FOLKETINGET
RIGSREVISIONEN

Juni 2024

Rigsrevisionens notat om
beretning om

beskyttelse mod ransomwareangreb

Opfølgning i sagen om beskyttelse mod ransomware-angreb (beretning nr. 11/2017)

27. maj 2024

RN 1406/24

I. Baggrund og konklusion

1. Rigsrevisionen følger i dette notat op på sagen om beskyttelse mod ransomware-angreb, som blev indledt med en beretning i 2018. Opfølgningen sker med henblik på at vurdere, om Banedanmark, Beredskabsstyrelsen, Sundhedsdatastyrelsen og Udenrigsministeriet har implementeret tiltag, der adresserer den kritik, der fremgår af Statsrevisorernes bemærkninger og Rigsrevisionens beretning. Vi har tidligere behandlet sagen i notater til Statsrevisorerne af 1. juni 2018 og 25. januar 2021.

2. Beretningen handlede om de 4 statslige institutioners beskyttelse mod ransomwareangreb, som typisk sker via e-mails. Undersøgelsen omfattede Banedanmark, Beredskabsstyrelsen, Sundhedsdatastyrelsen og Udenrigsministeriet. De 4 institutioner var udvalgt, fordi de varetager samfundsvigtige opgaver inden for transport, beredskab, sundhed, og udenrigsforhold.

3. Da Statsrevisorerne behandlede beretningen, fandt de, at de 4 institutioners beskyttelse mod ransomwareangreb ikke var tilfredsstillende, og at der hermed var 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.

Konklusion

Rigsrevisionen finder det meget utilfredsstillende, at alle 4 institutioner fortsat mangler at implementere tiltag til beskyttelse mod ransomwareangreb 6 år efter, at sårbarheden blev påpeget i beretningen. For Banedanmark og Udenrigsministeriet vedrører det bl.a. tekniske minimumskrav for statslige myndigheder, der er ufravigelige.

Rigsrevisionens opfølgning viser, at de 4 institutioner har gennemført enkelte tiltag, der medvirker til at reducere institutionernes sårbarhed over for ransomwareangreb, men at ingen af institutionerne er i mål med at implementere alle tiltag.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

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

Sagsforløb for en større undersøgelse

Beretning
↓
Ministerredegørelse
↓
§ 18, stk. 4-notat
↓
Fortsat notat
↓
Sagen afsluttes

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

II. Status på sagen

4. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkter:

Et opfølgningspunkt afsluttes, når Statsrevisorerne på baggrund af indstilling fra Rigsrevisionen vurderer, at myndighedernes initiativer er tilfredsstillende.

Opfølgningspunkt	Status
1. Institutionernes implementering af de tiltag, hvor Rigsrevisionen påpegede mangler.	Behandles i dette notat og følges fortsat.

III. Banedanmarks, Beredskabsstyrelsens, Sundhedsdatastyrelsens og Udenrigsministeriets tiltag til beskyttelse mod ransomwareangreb

5. Vi gennemgår i de følgende afsnit Banedanmarks, Beredskabsstyrelsens, Sundhedsdatastyrelsens og Udenrigsministeriets implementering af tiltag, hvor Rigsrevisionen påpegede mangler.

6. Opfølgningen er baseret på revisionsbesøg hos de 4 institutioner i perioden december 2023 - januar 2024 og en gennemgang af fremsendt dokumentation. Hertil kommer korrespondance og høringssvar fra hver enkelt institution i forbindelse med udarbejdelsen af notatet.

7. Statsrevisorerne bemærkede, at forebyggelsen mod ransomwareangreb ikke var tilstrækkelig, og at ingen af institutionerne fuldt ud havde sikret, at alle deres programmer havde de nyeste sikkerhedsopdateringer. Statsrevisorerne bemærkede, at ledelsen i Sundhedsdatastyrelsen og i Banedanmark ikke havde dækkende risikovurderinger for truslen fra ransomwareangreb, og 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.

Tabel 1

De 4 institutioners tiltag til beskyttelse mod ransomwareangreb: Opfølgningen i 2021 vs. 2024

Institution	Manglende tiltag mod ransomwareangreb		Heraf ufravigelige minimumskrav, der ikke er implementeret
	2021	2024	
Banedanmark	7	5	2
Beredskabsstyrelsen	5	4	0
Sundhedsdatastyrelsen	10	3	0
Udenrigsministeriet	8	6	2
I alt	**30**	**18**	**4**

Note: For Sundhedsdatastyrelsen er der ikke fulgt op på alle manglende tiltag i 2024, jf. pkt. 15.

Kilde: Rigsrevisionen.

Banedanmark

8. Det fremgik af notat til Statsrevisorerne af 25. januar 2021, at Banedanmark manglede at implementere 7 forskellige tiltag til beskyttelse mod ransomwareangreb. Rigsrevisionens opfølgning på de 7 tiltag er opsummeret i tabel 1.

9. Vores opfølgning viser, at Banedanmark siden 2021 har implementeret 2 tiltag til beskyttelse mod ransomwareangreb, hvoraf det ene er et ufravigeligt teknisk minimumskrav. Banedanmark mangler fortsat at implementere 5 tiltag. Rigsrevisionen konstaterer, at 2 af tiltagene, som Banedanmark mangler at implementere, vedrører ufravigelige tekniske minimumskrav. Rigsrevisionen finder det meget utilfredsstillende, at Banedanmark endnu ikke er i mål med at opfylde alle ufravigelige tekniske minimumskrav for statslige myndigheder.

