

Til Sundheds- og Ældreministeriet

Journal-nr.: 16043917

Dato: 16. januar 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 autogenerated 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	<p>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.</p>
Kun godkendte programmer kan afvikles	<p>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.</p>
Regionen kan hente sikkerhedsopdateringer fra producenter af relevante programmer	<p>Udbedret. Status er at regionen kan hente sikkerhedsopdateringer fra relevante producenter. Der er indført faste patchprocedure for servere og computere.</p> <p>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.</p> <p>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.</p>

Journal-nr.: 16043917

Dato: 16. januar 2018

	<p>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.</p> <p>Region Hovedstaden er i proces med at sikre de resterende XP-computere bag firewalls, indtil de kan opgraderes eller erstattes af nyere løsninger.</p>
Etablering af tiltag f.eks. segmenteret netværk, så en inficering i form af hackere eller malware ikke kan sprede sig ubegrænset	<p>Forbedret.</p> <p>Status er at der er macro segmentering i datacenteret.</p> <p>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.</p>
Begrænset antal medarbejdere, der permanent har privilegerede rettigheder	<p>Forbedret.</p> <p>Der arbejdes løbende med at minimere antal medarbejdere med privilegerede rettigheder.</p> <p>Styregruppen for Informationssikkerhed godkender kvartalsvist antal brugere med privilegerede rettigheder og antal service- og systemkonti til skriftlig godkendelse.</p> <p>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.</p> <p>Rigsrevisionen har fastlagt, at 10 er et rimeligt antal systemadministratorer uanset forretningens størrelse.</p> <p>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.</p>
Regelmæssig kontrol af medarbejdere med privilegerede adgangsrettigheder	<p>Udbedret.</p> <p>Styregruppen for Informationssikkerhed godkender kvartalsvist antal brugere med privilegerede rettigheder og antal service- og systemkonti til skriftlig godkendelse.</p>

Journal-nr.: 16043917

Dato: 16. januar 2018

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

Journal-nr.: 16043917

Dato: 16. januar 2018