11/2017

STATSREVISORERNE
RIGSREVISIONEN

Rigsrevisionens beretning om

beskyttelse mod ransomwareangreb

afgivet til Folketinget med Statsrevisorernes bemærkninger

1849
147.281
237
1976
114.6
22.480
908

Februar 2018

11 /
2017

Beretning om beskyttelse mod ransomwareangreb

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2018

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:
Statsrevisorerne fremsender med deres eventuelle bemærkninger Rigsrevisionens beretning til Folketinget og vedkommende minister.
Udenrigsministeren, forsvarsministeren, sundhedsministeren og transport-, bygnings- og boligministeren afgiver en redegørelse til beretningen.
Rigsrevisor afgiver et notat med bemærkninger til ministrenes redegørelser.
På baggrund af ministrenes redegørelser og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i juni 2018.
Ministrenes redegørelser, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2017, som afgives i februar 2019.

Henvendelse vedrørende
denne publikation rettes til:

Statsrevisorerne
Folketinget
Christiansborg
1240 København K
Telefon: 33 37 59 87
Fax: 33 37 59 95
E-mail: statsrevisorerne@ft.dk
Hjemmeside: www.ft.dk/statsrevisorerne

Yderligere eksemplarer kan
købes ved henvendelse til:

Rosendahls Lager og Logistik
Herstedvang 10
2620 Albertslund
Telefon: 43 22 73 00
Fax: 43 63 19 69
E-mail: distribution@rosendahls.dk
Hjemmeside: www.rosendahls.dk

ISSN 2245-3008
ISBN trykt 978-87-7434-550-3
ISBN pdf 978-87-7434-551-0

Statsrevisorernes bemærkning

BERETNING OM BESKYTTELSE MOD RANSOMWARE-ANGREB

Cyberangreb mod statslige institutioner – og særligt truslen fra såkaldte ransomware-angreb – er meget aktuel. Ransomware er skadelige programmer, der forhindrer adgang til data, bl.a. ved, at data bliver krypteret, så den ramte institution ikke kan anvende dem. Manglende tilgængelighed af data kan forhindre eller besværliggøre varetagelsen af vigtige samfundsmæssige funktioner. Fx måtte det britiske sundhedsvæsen i 2017 aflyse operationer af eller konsultationer med ca. 19.000 patienter som følge af et ransomware-angreb.

Beretningen handler om Sundhedsdatastyrelsens, Udenrigsministeriets, Banedanmarks og Beredskabsstyrelsens beskyttelse mod ransomwareangreb. Rigsrevisionen har undersøgt, om de 4 institutioner opfylder 20 almindelige tiltag, som reducerer risikoen for, at ransomware kommer ind i institutionerne via e-mails.

Statsrevisorerne finder, at Sundhedsdatastyrelsens, Udenrigsministeriets, Banedanmarks og Beredskabsstyrelsens beskyttelse mod ransomwareangreb ikke er tilfredsstillende. Hermed er der øget risiko for, at ransomware via e-mails kan forhindre adgang til institutionernes data, så de ikke kan varetage deres opgaver i kortere eller længere perioder.

Statsrevisorerne gør opmærksom på, at beskyttelse mod ransomwareangreb er en vigtig opgave for alle offentlige institutioner. Beretningen angiver en række tiltag, som alle institutioner kan iværksætte for at reducere risikoen for ransomware.

Statsrevisorerne bemærker:

- at forebyggelsen af ransomwareangreb ikke er tilstrækkelig, og at ingen af institutionerne fuldt ud har sikret, at alle deres programmer har de nyeste sikkerhedsopdateringer
- at ledelsen i Sundhedsdatastyrelsen og i Banedanmark ikke har dækkende risikovurderinger for truslen fra ransomwareangreb
- at Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen ikke har reaktive tiltag, der kan sikre, at institutionerne kan genetablere normal drift, efter de er blevet ramt af ransomwareangreb.

Statsrevisorerne finder det tilfredsstillende, at alle 4 institutioner de seneste 12 måneder har implementeret tiltag, som kan øge deres beskyttelse mod ransomwareangreb.

STATSREVISORERNE,
den 21. februar 2018

Peder Larsen
Henrik Thorup
Klaus Frandsen
Søren Gade
Henrik Sass Larsen
Villum Christensen

INDHOLDSFORTEGNELSE

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Rigsrevisionen har revideret regnskaberne efter § 2, stk. 1, nr. 1, jf. § 3 i rigsrevisorloven.

Beretningen vedrører finanslovens § 6. Udenrigsministeriet, § 12. Forsvarsministeriet, § 16. Sundheds- og Ældreministeriet og § 28. Transport-, Bygnings- og Boligministeriet.

I undersøgelsesperioden har der været følgende ministre:

Udenrigsministeriet:
Anders Samuelsen: november 2016 -

Forsvarsministeriet:
Claus Hjort Frederiksen: november til 2016 -

Sundheds- og Ældreministeriet:
Ellen Trane Nørby: november 2016 -

Transport-, Bygnings- og Boligministeriet:
Ole Birk Olesen: november 2016 -

Beretningen har i udkast været forelagt Udenrigsministeriet, Forsvarsministeriet, Sundheds- og Ældreministeriet og Transport-, Bygnings- og Boligministeriet, hvis bemærkninger er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. FORMÅL OG KONKLUSION

1. Denne beretning handler om, hvorvidt udvalgte, samfundsvigtige statslige institutioner har en tilfredsstillende beskyttelse mod ransomwareangreb.

2. Statslige institutioner er i meget høj grad truet af cyberangreb, og én af de mest aktuelle trusler kommer fra såkaldte ransomwareangreb. Ransomware er skadelige programmer, der fjerner adgangen til data. Det sker typisk ved, at data bliver krypteret, så den ramte institution ikke kan anvende dem. Hackere kræver løsepenge for at dekryptere data, så institutionen igen kan få adgang til dem. Ransomware er dermed særligt et problem for tilgængeligheden af data.

Manglende tilgængelighed af data kan akut forhindre eller besværliggøre varetagelsen af vigtige funktioner. Endvidere må institutioner, der er blevet ramt af et ransomwareangreb, typisk lukke dele af eller hele it-netværket ned for at afklare, hvor omfattende angrebet er. Endelig kan det have stor økonomisk betydning, fordi institutionerne lider et produktionstab, hvis de fx ikke kan tilgå deres it-netværk, eller hvis data, der er indsamlet og bearbejdet over lang tid, går tabt. Fx måtte det britiske sundhedsvæsen i 2017 aflyse operationer af eller konsultationer med ca. 19.000 patienter som følge af et ransomwareangreb. Derfor bør institutionerne have ledelsesmæssigt fokus på truslerne fra ransomware og etablere de nødvendige tiltag, der beskytter mod ransomwareangreb og kan reducere omfanget af skader, hvis institutionerne rammes af et angreb.

3. Undersøgelsen omfatter Sundhedsdatastyrelsen, Udenrigsministeriet, Banedanmark, og Beredskabsstyrelsen. De 4 institutioner er udvalgt, fordi de varetager samfundsvigtige opgaver inden for sundhed, udenrigsforhold, transport og beredskab, og manglende adgang til data derfor kan være kritisk. Sundhedsdatastyrelsen varetager endvidere koncern-it funktionen for hovedparten af Sundheds- og Ældreministeriets område.

4. Formålet med undersøgelsen er at vurdere, om de 4 institutioner har en tilfredsstillende beskyttelse mod ransomwareangreb, som kommer ind via e-mails. Derfor har vi undersøgt 20 almindelige tiltag, som giver en grundlæggende beskyttelse mod ransomware. Derudover gennemgår vi 5 tiltag, som institutionerne fremadrettet bør overveje, i forbindelse med at de udarbejder deres risikovurdering. På den baggrund kan institutionerne eventuelt implementere de fremadrettede tiltag. Fremadrettede tiltag er fx nye teknologier, som kan reducere antallet af falske e-mails, der kommer ind i en institution, eller som kan opdage og signalere atypiske hændelser på computere.

RANSOMWARE
Ransomware er en specifik type *malware*, der er betegnelsen for skadelig software.

RANSOMWAREANGREB
Ordet *ransomware* er en sammentrækning af det engelske ord for løsepenge *ransom* og *software*. Et ransomwareangreb fjerner typisk adgangen til data og opkræver løsepenge.

HACKER
En hacker betegner i denne beretning en person, som forsøger at inficere computere med ransomware.

Rigsrevisionen har selv taget initiativ til undersøgelsen, der bygger på 4 it-revisioner, som Rigsrevisionen har udført i perioden april-september 2017. Undersøgelsen tegner et øjebliksbillede af institutionernes beskyttelse mod ransomwareangreb. Efter afslutningen af it-revisionerne har institutionerne haft mulighed for at arbejde med at opfylde de 20 almindelige tiltag. Undersøgelsens resultater vedrører derfor institutionernes beskyttelse mod ransomwareangreb på revisionstidspunktet. Undersøgelsen giver en samlet præsentation af resultaterne for de 4 institutioner, men indeholder ikke en komparativ analyse og rangerer ikke institutionerne i forhold til hinanden.

KONKLUSION

Rigsrevisionen vurderer, at de 4 institutioner ikke har en tilfredsstillende beskyttelse mod ransomwareangreb. Undersøgelsen viser, at alle institutionerne mangler at opfylde flere almindelige tiltag, som beskytter mod ransomware. Dette gælder særligt Sundhedsdatastyrelsen og Banedanmark, der har flere væsentlige mangler. Det betyder, at der for alle institutionerne er en øget risiko for, at ransomware via e-mails kan kryptere institutionernes data, så de ikke kan varetage deres opgaver i en kortere eller længere periode. Alle institutionerne har oplyst, at de siden undersøgelsen har arbejdet med at implementere flere af tiltagene for at styrke deres beskyttelse mod ransomwareangreb.

