Region Hovedstaden

Center for It, Medico og Telefoni

Til Sundheds- og Ældreministeriet

Journal-nr.: 16043917

Dato: 1. februar 2018

Udtalelse fra regionsrådet i Region Hovedstaden til Sundheds- og Ældreministeriets redegørelse til Statsrevisorerne

Region Hovedstaden har kontinuerligt fokus på at forbedre og øge it-sikkerheden i takt med udviklingen i trusselsbilledet. Derfor tager Region Hovedstaden også Rigsrevisionens konklusioner og Statsrevisorernes udtalelser meget alvorligt og prioriterer at få løst de problemer, som Rigsrevisionen påpeger.

En af de store udfordringer for alle, der arbejder med it-sikkerhed, er, at trusselsbilledet forandrer sig konstant, da der er tale om stigende organiseret cyberkriminalitet samt stadig mere kreative og dygtige hackere.

Derfor har Region Hovedstaden blandt andet implementeret systemer, der kan identificere kendte sikkerhedsrisici og minimere risiko for skadelig adfærd. Ligesom der sker monitorering af regionens internetforbindelse døgnet rundt.

Region Hovedstaden vurderer og implementerer løbende nye sikkerhedstiltag for at styrke opbygning af en robust it- og sikkerheds-arkitektur. I dette arbejde inddrages regionens sikkerhedspartnere, ligesom der løbende via partnerne sker en afprøvning af sikkerhedstiltag. Regionen videndeler samtidig om cybersikkerhed med lignende organisationer, deltager i erfaringsudvekslingsfora i et regionalt og privat samarbejde samt har et løbende samarbejde med Center for Cybersikkerhed med henblik på at vurdere behovet for tilpasning af vores indsats.

Region Hovedstaden har også et stort fokus på medarbejdernes awareness ift. angreb gennem løbende informationstiltag, kampagner m.m. Hospitalernes ledelse og medarbejderne er således helt centrale medspillere ift. at reagere korrekt på eksempelvis phishing-mails, således at der centralt kan iværksættes effektive tiltag for regionen. Konkrete hændelser har vist at opmærksomheden på f.eks. phishing-mails er stor, og at medarbejderne er rigtig gode til at agere med sund skeptisk samt gøre vores Center for It, Medico og Telefoni opmærksom på, når de modtager mistænkelige mails.

Da Region Hovedstaden også på sikkerhedsområdet skal løse opgaven for de midler, der er til rådighed for området, er vi meget fokuserede på, at vi får prioriteret rigtigt, således at vi får mest mulig sikkerhed for midlerne.

Rigsrevisionen vurderer i deres rapport konkret i forhold til Region Hovedstaden, at regionen på følgende tre punkter - ud af de i alt 13 kritikpunkter - ikke har opfyldt Rigsrevisionens krav:

1. 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
2. At Region Hovedstaden ikke har sikret, at alle system- og servicekonti har autogenererede passwords og at dette er systemunderstøttet
3. At Region Hovedstaden ikke logger, når brugere med privilegerede rettigheder starter programmer, men kun, at de logger af og på.

Ad 1)
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 færdigimplementeret i første kvartal af 2018.

Ad 2)
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 3)
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.

Rigsrevisionen vurderer desuden, at Region Hovedstaden kun delvist har sikret, at regionen modtager sikkerhedsopdateringer fra producenterne af relevante produkter, idet regionen fortsat har pc'ere med Windows XP, som producenten ikke leverer sikker-

hedsopdateringer til mere. Regionen ønsker at tilføje, at regionen kan hente sikkerhedsopdateringer fra relevante producenter og der er indført faste patchprocedurer for servere og computere.

Regionen har desuden afviklet en betydelig del af sine XP-computere. Primo 2016 var det samlede antal XP-computere i Region Hovedstaden således 3500 XP-computere. I ultimo december 2017 var antallet reduceret til cirka 320. XP-computere udgør således under 1 % procent af regionens samlede antal pc'ere.

