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

Dato: 30-04-2018
Enhed: SUNDOK
Sagsbeh.: DEPMAHA
Sagsnr.: 1707648
Dok. nr.: 593539

Statsrevisorerne Sekretariatet
Prins Jørgens Gård 2, Folketinget, Christiansborg
ministersvar@ft.dk
1240 København K
DK, Danmark

Sundhedsministerens redegørelse til Statsrevisorerne vedr. Rigsrevisionens beretning nr. 11/2017 om beskyttelse mod ransomwareangreb

Statsrevisorerne har den 1. marts 2018 fremsendt beretning nr. 11/2017 om beskyttelse mod ransomwareangreb.

Denne redegørelse vedrører alene beretningens undersøgelse og konklusioner vedrørende Sundhedsdatastyrelsens beskyttelse mod ransomwareangreb.

Indledningsvist vil jeg gerne kvittere for, at beretningen sætter fokus på en væsentlig sikkerhedsdagsorden. Det øgede trusselsniveau mod blandet andet sundhedssektoren understreger, at sikkerhed og modstandsdygtighed er afgørende. Det er et emne som er højt prioriteret i Sundheds- og Ældreministeriet.

Derudover skal jeg gøre opmærksom på, at Sundhedsdatastyrelsen fungerer som koncern IT-funktion for koncernen (undtagen Lægemiddelstyrelsen), og at de identificerede ransomwareangreb har fundet sted inden for hele dette område.

Ligeledes skal det bemærkes, at alle de 13 identificerede ransomwareangreb alene har berørt fildrev i ministeriets institutioner. Der har således ikke været tale om, at angreb har berørt områder, hvor ministeriets institutioner understøtter den primære patientbehandling, f.eks. diagnostik, smitteovervågning og drift af det Fælles Medicinkort, idet der ikke anvendes fildrev til understøttelse af disse opgaver. Der har heller ikke været tale om, at følsomme oplysninger om borgernes sundhed har været i fare, da disse ikke er placeret på fildrev.

Rigsrevisionens beretning og statsrevisorernes bemærkninger
Statsrevisorerne finder, at alle fire institutioner, herunder Sundhedsdatastyrelsens beskyttelse mod ransomwareangreb ikke er tilfredsstillende. Statsrevisorerne bemærker yderligere vedrørende Sundhedsdatastyrelsen, at forebyggelsen mod ransomwareangreb ikke er tilstrækkelig, og at det ikke er fuldt ud sikret, at alle programmer har de nyeste sikkerhedsopdateringer. Derudover bemærker Statsrevisorerne, at ledelsen i styrelsen ikke har dækkende risikovurdering for truslen fra ransomwareangreb.

Sundheds- og Ældreministeriets bemærkninger og tiltag
Sundheds- og Ældreministeren kan konstatere, at af beretningens 20 kontrolmål og 5 fremadrettede anbefalinger opfylder Sundhedsdatastyrelsen 10 af de opstillede kontrolmål, 5 kontrolmål er delvist opfyldt og 5 kontrolmål er ikke opfyldt. Styrelsen klarer sig godt på de anbefalede, fremadrettede ydre sikringstiltag, og efter afslutningen af beretningssagen har Sundhedsdatastyrelsen endvidere etableret en

central logmanagement-løsning, der understøtter detektion af unormal adfærd i it-infrastrukturen.

Nedenfor redegøres der for Sundheds- og Ældreministeriets overvejelser i forhold til de kontrolmål, der i beretningen er angivet som *delvist opfyldt* eller *ikke opfyldt*. For hvert kontrolmål beskrives desuden allerede igangsatte eller planlagte sikringstiltag.

Delvist opfyldte kontrolmål

- Opfølgning på angreb

Rigsrevisionen kritik går på, at Sundheds- og Ældreministeriet først i 2017 har iværksat systematisk opfølgning på erfaringerne fra de identificerede ransomwareangreb.

Sundhedsdatastyrelsen har over for ministeriet tilkendegivet, at dette skyldtes, at der frem til 2016 var tale om meget afgrænsede angreb, som kun berørte en enkelt eller få medarbejdere. Siden har alle ransomwareangreb været behandlet som major incidents, indtil omfanget var afklaret. Dette har, kombineret med en hensigtsmæssig håndtering og test af back up sikret, at data har kunnet retableres inden for en tidsramme, som den forretningsmæssige ledelse har fundet acceptabel og inden for de retningslinjer, der er godkendt i det koncernfælles it-sikkerhedsudvalg.