WHITELISTING-LØSNING
Whitelisting-løsning eller application whitelisting-løsning er en systemunderstøttet liste over godkendte programmer, der må afvikles. En sådan liste vil medføre, at programmer, der ikke er på listen, ikke kan blive afviklet.

For det første er institutionernes forebyggelse af ransomwareangreb, der omfatter både ydre og indre tiltag, ikke tilstrækkelig. Særligt er det alvorligt, at ingen af institutionerne fuldt ud har sikret, at alle deres programmer har de nyeste sikkerhedsopdateringer, og at 3 af institutionerne ikke har implementeret en såkaldt whitelisting-løsning, som beskytter mod, at medarbejderne afvikler skadelige programmer. Det betyder, at der er øget risiko for, at ransomware kan komme ind i dele af eller i hele it-netværket og sprede sig.

For det andet har ledelsen i 3 af institutionerne ikke tilstrækkeligt fokus på truslen fra ransomwareangreb, og i Sundhedsdatastyrelsen og Banedanmark har ledelsen ikke haft en dækkende risikovurdering. Derved har institutionerne ikke en vurdering af den aktuelle trussel fra ransomwareangreb, hvilket svækker deres evne til at forebygge nye angreb og begrænse fremtidige skader. I Sundhedsdatastyrelsen og Banedanmark har der ikke været tilstrækkeligt ledelsesmæssigt fokus på at have en dækkende risikovurdering, hvilket betyder, at it-sikkerheden ikke er baseret på ledelsesmæssige prioriteringer.

For det tredje har 3 af institutionerne ikke i tilstrækkelig grad reaktive tiltag, der kan sikre, at institutionerne kan genetablere normal drift, efter de er blevet ramt af et ransomwareangreb. Særligt er det en væsentlig mangel, at 3 af institutionerne ikke systematisk tester, om de kan genetablere deres data og systemer efter et ransomwareangreb. Det betyder, at der er øget risiko for, at disse institutioners data går tabt i forbindelse med et ransomwareangreb, og at perioden, hvor institutionerne ikke kan varetage deres opgaver, forlænges.

Da risikobilledet ændrer sig løbende, er det vigtigt, at institutionerne overvejer at implementere nogle fremadrettede tiltag, som kan styrke deres modstandsdygtighed over for ransomwareangreb. Det drejer sig særligt om tiltag, som muliggør validering af afsendere, og som opdager og frasorterer potentielt skadelige e-mails. Alle institutionerne arbejder allerede med nogle af de mere fremadrettede tiltag, som kan øge deres beskyttelse mod ransomwareangreb.

1.2. BAGGRUND

5. Det fremgår af Center for Cybersikkerheds trusselsvurdering fra 2017, at truslen fra cyberangreb mod danske myndigheder generelt er meget høj og stigende i omfang og kompleksitet. Ifølge centret bliver stadig flere danske myndigheder, virksomheder og privatpersoner ramt af cyberangreb i form af ransomware.

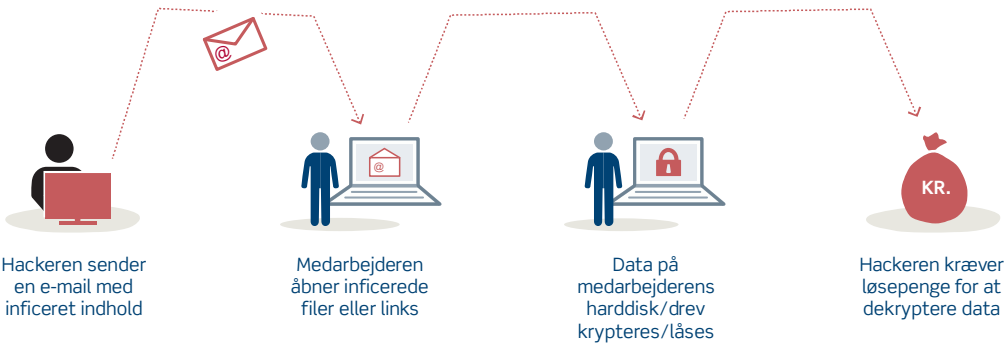
CENTER FOR CYBERSIKKERHED

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste under Forsvarsministeriet. Centret er sat i verden for at hjælpe danske myndigheder og virksomheder med at forebygge, imødegå og beskytte sig mod cyberangreb.

6. Ransomware kan ramme institutioner via flere forskellige angrebsflader. Én af de typiske angrebsflader er, at hackeren sender en e-mail med inficerede filer eller links til en medarbejder. Når medarbejderen åbner de fremsendte filer eller links, bliver medarbejderens computer inficeret med ransomware. Ransomwaren krypterer herefter sædvanligvis indholdet på medarbejderens harddisk og de drev, der er adgang til. Når krypteringen er fuldført, vil medarbejderen typisk blive mødt med en besked fra hackeren om, at data kan dekrypteres mod en løsesum. Figur 1 viser, hvordan ransomwareangreb via e-mails oftest finder sted.

FIGUR 1

ET RANSOMWAREANGREB VIA EN E-MAIL



Kilde: Rigsrevisionen på baggrund af Center for Cybersikkerheds vejledning *Reducér risikoen for ransomware* fra maj 2016.

Det fremgår af figur 1, ransomwaren skal stoppes så tidligt så muligt, før den aktiveres og gør data utilgængelige.

ENISA
ENISA er det europæiske agentur for netværks- og informationssikkerhed. ENISA har siden 2004 været et europæisk center for cybersikkerhedsekspertise og udgiver vejledninger, trusselsbilleder, anbefalinger og håndbøger. Derudover bidrager ENISA til samarbejdet mellem EU-medlemslandene via bl.a. tekniske øvelser og udveksling af information.

7. Ifølge det europæiske agentur for netværks- og informationssikkerhed, ENISA, er ransomware i løbet af 2017 blevet mere skadelig. Hvor ransomwareangrebene tidligere ofte forhindrede én medarbejders adgang til drev, er der i det seneste år set eksempler på ransomware, der fx spreder sig fra én til flere computere i netværket.

Formålet med ransomwareangreb er ifølge ENISA typisk økonomisk fortjeneste, men kan også have andre formål, fx en afledningsmanøvre i forbindelse med politisk spionage eller forretningsspionage. Ifølge ENISA er ransomwareangreb en indbringende type berigelseskriminalitet, der på globalt plan koster myndigheder, virksomheder og private milliarder af kroner og ofte påfører de ramte et væsentligt produktions- og datatab. Boks 1 viser 2 eksempler på ransomwareangreb og konsekvenserne af angrebene.

BOKS 1

EKSEMPLER PÅ RANSOMWAREANGREB

De 2 seneste globale ransomwareangreb i maj (WannaCry) og juni (NotPetya/Petya) 2017 ramte både offentlige institutioner og private virksomheder. Angrebet i maj 2017 ramte over 200.000 computere i flere end 150 lande, herunder Danmark og Storbritannien, og er ifølge EU's politienhed, Europol, uden fortilfælde. Det skal bemærkes, at der fortsat er en diskussion om, hvilke malware der var i brug i forbindelse med de 2 angreb, og hvad hackernes formål med angrebene var.

WannaCry
Det britiske sundhedsvæsen blev hårdt ramt af WannaCry, og ifølge den britiske rigsrevision måtte sundhedsvæsenet aflyse operationer af eller konsultationer med ca. 19.000 patienter. Den britiske rigsrevision pointerede, at angrebet ikke var avanceret, og det kunne have været undgået ved hjælp af almindelige tiltag, der beskytter mod ransomware. Også i USA har flere angreb haft direkte konsekvenser for patientbehandlingen på hospitaler.

NotPetya/Petya
NotPetya/Petya ramte bl.a. den danske virksomhed A.P. Møller – Mærsk. Dele af virksomheden var uden adgang til sit it-netværk i flere døgn, hvilket betød, at virksomheden var nødt til at stoppe driften i flere havneterminaler. Angrebet viste, hvordan ransomware kan sprede sig som en orm i dele af eller i hele it-netværket og dermed forårsage store skader. Derudover viste det, at ransomwareangreb, som spreder sig, i nogle tilfælde også rammer systemer, der sandsynligvis ikke var hackerens tiltænkte mål.

Kilde: Rigsrevisionen på baggrund af bl.a. en rapport fra den britiske rigsrevision samt Center for Cybersikkerheds trusselsvurderinger.

1.3. REVISIONSKRITERIER, METODE OG AFGRÆNSNING

Revisionskriterier

8. Formålet med undersøgelsen er at vurdere, om Sundhedsdatastyrelsen, Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen har en tilfredsstillende beskyttelse mod ransomwareangreb.

