FOLKETINGET
RIGSREVISIONEN

Februar 2021

Rigsrevisionens notat om
beretning om

# beskyttelse mod ransomwareangreb

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

25. januar 2021

RN 1402/19

1. Rigsrevisionen følger i dette notat op på sagen om beskyttelse mod ransomware-angreb, som blev indledt med en beretning i 2018. Vi har tidligere behandlet sagen i notat til Statsrevisorerne af 1. juni 2018.

## Konklusion

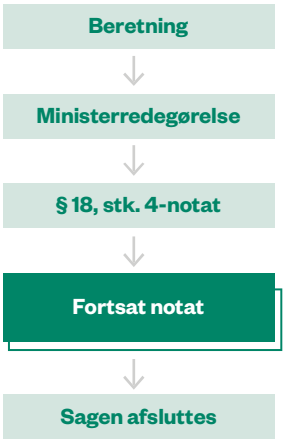
Sundhedsdatastyrelsen, Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen har siden Rigsrevisionens beretning fra 2018 arbejdet med at sikre beskyttelsen mod ransomwareangreb. De 4 institutioner opfylder i 2020 flere af de tiltag, hvor Rigsrevisionen i beretningen påpegede mangler, men mangler alle fortsat at opfylde flere tiltag. Institutionerne har oplyst, at de er i gang med initiativer til at opfylde hovedparten af disse tiltag.

Siden beretningen er 4 af tiltagene imidlertid blevet til ufravigelige krav til it-sikkerheden, som alle statslige myndigheder skal leve op til som led i den nationale cyber- og informationssikkerhedsstrategi. De ufravigelige krav skulle være implementeret senest den 1. januar 2020 og den 1. juli 2020. Rigsrevisionen konstaterer, at Udenrigsministeriet har fravalgt at efterleve de ufravigelige krav og i stedet vil implementere mitigerende foranstaltninger. Rigsrevisionen finder det utilfredsstillende, at Udenrigsministeriet endnu ikke har implementeret de mitigerende foranstaltninger i fuldt omfang. Derudover har undersøgelsen vist, at Sundhedsdatastyrelsen og Banedanmark ikke har sikret sig mod, at hackere kan anvende institutionernes identitet i hackerangreb mod andre, hvilket er et af de ufravigelige krav til it-sikkerheden. Banedanmark har dog sikret dette på alle sine domæner på nær ét domæne, som Banedanmark har oplyst vil blive afviklet. Sundhedsdatastyrelsen har oplyst, at tiltaget er ved at blive implementeret, og at tiltaget primo 2021 nu er implementeret på over 90 % af styrelsens domæner.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Sundhedsdatastyrelsens og Banedanmarks arbejde med at sikre, at institutionerne opfylder de ufravigelige krav til it-sikkerhed
- Udenrigsministeriets arbejde med at implementere de mitigerende foranstaltninger, og at ministeriet kan dokumentere, at de mitigerende foranstaltninger kan kompensere for manglende implementering af de ufravigelige krav til it-sikkerheden
- Sundhedsdatastyrelsens, Udenrigsministeriets, Banedanmarks og Beredskabsstyrelsens arbejde med at sikre, at de opfylder de resterende tiltag.

**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 4 samfundsvigtige, statslige institutioners beskyttelse mod ransomwareangreb. Undersøgelsen omfattede Sundhedsdatastyrelsen, Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen. De 4 institutioner var udvalgt, fordi de varetager samfundsvigtige opgaver inden for sundhed, udenrigsforhold, transport og beredskab, og fordi manglende adgang til data derfor kan være kritisk. Formålet med undersøgelsen var at vurdere, om de 4 institutioner havde en tilfredsstillende beskyttelse mod ransomwareangreb, som kommer ind via e-mails.

3. Da Statsrevisorerne behandlede beretningen, fandt 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. Endelig bemærkede Statsrevisorerne, at beretningen angiver en række tiltag, som alle institutioner kan iværksætte for at reducere risikoen for ransomware.

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. |

5. Vi redegør i dette notat for resultaterne af opfølgningen på ovenstående punkt.

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

# II. Sundhedsdatastyrelsens, Udenrigsministeriets, Banedanmarks og Beredskabsstyrelsens initiativer

6. Vi gennemgår i det følgende Sundhedsdatastyrelsens (under Sundheds- og Ældreministeriet), Udenrigsministeriets, Banedanmarks (under Transport- og Boligministeriet) og Beredskabsstyrelsens (under Forsvarsministeriet) initiativer i forhold til det udestående opfølgningspunkt. Vi gennemgår således status på institutionernes implementering af de tiltag, hvor Rigsrevisionen påpegede mangler i beretningen fra 2018, for temaerne ledelsesmæssigt fokus, ydre tiltag, indre tekniske tiltag, indre adfærdsmæssige tiltag og reaktive tiltag. Gennemgangen er baseret på stedlige revisionsbesøg, dokumentation fra institutionerne og brevveksling med institutionerne.