10. Rigsrevisionen vil fortsat følge Banedanmarks arbejde med at implementere de tiltag, hvor Rigsrevisionen påpegede mangler, herunder om Banedanmark overholder de ufravigelige krav til it-sikkerheden.

Beredskabsstyrelsen

11. Siden beretningens afgivelse er Beredskabsstyrelsen overgået til Forsvarsministeriets koncernfælles it-afdeling, Cyber Divisionen, der er en del af Forsvarsministeriets Materiel- og Indkøbsstyrelse. Det er derfor formelt Forsvarsministeriets Materiel- og Indkøbsstyrelse, som har ansvaret for Beredskabsstyrelsens it-løsninger. Af formidlingsmæssige årsager henviser vi i dette notat fortsat til Beredskabsstyrelsen.

12. Det fremgik af notat til Statsrevisorerne af 25. januar 2021, at Beredskabsstyrelsen manglede at implementere 5 tiltag til beskyttelse mod ransomwareangreb. Rigsrevisionens opfølgning på de 5 tiltag er opsummeret i tabel 1.

13. Vores opfølgning viser, at Beredskabsstyrelsen siden 2021 har implementeret ét af de 5 tiltag til beskyttelse mod ransomwareangreb. Beredskabsstyrelsen mangler fortsat at implementere 4 tiltag. 3 af de 4 tiltag er delvist implementeret. Rigsrevisionen finder det meget utilfredsstillende, at Beredskabsstyrelsen fortsat mangler at implementere tiltag til beskyttelse mod ransomwareangreb.

14. Rigsrevisionen vil fortsat følge Beredskabsstyrelsens arbejde med at implementere de tiltag, hvor Rigsrevisionen påpegede mangler.

Sundhedsdatastyrelsen

15. Det fremgik af notat til Statsrevisorerne af 25. januar 2021, at Sundhedsdatastyrelsen manglede at implementere 10 tiltag til beskyttelse mod ransomwareangreb. I dette notat har vi fulgt op på 4 af tiltagene. Det skyldes, at Sundhedsdatastyrelsen er overgået til at være kunde hos Statens It siden sidste opfølgning. Overgangen medfører, at 4 tiltag ikke længere håndteres af Sundhedsdatastyrelsen, men af Statens It. Herudover er 2 tiltag blevet undersøgt i forbindelse med opfølgningen på Rigsrevisionens beretning om 5 myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden. Rigsrevisionens opfølgning på den beretning blev gennemført i 2024 og viste, at Sundhedsdatastyrelsen ikke havde implementeret de 2 tiltag. Rigsrevisionens opfølgning på de 4 tiltag er opsummeret i tabel 1.

16. Vores opfølgning viser, at Sundhedsdatastyrelsen siden 2021 har implementeret ét af de 4 tiltag til beskyttelse mod ransomwareangreb. Initiativet, som Sundhedsdatastyrelsen har implementeret, vedrører et af de ufravigelige tekniske minimumskrav. Styrelsen mangler fortsat at implementere 3 tiltag, hvoraf ét tiltag er delvist implementeret. Rigsrevisionen finder det meget utilfredsstillende, at Sundhedsdatastyrelsen fortsat mangler at implementere tiltag til beskyttelse mod ransomwareangreb.

17. Sundhedsdatastyrelsen har oplyst, at de 3 manglende tiltag forventes at være implementeret senest i juli 2024.

18. Rigsrevisionen vil fortsat følge Sundhedsdatastyrelsens arbejde med at implementere de tiltag, hvor Rigsrevisionen påpegede mangler.

Udenrigsministeriet

19. Det fremgik af notat til Statsrevisorerne af 25. januar 2021, at Udenrigsministeriet manglede at implementere 8 tiltag til beskyttelse mod ransomwareangreb. Rigsrevisionens opfølgning på de 8 tiltag er opsummeret i tabel 1.

20. Vores opfølgning viser, at Udenrigsministeriet har implementeret 2 af de 8 tiltag til beskyttelse mod ransomwareangreb siden 2021. Ministeriet mangler fortsat at implementere 6 tiltag. Blandt de manglende tiltag er der 2 ufravigelige tekniske minimumskrav. Ministeriet oplyste i 2021, at ministeriet havde valgt ikke at implementere et mindre antal af minimumskravene og i stedet ville implementere mitigerende foranstaltninger. Ministeriet har ved denne opfølgning oplyst, at ministeriet fortsat har fravalgt ét minimumskrav, men at ministeriet arbejder på at nå i mål med implementeringen af det andet minimumskrav. Rigsrevisionen konstaterer, at Udenrigsministeriet ikke i tilstrækkelig grad er i mål med at dokumentere, at de mitigerende foranstaltninger kan kompensere for det fravalgte minimumskrav til it-sikkerheden, eller at relevante myndigheder med ressortansvar for minimumskravene har taget stilling til, om de mitigerende foranstaltninger er passende. Det finder Rigsrevisionen meget utilfredsstillende.

21. Rigsrevisionen vil fortsat følge Udenrigsministeriets arbejde med at implementere de tiltag, hvor Rigsrevisionen påpegede mangler, herunder om Udenrigsministeriet overholder de ufravigelige minimumskrav til it-sikkerheden eller kan dokumentere, at ministeriets mitigerende foranstaltninger kan opveje for fravigelsen af minimumskravene for it-sikkerheden.

---

22. Hele sagen kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

Birgitte Hansen