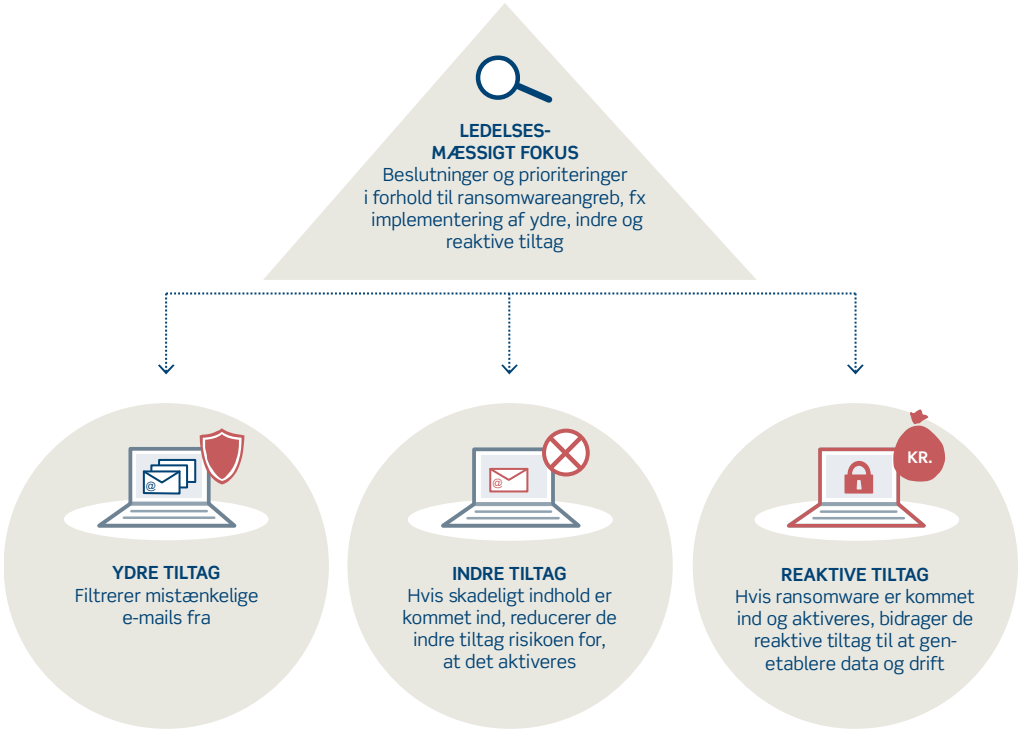
I vurderingen af, om institutionernes beskyttelse er tilfredsstillende, lægger vi til grund, at institutionerne opfylder en række almindelige tiltag, som sikrer en høj grad af beskyttelse. Vores valg af tiltag udspringer af anbefalinger i Center for Cybersikkerheds vejledninger *Reducér risikoen for ransomware* fra 2016 og *Cyberforsvar, der virker* fra 2017.

Undersøgelsens revisionskriterier tager udgangspunkt i, om institutionerne opfylder 20 almindelige tiltag og dermed reducerer risikoen for, at ransomware kommer ind i institutionerne via e-mails og forhindrer adgangen til data. Tiltagene er opdelt i 4 kategorier.

9. Figur 2 viser, hvordan hver kategori af tiltag har forskellige formål, afhængigt af hvor langt ransomwareangrebet er nået, fx om det er kommet ind i institutionen eller er blevet aktiveret.

FIGUR 2

DE 4 KATEGORIER AF TILTAG, SOM ØGER BESKYTTELSEN MOD RANSOMWAREANGREB



Kilde: Rigsrevisionen på baggrund af Center for Cybersikkerheds vejledning *Cyberforsvar, der virker* fra januar 2017.

Det fremgår af figur 2, at tiltagene er rettet mod forskellige tidspunkter i et ransomwareangreb. De 20 almindelige tiltag omfatter ledelsesmæssigt fokus og forebyggelse ved hjælp af ydre, indre og reaktive tiltag.

Det ledelsesmæssige fokus skal sikre, at institutionen har risikovurderinger, politikker og retningslinjer for it-sikkerhed, som er relevante for ransomware, men kan også omfatte andre typer risici. Ledelsen bør udstikke rammer for, hvordan ransomwareangreb skal forebygges, og hvordan skaderne begrænses. Herudover bør ledelsen forholde sig til, hvor ofte der er behov for at tage backup af data, og sikre, at institutionen følger op på angreb. Når det ledelsesmæssige fokus er tilstrækkeligt, har ledelsen taget stilling til sine forventninger til beskyttelse mod ransomwareangreb samt begrundet sine fravalg og implementeret nødvendige tiltag.

Institutionernes forebyggende tiltag består af både ydre og indre tiltag. De ydre tiltag skal forhindre, at ransomware via e-mails kommer ind i institutionerne. Når de ydre tiltag er implementeret, er der mindre risiko for, at medarbejderne kommer i kontakt med ransomware. De indre tiltag skal reducere risikoen for, at medarbejderne kan aktivere ransomware, hvis en e-mail med skadeligt indhold er kommet ind i institutionen. Når de indre tiltag er implementeret, er medarbejderne i højere grad beskyttet mod at kunne aktivere ransomware.

Endelig skal institutionernes reaktive tiltag træde i kraft, hvis ransomware er blevet aktiveret, dvs. at data fx er blevet krypteret og bliver utilgængelige. De reaktive tiltag kan begrænse skadesvirkningerne af et ransomwareangreb, fx fordi institutionerne kan genetablere deres data på baggrund af en backup. Når de reaktive tiltag er implementeret, kan institutionerne genetablere data og systemer i henhold til ledelsens forventninger.

10. Det er vigtigt at understrege, at tiltagene og de anbefalinger, de har afsæt i, ikke er statiske. Da risikobilledet ændrer sig løbende, vil anbefalingerne til god it-sikkerhedspraksis også ændre sig. Opfyldelsen af de 20 tiltag er dermed ikke ensbetydende med et tilstrækkeligt it-sikkerhedsniveau fremover.

Undersøgelsen indeholde derfor også nogle fremadrettede tiltag, der på sigt kan øge beskyttelsen mod ransomwareangreb. Institutionerne bør overveje relevansen af de fremadrettede tiltag i forbindelse med deres risikoarbejde, herunder risikovurdering, og eventuelt implementere disse tiltag. Det drejer sig om fremadrettede tiltag, der styrker den ydre og indre sikring. De fremadrettede tiltag tager udgangspunkt i ISO 27001 og en vejledning vedrørende vigtige it-sikkerhedskontroller fra det amerikanske Center for Internet Security (CIS). De fremadrettede tiltag kan ikke kompensere for manglende opfyldelse af de almindelige tiltag.

I undersøgelsen fokuserer vi på de 20 almindelige tiltag, som udspringer af Center for Cybersikkerheds anbefalinger, mens afrapporteringen af de fremadrettede tiltag fremgår af boks 2 og 3.

ISO 27001
Den internationale informationssikkerhedsstandard, som de statslige institutioner skulle følge fra januar 2014 og have færdigimplementeret primo 2016. ISO 27001 afløser den tidligere sikkerhedsstandard DS484.

CENTER FOR INTERNET SECURITY
Center for Internet Security (CIS) er en amerikansk tænketank, som opsamler og udvikler online it-sikkerhedskontroller og god praksis fra hele verden. CIS har tidligere været kendt under navnet SANS.

Metode

11. Undersøgelsen omfatter Sundhedsdatastyrelsen, Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen. Sundhedsdatastyrelsen varetager koncern-it funktionen på hele Sundheds- og Ældreministeriets område med undtagelse af Lægemiddelstyrelsen. Institutionerne er udvalgt, fordi de er samfundsvigtige institutioner, hvor datatab kan have store konsekvenser, og fordi de repræsenterer særligt vigtige sektorer inden for sundhed, udenrigsforhold, transport og beredskab. Ransomware kan som udgangspunkt ramme al data, dog har tendensen i perioden, hvor revisionen blev udført, primært været data på filservere.

Undersøgelsen er baseret på Rigsrevisionens it-revision, som er udført i perioden april-september 2017 i de 4 institutioner. Undersøgelsen tegner et øjebliksbillede af institutionernes beskyttelse mod ransomwareangreb.

12. Rigsrevisionen anser de 20 almindelige tiltag som væsentlige ud fra en it-sikkerhedsmæssig vurdering. Derudover kan institutionerne med fordel overveje at implementere de 5 fremadrettede tiltag. Undersøgelsen tager højde for, om ledelsen i institutionerne har fravalgt ét eller flere af de 20 tiltag på baggrund af en risikovurdering eller et lignende velbegrundet valg. Institutionernes implementering af de fremadrettede tiltag indgår ikke i vores vurdering af, om institutionernes beskyttelse mod ransomwareangreb er tilstrækkelig.

13. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

Afgrænsning

14. Undersøgelsen fokuserer på ransomware, der kommer ind via e-mails, da det på revisionstidspunktet var den mest anvendte metode. Ud over e-mails kan ransomware også kompromittere institutioner ved hjælp af andre angrebsflader, fx en hjemmeside. Vi har ikke undersøgt institutionernes beskyttelse mod angreb fra andre flader end e-mails. Dog kan nogle af de ydre og indre tiltag også reducere risikoen for angreb, der kommer ind via fx internettet eller usb-stik. Ligeledes kan de reaktive tiltag også anvendes i tilfælde af andre typer malware eller hændelser, hvor data og systemer er udsat. Derudover skelner undersøgelsen ikke mellem forskellige typer ransomwareangreb såsom angreb, hvor andet malware også tages i brug, fx til tyveri af data.

I undersøgelsen har vi lagt vægt på forebyggende tiltag, men også på udvalgte reaktive tiltag. Vi har imidlertid ikke undersøgt institutionernes parathed til at agere i tilfælde af et større ransomwareangreb, herunder krisehåndtering i form af fx beredskabstræning. Vi har endvidere ikke undersøgt forhold, der sikrer mod, at ransomware ligger i dvale, så backupdata gennem længere tid er blevet uhensigtsmæssigt krypteret. Undersøgelsen omfatter heller ikke den fysiske sikkerhed.

15. I bilag 1 er undersøgelsens metodiske tilgang nærmere beskrevet, herunder udvælgelsen af institutioner, revisionskriterier, dataindsamling og analyse. Bilag 2 indeholder en oversigt over resultaterne fra it-revisionen. Bilag 3 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. Beskyttelse mod ransomwareangreb

2.1. LEDELSESMÆSSIGT FOKUS

16. Vi har undersøgt, om ledelsen i institutionerne har et tilstrækkeligt fokus på truslen fra ransomware. Ledelsens beslutninger og prioriteringer i forhold til ransomwareangreb bør være afspejlet i skriftlige risikovurderinger, som vurderer de risici, der er forbundet med anvendelsen af it. Dermed bidrager tiltagene til, at ledelsen afklarer institutionens specifikke risikovillighed og sørger for, at ledelsens ønskede it-sikkerhedsniveau også implementeres i institutionen.