Det er aftalt, at der for alle identificerede ransomwareangreb udarbejdes en analyse af angrebet. Ligeledes indgår vurderingen af ransomwaretrusler i de trusselsvurderinger, der forelægges det koncernfælles informationssikkerhedsudvalg som minimum hvert halve år.

- Opfølgning på awareness-aktiviteter

Rigsrevisionen har anerkendt, at Sundhedsdatastyrelsen har fulgt op på den koncerndækkende kampagne, der blev gennemført i 2016, gennem en spørgeundersøgelse blandt medarbejderne, men da der ikke var tale om en opfølgning på effekten af kampagnen i form af før- og eftermålinger, finder Rigsrevisionen kontrolmålet kun delvist opfyldt.

Sundhedsdatastyrelsen har meddelt, at der vil blive gennemført en kampagne i løbet af 2018, hvor der også vil blive foretaget en effektmåling af awareness-aktiviteterne.

Herudover er der til koncernen anskaffet et værktøj, som kan anvendes til at løbende at lave kampagner rettet mod brugerne i alle styrelser. I den forbindelse vil det ligeledes blive overvejet, hvordan man kan måle effektiviteten af de kampagner, der gennemføres.

- Kun godkendte programmer kan afvikles

Sundhedsdatastyrelsen har over for Rigsrevisionen og ministeriet tilkendegivet, at der vil blive etableret en whitelisting-løsning i 2018.

- Ingen brug af privilegerede rettigheder, når der læses e-mail

Rigsrevisionen har kritiseret Sundhedsdatastyrelsen for, at foranstaltninger til at hindre medarbejdere med privilegerede rettigheder til at tilgå e-mail og internet med disse rettigheder ikke er fuldt ud dækkende.

Sundhedsdatastyrelsen har fremsendt dokumentation for implementerede policies på serverne, der forhindrer medarbejdere med privilegerede rettigheder i at læse

mails og gå på internettet. Samtidig har styrelsen tilkendegivet, at det ligger i sagens natur, at en bruger med meget høje privilegier vil kunne omgå implementerede policies, men at der vil i givet fald være tale om et bevidst brud på sikkerheden og et brud på Sundheds- og Ældreministeriets retningslinjer.

Sundhedsdatastyrelsen vil undersøge, om det er muligt at implementere kontroller i den centrale log management-løsning med henblik på at kunne følge op på evt. misbrug af privilegier.

- Sikring mod ubeskyttet adgang til internettet

Rigsrevisionen kritiserer, at der ikke er etableret en sandboxing-løsning, som forhindrer, at medarbejdere kan downloade potentielt skadelige filer, når de læser e-mails.

Sundhedsdatastyrelsen vil medio 2018 undersøge omkostningerne og konsekvenserne for medarbejdernes opgavevaretagelse ved indførelse af en sandboxing-løsning og herefter fremlægge løsningsforslag for ministeriets ledelse.

Sundhedsdatastyrelsen har over for Rigsrevisionen præciseret, at man ikke finder, at de gennemførte ransomwareangreb har haft et omfang, som i væsentlig grad har påvirket organisationens evne til at udføre sine opgaver, og at sikringstiltag, der kan reducere risikoen for angreb ud fra en risikobaseret tilgang skal vurderes op i mod, at man har en fungerende reaktiv kapacitet, der har sikret, at data har kunnet retableres ud fra backup inden for de retningslinjer, der er godkendt i det koncernfælles i-sikkerhedsudvalg.

Ikke opfyldte kontrolmål

- Ikke afsluttet opdatering af risikovurdering

Rigsrevisionen har kritiseret, at Sundhedsdatastyrelsens risikovurdering ikke er opdateret siden 2015 og derfor ikke forholder sig til aktuelle trusler. Derudover betyder organisationsændringer i Sundhedsdatastyrelsen (skal korrekt være i Sundheds- og Ældreministeriet), at risikovurderingen ikke tager udgangspunkt i institutionen, som den ser ud på nuværende tidspunkt.