7. Siden beretningen er Beredskabsstyrelsen overgået til Forsvarets fælles koncern-it, der er en del af Forsvarsministeriets Materiel og Indkøbsstyrelse (FMI). Det er således FMI, der har overtaget ansvaret for Beredskabsstyrelsens it-løsninger. I dette notat henviser vi til Beredskabsstyrelsen af formidlingsmæssige årsager, selv om ansvaret for it-løsningerne er overgået til FMI.

## Ledelsesmæssigt fokus

8. Statsrevisorerne bemærkede, at ledelsen i Sundhedsdatastyrelsen og i Banedanmark ikke havde dækkende risikovurderinger for truslen fra ransomwareangreb.

9. Tabel 1 viser resultaterne af Rigsrevisionens opfølgning på, om institutionernes ledelsesmæssige fokus på ransomware er tilstrækkeligt, og om det ledelsesmæssige fokus er forbedret siden 2018. Rigsrevisionen vurderede i beretningen, at det ledelsesmæssige fokus som minimum bør omfatte de 4 nævnte tiltag i tabel 1.

**Tabel 1**

**Status på, om institutionernes ledelsesmæssige fokus på ransomware er tilstrækkeligt i 2020 sammenholdt med 2017**

| | Sundhedsdata-styrelsen | | Udenrigs-ministeriet | | Banedanmark | | Beredskabs-styrelsen | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 |
| Dækkende risikovurderinger | 🔴 | 🟡 | 🟢 | - | 🔴 | 🔴 | 🟢 | - |
| Opdatering af it-sikkerhedspolitik og retningslinjer | 🟢 | - | 🟢 | - | 🟢 | - | 🟢 | - |
| Krav til backup | 🟢 | - | 🟡 | 🟢 | 🟢 | - | 🟢 | - |
| Opfølgning på ransomwareangreb | 🟡 | 🟢 | 🟢 | - | 🟡 | 🟢 | 🟢 | - |

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da institutionen allerede opfyldte tiltaget i 2017. Som det fremgår af tabellen, opfyldte Beredskabsstyrelsen alle 4 tiltag i 2017, og styrelsen har derfor ikke indgået i denne opfølgning for så vidt angår disse 4 tiltag.

**Kilde:** Rigsrevisionens beretning fra 2018 og opfølgning fra 2020.

10. Det fremgik af beretningen, at 3 af institutionerne ikke opfyldte alle tiltagene i 2017, mens Beredskabsstyrelsen opfyldte alle tiltag. Sundhedsdatastyrelsen og Banedanmark manglede begge dækkende risikovurderinger og opfølgning på ransomwareangreb. Udenrigsministeriet manglede ledelsesmæssigt fokus på krav til backup.

11. Vores opfølgning viser, at Udenrigsministeriet har udarbejdet en backupstrategi og derfor nu opfylder tiltaget om krav til backup.

Sundhedsdatastyrelsen og Banedanmark har begge foretaget opfølgning på ransomwareangreb, men de 2 institutioner har dog fortsat ikke dækkende risikovurderinger. Sundhedsdatastyrelsen er i gang med at opdatere styrelsens risikovurderinger, så de bliver dækkende og bl.a. tager højde for ransomwareangreb. Sundhedsdatastyrelsen forventer at være færdig med dette arbejde med udgangen af 1. kvartal 2021. Banedanmark er i 2020 gået i gang med at udarbejde en risikovurdering, som bl.a. tager højde for ransomware. Banedanmark har i maj 2020 godkendt en risikostyringsmetodik, men mangler fortsat bl.a. at kortlægge og udvælge kritiske systemer og processer og udarbejde risikovurderinger på de enkelte systemer. Banedanmark forventer, at arbejdet med risikovurderingen vil strække sig ind i 2021.

12. Rigsrevisionen vil fortsat følge Sundhedsdatastyrelsens og Banedanmarks arbejde med at færdiggøre risikovurderingerne.

## Ydre tiltag

13. Tabel 2 viser resultaterne af Rigsrevisionens opfølgning på, om institutionernes ydre tiltag mod ransomware er tilstrækkelige, og om de tiltagene er forbedret siden 2017. Rigsrevisionen vurderede i beretningen, at de ydre tiltag som minimum bør omfatte de 4 nævnte tiltag i tabel 2.

**Tabel 2**

**Status på, om institutionernes ydre tiltag mod ransomware er tilstrækkelige i 2020 sammenholdt med 2017**

| | Sundhedsdata-styrelsen | | Udenrigs-ministeriet | | Banedanmark | | Beredskabs-styrelsen | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 |
| Brug af antispam- og antivirusløsninger | ● | - | ● | - | ● | - | ● | - |
| Forhindre omgåelse af den centrale antispam- og antivirusløsning | ● | - | ● | - | ● | - | ● | - |
| Brug af 2-faktorlogin ved webmailløsninger[1)] | ● | ● | ● | ● | ● | ● | Ikke relevant | - |
| Forhindre brug af private e-mailløsninger | ● | ● | ● | ● | ● | ● | ● | ● |

[1)] Dette tiltag er et ufravigeligt krav, som alle myndigheder skulle leve op til pr. 1. januar 2020 som led i den nationale cyber- og informationssikkerhedsstrategi.

