RIGSREVISIONEN

Rigsrevisionens notat om beretning om

beskyttelse mod ransomwareangreb

Juni 2018

Vedrører:
Statsrevisorernes beretning nr. 11/2017 om beskyttelse mod ransomwareangreb

Udenrigsministerens redegørelse af 23. april 2018
Forsvarsministerens redegørelse af 23. april 2018
Sundhedsministerens redegørelse af 30. april 2018
Transport-, bygnings- og boligministerens redegørelse af 15. maj 2018

1. juni 2018

RN 1506/18

1. Rigsrevisionen vurderer i dette notat de tiltag, som ministrene har iværksat og vil iværksætte som følge af Statsrevisorernes bemærkninger og beretningens konklusioner.

KONKLUSION

Sundhedsministeren, udenrigsministeren, transport-, bygnings- og boligministeren og forsvarsministeren oplyser, at de har implementeret eller planlægger at iværksætte en række tiltag, der skal imødegå de mangler, som Rigsrevisionen påpegede, og dermed beskytte institutionerne mod ransomwareangreb.

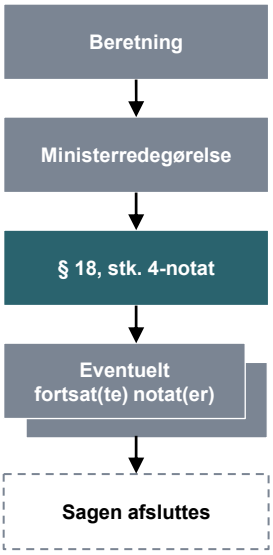
Rigsrevisionen vurderer dog, at ingen af ministrene redegør for deres håndtering af alle de mangler, som Rigsrevisionen påpegede. Det skyldes, at der er tiltag, som ministrene ikke har redegjort for, og at der er tiltag, hvor det er uklart, om de imødegår de påpegede mangler. Derudover oplyser 2 ministre, at de ikke planlægger at implementere ét af tiltagene, og det er uklart, hvilke kompenserende tiltag institutionerne eventuelt har iværksat, eller om risikoen fremgår af institutionernes risikoanalyse.

Rigsrevisionen har lagt til grund, at implementeringen af tiltagene sikrer en grundlæggende beskyttelse mod ransomwareangreb.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- institutionernes implementering af de tiltag, hvor Rigsrevisionen påpegede mangler.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

I. Baggrund

2. Rigsrevisionen afgav i februar 2018 en beretning om beskyttelse mod ransomwareangreb. Beretningen handlede om, hvad 4 udvalgte institutioner havde gjort for at beskytte sig selv mod ransomwareangreb. Ransomware er skadelige programmer, der fjerner adgangen til data, fx ved at data krypteres. Statslige institutioner er i meget høj grad truet af cyberangreb, hvor ransomwareangreb er ét af de mest aktuelle. Rigsrevisionen undersøgte derfor, om de 4 institutioner opfyldte 20 almindelige tiltag, der reducerer risikoen for, at ransomware kommer ind i institutionen via e-mails.

Beretningen omhandlede Sundhedsdatastyrelsen (under Sundheds- og Ældreministeriet), Udenrigsministeriet, Banedanmark (under Transport-, Bygnings- og Boligministeriet) og Beredskabsstyrelsen (under Forsvarsministeriet). Rigsrevisionen udvalgte de 4 institutioner, fordi de varetager samfundsvigtige opgaver inden for sundhed, udenrigsforhold, transport og beredskab.

3. Da Statsrevisorerne behandlede beretningen, bemærkede de, at Sundhedsdatastyrelsens, Udenrigsministeriets, Banedanmarks og Beredskabsstyrelsens beskyttelse mod ransomwareangreb ikke var tilfredsstillende. Hermed var der øget risiko for, at ransomware via e-mails kunne forhindre adgang til institutionernes data, så de ikke kunne varetage deres opgaver i kortere eller længere perioder. Statsrevisorerne gjorde opmærksom på, at beskyttelse mod ransomwareangreb er en vigtig opgave for alle offentlige institutioner.