De resterende XP-computere udfases hurtigst muligt. Der er dog helt specifikke grunde til, at de sidste pc'ere er vanskelige at få afviklet. Herunder har en del af de resterende XP-computere softwareprogrammer installeret, som ikke findes i en udgave der kan afvikles på operativsystemer, der er nyere end Windows XP.
Region Hovedstaden er i proces med at sikre de resterende XP-computere bag firewalls, indtil de kan opgraderes eller erstattes af nyere løsninger.

Rigsrevisionen påpeger i beretningen også andre punkter, hvor Region Hovedstaden kun delvist opfylder kravene. 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.

Region Hovedstaden har, som allerede nævnt, kontinuerligt fokus på at forbedre og øge it-sikkerheden. En god it-sikkerhed er en nødvendighed for at sikre data og stabil drift på systemerne i det daglige arbejde på hospitalerne. Regionen har iværksat indsatser og opfølgning på alle kritikpunkterne fra Rigsrevisionen.

Region Hovedstaden

Center for It, Medico og Telefoni

Til Sundheds- og Ældreministeriet

Journal-nr.: 16043917

Dato: 1. februar 2018

Bilag: Status for udbedring af Rigsrevisionens kritik af Region Hovedstaden

Kritikpunkt	Status
Angivet som "Ikke opfyldt" i Rigsrevisionsrapporten	
Sikring af, at medarbejdere med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med de rettigheder	**Under udbedring.** Region Hovedstaden arbejder med en løsning der sikrer, at medarbejderne med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder. Løsningen forventes færdigimplementeret i første kvartal 2018.
Passwords til system- og servicekonti med privilegerede rettigheder følger god praksis og er systemunderstøttede	**Delvis udbedret. Rest udestår.** 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 stade, så de ikke er privilegerede. Dette arbejde forventes at kunne gøres færdigt i første kvartal af 2018.
Logning af konti med privilegerede rettigheder, når de starter programmer	**Under udbedring.** Systemet til understøttelse af dette er under indkøb. Implementeringen er omfattende og er opdelt i 3 faser. Første fase af implementeringen forventes færdig i udgangen af 2018.

Kritikpunkt	Status
Angivet som "Delvist opfyldt" i Rigsrevisionsrapporten	
Begrænset download af programmer	**Delvis opfyldt. Rest under analyse.** Det er kun muligt for administratorer at installere software. Derfor vil en almindelig bruger, der f.eks. prøver at opdatere et program der downloader software, blive forhindret i det. Den påpegede risiko er allerede meget minimeret i Region Hovedstaden, idet det alene er den meget begrænsede gruppe af administratorer, der har adgang til pc'en der kan installere software. Der pågår en analyse af, hvilke tekniske tiltag der er mulige for at adressere dette, uden at øge risikoen for at nødvendige programmer til patientbehandling ikke kan afvikles korrekt.
Kun godkendte programmer kan afvikles	**Under udbedring / vurdering.** Systemet som kan sikre dette er pt. i "læringsmode". Vurdering af om systemets 'whitelisting' i praksis kan indføres tages ved udgangen af første kvartal 2018. Vurdering omfatter ligeledes vurdering af potentiel øget risiko for at nødvendige programmer til patient behandling ikke kan afvikles korrekt.
Regionen kan hente sikkerhedsopdateringer fra producenter af relevante programmer	**Udbedret.** Status er at regionen kan hente sikkerhedsopdateringer fra relevante producenter. Der er indført faste patchprocedure for servere og computere. Rigsrevisionen vurderer desuden, at Region Hovedstaden kun delvist har sikret, at regionen modtager sikkerhedsopdateringer fra producenterne af relevante produkter, idet regionen fortsat har pc'ere med Windows XP, som producenten ikke leverer sikkerhedsopdateringer til mere. Regionen ønsker at tilføje, at regionen kan hente sikkerhedsopdateringer fra relevante producenter og der er indført faste patchprocedurer for servere og computere. Regionen har desuden afviklet en betydelig del af sine XP-computere. Primo 2016 var det samlede antal XP-computere i Region Hovedstaden således 3500 XP-computere. I ultimo december 2017 var antallet reduceret til cirka 320. XP-computere udgør således under 1 % procent af regionens samlede antal pc'ere.