Note: Farverne angiver, om tiltaget er opfyldt (grøn) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da institutionen allerede opfyldte tiltaget i 2017.

**Kilde:** Rigsrevisionens beretning fra 2018 og opfølgning fra 2020.

14. Det fremgik af beretningen, at alle 4 institutioner anvendte antispam- og antivirusløsninger og forhindrede omgåelse af den centrale antispam- og antivirusløsning. Derudover fremgik det, at 3 af institutionerne ikke anvendte 2-faktorlogin ved webmailløsninger, og at ingen af institutionerne forhindrede brug af private e-mailløsninger.

15. Siden beretningen er brug af 2-faktorlogin ved webmailløsninger blevet et ufravigeligt krav til alle myndigheder pr. 1. januar 2020 som led i den nationale cyber- og informationssikkerhedsstrategi. Manglende 2-faktorlogin ved webmailløsninger kan betyde, at en hacker kan få adgang til at sende inficerede e-mails, herunder ransomware, uden at disse har været igennem virksomhedens ydre sikringstiltag. Vores opfølgning viser, at Udenrigsministeriet og Banedanmark har etableret 2-faktorlogin ved brug af webmailløsninger, men at Sundhedsdatastyrelsen endnu ikke opfylder kravet. Sundhedsdatastyrelsen har oplyst, at arbejdet med etablering af 2-faktorlogin er påbegyndt, og at styrelsen prioriterer implementeringen af 2-faktorlogin. Tidsplanen for implementeringen påvirkes af overgangen til Statens It og styrelsens opgaver med at it-understøtte den hidtidige, aktuelle og fremadrettede COVID-19- og vaccineindsats. Sundhedsdatastyrelsens ledelse vil følge implementeringen tæt og sikre fremdrift

Derudover viser vores opfølgning, at Beredskabsstyrelsen som den eneste har forhindret brug af private e-mailløsninger, mens man er logget på systemet. De 3 øvrige institutioner har oplyst, at de aktivt har valgt at tillade medarbejderne at bruge private e-mailløsninger. Banedanmark har oplyst, at beslutningen om at tillade brug af private e-mailløsninger er risikovurderet og ledelsesgodkendt, men har ikke fremlagt dokumentation herfor. Sundhedsdatastyrelsen og Udenrigsministeriet har ikke dokumenteret en ledelsesgodkendt beslutning og risikovurdering af at tillade medarbejdernes brug af private e-mailløsninger. Rigsrevisionen vurderer, at brug af private e-mailløsninger på institutionernes netværk udgør en sikkerhedsrisiko for ransomwareangreb. Rigsrevisionen finder på den baggrund, at beslutningen om at tillade brug af private e-mailløsninger som minimum bør bygge på en dokumenteret risikovurdering, der er ledelsesgodkendt. Udenrigsministeriet har oplyst, at beslutningen om at tillade adgang til private e-mailløsninger vil blive risikovurderet og ledelsesgodkendt primo 2021.

16. Rigsrevisionen finder det utilfredsstillende, at Sundhedsdatastyrelsen ikke lever op til det ufravigelige krav om at etablere 2-faktorlogin ved webmailløsninger, på trods af at dette er et ufravigeligt krav og skulle være implementeret pr. 1. januar 2020. Rigsrevisionen vil fortsat følge Sundhedsdatastyrelsens arbejde med at etablere 2-faktorlogin ved webmailløsninger. Derudover vil Rigsrevisionen følge op på, om Sundhedsdatastyrelsen, Udenrigsministeriet og Banedanmark forhindrer, at medarbejderne kan anvende private e-mailløsninger, eller som minimum risikovurderer og ledelsesgodkender beslutningen om at tillade brug private e-mailløsninger.

### Fremadrettede ydre tiltag

17. I beretningen indgik 3 fremadrettede ydre tiltag. På tidspunktet for beretningen var der tale om nye tiltag, som Rigsrevisionen fandt det relevant for institutionerne at overveje i forhold til beskyttelse mod ransomwareangreb. Siden beretningen er de fremadrettede ydre tiltag blevet ufravigelige krav til alle myndigheder pr. 1. juli 2020 som led i den nationale cyber- og informationssikkerhedsstrategi. Tabel 3 viser resultaterne af vores opfølgning på, om de 4 institutioner har implementeret de 3 nævnte tiltag sammenholdt med 2017.

