regioner.

Det er min klare forventning, at regionerne arbejder – og fremadrettet forsat vil arbejde aktivt og systematisk med at beskytte adgange til it-systemer og sundhedsdata for at forebygge hackerangreb, som naturligt led i det ansvar regionerne har for it og sikkerhed på sygehusene.

- *Overvejelser ift. regionens bemærkninger*

Regionsrådenes udtalelser vider om, at alle tre regioner arbejder med at forbedre deres sikkerhed, og at alle 3 regioner har iværksat tiltag, der retter op på store dele af kritikpunkterne i beretningen. Beretningen er således med til at rette et relevant fokus og fremadrettet forbedre sikkerheden i regionerne, og regionerne har flere steder taget kritikken til efterretning.

Jeg noterer mig dog flere steder, at regionerne oplyser, at de forventer at imødekomme dele af kritikken i løbet af 2018, uden en nærmere præcisering af tidspunktet for udbedring.

Derudover er det min klare forventning, at regionerne iværksætter indsatser, der dels imødekommer Rigsrevisionens konkrete kritikpunkter, og dels fremadrettet arbejder med at forbedre og sikre beskyttelsen af adgangen til it-systemer og sundhedsdata i takt med, at trusselbilledet og teknologien udvikler sig over tid. Det er en del af regionernes ansvarsforpligtelse som driftsherrer af sundhedsvæsenet.

- *Sundheds- og Ældreministeriets tiltag*

Jeg skal indledningsvist oplyse, at regeringen og regionerne i forbindelse med økonomiaftalen for 2016 har aftalt at gøre sikkerhedsstandarden ISO27001 obligatorisk. Det fremgår samtidig af Den fællesoffentlige digitaliseringsstrategi, at alle offentlige myndigheder skal følge principperne i den internationale standard for informationssikkerhed. Standarden udstikker retningslinjer og krav til informationssikkerhed, risikostyring og kontroller herunder af adgangen til it-systemer og sundhedsdata.

Det er min vurdering, at beretningens konklusioner tydeliggør et behov for en systematisk indsats for at hæve niveauet for beskyttelse af adgange til it-systemer og sundhedsdata i regionerne.

Regeringen offentliggør inden længe en ny national strategi for cyber- og informationssikkerhed, hvoraf det fremgår, at de særligt udsatte sektorer, herunder sundhedssektoren skal udarbejde en sektorspecifik cyber- og informationssikkerhedsstrategi. Sundheds- og Ældreministeriet udarbejder i samarbejde med Danske Regioner og KL, herunder med inddragelse af praksissektoren m.fl. denne strategi, netop fordi ansvaret for beskyttelse af sundhedsdata ligger hos driftsherrerne.

Strategien for sundhedssektoren har til formål at sikre et forsvarligt informationssikkerhedsmæssigt beredskab inden for sundhedssektoren samt styrke og ensrette arbejdet med cyber- og informationssikkerhed på tværs af sektoren med henblik på at forudsige, forebygge, opdage og håndtere cyberangreb. Strategien vil således sætte rammen for, at sundhedssektoren arbejder systematisk og risikobaseret med cyber- og informationssikkerhed.

Ved implementering af EU-direktivet om net- og informationssystemer i sundhedssektoren (NIS-direktivet) vil der bl.a. blive stillet krav om, at operatører af væsentlige tjenester træffer passende sikkerhedsforanstaltninger, der står mål med risikoen. Regionerne forventes, i dele af deres funktion, at være en operatør af en

væsentlig tjeneste. Desuden etableres der en statslig tilsynsfunktion i Sundhedsdatastyrelsen, som skal sikre, at operatørerne opretholder et passende sikkerhedsniveau. Implementering af NIS-direktivet stiller således en række krav til operatørerne med henblik på at opretholde et funktionelt sundhedsvæsen, og hvor borgerne har tillid til digitale løsninger i sundhedsvæsenet.

Endelig har regeringen, med den netop lancerede Strategi for digital sundhed 2018-2022, i samarbejde med Danske Regioner og KL også under overskriften "Tillid og sikkerhed om data" lagt spor for de fortsatte indsatser med cyber- og informationssikkerhed. Det gælder bl.a. borgeradgang til logoplysninger fra hospitaler, modernisering af it-sikkerhedsstandarder i sundhedsvæsenet, og ikke mindst, etablering af et politisk cyberforum, hvor parterne på politisk niveau kan drøfte og sætte retning for håndtering af udfordringer knyttet til cybersikkerhed mv.

Kopi af denne redegørelse er sendt til Rigsrevisionen på rr@rigsrevisionen.dk.

Med venlig hilsen

Ellen Trane Nørby