17. Tabel 1 viser undersøgelsens resultater af, om institutionernes ledelsesmæssige fokus på ransomware er tilstrækkeligt. Rigsrevisionen lægger til grund, at det ledelsesmæssige fokus som minimum bør omfatte 4 tiltag i forhold til ransomwareangreb.

TABEL 1

LEDELSESMÆSSIGT FOKUS

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Dækkende risikovurdering	🔴	🟢	🔴	🟢
Opdateret it-sikkerhedspolitik og -retningslinjer	🟢	🟢	🟢	🟢
Krav til backup	🟢	🟡	🟢	🟢
Opfølgning på ransomwareangreb	🟡	🟢	🟡	🟢

🔴 Ikke opfyldt
🟡 Delvist opfyldt
🟢 Opfyldt

Kilde: Rigsrevisionen.

Det fremgår af tabel 1, at 3 af institutionerne ikke opfylder alle tiltagene, mens Beredskabsstyrelsen opfylder alle tiltag. Alle institutionerne har en it-sikkerhedspolitik og -retningslinjer, der fx beskriver, hvordan medarbejderne skal agere, hvis de rammes af et ransomwareangreb. Sundhedsdatastyrelsen og Banedanmark har begge en it-sikkerhedspolitik og -retningslinjer, selv om de ikke har en dækkende risikovurdering.

18. Undersøgelsen viser, at det kun er ledelsen i Beredskabsstyrelsen, der har haft tilstrækkeligt fokus på truslen fra ransomwareangreb.

Udenrigsministeriets ledelse har fokus på alle undersøgte områder på nær risikotolerance for datatab, hvor ministeriet ikke kan dokumentere, at den valgte backupfrekvens er godkendt af ledelsen. Det betyder, at den risiko, ministeriet løber i forhold til tab af data, ikke nødvendigvis stemmer overens med ledelsens forventninger. Udenrigsministeriet har oplyst, at ministeriet planlægger at sikre, at backupfrekvenser bliver ledelsesgodkendt, og at en revideret backuppolitik forventes ledelsessanktioneret primo 2018.

TAB AF DATA
Tab af data kan være, at et helt dokument går tabt, men kan også være det tab af ændringer, der er foretaget siden sidste backup.

Banedanmarks risikovurdering indeholder kun i begrænset omfang en vurdering af de trusler og sårbarheder, der er relevante i forhold til ransomware. Endvidere indeholder risikovurderingen ikke en redegørelse for, hvilke foranstaltninger Banedanmark har eller har iværksat for at reducere risici. Desuden kan Banedanmark ikke i tilstrækkeligt omfang dokumentere, at drøftelser vedrørende opfølgninger på ransomwareangreb bidrager til ledelsens fokus på og overvejelser om it-sikkerhed. Den manglende dokumentation skyldes ifølge Banedanmark, at de ikke har været ramt af angreb, som har været alvorlige nok til at blive drøftet på ledelsesniveau.

Sundhedsdatastyrelsens risikovurdering er ikke opdateret siden 2015 og forholder sig således ikke til aktuelle trusler. Derudover har der været flere organisationsændringer i styrelsen efter udarbejdelsen af risikovurderingen, hvilket betyder, at risikovurderingen ikke tager udgangspunkt i styrelsen, som den ser ud på nuværende tidspunkt. Sundhedsdatastyrelsen har oplyst, at styrelsens opdatering af risikovurderingen bl.a. er blevet forsinket på grund af en organisationsomlægning og frasalg af vaccineproduktionen.

Sundhedsdatastyrelsen har siden 2015 været ramt af flere ransomwareangreb. Angrebene betød bl.a., at styrelsen måtte lukke flere medarbejderes computere i en periode. Undersøgelsen viser, at Sundhedsdatastyrelsen i 2016 iværksatte nogle initiativer i forhold til sikkerhedshændelser. Styrelsen har oplyst, at normal tilstand i alle tilfælde er blevet reetableret i løbet af en arbejdsdag, og at styrelsen gradvist siden 2016 har fulgt op på de pågældende sikkerhedshændelser. Undersøgelsen viser imidlertid, at Sundhedsdatastyrelsen og Sundheds- og Ældreministeriet først i 2017 iværksatte en opfølgning på erfaringerne fra de seneste års angreb. Det er Rigsrevisionens opfattelse, at Sundhedsdatastyrelsen – set i lyset af antallet af angreb – tidligere burde have iværksat en opfølgning.

RESULTATER

Undersøgelsen viser, at ledelsen i 3 af institutionerne ikke har haft tilstrækkeligt fokus på ransomware. Det er særligt alvorligt, at ledelsen i 2 af institutionerne ikke har sikret, at institutionerne har en dækkende risikovurdering, som tager udgangspunkt i institutionens data, systemer og den aktuelle risiko for ransomwareangreb. Det svækker institutionernes evne til at forebygge ransomwareangreb og begrænse skadesvirkningerne. Derudover sikrer risikovurderinger, at institutionernes håndtering af risici er baseret på ledelsens prioriteringer.

2.2. YDRE TILTAG

19. Vi har undersøgt, om institutionerne opfylder tiltag, der bidrager til at forhindre ransomware i at komme ind i institutionen. Her er der tale om de ydre tiltag, der forhindrer, at e-mails med skadeligt indhold kommer frem til medarbejderne. Dermed kan de ydre tiltag medvirke til at afværge angreb.

20. Tabel 2 viser undersøgelsens resultater af, om institutionerne i tilstrækkelig grad opfylder de ydre tiltag.

TABEL 2

YDRE TILTAG

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Brug af antispam- og antivirusløsning	●	●	●	●
Forhindre omgåelse af den centrale antispam- og antivirusløsning	●	●	●	●
Brug af 2-faktor login ved webmailløsninger	●	●	●	Ikke relevant
Forhindre brug af private e-mailløsninger	●	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

Det fremgår af tabel 2, at alle institutionerne mangler at opfylde mindst ét tiltag.

ANTISPAM- OG ANTIVIRUSLØSNING
En opdateret og central antispam- og antivirusløsning frasorterer mistænkelige e-mails, der bliver sendt til institutionen. En sådan løsning kan medvirke til at forhindre e-mails med ransomware i at lande i medarbejderes indbakke.

21. Undersøgelsen viser, at alle 4 institutioner har en central antispam- og antivirusløsning, der frasorterer mistænkelige e-mails, som sendes til institutionerne. Alle institutionerne har desuden sikret, at e-mails ikke kan omgå den centrale antispam- og antivirusløsning for indgående e-mails til institutionerne. Det betyder, at institutionerne har gjort det sværere for hackere at sende skadeligt indhold til institutionerne via e-mails fra eksterne e-mailkonti.

22. Undersøgelsen viser desuden, at ingen af institutionerne, som har en webmailløsning, gør brug af 2-faktor login.

Uden 2-faktor login er det nemmere for en hacker at få adgang til institutionernes interne e-mailløsninger, hvis hackeren allerede har fået adgang til én eller flere medarbejderes password. Det betyder, at e-mails sendt på denne måde kan omgå de andre ydre tiltag såsom centrale antivirusløsninger. Det skyldes, at disse tiltag ofte er designet til at fange skadelige e-mails fra eksterne e-mailkonti. Dermed er der en øget risiko for, at hackere kan anvende institutionernes mailsystem og sende e-mails, som fremstår troværdige, men som kan være inficerede med ransomware.

Banedanmark har oplyst, at 2-faktor login er ved at blive implementeret på deres webmailløsning. Udenrigsministeriet har oplyst, at 2-faktor login på webmailløsningen blev implementeret pr. 1. januar 2018.

Beredskabsstyrelsen har ikke en webmailløsning, og derfor er tiltaget ikke relevant for styrelsen. Beredskabsstyrelsen har oplyst, at styrelsen har fravalgt webmailløsningen, bl.a. fordi den medfører øget sårbarhed over for bl.a. ransomwareangreb. Sundhedsdatastyrelsen har oplyst, at styrelsen arbejder på at udfase webmailløsningen medio 2018.

23. Endelig viser undersøgelsen, at ingen af institutionerne har begrænset medarbejderenes adgang til deres private e-mailløsninger. Da private e-mailløsninger ikke er omfattet af institutionernes tiltag, der skal frasortere mistænkelige e-mails, kan en medarbejder via sin private e-mail risikere at hente skadeligt indhold såsom ransomware.

Risikoen ved at anvende private e-mailløsninger er dog reduceret hos Udenrigsministeriet, da ministeriet har implementeret et andet tiltag, der beskytter medarbejdernes adgang til internettet. Vores gennemgang viser, at medarbejderne i Beredskabsstyrelsen kunne tilgå eksterne e-mailløsninger, da den foranstaltning, der skulle forhindre adgangen, var defekt. Styrelsen har efterfølgende oplyst, at medarbejderne ikke længere kan benytte eksterne e-mailløsninger.

2-FAKTOR LOGIN VED WEBMAILLØSNINGER

2-faktor login ved webmailløsninger betyder, at medarbejderne skal validere deres identitet ved hjælp af 2 eller flere faktorer, når de logger på deres arbejdsmail udefra. Det er en kombination af noget, som brugeren ved (fx password), og noget, som brugeren har eller får (fx usb-nøgle eller en kode sendt til mobiltelefonen).

24. Ud over de 3 almindelige ydre tiltag, som kan forhindre e-mails med ransomware i at komme ind i institutionen, er der 3 fremadrettede ydre tiltag, jf. boks 2.