Journal-nr.: 16043917

Dato: 16. januar 2018

	De resterende XP-computere udfases hurtigst muligt. Der er dog helt specifikke grunde til, at de sidste pc'ere er vanskelige at få afviklet. Herunder har en del af de resterende XP-computere softwareprogrammer installeret, som ikke findes i en udgave der kan afvikles på operativsystemer, der er nyere end Windows XP. Region Hovedstaden er i proces med at sikre de resterende XP-computere bag firewalls, indtil de kan opgraderes eller erstattes af nyere løsninger.
Etablering af tiltag f.eks. segmenteret netværk, så en inficering i form af hackere eller malware ikke kan sprede sig ubegrænset	**Forbedret.** Status er at der er macro segmentering i datacenteret. Derudover er der IP-segmentering på netværket. Derved vil det være begrænset hvor store områder en hacker kan få adgang til ved et eventuelt brud.
Begrænset antal medarbejdere, der permanent har privilegerede rettigheder	**Forbedret.** Der arbejdes løbende med at minimere antal medarbejdere med privilegere rettigheder. Styregruppen for Informationssikkerhed godkender kvartalsvist antal brugere med privilegerede rettigheder og antal service- og systemkonti til skriftlig godkendelse. Der er inden da foretaget en konkret faglig vurdering af hver brugers rettigheds og relevans i de privilegerede grupper. Brugerne har disse rettigheder for at kunne udføre deres arbejde. Rigsrevisionen har fastlagt, at 10 er et rimeligt antal systemadministratorer uanset forretningens størrelse. Dette antal matcher ikke med Region Hovedstadens størrelse og behov, hvilket vi også har debatteret med Rigsrevisionen. Rigsrevisionens bemærkning hertil er, at så længe ledelsen er informeret og forholder sig til risikoen (hvilket løbende sker i regi af Styregruppen for Informationssikkerhed i CIMT), således at risiko er kendt og behandlet, hvilket anses som mitigerende.
Regelmæssig kontrol af medarbejdere med privilegerede adgangsrettigheder	**Udbedret.** Styregruppen for Informationssikkerhed godkender kvartalsvist antal brugere med privilegerede rettigheder og antal service- og systemkonti til skriftlig godkendelse.

	Der er inden da foretaget en konkret faglig vurdering af hver brugers rettigheds og relevans i de privilegerede grupper. Brugerne har disse rettigheder for at kunne udføre deres arbejde. Der arbejdes løbende på at nedbringe antallet af brugere med privilegerede rettigheder. Dette afrapporteres hver måned i månedens nøgletal.
Personlige password til konti med privilegerede rettigheder følger god praksis og er systemunderstøttede	**Udbedret.**
Begrænset antal system- og servicekonti	**Udbedret.** Styregruppen for Informationssikkerhed godkender kvartalsvist antal brugere med privilegerede rettigheder og antal service- og systemkonti til skriftlig godkendelse. Der er inden da foretaget en konkret faglig vurdering af hver brugers rettigheds og relevans i de privilegerede grupper. Brugerne har disse rettigheder for at kunne udføre deres arbejde. Der arbejdes løbende på at nedbringe antallet af brugere med privilegerede rettigheder. Dette afrapporteres hver måned i månedens nøgletal.
Logfiler gennemgås regelmæssigt	**Forbedret.** Der er indført fast procedure for gennemgang af logfiler i SIEM-systemet. Det vurderes løbende hvilke systemer der skal være omfattet og indgår i logfil gennemgangen.
Medarbejdere med privilegerede rettigheder, der logges, ikke har adgang til loggen	**Forbedret.** For alle systemer, der overfører logs til SIEM-systemet er det ikke muligt for brugerne at redigere i de logs.