SUNDHEDSMINISTERIET

Sundhedsministeren

Holbergsgade 6
DK-1057 København K

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

Dato: 13-03-2022
Enhed: KOK
Sagsbeh.: DEPCHVE
Sagsnr.: 2204269
Dok. nr.: 2172401

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

Sundhedsministerens redegørelse til Statsrevisorerne vedr. Rigsrevisionens Beretning nr. 9/2021 om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerhed

Statsrevisorerne har den 17. januar 2022 afgivet deres bemærkninger til Rigsrevisionens beretning nr. 9/2021 om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerhed.

Indledende bemærkninger

Indledningsvist vil jeg vil gerne bemærke, at jeg er helt enig med såvel statsrevisorerne som Rigsrevisionen i, at der netop er tale om minimumskrav, vi som offentlige myndigheder bør og skal leve op til. Det er fornuftige krav, der skal bidrage til at sikre os mod brud på informationssikkerheden, risikoen for cyberangreb, så vi undgår, at der er sårbarheder i vores it-systemer, telefoner og på vores websider.

Derfor arbejder vi på Sundhedsministeriets område også målrettet på at komme i mål med samtlige uopfyldte minimumskrav og har gjort det løbende. Det er Sundhedsdatastyrelsens vurdering, at vi på ministerområdet lever op til samtlige krav i løbet af tredje kvartal 2022.

De sidste to års opgaver relateret til indsatsen mod covid-19 har imidlertid stillet hele ministerområdet, herunder også Sundhedsdatastyrelsen og vores koncern-it-funktion, i en helt ekstraordinær situation. Det har udfordret vores arbejde for fuld målopfyldelse. Covid-19-indsatsen er i vid udstrækning en digital indsats, og alle ressourcer i koncernens it-funktion samt styrelserne har været sat ind for at sikre den nødvendige it-udvikling og it-understøttelse til denne.

I september 2020 påbegyndte Sundhedsministeriets koncern den meget omfattende transition af den basale it-drift til Statens It, hvilket også har trukket på centrale it-ressourcer i ministeriets koncern-it funktion og i institutionerne.

Det ændrer ikke på, at samtlige minimumkrav skal opfyldes, og trods det vedvarende pres ift. covid-19-indsatsen er der siden revisionsbesøget i august 2021 sket betydelige fremskridt.

Således vurderer Sundhedsdatastyrelsen, at vi på ministerområdet lever op til 16 af de 20 krav og som nævnt forventer at kunne leve op til samtlige krav ved udgangen af tredje kvartal i år. Styrelsen har også oplyst, at de ikke har viden om, at borgernes data på noget tidspunkt har været kompromitteret.

Transitionen med Statens It betyder samtidigt, at arbejdet med IT-sikkerheden og overholdelse af de 20 tekniske minimumskrav fremadrettet vil ske i et tæt samarbejde med Statens It, som helt eller delvist overtager ansvaret for målopfyldelse af kravene.

I koncernens nye Digitaliseringsboard, der har ansvar for at træffe beslutning om større digitaliseringsprojekter og sætte rammerne for it-udviklingen i koncernen, følger ledelsen løbende op på arbejdet med målopfyldelsen og sikrer dermed stor ledelsesmæssig opmærksomhed på at prioritere indsatsen.

Udvikling i efterlevelse af minimumskravene

Jeg vil i det følgende redegøre nærmere for de foranstaltninger og overvejelser, som Rigsrevisionens beretning og statsrevisorernes bemærkninger har givet mig anledning til. Fokus vil være på, hvordan ministeriet har til hensigt at sikre efterlevelse af de 8 minimumskrav, der ikke var opfyldt ved revisionstidspunktet i august 2021.

Krav som Sundhedsdatastyrelsen nu vurderer, er opfyldt

Krav 5. Regelmæssig opdatering af klienter

Det fremgår af beretningen, at Sundhedsdatastyrelsen/Sundhedsministeriet ikke efterlever krav 5 med hensyn til en enkelt applikation (Java-applikation), der ikke er regelmæssigt opdateret, og at styrelsen har opdateret alle øvrige applikationer.

Sundhedsdatastyrelsen har oplyst mig, at de i januar 2022 har afinstalleret ikke opdaterede Java-versioner, som var det eneste udestående. Styrelsen vurderer nu at leve op til kravet.