BOKS 2

FREMADRETTEDE YDRE TILTAG

Alle 4 institutioner har iværksat fremadrettede tiltag for at styrke den ydre sikkerhed. Tabellen nedenfor viser, hvor langt institutionerne er nået.

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Sikring mod, at hackere kan anvende institutionens domænenavne som afsenderdomænenavn, når de sender indgående e-mails	✓	(✓)	✓	(✓)
Kontrol af indgående e-mails i forhold til afsender-identitet 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	(✓)	(✓)	÷	(✓)

÷ Ikke opfyldt
(✓) Delvist opfyldt
✓ Opfyldt

Det fremgår af tabellen, at alle institutionerne har haft fokus på at sikre, at hackere ikke kan anvende institutionens mailadresser som afsender på e-mails. Hvis hackere kan bruge interne domænenavne, fremstår e-mailene som interne, hvilket øger risikoen for, at modtageren har tillid til e-mailen og derfor klikker på links eller åbner vedhæftede filer, som kan være inficerede. Det betyder, at institutionerne har reduceret risikoen for, at medarbejderne modtager e-mails, der ser ud som om, de kommer fra en intern e-mailadresse, men som er sendt af en hacker og kan indeholde ransomware.

Det fremgår desuden af tabellen, at Sundhedsdatastyrelsen sikrer validering af indkomne e-mails, da styrelsen kontrollerer indgående e-mails på baggrund af SPF-, DMARC- og DKIM-teknologierne. De 3 øvrige institutioner har ikke implementeret validering af e-mails i samme omfang eller har slet ikke implementeret tiltaget. Det betyder, at det er sværere for disse 3 institutioner at validere afsenderen på en e-mail og at frasortere e-mails med forfalsket afsenderidentitet, hvor risikoen for skadeligt indhold, fx ransomware, er større. Udenrigsministeriet har dog implementeret andre tiltag, som ministeriet vurderer giver en høj grad af beskyttelse.

Endelig fremgår det af tabellen, at 3 af institutionerne har implementeret et tiltag, der i nogen grad begrænser muligheden for, at institutionerne står som afsender på en e-mail med skadeligt indhold og derved bliver misbrugt i et ransomwareangreb mod en anden institution. Institutionerne har valgt at implementere SPF-teknologien. Det betyder, at det bliver sværere for hackere at bruge institutionerne som dække, og der er dermed tale om en slags nabohjælp. Institutionerne har dog ikke en fuldstændig sikring. Fx er tiltagene ikke implementeret på alle de domænenavne, som institutionerne har brugsret over. Derudover er der øget risiko for, at institutionernes identitet fortsat kan blive misbrugt, når kun SPF-teknologien anvendes, fordi denne sikringforanstaltning let kan omgås, hvis ikke den kombineres med DMARC-teknologien.

Note: SPF-, DMARC- og DKIM- teknologierne er teknologier, som sikrer organisationer mod misbrug af domænet til svindel med e-mailadresser og dermed begrænser hackeres mulighed for at udgive sig for at være afsendere fra organisationer – såkaldt e-mail-spoofing. Center for Cybersikkerheds vejledning *Reducér risikoen for falske mails* fra november 2017 anbefaler også disse teknologier, da de beskytter mod falske e-mails.

Kilde: Rigsrevisionen.

RESULTATER

Undersøgelsen viser, at institutionernes almindelige ydre tiltag ikke er tilstrækkelige. Institutionerne reducerer ikke i tilstrækkelig grad risikoen for, at ransomware kommer ind i institutionerne, fx via uautoriseret adgang til institutionernes webmailløsning eller via adgang til private e-mailløsninger. Det øger risikoen for, at e-mails med skadeligt indhold, fx ransomware, kommer ind i institutionerne.

2.3. INDRE TILTAG

25. Vi har undersøgt, om institutionerne i tilstrækkelig grad opfylder tiltag, der kan forhindre, at ransomware bliver aktiveret, hvis den alligevel kommer ind i institutionen. Her er der tale om de tilfælde, hvor ransomware er kommet ind gennem institutionens ydre sikringsbarriere, og hvor en medarbejder derfor alligevel modtager en e-mail med skadeligt indhold og aktiverer indholdet, fx ved at klikke på et link. Det er muligt at reducere risikoen for, at medarbejderen aktiverer det skadelige indhold, hvis institutionen har etableret indre tiltag, som forhindrer og begrænser ransomware i at kunne aktiveres og spredes. Det gælder dels tekniske tiltag, dels tiltag vedrørende medarbejdernes adfærd.

Tekniske tiltag

26. Tabel 3 viser undersøgelsens resultater af, om institutionerne i tilstrækkelig grad opfylder de indre tiltag af teknisk karakter.

TABEL 3

INDRE TEKNISKE TILTAG

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Lokaladministratorer har et arbejdsbetinget behov	●	●	●	●
Opdatering af styresystemer	●	●	●	●
Opdatering af programmer, som er tredjepartsprodukter	●	●	●	●
Kun godkendte programmer kan afvikles (whitelisting-løsning)	●	●	●	●
Ingen brug af privilegerede rettigheder, når der læses e-mails	●	●	●	●
Sikring mod ubeskyttet adgang til internettet, og at medarbejderne ikke kan downloade potentielt skadelige filer, når de læser e-mails (fx i form af en sandboxing-løsning)	●	●	●	●
Rettighedstildeling på fildrevniveau i overensstemmelse med egne retningslinjer	●	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

Det fremgår af tabel 3, at alle institutionerne mangler at opfylde ét eller flere tiltag.

27. Undersøgelsen viser, at 2 af institutionerne har begrænset brugen af lokaladministratorer, så det kun er medarbejdere, der har et arbejdsbetinget behov, som har disse rettigheder. I Udenrigsministeriet og Beredskabsstyrelsen er det kun medarbejdere, som skal supportere it-arbejdspladserne, der bliver tildelt lokaladministratorrettigheder. Banedanmark og Sundhedsdatastyrelsen har væsentlige mangler, fordi der er medarbejdere ud over it-supporterne, som har adgang til computere med lokaladministratorrettigheder. Med lokaladministratorrettigheder er det muligt at deaktivere tiltag på den lokale computer. Derfor udgør det en øget risiko, hvis antallet af medarbejdere med disse rettigheder er stort, fordi der dermed er flere "indgange" for hackere. Det betyder, at der er øget risiko for, at hackere kan kompromittere institutionens computere og afvikle skadelige programmer, som potentielt kan sprede sig og skade dele af eller hele institutionens netværk.

ARBEJDSBETINGET BEHOV
Et arbejdsbetinget behov er, når en medarbejders kernefunktion omfatter afhjælpning af it-problemer, fx medarbejdere, som supporterer andre med it-driften. Dermed kan det ikke betegnes som et arbejdsbetinget behov, hvis institutionerne anvender software, der kræver lokaladministratorrettigheder.

AFVIKLING
En afvikling kendetegner den proces, hvor et program åbnes og kører på computeren.

Sundhedsdatastyrelsen og Banedanmark har oplyst, at de fortsat har fokus på at nedbringe antallet af medarbejdere med lokaladministratorrettigheder. På Sundheds- og Ældreministeriets område har Sundhedsdatastyrelsen det seneste år reduceret antallet af medarbejdere med lokaladministratorrettigheder fra ca. 1.500 til ca. 200. Både Sundhedsdatastyrelsen og Banedanmark har endvidere oplyst, at behovet for lokaladministratorrettigheder bl.a. skyldes, at flere typer software, som institutionerne benytter, kræver, at medarbejderen har disse rettigheder.

Rigsrevisionen vurderer, at Sundhedsdatastyrelsen og Banedanmark dermed har en øget risiko for at blive udsat for ransomware. Begge institutioner bør derfor overveje yderligere tiltag for at tage højde for, at de i nogle tilfælde er nødsaget til at give mange medarbejdere lokaladministratorrettigheder på grund af specifikationerne i de typer software, som institutionerne benytter.

28. Undersøgelsen viser desuden, at alle institutionerne har sikret opdateringer af deres styresystemer. Det betyder, at det er sværere for hackere at udnytte kendte svagheder i styresystemerne.

STYRESYSTEM
Et styresystem er software, som styrer udvekslingen af data mellem fx computerens dele. Det kan anskues som computerens nervesystem, der forbinder mange elementer.

29. Undersøgelsen viser endvidere, at ingen af institutionerne i tilstrækkelig grad har sikret, at der er installeret sikkerhedsopdateringer til relevante og almindeligt anvendte programmer, som er tredjepartsprodukter. Det betyder, at kendte svagheder i programmerne kan udnyttes i et ransomwareangreb.

TREDJEPARTS-PRODUKTER
Tredjepartsprodukter er typisk programmer udviklet af virksomheder, som leverer en service, fx tekstbehandling.

Udenrigsministeriet og Beredskabsstyrelsen har dog delvist sikret, at relevante programmer sikkerhedsopdateres, fx ved at have en fastlagt opdateringsproces for udvalgte programmer, men nogle få programmer havde ikke de seneste sikkerhedsopdateringer. Udenrigsministeriet har oplyst, at ministeriet har iværksat procedurer, der forventes at optimere opdateringen af programmer mest muligt under hensyntagen til stabil drift.

Sundhedsdatastyrelsen og Banedanmark har ikke en systematisk tilgang til sikkerhedsopdateringer, som omfatter alle relevante programmer. Vores gennemgang viser, at der i begge institutioner var flere relevante programmer, som ikke var blevet sikkerhedsopdateret i flere år. Nogle af de programmer, der blev undersøgt, har mange kendte sårbarheder. Det øger risikoen for, at ransomwareangreb kan ramme institutionerne. Sundhedsdatastyrelsen har oplyst, at styrelsen har en central løsning til systematisk sikkerhedsopdatering af programmer, men at styrelsen har lokalt installerede programmer, der ikke er blevet opdateret.