Statsrevisorerne fandt det tilfredsstillende, at alle 4 institutioner inden for det seneste år har implementeret tiltag, som kan øge deres beskyttelse mod ransomwareangreb.

4. Hele sagen og dens dokumenter kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

II. Gennemgang af ministrenes redegørelser

Beskyttelse mod ransomwareangreb

5. Statsrevisorerne bemærkede, at ingen af de 4 undersøgte institutioner fuldt ud havde sikret, at alle deres programmer havde de nyeste sikkerhedsopdateringer. Statsrevisorerne bemærkede også, at ledelsen i Sundhedsdatastyrelsen og i Banedanmark ikke havde dækkende risikovurderinger for truslen fra ransomwareangreb. Statsrevisorerne bemærkede endelig, at Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen ikke havde reaktive tiltag, der kan sikre, at institutionerne kan genetablere normal drift, efter de er blevet ramt af ransomwareangreb.

6. Det fremgik af beretningen, at manglerne betød, at der for alle institutionerne var en øget risiko for ransomwareangreb, fx fordi institutionerne ikke i tilstrækkelig grad havde sikret, at ransomware ikke kunne finde ind i institutionernes it-netværk via e-mails, fordi institutionernes risikovurderinger af trusselsbilledet ikke var dækkende, og fordi institutionerne ikke i tilstrækkelig grad havde tiltag, der sikrer, at en normal drift kan genetableres efter et angreb.

I det følgende vil vi gennemgå, hvordan de 4 institutioner har imødegået disse mangler. Det betyder, at vi gennemgår, om ministrene har redegjort for de tiltag, hvor beretningen viste, at tiltagene i institutionerne ikke var opfyldt eller var delvist opfyldt. I beretningen lagde vi til grund, at de 20 almindelig tiltag skulle implementeres af institutionerne for at opnå en grundlæggende beskyttelse mod ransomwareangreb. De 20 tiltag er opdelt i 4 kategorier: ledelsesmæssigt fokus, ydre tiltag, indre tiltag og reaktive tiltag.

7. Alle 4 institutioner oplyste i forbindelse med undersøgelsen, at de havde påbegyndt implementeringen af en række tiltag for at beskytte sig mod ransomwareangreb. De 4 ministre har fulgt op på denne status i deres redegørelser.

Ledelsesmæssigt fokus
8. Det fremgik af beretningen, at Sundhedsdatastyrelsen, Udenrigsministeriet og Banedanmark havde mangler i forhold til det ledelsesmæssige fokus. Rigsrevisionen vurderede bl.a., om institutionerne havde dækkende risikovurderinger, krav til backup og fulgte op på ransomwareangreb.

Sundhedsministeren oplyser, at Sundhedsdatastyrelsens opdatering af styrelsens risikovurdering fra 2015 endnu ikke er afsluttet, idet styrelsen mangler at gennemføre sårbarhedsvurderinger af systemer og infrastruktur. Ministeren oplyser, at Sundhedsdatastyrelsen vil have fokus på at sårbarhedsvurdere de mest kritiske forretningsprocesser i 2018 og derefter udarbejde et første risikoregister til brug for ledelsens prioritering af sikringstiltag. Ministeren har ikke redegjort for, om Sundhedsdatastyrelsens krav til backup er godkendt af ledelsen. Ministeren oplyser også, at Sundhedsdatastyrelsen fremover vil følge op på alle identificerede ransomwareangreb med en analyse.

Udenrigsministeren oplyser, at Udenrigsministeriet har udviklet en ny backuppolitik, og at den er ledelsesgodkendt i april 2018.

Transport-, bygnings- og boligministeren oplyser, at Banedanmark fremover vil opdatere sin risikovurdering, så den afspejler de aktuelle risici på it-miljøet og de enkelte it-systemer og de foranstaltninger, der er implementeret, for at reducere risikoen for bl.a. ransomwareangreb. Ministeren oplyser også, at Banedanmark vil sikre, at beslutninger om ændringer af adfærd og sikkerhedsforanstaltninger, der drøftes i informationssikkerhedsudvalget, føres til referat som "lessons learned". Ministeren har ikke redegjort for, hvordan Banedanmark vil sikre, at der følges op på ransomwareangreb.