Sundhedsdatastyrelsen har anerkendt, at arbejdet med at opdatere den i 2015 gennemførte risikovurdering ikke er tilendebragt, men pågår. Der er således gennemført en fornyet forretningsmæssig konsekvensvurdering i 2017, som er en integreret del i risikovurderingen, men der udestår gennemførelse af fornyede sårbarhedsvurderinger af systemer og infrastruktur. Forsinkelsen skyldes primært et stort ressourcetræk i forbindelse med frasalg af vaccineproduktionen på SSI, organisationsændringer på ministeriets område og gennemførelse af ministeriets serviceeftersyn. Det er aftalt, at sårbarhedsvurderinger af de mest kritiske forretningsprocesser gennemføres primo 2018, hvorefter der vil blive udarbejdet et første risikoregister til brug for ledelsens prioritering af sikringstiltag.

Fremover vil risikovurdering og vedligeholdelse af risikoregisteret blive håndteret som en løbende proces. Der er derfor fra 2018 afsat ekstra ressourcer til området for at sikre, at der kan etableres et årshjul for risikovurdering, der både tilgodeser behovet for en fortløbende risikovurderingsproces og behovet for vurdering af risici i forbindelse med udefrakommende trusler, ny organisering eller ny teknologi.

- Brug af to-faktor login til webmail

Rigsrevisionen har kritiseret Sundhedsdatastyrelsen for, at den eksisterende webmail-løsning kan anvendes uden 2-faktor login. Dette gør det nemmere for en hacker at få adgang til institutionernes interne e-mailløsninger, hvis hackeren allerede har fået adgang til en eller flere brugeres password.

Sundhedsdatastyrelsen har over for ministeriet tilkendegivet, at man tager kritikken til efterretning. Sundhedsdatastyrelsen er i gang med at etablere en MDM (Mobile Device Management) løsning, der giver medarbejderne adgang til mail og kalender på en sikker måde på deres mobile enheder. Herefter vurderes adgangen til webmail helt kunne lukkes. Der arbejdes på at kunne etablere MDM-løsningen inden udgangen af 2. kvartal 2018.

- Begrænsning af brugen af private mailløsninger

Rigsrevisionens har kritiseret, at man ikke har begrænset medarbejdernes adgang til deres private e-mailløsninger, f.eks. Gmail og Facebook.

I forbindelse med indførelsen af MDM-løsningen vil det blive anbefalet medarbejderne, at man tilgår sin private mail, Facebook o.l. fra telefonen og ikke fra PC-arbejdspladsen.

Sundhedsdatastyrelsen har over for ministeriet tilkendegivet, at man er i gang med at udarbejde en positivliste over programmer, der må anvendes, og at man derudover planlægger at implementere en løsning, der kan identificere og fjerne uønskede programmer, som medarbejderne har installeret, f.eks. webbaserede e-mailløsninger.

Men eftersom Facebook, Twitter og andre platforme også anvendes af institutionerne i deres kommunikation udadtil, vil en fuldstændig lukning kunne få betydelige implikationer, og det skal derfor ledelsesmæssigt vurderes, hvilke yderligere tiltag, der skal iværksættes.

- Antallet af brugere med lokaladministratorrettigheder

Rigsrevisionens kritiserer Sundhedsdatastyrelsen for, at der er medarbejdere, ud over it-supportere, der har adgang til computere med lokaladministratorrettigheder. Med lokaladministratorrettigheder er det muligt at deaktivere tiltag på den lokale computer, hvorved der etableres flere 'indgange' for hackere, som kan kompromittere institutionens computere og afvikle skadelige programmer, som potentielt kan sprede sig og skade dele af eller hele institutionens netværk.

Sundhedsdatastyrelsen har i en længere periode arbejdet med institutionerne i koncernen på at nedbringe antallet af lokaladministratorer. På Statens Serum Institut har det historisk været hovedreglen, at den enkelte bruger havde lokaladministratorrettigheder.

Sundhedsdatastyrelsens har i forlængelse heraf over for Rigsrevisionen anført, at man har nedbragt antallet af brugere med lokaladministratorrettigheder med 90 pct. fra ca. 1.500 til 134.

Inden for koncernen er der imidlertid fortsat en række it-understøttede arbejdsfunktioner, som kun kan løses med anvendelse af lokaladministratorrettigheder, f.eks. håndtering af undersøgelses- og analyseudstyr

på Statens Serum Institut og Statens Institut for Strålehygiejne. Her er disse rettigheder en nødvendig forudsætning for opgavernes varetagelse.