WHITELISTING-LØSNING
En whitelisting-løsning er en systemunderstøttet liste over godkendte programmer, der må afvikles. En sådan liste vil medføre, at programmer, som ikke er på listen, ikke kan blive afviklet. Løsningen kaldes en application whitelisting-løsning.

BLACKLISTING-LØSNING
En blacklisting-løsning er en systemunderstøttet liste over programmer, der ikke må afvikles. En sådan liste vil medføre, at alle programmer, som er på listen, ikke kan blive afviklet.

PRIVILEGEREDE RETTIGHEDER
Privilegerede rettigheder giver medarbejderen udvidet adgang til og kontrol med institutionens it-systemer og data. Hvis medarbejdere med privilegerede rettigheder kan tilgå e-mails, øger det risikoen for at blive ramt af ransomwareangreb.

SANDBOXING-LØSNINGER
Sandboxing-løsninger øger beskyttelsen mod både kendte og ukendte skadelige filer, og hjemmesider bliver undersøgt og bremset, inden skaden sker. Sandboxing er en virksom beskyttelse, da denne teknologi kontrollerer, om filer og andet indhold fra hjemmesider er skadelige, før brugeren tilgår indholdet. Sandboxing modvirker derfor ransomware, som institutionens medarbejdere kommer i berøring med via internettet, fx via private e-mail-løsninger.

30. Undersøgelsen viser også, at det kun er Udenrigsministeriet, der har etableret en whitelisting-løsning og dermed sikrer, at det kun er godkendte programmer, der kan afvikles. Whitelisting-løsninger beskytter mod ukendt software, herunder skadeligt software.

De øvrige institutioner har ikke implementeret en sådan løsning, men har alle implementeret antivirusløsninger, hvilket er en blacklisting-løsning, som i mindre grad kompenserer for manglen. Antivirusløsninger forhindrer dog kun kendt skadelig software i at blive afviklet. Da ransomware typisk ikke er kendt, er der i institutionerne uden en whitelisting-løsning øget risiko for, at ukendt skadelig software afvikles, herunder ransomware. Sundhedsdatastyrelsen har oplyst, at styrelsen forventer at implementere en whitelisting-løsning medio 2018.

31. Undersøgelsen viser derudover, at det kun er Udenrigsministeriet, der har sikret, at medarbejdere med privilegerede rettigheder ikke kan læse e-mails, når de er logget på med disse rettigheder. Sundhedsdatastyrelsen har dels retningslinjer, dels nogle foranstaltninger, der i nogen grad begrænser medarbejdere med privilegerede rettigheder mulighed for at tilgå internettet, men denne foranstaltning kan let omgås af medarbejdere med privilegerede rettigheder og er ikke fuldt ud dækkende. Beredskabsstyrelsen har foranstaltninger, der delvist sikrer dette, fordi styrelsen har retningslinjer, hvoraf det fremgår, at medarbejdere med privilegerede rettigheder ikke må tilgå internettet og læse e-mails, når de arbejder med disse rettigheder. Banedanmark har ingen foranstaltninger, der forhindrer, at medarbejdere med privilegerede rettigheder kan læse e-mails, ligesom Banedanmark heller ikke har fastsat retningslinjer for dette område.

Det betyder, at der i Sundhedsdatastyrelsen og Beredskabsstyrelsen og navnligt i Banedanmark er en øget risiko for, at medarbejdere med privilegerede rettigheder læser e-mails, når de er logget på med disse privilegerede rettigheder, og at ransomware dermed vil kunne sprede sig og kryptere data i dele af eller i hele it-netværket.

32. Undersøgelsen viser videre, at det kun er Udenrigsministeriet, der har beskyttet medarbejdernes adgang til internettet og begrænset deres mulighed for at downloade filer ved hjælp af en såkaldt sandboxing-løsning.

De øvrige institutioner har alle løsninger, der udelukkende blokerer for allerede kendte skadelige hjemmesider og filtyper. Da ransomware typisk vil være ukendt software, er der derfor en øget risiko for, at institutionerne kan blive ramt, end hvis de havde en sandboxing-løsning.

33. Endelig viser undersøgelsen, at alle institutionerne har retningslinjer for, hvilke medarbejdere der har adgang til institutionens forskellige fildrev, og at disse retningslinjer også følges ved tildelingen af rettigheder til fildrev. Det betyder, at de beslutninger, der er taget i forhold til tildeling af rettigheder til fildrev, som udgangspunkt også bliver efterlevet.

Adfærdsrelaterede tiltag

34. Tabel 4 viser undersøgelsens resultater af, om institutionerne opfylder de indre tiltag relateret til medarbejderadfærd.

TABEL 4

INDRE ADFÆRDSRELATEREDE TILTAG

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Gennemførelse af awareness-aktiviteter	●	●	●	●
Opfølgning på awareness-aktiviteter	●	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

Det fremgår af tabel 4, at ingen af institutionerne har opfyldt begge tiltag.

35. Undersøgelsen viser, at alle institutionerne i løbet af de seneste 12 måneder har gennemført aktiviteter med det formål at øge kendskabet til cybertrusler, herunder ransomware, blandt deres medarbejdere. Aktiviteterne har typisk været i form af oplysningskampagner, hvor institutionerne via bl.a. møder og informationsvideoer orienterer medarbejderne. Fx har Udenrigsministeriet etableret et obligatorisk it-kursus for nye medarbejdere, der bl.a. også omfatter sikker brug af it.

Aktiviteterne øger medarbejdernes bevidsthed om truslen fra hackere og øger deres kendskab til fornuftige forholdsregler, fx ikke at klikke på links eller åbne vedhæftede filer i e-mails med ukendt afsender. Det betyder, at medarbejderne som udgangspunkt er oplyst om forebyggelse, identifikation og håndtering af et ransomwareangreb. I sammenhæng med de tekniske tiltag medvirker dette til at reducere risikoen for ransomwareangreb.

36. Undersøgelsen viser dog også, at 3 af institutionerne ikke har fulgt op på de aktiviteter, de har sat i gang. Det betyder, at institutionerne ikke har tilstrækkelig viden om, hvordan aktiviteterne har virket, og hvor og hvordan der fortsat skal sættes ind for at oplyse og vejlede medarbejderne. Hermed er der en risiko for, at institutionerne ikke bruger de mest virksomme aktiviteter i forhold til at øge kendskabet blandt medarbejderne.

Sundhedsdatastyrelsen har udarbejdet en brugerevaluering med henblik på at undersøge, i hvilken grad medarbejderne fandt, at de havde fået ny viden på baggrund af de afholdte aktiviteter. Styrelsen har dog ikke gennemført egentlige opfølgninger af effekten af sine awarenes-aktiviteter.

Udenrigsministeriet og Beredskabsstyrelsen har oplyst, at de vil undersøge effekten af deres awarenes-aktiviteter, herunder hvilke der har størst effekt. Banedanmark har oplyst, at de har købt et værktøj, som bl.a. også vil understøtte awarenes-aktiviteter og opfølgning på disse.

37. Ud over de 9 indre tiltag, som er gennemgået ovenfor, er der 2 indre tiltag, som fremadrettet kan bruges til at begrænse skadesvirkningerne af et ransomwareangreb, som er blevet aktiveret, jf. boks 3.

BOKS 3

FREMADRETTEDE INDRE TILTAG

2 af institutionerne har iværksat fremadrettede indre tiltag for at styrke deres evne til at opdage et ransomwareangreb, hvis ransomware er blevet aktiveret. Tabellen nedenfor viser de 2 anbefalede tiltag.

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Programmer med atypiske adfærdsmønstre opdages	÷	÷	✓	✓
Programmer med atypiske adfærdsmønstre stoppes eller begrænses	÷	÷	(✓)	÷

÷ Ikke opfyldt
(✓) Delvist opfyldt
✓ Opfyldt

Det fremgår af tabellen, at Banedanmark og Beredskabsstyrelsen begge har tiltag, der hjælper institutionerne til at opdage og alarmere, hvis der optræder atypiske adfærdsmønstre. Disse tiltag er hovedsageligt baseret på logning. Undersøgelsen viser, at de 2 institutioner har implementeret SIEM-løsninger, der sender alarmmails til udvalgte nøglemedarbejdere. Alarmmails sendes fx ud, hvis et større antal filer pludselig ændres, eller hvis der sker kommunikation med eksterne IP-adresser, som er kendt for at blive anvendt til ransomware. Udenrigsministeriet og Sundhedsdatastyrelsen har ikke lignende tiltag, der opdager og alarmerer, hvis der er atypisk adfærd. Begge institutioner har oplyst, at de forventer at iværksætte tiltag, der på sigt vil kunne give denne beskyttelse. Sundhedsdatastyrelsen har oplyst, at styrelsen ved udgangen af 2017 har implementeret en SIEM-løsning, som styrelsen på sigt forventer kan bruges til at opsætte alarmmails.

Desuden fremgår det af tabellen, at Banedanmark delvist opfylder et tiltag, der kan stoppe eller begrænse atypiske adfærdsmønstre, når de opdages. Det kræver, at institutionen har implementeret et tiltag, der kan opdage sådanne adfærdsmønstre. Banedanmark har implementeret en funktionalitet rettet mod ransomware, som kan stoppe atypiske adfærdsmønstre. Undersøgelsen viser dog, at det i et vist omfang er muligt at omgå dette, da Banedanmark siden implementeringen har været ramt af ransomware. De øvrige 3 institutioner har ikke systemer, der på baggrund af overvågning af logs eller på anden måde automatisk stopper eller begrænser ransomware i at sprede sig. Udenrigsministeriet har oplyst, at ministeriet forventer, at et sådant tiltag bliver implementeret primo 2018, og at ministeriet også forventer at implementere yderligere tiltag. Beredskabsstyrelsen har oplyst, at styrelsen vil overveje dette tiltag i sin fremtidige sårbarhedsvurdering. Sundhedsdatastyrelsen har oplyst, at styrelsen forventer at implementere dette tiltag primo 2018.

