



JUSTITSMINISTERIET

Statsrevisorernes Sekretariat
Folketinget
Christiansborg

Dato: 25-03-2022
Sagsnr.: 2021-010-0122
Dok.: 2320234

Ministerredegørelse vedrørende Statsrevisorernes beretning nr. 9/2021 om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden

1. Jeg har den 18. januar 2022 modtaget Statsrevisorernes beretning nr. 9/2021 om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden. Statsrevisorerne har på den baggrund anmodet mig om en redegørelse for, hvilke foranstaltninger og overvejelser beretningen giver anledning til, jf. § 18, stk. 2 i lov om revisionen af statens regnskaber m.m.

2. Det fremgår af beretningen, at Statsrevisorerne finder det utilfredsstillende, at ingen af de fem undersøgte statslige myndigheder, herunder kriminalforsorgen, har efterlevet alle de 20 tekniske minimumskrav til it-sikkerheden i staten, på trods af at de trådte i kraft for 1-1/2 år siden. Det fremgår endvidere, at Statsrevisorerne finder, at sårbarhed i myndighedernes it-systemer, hjemmesider, mobiltelefoner og tablets derfor har medført øget risiko for cyberangreb og misbrug.

3. Ifølge Rigsrevisionens beretning efterlevede kriminalforsorgen på revisionsstidspunktet ikke fire af de 20 tekniske minimumskrav i form af krav nr. 5 om opdatering af klienter, krav nr. 11 om DMARC reject-policy på domæner, krav nr. 7 sikkerhedsopdateret operativsystem og krav nr. 13 om opdatering af mobile enheder. Kriminalforsorgen vurderer, at der nu sker fuld efterlevelse af krav nr. 11 om DMARC reject-policy på domæner og krav nr. 7 om sikkerhedsopdateret operativsystem, mens der endnu ikke sker

fuld efterlevelse af krav nr. 5 om opdatering af klienter og krav nr. 13 om opdatering af mobile enheder.

5. Ifølge krav nr. 13 skal der ske regelmæssig opdatering af mobile enheder. I beretningen konstaterer Rigsrevisionen, at kravet er formuleret upræcist, og anbefaler en præcisering af kravet. Rigsrevisionen lægger i sin operationalisering af kravet til grund, at software så vidt muligt skal opdateres, så snart leverandøren udgiver opdateringer, og at myndigheden skal undlade at anvende versioner af operativsystemet, der indeholder kendte sårbarheder. Desuden skal myndighederne have retningslinjer, der følger op på, at medarbejderne foretager opdateringerne.

Af beretningen fremgår det, at Digitaliseringsstyrelsen har anført, at kravet er opfyldt, hvis der er truffet tekniske og/eller organisatoriske foranstaltninger til at sikre regelmæssig opdatering af operativsystem (OS) og applikationer på mobile enheder.

Rigsrevisionen konstaterer i beretningen, at kriminalforsorgen på revisions-tidspunktet havde 321 Apple-enheder, hvoraf kun 30 enheder anvendte den på revisionstidspunktet påkrævede version. Desuden havde kriminalforsorgen 186 Android-enheder, hvoraf 13 ikke var supporteret med sikkerhedsopdateringer. Rigsrevisionen vurderer samtidig, at kriminalforsorgens retningslinjer ikke har ført til regelmæssig opdatering af mobile enheder, og at de derfor er utilstrækkelige.

Kriminalforsorgen oplyser, at organisatoriske foranstaltninger til at sikre opdatering af mobile enheder har været implementeret siden 2019, og at der løbende er gennemført stikprøver af, om opdateringerne har fundet sted. Kriminalforsorgen oplyser endvidere, at der på revisionstidspunktet var påbegyndt en implementering af en Mobile Device Management-løsning, der gør det muligt at nægte en medarbejder adgang til sin mobiltelefon, indtil vedkommende installerer en opdatering.

Mobile Device Management-løsningen forventes implementeret inden udgangen af 2. kvartal 2022. Kriminalforsorgen bemærker, at kriminalforsorgen alene har kendskab til tekniske løsninger, der kan sikre opdatering af styresystemet i form af Android eller iOS og de af kriminalforsorgen udbudte apps og dermed ikke apps installeret til privat brug. Efterlevelse af krav nr. 13 vil derfor for fremtiden blive sikret delvist gennem organisatoriske foranstaltninger.

6. Ifølge krav nr. 7 skal myndigheden sikre, at det anvendte operativsystem er så nyt som muligt og som minimum supporteret med sikkerhedsopdateringer. Kriminalforsorgen havde ved afslutningen af Rigsrevisionens kontrol blot én enkelt pc med en forældet og usupporteret version af operativsystemet ud af i alt 3.747 pc'er. Rigsrevisionen vurderede på den baggrund, at krav nr. 7 ikke var opfyldt.

Den forældede version af operativsystemet er nødvendig for at sikre kompatibilitet med den software, der anvendes til udstedelse af fysiske adgangskort i direktoratet til sikring af den fysiske sikkerhed. Kriminalforsorgen oplyser, at kravet er efterlevet fra oktober 2021 gennem indgåelse af en aftale om sikkerhedsopdateringer til pc'en.

7. Ifølge krav nr. 5 skal der ske regelmæssig opdatering af klienter, herunder både på operativsystem og applikationer.

Kriminalforsorgen oplyser, at der på revisionstidspunktet skete regelmæssig opdatering af visse applikationer, men at en delmængde udestod. Kravet forventes efterlevet ved udgangen af 2022.

8. Ifølge krav nr. 11 skal der implementeres DMARC reject-policy på alle domæner tilhørende myndigheder med henblik på at forhindre, at en ondsindet mailafsender kan give sig ud for at være en anden.

Kriminalforsorgen havde ved afslutningen af Rigsrevisionens revision ét domæne, hvorpå der ikke var implementeret DMARC reject-policy. Kriminalforsorgen oplyser, at DMARC reject-policy blev implementeret på dette domæne i juni 2021.

9. Det er meget vigtigt, at myndighederne på Justitsministeriets område har iværksat foranstaltninger, der kan imødegå risici for cyberangreb og misbrug, og at kendte sikkerhedshuller og sårbarheder lukkes, således at disse ikke kan udnyttes af ondsindede aktører.

Justitsministeriet har derfor stort fokus på informationssikkerhed og følger løbende op på området i dialog med myndighederne, herunder kriminalforsorgen. Justitsministeriet vil særskilt følge op på, at kriminalforsorgen kommer i mål med implementeringen af de udestående krav.

En kopi af dette brev er samtidig fremsendt til Rigsrevisionen.

Med venlig hilsen

Nick Hækkerup