Sundhedsdatastyrelsen arbejder løbende for at etablere betingelserne for yderligere at kunne nedbringe antallet af brugere med lokaladministratorrettigheder gennem f.eks. etablering af et softwarecenter, hvor arbejdsrelevante programmer kan installeres fra eller gennem segmentering af udstyr, der kræver lokaladministratorrettigheder, fra det resterende netværk.

Leverandører af analyseudstyr er imidlertid ofte ikke væsentligt motiverede for at efterkomme ønsker om at ændre opsætningen på deres analyseudstyr, og det må derfor forventes, at det vil tage lang tid, inden man kan fjerne brugen af lokaladministratorrettigheder her.

I lyset heraf er der for de resterende brugere med behov for lokaladministratorrettigheder etableret en dispensationsprocedure, hvor kun ledelsesgodkendte brugere med et anerkendt arbejdsbetinget behov får tildelt lokaladministratorrettigheder. Disse rettigheder tildeles på en særskilt administratorkonto, der ikke kan anvendes til at tilgå mail eller fildrev.

Sundhedsdatastyrelsen har igennem de seneste år foretaget en modernisering af netværket, som skal sikre, at der kan foretages nødvendig segmentering af netværket. Arbejdet har været sat midlertidigt i bero, da der viste sig behov for at opgradere den eksisterende kabling, inden de nye netværksenheder kan installeres. Dette er netop prioriteret i forbindelse med handling til opfølgning på koncernens serviceeftersyn. Når dette er gennemført, vil en større del af det udstyr, der kræver lokaladministratorrettigheder, kunne isoleres fra det generelle netværk. Det vil ikke nedbringe antallet af lokaladministratorer, men sikre, at evt. malware ikke kan spredes.

- Sikkerhedsopdateringer af tredjepartsprogrammer

Rigsrevisionen kritiserer Sundhedsdatastyrelsen for ikke at have en systematisk tilgang til sikkerhedsopdateringer, som omfatter alle relevante programmer.

Sundhedsdatastyrelsen har over for Rigsrevisionen anført, at der igennem de seneste år netop er etableret en SCCM-løsning, der sikrer systematisk og automatiseret opdatering af såvel arbejdsstationer som servere, herunder tredjepartssoftware.

Men som følge af, at brugerne tidligere havde lokaladministratorrettigheder og selv kunne installere programmer, findes der – især på SSI – tidligere versioner af f.eks. Adobe, Flash og Java, som ikke bliver automatisk opdateret.
Sundhedsdatastyrelsen har siden inspektionens afslutning identificeret og afinstalleret gamle versioner af de 10-15 mest anvendte programmer, og sikret, at der fremover kun anvendes versioner, der opdateres automatisk.

Sundheds- og Ældreministeriets afsluttende bemærkninger
På baggrund af ovenstående beskrivelse af Sundhedsdatastyrelsens iværksatte eller planlagte sikringstiltag, er det min vurdering, at Sundhedsdatastyrelsen arbejder aktivt med at udbedre de kritikpunkter, som Rigsrevisionen har rejst.

Sundhedsdatastyrelsen har på lagt de fleste områder, iværksat eller forventer at iværksætte tiltag, som kan øge beskyttelsen mod ransomwareangreb, herunder øget det ledelsesmæssige fokus på området.

Jeg kan desuden oplyse, at Sundheds- og Ældreministeriet i 2017 gennemførte et eksternt serviceeftersyn af informationssikkerheden i hele Sundheds- og Ældreministeriets koncern med henblik på at forbedre informationssikkerheden. Som opfølgning på serviceeftersynets anbefalinger har ministeriet udarbejdet en koncernfælles handleplan med organisatoriske, governance- og styringsmæssige og tekniske initiativer, som samlet har til formål at sikre et tidssvarende informationssikkerhedsniveau i hele koncernen.

Handleplanen er således med til at sikre, at ikke kun Sundhedsdatastyrelsen, men hele koncernen fremover arbejder systematisk og helhedsorienteret med at øge informationssikkerheden, herunder også i forhold til at styrke beskyttelsen mod ransomwareangreb. Hertil kan det oplyses, at Sundheds- og Ældreministeriet fra 2018 har afsat ekstra ressourcer til prioritering af området og til implementering af initiativer i handleplanen.

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

Med venlig hilsen

Ellen Trane Nørby