Note: Logning øger chancen for at kunne undersøge et angreb til bunds. Alle handlinger på institutionens systemer genererer et digitalt fingeraftryk, som kan opsamles i en log. Logning af konti med privilegerede rettigheder kan fx vise, om personer har logget sig på it-systemer, og hvad de har brugt rettighederne til.

SIEM står for Security Information and Event Management. SIEM-løsninger betegner teknologier, der i realtid analyserer sikkerhedshændelser fra netværksenheder, programmer mfl.

Kilde: Rigsrevisionen.

RESULTATER

Undersøgelsen viser, at institutionernes indre tiltag ikke er tilstrækkelige, fordi ingen af institutionerne fuldt ud opfylder de almindelige tekniske tiltag eller tiltagene relateret til medarbejderadfærd.

Blandt de tekniske tiltag er der flere væsentlige mangler. Særligt væsentligt er det, at Sundhedsdatastyrelsen og Banedanmark har medarbejdere, som har lokaladministratorrettigheder, uden at de har et arbejdsbetinget behov. Derudover er det væsentligt, at alle institutionerne mangler at implementere sikkerhedsopdateringer af tredjepartsprodukter. Endelig er det væsentligt, at kun Udenrigsministeriet har implementeret en whitelisting-løsning, mens de øvrige institutioner ikke har en sådan løsning. Disse mangler betyder, at ransomware, som er kommet igennem den ydre sikring, nemmere kan anvende kendte sårbarheder og derved sprede sig i institutionernes netværk.

Blandt tiltagene relateret til medarbejderadfærd har alle institutionerne gennemført awareness-aktiviteter, men det er kun Sundhedsdatastyrelsen, som delvist har fulgt op på udbyttet heraf. Det betyder, at institutionerne ikke har et overblik over, hvilke aktiviteter der virker bedst, og hvor nye aktiviteter bør sættes ind.

2.4. REAKTIVE TILTAG

38. Vi har undersøgt, om institutionerne opfylder en række reaktive tiltag, så de kan genetablere normal drift efter et ransomwareangreb. Her er der tale om en situation, hvor det ikke har været muligt at stoppe et angreb fra at kryptere data og eventuelt systemer i institutionerne. I en sådan situation kan reaktive tiltag sikre, at institutionerne kan genetablere data, så medarbejderne kan tilgå de data og systemer, de skal bruge for at sikre driften og opgavevaretagelsen i institutionerne. Dette medvirker også til, at de økonomiske omkostninger ved et ransomwareangreb kan nedbringes.

39. Tabel 5 viser undersøgelsens resultater af, om institutionerne opfylder de reaktive tiltag.

TABEL 5

REAKTIVE TILTAG

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
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	●	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

Det fremgår af tabel 5, at 3 af institutionerne mangler at opfylde mindst ét tiltag, mens Sundhedsdatastyrelsen opfylder alle 3 reaktive tiltag.

40. Undersøgelsen viser, at alle institutionerne har tiltag, der sikrer, at de kan genetablere data. Det betyder, at institutionerne som udgangspunkt kan genetablere data, som er blevet krypteret, fordi der er en backup af disse data.

41. Undersøgelsen viser også, at 3 af institutionerne har sikret, at de backupsystemer, de bruger, ikke kan blive ramt af et eventuelt ransomwareangreb. Det betyder, at institutionerne har reduceret risikoen for, at backuppen bliver inficeret og krypteret i forbindelse med angrebet.

I Udenrigsministeriet er backuppen dog sårbar, fordi den ikke er tilstrækkeligt adskilt fra det almindelige produktionsmiljø. Hermed er der en risiko for, at et ransomwareangreb på dele af ministeriets brugermiljø også vil kunne sprede sig til backuppen. Udenrigsministeriet har oplyst, at ministeriet nu har implementeret en ny løsning, hvor backuppen er isoleret fra produktionsmiljøet.

PRODUKTIONSMILJØ
Et produktionsmiljø er det it-mæssige arbejdsmiljø, som institutionens daglige arbejde udføres i, hvilket bl.a. er de computere og systemer, som medarbejderne arbejder ved eller med.

42. Endelig viser undersøgelsen, at det kun er Sundhedsdatastyrelsen, der sikrer systematiske tests af, om styrelsens systemer og data kan genetableres fra backuppen. Det betyder, at styrelsen har en varieret testplan og løbende tester, om styrelsen kan genetablere data på baggrund af den valgte backupløsning. En sådan test er med til at sikre, at Sundhedsdatastyrelsen kan genetablere normal drift, efter et ransomwareangreb har krypteret styrelsens data.

Beredskabsstyrelsen har en testplan og afprøver hvert kvartal, om data kan genetableres. Testplanen omfatter dog efter Rigsrevisionens opfattelse ikke en tilstrækkelig variation af scenarier. I henhold til Beredskabsstyrelsens testplan har styrelsen de seneste 12 måneder kun foretaget tests på baggrund af virkelige hændelser, dvs. når styrelsen har haft brug for at genetablere data. Det betyder, at styrelsen risikerer ikke at kunne genetablere data i alle de forventede scenarier.

Udenrigsministeriet og Banedanmark har ikke en testplan og tester ikke systematisk, om de kan genetablere data på baggrund af deres backup. De efterprøver kun deres backup i forbindelse med virkelige hændelser, hvor de har et reelt behov for at genetablere data. Det betyder, at der ikke er tilstrækkelig sikkerhed for, at institutionernes backupløsning kan genetablere data, hvis de rammes af et ransomwareangreb. Udenrigsministeriet har oplyst, at ministeriet primo 2018 vil afdække, hvilke procedurer for systematiske tests ministeriet har behov for.

RESULTATER

Undersøgelsen viser, at 3 af institutionerne ikke har tilstrækkelige reaktive tiltag, fordi de ikke systematisk tester, om deres data kan genetableres på baggrund af deres backup. Det betyder, at institutionerne ikke har det fulde overblik over deres evne til at genetablere data. Derudover mangler én af institutionerne at isolere sine backupdata tilstrækkeligt for at undgå, at ransomware også kan ramme backuppen, hvilket øger risikoen for at miste data i forbindelse med et ransomwareangreb.

Rigsrevisionen, den 14. februar 2018

Lone Strøm

/Mads Nyholm Jacobsen

BILAG 1. METODISK TILGANG

Formålet med undersøgelsen er at vurdere, om udvalgte institutioner har en tilfredsstillende beskyttelse mod ransomwareangreb. Derfor har vi undersøgt følgende:

- Har institutionens ledelse tilstrækkeligt fokus på ransomware?
- Har institutionen tilstrækkelige ydre tiltag?
- Har institutionen tilstrækkelige indre tiltag?
- Har institutionen tilstrækkelige reaktive tiltag?

Udvælgelse af institutioner

Med udgangspunkt i alle statslige institutioner udvalgte vi en række institutioner, der kendetegnes ved at have ansvaret for landsdækkende data for hele befolkningen, som enten er persondata eller følsomme data. Herudover har vi taget højde for Center for Cybersikkerheds vejledning *Reducér risikoen for ransomware* fra maj 2016, der peger på sektorer, som er særligt udsatte, herunder sundhed, udenrigsforhold, transport og beredskab. Endelig har vi fravalgt nogle statslige institutioner, bl.a. af hensyn til andre igangværende revisioner på deres områder.

Herefter blev der holdt 6 sondringsmøder med Rigspolitiet, Sundhedsdatastyrelsen, Banedanmark, Energinet.dk, Udenrigsministeriet og Beredskabsstyrelsen, som ledte til udvælgelsen af 4 institutioner: Sundhedsdatastyrelsen, Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen.

Institutionerne er udvalgt, fordi det er vores vurdering, at det er vigtige institutioner, hvor betydningen af manglende datatilgængelighed eller datatab kan være kritisk. De 4 institutioner repræsenterer hermed forskellige samfundsvigtige sektorer inden for sundhed, udenrigsforhold, transport og beredskab.

Undersøgelsen præsenterer resultaterne for de 4 institutioner samlet, men indeholder ikke en komparativ analyse og rangerer ikke institutionerne i forhold til hinanden.

Revisionskriterier

Virksomheder og myndigheder kan ikke beskytte sig fuldstændigt mod hackerangreb (herunder ransomware), men Center for Cybersikkerhed har bl.a. i samarbejde med Digitaliseringsstyrelsen udarbejdet vejledninger med tiltag, som giver en ganske høj grad af beskyttelse. Det gælder vejledningen *Cyberforsvar, der virker* fra 2017, som blev udarbejdet i tilknytning til Rigsrevisionens beretning om hackerangreb. Herudover har Center for Cybersikkerhed i maj 2016 udarbejdet en vejledning om, hvordan man reducerer risikoen for ransomware. Størstedelen af undersøgelsens revisionskriterier lægger sig op ad disse vejledninger, mens de øvrige revisionskriterier er et udtryk for god praksis. Disse revisionskriterier er udmøntet i 20 almindelige tiltag.

Herudover er der et mindre antal revisionskriterier, der er udmøntet i 5 fremadrettede tiltag, som vi vurderer, at institutionerne bør overveje at etablere. Da disse tiltag dermed har en mere anbefalende og fremadrettet karakter, vil de ikke blive vurderet på samme måde som de øvrige tiltag, men de er medtaget, fordi det er vores vurdering, at det er virksomme tiltag i beskyttelsen mod ransomwareangreb.