**Tabel 3**

**Status på, om institutionerne har implementeret ufravigelige krav til ydre tiltag i 2020 sammenholdt med 2017**

| | Sundhedsdata-styrelsen | | Udenrigs-ministeriet | | Banedanmark | | Beredskabs-styrelsen | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 |
| Sikring mod, at hackere kan anvende institutionernes domænenavne som afsenderdomænenavne, når de sender indgående e-mails | ● | - | ● | ● | ● | - | ● | ● |
| Kontrol af eventuelle indgående e-mails i forhold til afsenderidentiteten og eventuel frasortering, fx ved hjælp af SPF-, DMARC- og DKIM-teknologierne | ● | - | ● | ● | ● | ● | ● | ● |
| Sikring mod misbrug af identitet ved angreb mod andre, fx ved hjælp af SPF-, DMARC- og DKIM-teknologierne | ● | ● | ● | ● | ● | ● | ● | ● |

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da institutionen allerede opfyldte tiltaget i 2017. Farveændringerne fra gule vurderinger i 2017 til røde i 2020 skyldes, at der siden 2017 er blevet tale om ufravigelige krav, hvorfor det ikke er tilstrækkeligt med en delvis opfyldelse.

**Kilde:** Rigsrevisionens beretning fra 2018 og opfølgning fra 2020.

**SPF-, DMARC- og DKIM-teknologier**

SPF-, DMARC- og DKIM-teknologierne er teknologier, som sikrer institutioner mod misbrug af domænet til svindel med e-mailadresser og dermed begrænser muligheden for, at institutionernes identitet bliver misbrugt som afsenderadresse.

18. Det fremgik af beretningen, at Udenrigsministeriet og Beredskabsstyrelsen ikke opfyldte nogen af de 3 tiltag i fuldt omfang. Derudover fremgik det, at Sundhedsdatastyrelsen og Banedanmark havde sikret, at hackere ikke kunne anvende institutionernes domænenavne som afsenderdomænenavne, når de sendte indgående e-mails, dvs. at hackere ikke kunne anvende institutionernes e-mailadresser som afsender på e-mails til medarbejderne. Endelig fremgik det, at Sundhedsdatastyrelsen havde sikret, at indgående mails blev kontrolleret i forhold til afsenderidentiteten og eventuelt frasorteret på den baggrund, mens Banedanmark ikke havde sikret dette.

19. Vores opfølgning viser, at Banedanmark i 2020 nu opfylder kravet om, at indgående e-mails skal kontrolleres i forhold til afsenderidentiteten og eventuelt frasorteres. Sundhedsdatastyrelsen og Banedanmark har dog i 2020 fortsat ikke sikret sig mod, at hackere kan anvende institutionernes identitet i hackerangreb mod andre. Banedanmark har implementeret tiltaget på alle sine domæner på nær ét domæne, som Banedanmark har oplyst vil blive afviklet. Sundhedsdatastyrelsen har oplyst, at styrelsen er i gang med at opfylde tiltaget, og at status primo 2021 er, at styrelsen nu lever op til tiltaget på over 90 % af sine domæner.

Derudover viser vores opfølgning, at Udenrigsministeriet fortsat i 2020 ikke opfylder nogen af de 3 ufravigelige krav. Udenrigsministeriet har oplyst, at ministeriet har fravalgt de 3 tiltag af faglige hensyn og i stedet vil iværksætte mitigerende foranstaltninger, som ifølge ministeriet vil imødekomme en del af risikoen ved ikke at implementere de 3 tiltag. Nogle af foranstaltningerne er implementeret, mens Udenrigsministeriet har oplyst, at de resterende mitigerende foranstaltninger vil blive implementeret i 2021. Udenrigsministeriet har ultimo 2020 risikovurderet ministeriets ydre tiltag i forhold til misbrug af ministeriets domænenavne til angreb mod andre eller til angreb mod ministeriet gennem e-mails. I risikovurderingen tages der stilling til fravalget af implementering af de 3 tiltag, og hvilke mitigerende foranstaltninger der i stedet skal implementeres. Risikovurderingen er ultimo 2020 godkendt af Udenrigsministeriets sikkerhedsudvalg.

Endelig viser vores opfølgning, at Beredskabsstyrelsen i 2020 opfylder alle 3 ufravigelige krav til ydre tiltag.

20. Rigsrevisionen konstaterer, at Udenrigsministeriet fortsat ikke lever op til alle 3 ufravigelige krav til ydre tiltag, på trods af at tiltagene skulle have været implementeret pr. 1. juli 2020. Rigsrevisionen konstaterer videre, at Udenrigsministeriet i stedet vil implementere mitigerende foranstaltninger, som ifølge ministeriet vil imødekomme en del af risikoen ved ikke at implementere de 3 tiltag. Rigsrevisionen finder det utilfredsstillende, at Udenrigsministeriet endnu ikke har implementeret disse foranstaltninger i fuldt omfang. Da Udenrigsministeriet ikke har implementeret de mitigerende foranstaltninger i fuldt omfang, er det ikke muligt for Rigsrevisionen at vurdere disse foranstaltninger. Rigsrevisionen vil derfor, når foranstaltningerne er iværksat, følge op på, om Udenrigsministeriet kan dokumentere, at de mitigerende foranstaltninger kan kompensere for manglende implementering af de ufravigelige krav. Umiddelbart finder Rigsrevisionen dog – når de ufravigelige krav ikke følges – at der er en øget risiko for, at Udenrigsministeriets it-sikkerhed ikke er tilstrækkelig, herunder risiko for, at myndigheder og personer ikke i alle tilfælde kan stole på mailkommunikation via Udenrigsministeriets domæner. Rigsrevisionen konstaterer derudover, at Sundhedsdatastyrelsen og Banedanmark begge mangler at opfylde ét af de ufravigelige krav til ydre tiltag. Rigsrevisionen vil fortsat følge Sundhedsdatastyrelsens og Banedanmarks opfyldelse af tiltaget samt Udenrigsministeriets implementering af de mitigerende foranstaltninger.