Krav 10. 2-faktor-autentifikation eller direkte VPN-forbindelse

Det fremgår af beretningen, at Sundhedsdatastyrelsen/Sundhedsministeriet i august ikke anvendte 2-faktor-autentifikation til at tilgå webmail, når brugeren ikke var på styrelsens netværk. Det fremgår også af Rigsrevisionens beretning, at Sundhedsdatastyrelsen i november 2021 oplyste, at multifaktor-autentifikation nu var implementeret på hele ministerområdet

Sundhedsdatastyrelsen har oplyst mig, at dette stadig er gældende, og kravet derfor er opfyldt.

Krav 11. DMARC REJECT-policy implementeres på alle domæner

Det fremgår af Rigsrevisionens beretningen, at Sundhedsdatastyrelsen/Sundhedsministeriet i august ikke havde implementeret DMARC REJECT-policy på alle domæner (sikkerhedsstandard der bidrager til bekæmpelsen af blandt andet phishing-mails). Det fremgår også af Rigsrevisionens beretning, at Sundhedsministeriet/Sundhedsdatastyrelsen i november 2021 oplyste, at man havde implementeret DMARC REJECT på alle domæner.

Sundhedsdatastyrelsen har oplyst mig, at dette stadig er gældende, og kravet derfor er opfyldt.

Krav 15. Krav om logning på alle systemer og tjenester på netværksservere

Det fremgår af Rigsrevisionens beretning, at Sundhedsdatastyrelsen/Sundhedsministeriet ikke har sikret tilstrækkelig logning (herunder log på alle systemer og tjenester) på netværksservere.

Rigsrevisionen vurderer, at logningen er utilstrækkelig af 2 årsager. Sundhedsdatastyrelsen anvender et logningssystem (en såkaldt SIEM-løsning), der opsamler logs fra mange af Sundhedsdatastyrelsens forskellige systemer. Her konstaterer Rigsrevisionen, at loggen ikke har været beskyttet i tilstrækkelig grad, da de it-medarbejdere, der administrerede diverse systemer, også havde fuld adgang til SIEM-løsningen. Der har således ikke været en tilstrækkelig funktionsadskillelse, og dermed har medarbejdere potentielt kunnet manipulere eller helt slette logs fra SIEM-løsningen. Dette er dog ikke konstateret. Det fremgår også af Rigsrevisionens beretning, at Sundhedsdatastyrelsen, i forlængelse af revisionen oplyste, at styrelsen havde begrænset de adgange, som medarbejderne havde til SIEM-løsningen.

Den anden årsag til den manglende efterlevelse er, at der blev logget data fra netværksudstyr, som ikke blev sendt til SIEM-løsningen, og som kun blev gemt i 30 dage.

Sundhedsdatastyrelsen har oplyst mig, at funktionsadskillelsen fortsat er implementeret og gældende, og at netværksudstyret igen sender til SIEM-løsningen, hvor data gemmes i 13 måneder. Styrelsen vurderer derfor at leve fuldt op til kravet.

Krav som Sundhedsdatastyrelsen fortsat arbejder på at opfylde

Krav 7. Sikkerhedsopdateret operativsystem

Det fremgår af beretningen, at Sundhedsdatastyrelsen/Sundhedsministeriet ved begyndelsen af it-revisionen havde 273, ud af i alt 4.309 klienter, der ikke var supporteret med sikkerhedsopdateringer. I løbet af revisionen fik styrelsen/ministeriet afviklet en del af disse klienter, og der udestod i august 2021 afvikling af 73 klienter.

Sundhedsdatastyrelsen har oplyst mig, at årsagen til den manglende opfyldelse af kravet skyldes ikke-opdaterede Win10 og Win7 PC'ere. Alle PC'ere på ministerområdet er nu opdateret, men opdateringen af de sidste 100 PC'ere hos Statens Serum Institut er først mulig med udskiftning af de nuværende ældre PC'ere, som grundet deres alder ikke kan opdateres. Maskinerne er imidlertid i restance på grund af de globale forsyningsvanskeligheder og forventes først af kunne blive leveret senere i 2022. Som supplerende foranstaltning er Sundhedsdatastyrelsen netop ved at afslutte et netværkssegmenteringsprojekt, som isolerer de sidste ikke-opdaterede PC'ere. Med afslutning af segmenteringsprojektet og med udskiftning af de ældre PC'ere til nye opdaterede PC'ere hos Statens Serum Institut vurderer Sundhedsdatastyrelsen således, at kravet vil være opfyldt inden udgangen af tredje kvartal 2022.

