Transport-, Bygnings- og Boligministeriet

MINISTEREN

Statsrevisorernes sekretariat
Folketinget
Christiansborg
1240 København K

Dato 15. maj 2018
J. nr. 2017-2119

Frederiksholms Kanal 27 F
1220 København K

Telefon 41 71 27 00

Ministerredegørelse om beretning nr. 11/2017 til Statsrevisorerne om beskyttelse mod ransomware

Statsrevisorerne har fremsendt ovennævnte beretning og har bedt om en redegørelse for de foranstaltninger og overvejelser, som beretningen har givet anledning til.

Revisionen omhandlede fire institutioner, hvoraf Banedanmark indgår i undersøgelsen på Transport-, Bygnings- og Boligministeriets område.

I Rigsrevisionens beretning indgår 20 kontrolpunkter, hvor Banedanmark i forhold til 9 kontrolpunkter *'opfylder'* alle krav, i 4 tilfælde *'delvis opfylder'* og i 7 tilfælde *'ikke opfylder'* alle krav i forhold til bedre beskyttelse mod ransomwareangreb.

Det er vigtigt at understrege, at der her ikke er tale om angreb, som på nogen som helst måde kan påvirke togdriften eller trafikstyringen. Styringen af S-togstrafikken kører eksempelvis på et helt separat og lukket netværk. Rapporten omhandler alene ransomware, hvor enkelte eller flere medarbejdere ikke kan udføre deres arbejde via deres computere i en kortere periode.

Banedanmark tager Rigsrevisionens anbefalinger til efterretning og har i forbindelse med revisionens afslutning udarbejdet en samlet plan for tiltag, der på baggrund af Rigsrevisionens anbefalinger medvirker til en bedre beskyttelse mod ransomwareangreb.

En række tiltag er allerede helt eller delvist implementeret og alle tiltag forventes afsluttet i indeværende år. De vigtigste tiltag omfatter bl.a.:

- Banedanmark vil opdatere sin nuværende risikovurdering således, at den afspejler de aktuelle risici på IT miljøet og de enkelte IT systemer, samt hvilke foranstaltninger der er implementeret for at reducere risici for bl.a. ransomwareangreb.

- Banedanmark vil sikre, at beslutninger om ændringer af adfærd og sikkerhedsforanstaltninger der drøftes i informationssikkerhedsudvalget føres til referat som dokumentation for 'lesson learned'.

- I forbindelse med Banedanmarks implementering af MS Office365 programpakken i 2018 genvurderes identitetsvalidering af indgående e-

mails, herunder fortsat anvendelse af DMARC proben og andre identitetsteknologier. Dette skal medvirke til, at forbedre muligheden for at opdage og blokere for falske mails eller mails indeholdende f.eks. ransomware.

- Banedanmark har iværksat en nærmere afklaring af, hvilke tiltag der kan begrænse muligheden for, at virksomhedens identitet bliver misbrugt i ransomwareangreb mod andre – såkaldt *typosquatting*.).

- Banedanmark arbejder på at implementere en ny mailløsning i forbindelse med overgangen til MS Office365, der bl.a. har til formål at forbedre adgangskontrollen til webmail løsningen til en 2-faktor identifikation, som Rigsrevisionen anbefaler.

- For at forbedre indsatsen og effekten af awareness-kampagner vil Banedanmark tage initiativ til at gennemføre effektmålinger af de gennemførte awareness-kampagner, som Rigsrevisionen anbefaler.

- Banedanmark vil begrænse udbredelsen af lokal administrator rettigheder, samt begrænse muligheden for at kunne tilgå mails udefra i rollen som administrator. Dette gøres bl.a. i takt med, at nyt programmel og muligheder tages i anvendelse.

- Banedanmark vil iværksætte en øget anvendelse af såkaldt 'Sandboxing' i forbindelse med åbning af vedhæftede filer i indgående mails. Derved sikres, at evt. skadeligt indhold fanges i sandkassen. Løsningen identificeres og implementeres i forbindelse med den forestående opdatering af det administrative netværk.

- Banedanmark har installeret anti-ransomware software, men har oplevet, at det har været muligt at omgå softwaren. Banedanmark vil tage initiativ til, at softwaren ajourføres og evt. suppleres med yderligere funktionalitet.

- Banedanmark har igangsat et arbejde med at beskrive og afprøve forskellige metoder til gendannelse af system og datagenetablering, således at evt. følgeskader af ransomware begrænses mest muligt.

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

Med venlig hilsen

Ole Birk Olesen