Ydre tiltag
9. Det fremgik af beretningen, at alle 4 institutioner havde mangler i forhold til de ydre tiltag. Rigsrevisionen vurderede bl.a., om institutionerne brugte 2-faktor login ved webmailløsninger og forhindrede, at medarbejderne kunne bruge private e-mailløsninger.

Sundhedsministeren oplyser, at Sundhedsdatastyrelsen er i gang med at etablere en MDM-løsning (Mobile Device Management), der giver medarbejderne sikker adgang til bl.a. e-mails via mobile enheder, og styrelsen vurderer, at adgangen til webmail herefter kan lukkes. Ministeren oplyser også, at Sundhedsdatastyrelsen ikke vil implementere tiltag, der forhindrer adgangen til private e-mailløsninger fra pc-arbejdspladsen.

Udenrigsministeren oplyser, at Udenrigsministeriet har indført 2-faktor login ved webmailløsninger. Ministeren oplyser også, at ministeriet ikke vil implementere tiltag, der forhindrer medarbejdernes brug af private e-mailløsninger, da ministeriet vurderer, at det vil være en uhensigtsmæssig tung byrde i forhold til medarbejdernes arbejdsrytme og fleksibilitet. Ifølge ministeren er der i stedet gennemført tiltag, der forhindrer, at skadelige filer mv. kan downloades og afvikles. Ministeren redegør dog ikke konkret for, hvilke tiltag der skal forhindre risikoen ved adgangen til private e-mailløsninger.

Transport-, bygnings- og boligministeren oplyser, at Banedanmark i forbindelse med overgangen til en ny programpakke indfører 2-faktor login til webmail. Ministeren har ikke redegjort for, hvordan Transport-, Bygnings- og Boligministeriet vil imødegå risikoen for ransomwareangreb ved at forhindre, at medarbejderne har adgang til private e-mailløsninger.

Forsvarsministeren oplyser, at Beredskabsstyrelsen har udarbejdet handlingsplaner til forbedring af tiltag på de punkter, hvor Rigsrevisionen påpeger, at beskyttelsen ikke er tilstrækkelig. Ministeren har dog ikke konkret redegjort for, hvordan Forsvarsministeriet vil imødegå risikoen for ransomwareangreb ved at forhindre, at medarbejderne har adgang til private e-mailløsninger.

Indre tiltag

10. Det fremgik af beretningen, at alle 4 institutioner havde mangler i forhold til de indre tiltag. Rigsrevisionen vurderede bl.a., om lokaladministratorer havde et arbejdsbetinget behov, om institutionerne sikrede opdatering af tredjepartsprodukter, om privilegerede rettigheder kunne misbruges ved læsning af e-mails, og om institutionerne sikrede sig mod ubeskyttet adgang til internettet, fx via en sandboxing-løsning.

Sundhedsministeren oplyser, at Sundhedsdatastyrelsen over en længere periode har nedbragt antallet af medarbejdere med lokaladministratorrettigheder væsentligt. Ministeren oplyser også, at der er etableret en SCCM-løsning, der sikrer en systematisk og automatiseret opdatering af såvel arbejdsstationer som servere, herunder tredjepartsprogrammer. Derudover har Sundhedsdatastyrelsen siden undersøgelsens afslutning identificeret og afinstalleret gamle versioner af 10-15 programmer, så det sikres, at der fremover anvendes programmer, som opdateres automatisk. Ministeren oplyser videre, at Sundhedsdatastyrelsen etablerer en whitelisting-løsning i 2018. Ministeren oplyser desuden, at Sundhedsdatastyrelsen vil undersøge, om det er muligt at implementere kontroller med henblik på at kunne følge op på eventuelle misbrug af privilegerede rettigheder, når der læses e-mails, og undersøge konsekvenser og omkostninger ved at indføre en sandboxing-løsning. Ministeren oplyser endelig, at opfølgning på awareness-aktiviteter vil finde sted i 2018, og at Sundhedsdatastyrelsen fremadrettet vil overveje, hvordan effekten af awareness-aktiviteter kan måles.

