FOLKETINGET
RIGSREVISIONEN

Oktober 2025

Rigsrevisionens notat om
beretning om

beskyttelse mod ransomwareangreb

Opfølgning i sagen om beskyttelse mod ransomwareangreb (beretning nr. 11/2017)

24. september 2025

RN 1406/25

I. Baggrund og konklusion

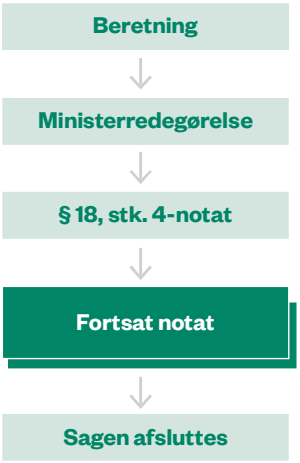
1. Rigsrevisionen følger i dette notat op på sagen om beskyttelse mod ransomwareangreb, som blev indledt med en beretning i 2018. Opfølgningen sker med henblik på at vurdere, om de initiativer, som udenrigsministeren, indenrigs- og sundhedsministeren, transportministeren og ministeren for samfundssikkerhed og beredskab har stillet Statsrevisorerne i udsigt i lyset af Statsrevisorernes bemærkninger og Rigsrevisionens beretning, er gennemført. Vi har tidligere behandlet sagen i notater til Statsrevisorerne af 1. juni 2018, 25. januar 2021 og 27. maj 2024.

2. Beretningen handlede om fire statslige institutioners beskyttelse mod ransomwareangreb. Når institutioner rammes af ransomwareangreb, er der risiko for, at data og systemer ikke længere kan anvendes. Det sker typisk via e-mails. Undersøgelsen omfattede Banedanmark, Beredskabsstyrelsen, Sundhedsdatastyrelsen og Udenrigsministeriet. De fire institutioner var udvalgt, fordi de varetager samfundsvigtige opgaver inden for transport, beredskab, sundhed, og udenrigsforhold.

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

4. Statsrevisorerne bemærkede i forbindelse med Rigsrevisionens notat til Statsrevisorerne af maj 2024, jf. Endelig betænkning over statsregnskabet for 2023, at de fandt det kritisabelt, at Banedanmark, Beredskabsstyrelsen, Sundhedsdatastyrelsen og Udenrigsministeriet fortsat ikke havde implementeret alle tiltagene til beskyttelse mod ransomwareangreb 6 år efter, at sårbarheden i institutionernes it-sikkerhed blev påpeget. Statsrevisorerne fandt det særligt kritisabelt, at Banedanmark og Udenrigsministeriet fortsat manglede at implementere ufravigelige tekniske minimumskrav.

Sagsforløb for en større undersøgelse



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

Statsrevisorerne opfordrede på det kraftigste til, at institutionerne fik implementeret tiltagene til beskyttelse mod ransomwareangreb. Statsrevisorerne anmodede i den forbindelse digitaliseringsministeren om en skriftlig redegørelse for fremdriften i implementeringen af tiltagene hos de pågældende institutioner. Ressortansvaret for sager og opgaver vedrørende digital informationssikkerhed er i mellemtiden overdraget til Ministeriet for Samfundssikkerhed og Beredskab, og det er derfor ministeren for samfundssikkerhed og beredskab, der har svaret Statsrevisorerne.

Konklusion

Rigsrevisionen finder det meget utilfredsstillende, at alle fire institutioner fortsat mangler at implementere tiltag til beskyttelse mod ransomwareangreb længe efter, at sårbarheden blev påpeget i beretningen. Rigsrevisionen finder det utilfredsstillende, at sagen har trukket i langdrag, særligt set i lyset af det høje trusselsbillede. Rigsrevisionen finder det meget utilfredsstillende at Banedanmark og Udenrigsministeriet fortsat ikke efterlever de tekniske minimumskrav, der er ufravigelige for statslige myndigheder.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Banedanmarks, Beredskabsstyrelsens, Sundhedsdatastyrelsens og Udenrigsministeriets implementering af de tiltag, hvor Rigsrevisionen påpegede mangler.

II. Status på sagen

5. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkt:

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

6. Vi gennemgår i det følgende de fire institutioners implementering af tiltag, hvor Rigsrevisionen påpegede mangler.

7. Opfølgningen er baseret på revisionsbesøg, korrespondance og dokumentgennemgang hos de fire institutioner i perioden januar-maj 2025.

8. 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 tiltag, der kan sikre, at institutionerne kan genetablere normal drift, efter de er blevet ramt af ransomwareangreb.

9. Det fremgår af Center for Cybersikkerheds (nu en del af Styrelsen for Samfundssikkerhed) trusselsvurdering fra 2024, at truslen for cyberkriminalitet mod bl.a. danske myndigheder er meget høj, og at det er meget sandsynligt, at myndigheder vil blive ramt af cyberkriminalitet inden for de næste 2 år. Set i lyset af dette høje trusselsbillede finder Rigsrevisionen det vigtigt, at myndighederne kommer i mål med at implementere tiltag, der skal forbygge ransomwareangreb.