## Indre tekniske tiltag

21. 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.

22. Tabel 4 viser resultaterne af Rigsrevisionens opfølgning på, om institutionerne i tilstrækkelig grad opfylder de indre tekniske tiltag mod ransomware, og om tiltagene er forbedret siden 2017. Rigsrevisionen vurderede i beretningen, at de indre tekniske tiltag som minimum bør omfatte de 7 nævnte tiltag i tabel 4.

**Tabel 4**

**Status på, om institutionernes indre tekniske tiltag mod ransomware er tilstrækkelige i 2020 sammenholdt med 2017**

| | Sundhedsdata-styrelsen | | Udenrigs-ministeriet | | Banedanmark | | Beredskabs-styrelsen | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 |
| Lokaladministrator har et arbejdsbetinget behov | 🔴 | 🔴 | 🟢 | - | 🔴 | 🟡 | 🟢 | - |
| Opdatering af styresystemer | 🟢 | - | 🟢 | - | 🟢 | - | 🟢 | - |
| Opdatering af programmer, som er tredjeparts-produkter | 🔴 | 🟢 | 🟡 | 🟡 | 🔴 | 🔴 | 🟡 | 🟢 |
| Kun godkendte programmer kan afvikles (whitelistingløsning) | 🟡 | 🟡 | 🟢 | - | 🟡 | 🟢 | 🟡 | 🟡 |
| Ingen brug af privilegerede rettigheder, når der læses e-mails | 🟡 | 🟡 | 🟢 | - | 🔴 | 🟢 | 🟡 | 🟢 |
| Sikring mod ubeskyttet adgang til internettet og mod, at medarbejdere ikke kan downloade potentielt skadelige filer, mens de læser e-mails. | 🟡 | 🟡 | 🟢 | - | 🟡 | 🟢 | 🟡 | 🟡 |
| Rettighedstildeling på filniveau i overensstemmelse med egne retningslinjer | 🟢 | - | 🟢 | - | 🟢 | - | 🟢 | - |

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da institutionen allerede opfyldte tiltaget i 2017.

**Kilde:** Rigsrevisionens beretning fra 2018 og opfølgning fra 2020.

23. Det fremgik af beretningen, at alle institutionerne havde sikret, at styresystemerne blev opdateret, og at rettighedstildeling på filniveau var i overensstemmelse med egne retningslinjer. Derudover fremgik det, at institutionerne manglede at opfylde 1-5 indre tekniske tiltag.

24. Vores opfølgning viser, at ingen af institutionerne opfylder alle indre tekniske tiltag, og at institutionerne fortsat mangler at opfylde 1-4 tiltag.

Sundhedsdatastyrelsen og Banedanmark mangler begge at sikre, at ingen medarbejdere ud over it-supportere og lignende med et arbejdsbetinget behov tildeles lokaladministratorrettigheder. Vores opfølgning viser, at antallet af medarbejdere med lokaladministratorrettigheder hos Sundhedsdatastyrelsen er steget siden 2017. Sundhedsdatastyrelsen har oplyst, at det skyldes COVID-19-situationen, hvor der er opstået et midlertidigt behov for flere medarbejdere med lokaladministratorrettigheder, og at behovet for antal lokaladministratorer vil blive revurderet, i forbindelse med at styrelsen overgår til Statens It i 2021. Sundhedsdatastyrelsen har derudover oplyst, at styrelsen i 2020 har skærpet dispensationsansøgninger om lokaladministratorrettigheder, så de er af maksimalt 6 måneders varighed, og at styrelsens ledelse løbende forelægges data om antal dispensationsansøgninger med henblik på at risikovurdere og ledelsesgodkende en eventuel forlængelse af dispensationer. Rigsrevisionen har forståelse for, at der under COVID-19-pandemien har været behov for tildeling af flere lokaladministratorrettigheder. Rigsrevisionen finder dog, at varigheden af lokaladministratorrettigheder i forbindelse med sådanne nødprocedurer bør være så kort som muligt, og at Sundhedsdatastyrelsen bør undersøge, om lokaladministratorrettigheder kan gives for en endnu kortere periode fremadrettet. Rigsrevisionen vurderer, at der ellers kan være risiko for, at Sundhedsdatastyrelsens øvrige it-sikkerhedstiltag obstrueres af den betydelige sikkerhedsrisiko, som følger af et højt antal lokaladministratorrettigheder.