Udenrigsministeren oplyser, at Udenrigsministeriet har tilpasset sine procedurer, så opdatering af tredjepartsprodukter optimeres mest muligt. Ministeren redegør ikke for, hvordan ministeriet vil følge op på effekten af awareness-aktiviteter.

Transport-, bygnings- og boligministeren oplyser, at Banedanmark, i takt med at nye programmer og muligheder tages i anvendelse, vil begrænse udbredelsen af medarbejdere med lokaladministratorrettigheder og begrænse muligheden for, at medarbejdere kan anvende privilegerede rettigheder i forbindelse med læsning af e-mails. Ministeren oplyser også, at Banedanmark i øget omfang vil anvende en sandboxing-løsning i forbindelse med åbning af vedhæftede filer i indgående e-mails. Ministeren har ikke redegjort for, hvordan Banedanmark vil sikre, at kun godkendte programmer afvikles (whitelisting-løsning), eller hvilke tiltag Banedanmark har sat i værk for at sikre, at tredjepartsprodukter opdateres. Ministeren oplyser endelig, at Banedanmark fremadrettet vil gennemføre effektmålinger af awareness-aktiviteter.

Forsvarsministeren oplyser, at Beredskabsstyrelsen har indført yderligere kontroller af status på installation af sikkerhedsopdateringer til tredjepartsprodukter, så det sikres, at udsendte opdateringer bliver installeret. Ministeren har ikke redegjort for, hvordan Beredskabsstyrelsen vil sikre, at kun godkendte programmer kan afvikles. Ministeren har heller ikke redegjort for, hvilke tiltag ministeren vil iværksætte for at sikre, at privilegerede rettigheder ikke misbruges ved læsning af e-mails, og om Beredskabsstyrelsen vil sikre mod udbeskyttet adgang til internettet, fx via en sandboxing-løsning.

Reaktive tiltag

11. Det fremgik af beretningen, at Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen havde mangler i forhold til de reaktive tiltag. Rigsrevisionen vurderede bl.a., om institutionernes backup var beskyttet mod ransomwareangreb, og om institutionerne systematisk testede evnen til at genetablere systemer og data.

Udenrigsministeren oplyser, at Udenrigsministeriet har implementeret en systematisk offline backup og har iværksat en afdækning af procedurer for, hvordan data og systemer kan genetableres.

Transport-, bygnings- og boligministeren oplyser, at Banedanmark har igangsat et arbejde med at prøve forskellige metoder til at gendanne systemer og data, så konsekvenserne af ransomwareangreb begrænses mest muligt.

Forsvarsministeren oplyser, at Beredskabsstyrelsen har revideret styrelsens plan for test af backupsystemet, så planen nu omfatter alle kendte variationer af genetableringsscenarier.

Opsummering

12. Sundhedsministeren, udenrigsministeren, transport-, bygnings- og boligministeren og forsvarsministeren oplyser, at de har implementeret eller planlægger at iværksætte en række tiltag, der skal imødegå de mangler, som Rigsrevisionen påpegede, og dermed beskytte institutionerne mod ransomwareangreb.

Rigsrevisionen vurderer dog, at ingen af ministrene redegør for deres håndtering af alle de mangler, som Rigsrevisionen påpegede. Det skyldes, at der er tiltag, som ministrene ikke har redegjort for, og at der er tiltag, hvor det er uklart, om de imødegår de påpegede mangler. Derudover oplyser 2 ministre, at de ikke planlægger at implementere ét af tiltagene, og det er uklart, hvilke kompenserende tiltag institutionerne eventuelt har iværksat, eller om risikoen fremgår af institutionernes risikoanalyse.

Rigsrevisionen har lagt til grund, at implementeringen af tiltagene sikrer en grundlæggende beskyttelse mod ransomwareangreb. Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om institutionernes implementering af de tiltag, hvor Rigsrevisionen påpegede mangler.

Lone Strøm