10. Det fremgik af ministeren for samfundssikkerhed og beredskabs skriftlige redegørelse til Statsrevisorerne af 20. december 2024 om fremdriften:

- at Banedanmark havde oplyst, at to tiltag var opfyldt, to var planlagt til at blive opfyldt i 1. kvartal 2025, og at ét tiltag ville blive prioriteret, men at der ikke var fastlagt et tidspunkt for det endnu.
- at Beredskabsstyrelsen havde oplyst, at deres it-leverandør i marts 2024 havde udarbejdet en plan for implementering af de manglende tiltag. Planen bestod af en række initiativer, hvoraf enkelte afventede igangsættelse.
- at Sundhedsdatastyrelsen havde oplyst, at to tiltag var implementeret i oktober 2024, og at styrelsen forventede at have det sidste tiltag implementeret inden udgangen af 2024.
- at Udenrigsministeriet havde oplyst, at de – med undtagelse af ét tiltag – forventede at have implementeret alle tiltag senest i 1. kvartal 2025.

11. Tabel 1 viser resultaterne af Rigsrevisionens gennemgang af institutionernes implementering af tiltagene.

Tabel 1

De fire institutioners manglende tiltag til beskyttelse mod ransomwareangreb ved opfølgningerne i 2021, 2024 og 2025

Institution	Manglende tiltag mod ransomwareangreb			Heraf ufravigelige minimumskrav, der ikke er implementeret
	2021	2024	2025	
Banedanmark	7	5	3	1
Beredskabsstyrelsen	5	4	3	0
Sundhedsdatastyrelsen	10	3	2	0
Udenrigsministeriet	8	6	4	3[1)]
I alt	**30**	**18**	**12**	**4**

[1)] Der er sket en stigning i Udenrigsministeriets antal af ikke-implementerede ufravigelige minimumskrav siden sidste opfølgning i 2024, hvor ministeriet ikke havde implementeret to ufravigelige krav. Det skyldes, at Digitaliseringsstyrelsen har præciseret og udvidet de tekniske minimumskrav. Det betyder, at ét af de tiltag, som Udenrigsministeriet manglede ved opfølgningen i 2024, nu også er et ufravigeligt minimumskrav.

Kilde: Rigsrevisionen.

Banedanmark

12. Vores opfølgning viser, at Banedanmark siden 2024 har implementeret to af de fem tiltag til beskyttelse mod ransomwareangreb. Banedanmark mangler fortsat at implementere tre tiltag, heraf ét ufravigeligt teknisk minimumskrav. Banedanmark har oplyst, at de forventer at efterleve to af tiltagene inden for 2 år, mens det sidste tiltag, som omhandler det udestående ufravigelige krav, tager længere tid at komme i mål med, da det er mere resursekrævende. Rigsrevisionen finder det meget utilfredsstillende, at Banedanmark fortsat mangler at implementere tre tiltag, herunder ét ufravigeligt teknisk minimumskrav.

Beredskabsstyrelsen

13. Ved kongelig resolution af 29. august 2024 er Beredskabsstyrelsen overgået fra Forsvarsministeriet til Ministeriet for Samfundssikkerhed og Beredskab.

14. Vores opfølgning viser, at Beredskabsstyrelsen siden 2024 har implementeret ét af de fire tiltag til beskyttelse mod ransomwareangreb og dermed fortsat mangler at implementere tre tiltag. Det finder Rigsrevisionen meget utilfredsstillende.

Sundhedsdatastyrelsen

15. Vores opfølgning viser, at Sundhedsdatastyrelsen siden 2024 har implementeret ét af de tre tiltag til beskyttelse mod ransomwareangreb. Sundhedsdatastyrelsen mangler fortsat at implementere to tiltag. Det finder Rigsrevisionen meget utilfredsstillende.

Udenrigsministeriet

16. Vores opfølgning viser, at Udenrigsministeriet siden 2024 har implementeret to af de seks tiltag til beskyttelse mod ransomwareangreb og dermed fortsat mangler at implementere fire tiltag.

Rigsrevisionen konstaterer, at tre af tiltagene, som Udenrigsministeriet mangler at implementere, vedrører ufravigelige tekniske minimumskrav. Rigsrevisionen finder det meget utilfredsstillende, at ministeriet endnu ikke er i mål med at opfylde de resterende krav.

17. Rigsrevisionen konstaterer, at Udenrigsministeriet på baggrund af en risikovurdering har valgt ikke at implementere ét af de tre udestående ufravigelige tekniske minimumskrav. Ministeriet vurderer, at der vil være flere gener i forhold til ministeriets arbejdsopgaver end sikkerhedsmæssige fordele ved at indføre kravet, når ministeriets mitigerende tiltag tages i betragtning. Vi bemærker, at de tekniske minimumskrav er ufravigelige. Det er derfor bekymrende, at Udenrigsministeriet ikke vil implementere kravet. Rigsrevisionen må dog tage ministeriets beslutning til efterretning og vurderer på den baggrund, at vi ikke kan bringe denne del af sagen videre.

18. Rigsrevisionen vil fortsat følge de fire institutioners arbejde med at implementere de sidste tiltag mod ransomwareangreb, herunder Banedanmarks og Udenrigsministeriets efterlevelse af de ufravigelige minimumskrav.

---

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

Birgitte Hansen