Banedanmark har siden 2018 nedbragt antallet af lokaladministratorer med knap 30 %. Derudover har Banedanmark oplyst, at lokaladministratorrettigheder højst tildeles for 1 år ad gangen, og at rettighederne fjernes, når medarbejderen ikke har brug for dem længere. Vores opfølgning viser, at Banedanmark gennemgår listen med lokaladministratorer uden fast procedure. Banedanmark har oplyst, at der primo 2021 vil blive etableret procedurer for løbende opfølgning og kontrol.

Udenrigsministeriet og Banedanmark mangler i tilstrækkelig grad at sikre opdateringerne af programmer, som er tredjepartsprodukter. Udenrigsministeriet har en løsning, der sikrer systematisk opdatering af en del af ministeriets tredjepartsprodukter, men de resterende produkter opdateres ikke systematisk. Banedanmark har ikke sikret en systematisk opdatering af tredjepartsprodukter, men har oplyst, at sådanne opdateringer foretages manuelt efter behov. Banedanmark har oplyst, at en systematisk opdatering af tredjepartsprodukter vil kunne finde sted i 2021 eller 2022, når en række ældre systemer er blevet udskiftet. Rigsrevisionen konstaterer, at den valgte tilgang, som udgør en sikkerhedsmæssig risiko, ikke er risikovurderet og godkendt af ledelsen i Banedanmark.

Derudover har Banedanmark sikret, at kun godkendte programmer kan afvikles, fx ved hjælp af en whitelistingløsning, mens Sundhedsdatastyrelsen og Beredskabsstyrelsen fortsat kun delvist har sikret dette. Sundhedsdatastyrelsen anvender ikke en whitelistingløsning, men har sikret, at kun medarbejdere med lokaladministratorrettigheder selv kan installere software. Rigsrevisionen bemærker dog, at antallet af lokaladministratorer i Sundhedsdatastyrelsen er steget, hvilket udgør en risiko for, at disse medarbejdere kan komme til at installere skadelig software. Beredskabsstyrelsen har på hovedparten af styrelsens pc'er sikret, at kun godkendte programmer kan afvikles. Beredskabsstyrelsen har oplyst, at styrelsen er i gang med at udfase de resterende pc'er fremfor at installere whitelistingteknologier på disse.

Endvidere har Banedanmark og Beredskabsstyrelsen sikret, at der ikke kan anvendes privilegerede rettigheder, mens der læses e-mails, mens Sundhedsdatastyrelsen fortsat kun delvist opfylder dette tiltag. Sundhedsdatastyrelsen har retningslinjer, der præciserer, at medarbejdere med privilegerede rettigheder ikke må læse e-mails, mens disse rettigheder anvendes. Sundhedsdatastyrelsen har dog enkelte konti med privilegerede rettigheder, der har tilknyttede e-mailadresser og dermed mulighed for at tilgå e-mails. Sundhedsdatastyrelsen har oplyst, at styrelsen primo 2021 har gennemgået og vurderet de konti med privilegerede rettigheder, som har adgang til e-mails, og i den forbindelse har lukket flere kontis e-mailadgang. Gennemgangen har dog vist, at antallet af konti med privilegerede rettigheder, der har adgang til e-mails, samlet set er steget siden revisionens start. Sundhedsdatastyrelsen har oplyst, at disse konti tilhører brugere, som har et arbejdsbetinget behov, og at det overvåges, at brugerne ikke anvender e-mails, når de bruger disse konti. Derudover har Sundhedsdatastyrelsen oplyst, at antallet af disse konti vil blive revurderet løbende og senest i forbindelse med overgangen til Statens It i 2021. Rigsrevisionen finder det utilfredsstillende, at antallet af konti med privilegerede rettigheder, der har adgang til e-mails, er steget i undersøgelsesperioden, og vurderer, at det udgør en risiko for Sundhedsdatastyrelsens it-sikkerhed.

Endelig har Banedanmark implementeret en teknisk løsning, som blokerer for visse filtyper. Banedanmark har oplyst, at den tekniske løsning også begrænser andre filtyper, hvilket er beskrevet i produktejers systemdokumentation. Sundhedsdatastyrelsen og Beredskabsstyrelsen har fortsat kun delvist sikret sig mod ubeskyttet adgang til internettet. Sundhedsdatastyrelsen anvender hovedsageligt løsninger, hvor der blokeres for kendt skadeligt indhold. På baggrund heraf er det Rigsrevisionens vurdering, at Sundhedsdatastyrelsen ikke er beskyttet i tilstrækkelig grad mod ukendt skadeligt indhold. Beredskabsstyrelsen har på hovedparten af styrelsens pc'er sikret, at der ikke er ubeskyttet adgang til internettet, og at medarbejderne ikke kan downloade potentielt skadelige filer. Beredskabsstyrelsen har oplyst, at styrelsen er i gang med at udfase de resterende pc'er.

25. Rigsrevisionen vil fortsat følge Sundhedsdatastyrelsens, Udenrigsministeriets, Banedanmarks og Beredskabsstyrelsens arbejde med at opfylde de resterende indre tekniske tiltag.