Krav 13. Regelmæssig opdatering af mobile enheder

Det fremgår af beretningen, at ingen af de 5 myndighederne i den samlede revisionsberetning efterlever krav 13, og at alle 5 myndigheder har mobile enheder,

der ikke er opdateret, og dermed har software, der indeholder kendte sikkerhedshuller eller sårbarheder.

Sundhedsdatastyrelsen har oplyst mig, at der i Sundhedsdatastyrelsen/Sundhedsministeriet stilles krav om installation af Mobile Device Management (MDM) på alle mobile enheder. Styrelsen har endvidere oplyst, at man i regi af koncernens tværgående digitaliseringsboard og koordinationsforum har bedt institutionernes ledelser om at sikre, at deres medarbejdere installerer Mobile Device Management på deres mobile enheder.

Statens It overtager håndteringen og sikringen af mobile enheder fra august 2022, hvorefter alle mobile enheder, som tilgår SUM's systemer, vil være dækket af Statens It's Mobile Device Managementløsning.

Krav 16. Tilknytning af DNSSEC til alle webdomænenavne

Det fremgår af beretningen, at Sundhedsdatastyrelsen/Sundhedsministeriet har tilknyttet sikkerhedsteknologien DNSSEC til alle domænenavne. Rigsrevisionen tog en stikprøve på 6 webdomæner og kunne konstatere, at halvdelen af domænerne ikke havde konfigureret og aktiveret DNSSEC. Det fremgår også af beretningen, at Sundhedsdatastyrelsen havde oplyst, at styrelsen var i gang med at afvikle de sidste domæner uden DNSSEC.

Sundhedsdatastyrelsen har oplyst mig, at det aktuelt drejer sig om to færøske domæner under det færøske landsstyre, som er knyttet til Styrelsen for Patientsikkerhed, og seks EU-domæner, som er knyttet til Statens Serum Institut, der ikke har DNSSEC.

Kravet forventes opfyldt i andet kvartal 2022.

Krav 18. Kryptering af kommunikation til hjemmesider

Det fremgår af beretningen, at Sundhedsdatastyrelsen/Sundhedsministeriet efterlever den del af kravet, der omhandler brug af TLS 1.2., men at ministerområdet har hjemmesider, hvor https ikke er slået til. Rigsrevisionen kunne også konstatere, at styrelsen/ministeriet har nogle hjemmesider, der tilsyneladende ikke anvendes, men samtidig ikke er tomme for indhold, da der er indsat en placeholder på dem.

Sundhedsdatastyrelsen har oplyst mig, at https nu er slået til på samtlige af ministerområdets hjemmesider.

Der er en enkelt udfordring ift. ét domæne i Nationalt Center for Etik, som endnu ikke opfylder TLS 1.2. Her har Sundhedsdatastyrelsen givet Nationalt Center for Etik en dispensation, da Nationalt Center for Etik har i gangsat mitigerende handlinger og har en plan for målopfyldelse i løbet af tredje kvartal 2022.

Afrunding

Jeg håber, at jeg med denne redegørelse har beskrevet, hvordan vi på ministerområdet med ledelsesmæssig forankring arbejder aktivt for at efterleve de 20 tekniske minimumskrav til it-sikkerheden.

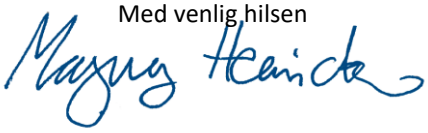
Der er en række forhold, som gør, at vi endnu ikke er fuldt i mål med de sidste 4 krav, men hvor vi har planer for, hvordan de sidste få udeståender opfyldes snarest muligt i 2022.

Samtidig indgår efterlevelsen af de 20 tekniske minimumskrav også i vores aktuelle og højtprioriterede arbejde med yderligere robustgørelse af ministerområdets it-, cyber- og informationssikkerhed.

Med transitionen til Statens It i 2022 har vi yderligere en stærk samarbejdsparter til at sikre og fortsætte denne robustgørelse.

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

Med venlig hilsen



Magnus Heunicke