**Fremadrettede tekniske tiltag**

26. I beretningen indgik 2 fremadrettede indre tiltag. På tidspunktet for beretningen var der tale om nye tiltag, som Rigsrevisionen fandt det relevant for institutionerne at overveje i forhold til beskyttelse mod ransomwareangreb. Rigsrevisionen vurderer, at tiltagene siden 2017 er blevet yderligere relevante, og derfor har vi fulgt op på, om institutionerne opfylder de 2 nævnte tiltag i 2020. Tabel 5 viser resultaterne af Rigsrevisionens opfølgning på, om institutionerne har implementeret de 2 fremadrettede indre tiltag mod ransomwareangreb i 2020 sammenholdt med 2017.

**Tabel 5**

**Status på, om institutionerne opfylder de fremadrettede indre tiltag mod ransomware i 2020 sammenholdt med 2017**

| | Sundhedsdata-styrelsen | | Udenrigs-ministeriet | | Banedanmark | | Beredskabs-styrelsen | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 |
| Programmer med atypiske adfærdsmønstre opdages | ● | ● | ● | ● | ● | - | ● | - |
| Programmer med atypiske adfærdsmønstre stoppes eller begrænses | ● | ● | ● | ● | ● | ● | ● | ● |

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da institutionen allerede opfyldte tiltaget i 2017.

**Kilde:** Rigsrevisionens beretning fra 2018 og opfølgning fra 2020.

27. Det fremgik af beretningen, at Banedanmark og Beredskabsstyrelsen i 2017 havde sikret, at programmer med atypiske adfærdsmønstre blev opdaget, mens Sundhedsdatastyrelsen og Udenrigsministeriet ikke opfyldte tiltaget. Derudover fremgik det, at Sundhedsdatastyrelsen, Udenrigsministeriet og Beredskabsstyrelsen ikke sikrede, at programmer med atypiske adfærdsmønstre blev stoppet eller begrænset, mens Banedanmark delvist opfyldte tiltaget.

28. Vores opfølgning viser, at Udenrigsministeriet nu har sikret, at programmer med atypiske adfærdsmønstre opdages. Sundhedsdatastyrelsen har delvist etableret sikringstiltag, der kan opdage og alarmere om atypiske adfærdsmønstre. Konkret har Sundhedsdatastyrelsen implementeret et redskab, der sikrer, at nogle applikationer, brugere og enheder med atypiske adfærdsmønstre stoppes eller begrænses. Sundhedsdatastyrelsen har oplyst, at det fortsat udestår at kommunikere ud til alle medarbejdere i Sundheds- og Ældreministeriet, at Sundhedsdatastyrelsen kan kontaktes ved risikofyldt aktivitet. Derudover har Sundhedsdatastyrelsen oplyst, at styrelsen og Sundheds- og Ældreministeriets departement i foråret 2021 vil beslutte, hvilken løsning der skal være gældende permanent fra 2022.

Derudover viser vores opfølgning, at Banedanmark har sikret, at programmer med atypiske adfærdsmønstre stoppes eller begrænses, mens de 3 øvrige institutioner delvist har sikret dette. Sundhedsdatastyrelsen har via tekniske tiltag delvist sikret, at atypiske adfærdsmønstre stoppes eller begrænses. Udenrigsministeriet har ikke implementeret et værktøj til at stoppe atypiske adfærdsmønstre i realtid, men har implementeret kompenserende kontroller, der reducerer sikkerhedsrisikoen. Beredskabsstyrelsen har implementeret tekniske løsninger, der understøtter overvågning og analysering af atypiske brugsmønstre. Disse tekniske løsninger er implementeret på hovedparten af styrelsens pc'er. Beredskabsstyrelsen har oplyst, at de resterende pc'er er under udfasning. Rigsrevisionen vurderer, at de 3 institutioner fortsat bør arbejde med at sikre, at programmer med atypiske adfærdsmønstre stoppes eller begrænses.

29. Rigsrevisionen vil fortsat følge Sundhedsdatastyrelsens, Udenrigsministeriets og Beredskabsstyrelsens arbejde med at opfylde de fremadrettede indre tekniske tiltag.

## Indre adfærdsmæssige tiltag

30. Tabel 6 viser resultaterne af Rigsrevisionens opfølgning på, om institutionernes indre adfærdsmæssige tiltag mod ransomware er opfyldt, og om tiltagene er forbedret siden 2017. Rigsrevisionen vurderede i beretningen, at de indre adfærdsmæssige tiltag som minimum bør omfatte de 2 nævnte tiltag i tabel 6.

**Tabel 6**

**Status på, om institutionernes indre adfærdsmæssige tiltag mod ransomware er tilstrækkelige i 2020 sammenholdt med 2017**

| | Sundhedsdata-styrelsen | | Udenrigs-ministeriet | | Banedanmark | | Beredskabs-styrelsen | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 |
| Gennemførelse af awarenessaktiviteter | ● | - | ● | - | ● | - | ● | - |
| Opfølgning på awarenessaktiviteter | ● | ● | ● | ● | ● | ● | ● | ● |

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da institutionen allerede opfyldte tiltaget i 2017.

**Kilde:** Rigsrevisionens beretning fra 2018 og opfølgning fra 2020.

31. Det fremgik af beretningen, at alle 4 institutioner havde gennemført awarenessaktiviteter. Derudover fremgik det, at 3 af institutionerne ikke havde fulgt op på de gennemførte awarenessaktiviteter, mens Sundhedsdatastyrelsen delvist opfyldte tiltaget.

32. Vores opfølgning viser, at Sundhedsdatastyrelsen siden 2017 har etableret opfølgning på awarenessaktiviteter, mens de 3 resterende institutioner fortsat ikke i tilstrækkeligt omfang har fulgt op på gennemførte awarenessaktiviteter. Udenrigsministeriet har ultimo 2019 gennemført en baselinemåling af medarbejdernes awareness og har oplyst, at der primo 2021 på baggrund heraf vil blive gennemført en effektmåling af awarenessaktiviteter. Beredskabsstyrelsen har ligeledes gennemført en baselinemåling i 2020 og vil i 2021 gennemføre en opfølgende måling for at følge op på effekten af gennemførte awarenesstiltag. Banedanmark har endnu ikke foretaget effektmålinger, men har oplyst, at Banedanmark i 2021 planlægger en it-understøttet proces, som ved hjælp af data kan påvise effektmål af de enkelte awarenesstiltag.

33. Rigsrevisionen finder det tilfredsstillende, at Udenrigsministeriet og Beredskabsstyrelsen har påbegyndt et arbejde med at følge op på gennemførte awarenessaktiviteter og konstaterer, at Banedanmark planlægger at gøre det. Rigsrevisionen vil fortsat følge de 3 institutioners arbejde med at følge op på awarenessaktiviteterne.

## Reaktive tiltag

34. Statsrevisorerne bemærkede, 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.

35. Tabel 7 viser resultaterne af Rigsrevisionens opfølgning på, om institutionernes reaktive tiltag mod ransomware er tilstrækkelige, og om tiltagene er forbedret siden 2017. Rigsrevisionen vurderede i beretningen, at de reaktive tiltag som minimum bør omfatte de 3 nævnte tiltag i tabel 7.

**Tabel 7**

**Status på, om institutionernes reaktive tiltag mod ransomware er tilstrækkelige i 2020 sammenholdt med 2017**

| | Sundhedsdata-styrelsen | | Udenrigs-ministeriet | | Banedanmark | | Beredskabs-styrelsen | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 |
| Foranstaltninger, der kan genetablere data, er implementeret | ● | - | ● | - | ● | - | ● | - |
| Genetableringsforanstaltningerne er sikret, så de ikke bliver inkluderet i en krypteringsproces | ● | - | ● | ● | ● | - | ● | - |
| Systematiske tests af evnen til at genetablere systemer og data | ● | - | ● | ● | ● | ● | ● | ● |

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da institutionen allerede opfyldte tiltaget i 2017.

**Kilde:** Rigsrevisionens beretning fra 2018 og opfølgning fra 2020.

36. Det fremgik af beretningen, at alle 4 institutioner i 2017 havde implementeret foranstaltninger, der kunne genetablere data efter ransomwareangreb. Derudover havde 3 af institutionerne sikret, at genetableringsforanstaltningerne ikke blev inkluderet i en krypteringsproces, mens Udenrigsministeriet ikke havde sikret dette. Endelig havde Udenrigsministeriet og Banedanmark ikke gennemført systematiske tests af evnen til at genetablere systemer og data, mens Beredskabsstyrelsen delvist opfyldte tiltaget.

37. Vores opfølgning viser, at alle 4 institutioner har sikret genetableringsforanstaltninger, så de ikke inkluderes i en krypteringsproces i tilfælde af ransomwareangreb. Derudover viser opfølgningen, at det fortsat kun er Sundhedsdatastyrelsen, der har tilstrækkeligt systematiske tests af systemer og data, mens de 3 øvrige institutioner delvist opfylder tiltaget.

Både Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen har sikret, at der er blevet gennemført tests af evnen til at genetablere systemer og data. Disse tests gennemføres dog ikke systematisk efter en testplan. Udenrigsministeriet har ultimo 2020 udarbejdet en testplan, men har endnu ikke gennemført tests efter planen. Beredskabsstyrelsen har oplyst, at der vil blive udarbejdet en testplan, som forventes at være færdig primo 2021, mens Banedanmark har oplyst, at Banedanmark vil stille krav om en testplan med proaktive tests af evnen til at genetablere systemer og data i forbindelse med en ny it-driftsaftale medio 2022.

38. Rigsrevisionen vil fortsat følge Udenrigsministeriets, Banedanmarks og Beredskabsstyrelsens arbejde med det sidste reaktive tiltag.

Lone Strøm