Vi har drøftet tiltagene med Center for Cybersikkerhed og et privat konsulentfirma, der leverer og supporterer it-sikkerhedsløsninger hos både private og offentlige virksomheder. Center for Cybersikkerhed og konsulentfirmaet har overordnet erklæret sig enige i vores revisionskriterier og har samtidig bidraget til at kvalificere de enkelte kriterier.

Afgrænsning

Rigsrevisionen understreger, at revisionskriterierne og de anbefalinger, de har afsæt i, ikke er statiske. Da risikobilledet ændrer sig løbende, vil anbefalingerne til god praksis også ændre sig. Opfyldelsen af revisionskriterierne er dermed ikke ensbetydende med et tilstrækkeligt it-sikkerhedsniveau fremover. De undersøgte tiltag er væsentlige og effektive i beskyttelsen mod ransomwareangreb, men er ikke udtømmende.

Vi har i denne undersøgelse fokuseret på ransomware, der kommer ind via e-mails, da det på revisionstidspunktet var den mest anvendte metode. Vi har særligt set på forebyggende tiltag, men også på udvalgte tiltag, som institutionerne sætter i værk, hvis ransomware er kommet ind i institutionerne, fx backup af data. Vi har imidlertid ikke undersøgt institutionernes parathed til at agere i tilfælde af et større ransomwareangreb, herunder om virksomhederne træner deres beredskab.

Vi har desuden ikke undersøgt forhold, der sikrer mod, at ransomware ligger i dvale, så backupdata gennem længere tid er blevet uhensigtsmæssigt krypteret. Vi har heller ikke undersøgt den fysiske sikkerhed i forhold til at afværge, at skadeligt indhold kommer ind og inficerer institutionernes it-systemer.

Ransomware kan som udgangspunkt ramme al data, dog har tendensen i perioden, hvor revisionen blev udført, primært været data på filservere. For alle 4 institutioner gælder det som hovedregel, at data både findes i databaser og på fildrev. De data, som ligger i databaser, kan dermed ikke nødvendigvis rammes af de aktuelle typer ransomwareangreb. Dog kan ransomwareangreb ikke desto mindre forhindre adgangen til de pågældende data, da dele af eller hele institutionens it-netværk i en periode kan blive utilgængeligt. Derfor vil medarbejderne ikke kunne anvende data – heller ikke data, som ligger i databaser. Det betyder, at omkostningerne ved et ransomwareangreb fortsat kan være høje, selv om vigtige data ikke er blevet krypteret. Derudover skal det understreges, at ransomware er i udvikling, og at ransomware og lignende malware derfor muligvis også kan ramme databaser i fremtiden.

Dataindsamling

Undersøgelsen er baseret på Rigsrevisionens it-revision, som er udført i perioden april-september 2017 i de 4 institutioner. Der foreligger på den baggrund it-revisionsrapporter og underliggende substansrevision.

It-revisionen bestod af revisionsbesøg hos hver institution og opfølgende møder. De indsamlede data omfatter dataudtræk, skærmbilleder og analyser af relevant, skriftlig materiale fra de 4 institutioner.

For at sikre ensartethed på tværs af institutionerne har vi ved it-revisionerne undersøgt, om institutionerne opfylder de samme revisionskriterier, jf. bilag 2. Vi gør dog opmærksom på, at institutionernes it-sikkerhed skal tage højde for institutionernes specifikke forhold, fx data, systemer og arbejdsprocesser, og at institutionerne derfor ikke kan sammenlignes.

Analyse

For at vurdere, om institutionerne opfylder de 20 almindelige tiltag og de 5 fremadrettede tiltag, har vi fremsat målepunkter for hvert enkelt tiltag. Målepunkterne er blevet brugt til at vurdere, om en institution opfylder det enkelte tiltag. Ved at analysere de indsamlede data i forhold til hvert enkelt tiltags målepunkter har det været muligt at give hver institution en vurdering af hvert tiltag. Målepunkterne varierer fra tiltag til tiltag og viser, hvad der er udslagsgivende i Rigsrevisionens vurdering. Dog er det fælles for målepunkterne, at grøn viser, at institutionen opfylder det pågældende tiltag, gul viser, at tiltaget er delvist opfyldt, og rød viser, at tiltaget ikke er opfyldt. Der ligger en faglig vurdering fra en erfaren it-revisor til grund i forhold til at vurdere, om institutionen opfylder tiltagene i henhold til målepunkterne. Disse vurderinger er understøttet af revisionsbeviser.

Undersøgelsen tager højde for, om ledelsen i institutionerne har fravalgt ét eller flere af de 20 tiltag på baggrund af en risikovurdering eller et lignende velbegrundet valg. Det betyder fx, at hvis én af institutionerne i forbindelse med revisionen på velbegrundet vis kunne dokumentere, at ledelsen på baggrund af risikovurderingen havde fravalgt et tiltag, ville dette fremgår af rapporten. Fx har vi for det ydre tiltag *brug af 2-faktor login ved webmailløsninger* markeret dette som "ikke relevant" for Beredskabsstyrelsen, da styrelsen ikke har en webmailløsning.

Analysen har taget udgangspunkt i, at institutionerne skulle opfylde alle 20 tiltag, for at deres beskyttelse mod ransomwareangreb kunne vurderes som tilfredsstillende. Dog gælder dette ikke, hvis en institution har fravalgt et tiltag som bekrevet ovenfor. Det er Rigsrevisionens opfattelse, at de 20 tiltag er grundlaget for god it-sikkerhedspraksis i forhold til ransomware og dermed sikrer en grundlæggende beskyttelse mod ransomwareangreb. Dog fremhæver vi i analysen visse steder udvalgte tiltag, der ifølge Rigsrevisionens faglige vurdering – og understøttet af bl.a. anbefalinger fra Center for Cybersikkerhed – er særligt vigtige. De 5 fremadrettede tiltag har ikke indgået i vurderingen.

Høringsprocedure

De 4 institutioner har i forbindelse med både it-revisionen og undersøgelsen afgivet høringssvar. I den forbindelse har institutionerne haft mulighed for at rette faktuelle fejl, stille spørgsmål og komme med oplysninger. Beretningen har i udkast været forelagt institutionerne samt Forsvarsministeriet, Sundheds- og Ældreministeriet og Transport-, Bygnings- og Boligministeriet, hvis bemærkninger er afspejlet i beretningen.

I forbindelse med høringerne har vi bl.a. drøftet med institutionerne, hvilke sårbarheder undersøgelsen eksponerer. Vi har på den baggrund så vidt muligt taget højde for eventuelle sårbarheder.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision. Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).

BILAG 2. RESULTATER FRA IT-REVISIONERNE

DE 20 ALMINDELIGE TILTAG TIL BESKYTTELSE MOD RANSOMWAREANGREB

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Ledelsesmæssigt fokus				
Dækkende risikovurdering	🔴	🟢	🔴	🟢
Opdateret it-sikkerhedspolitik og -retningslinjer	🟢	🟢	🟢	🟢
Krav til backup	🟢	🟡	🟢	🟢
Opfølgning på ransomwareangreb	🟡	🟢	🟡	🟢
Ydre tiltag				
Brug af antispam- og antivirusløsning	🟢	🟢	🟢	🟢
Forhindre omgåelse af den centrale antispam- og antivirusløsning	🟢	🟢	🟢	🟢
Brug af 2-faktor login ved webmailløsninger	🔴	🔴	🔴	Ikke relevant
Forhindre brug af private e-mailløsninger	🔴	🔴	🔴	🔴
Indre tekniske tiltag				
Lokaladministratorer har et arbejdsbetinget behov	🔴	🟢	🔴	🟢
Opdatering af styresystemer	🟢	🟢	🟢	🟢
Opdatering af programmer, som er tredjepartsprodukter	🔴	🟡	🔴	🟡
Kun godkendte programmer kan afvikles (whitelisting-løsning)	🟡	🟢	🟡	🟡
Ingen brug af privilegerede rettigheder, når der læses e-mails	🟡	🟢	🔴	🟡
Sikring mod ubeskyttet adgang til internettet, og at medarbejderne ikke kan downloade potentielt skadelige filer, når de læser e-mails (fx i form af en sandboxing-løsning)	🟡	🟢	🟡	🟡
Rettighedstildeling på fildrevniveau i overensstemmelse med egne retningslinjer	🟢	🟢	🟢	🟢

🔴 Ikke opfyldt
🟡 Delvist opfyldt
🟢 Opfyldt

DE 20 ALMINDELIGE TILTAG TIL BESKYTTELSE MOD RANSOMWAREANGREB

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Indre adfærdsrelaterede tiltag				
Gennemførelse af awareness-aktiviteter	●	●	●	●
Opfølgning på awareness-aktiviteter	●	●	●	●
Reaktive tiltag				
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	●	●	●	●
Samlet resultat	● **5** ● **5** ● **10**	● **5** ● **2** ● **13**	● **8** ● **3** ● **9**	● **2** ● **5** ● **12**

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

DE 5 FREMADRETTEDE/ANBEFALENDE TILTAG TIL BESKYTTELSE MOD RANSOMWAREANGREB

	Sundhedsdata-styrelsen	Udenrigs-ministeriet	Banedanmark	Beredskabs-styrelsen
Ydre tiltag				
Sikring mod, at hackere kan anvende institutionens domænenavne som afsenderdomænenavn, når de sender indgående e-mails	✓	(✓)	✓	(✓)
Kontrol af indgående e-mails i forhold til afsenderidentitet 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	(✓)	(✓)	÷	(✓)
Indre tiltag				
Programmer med atypiske adfærdsmønstre opdages	÷	÷	✓	✓
Programmer med atypiske adfærdsmønstre stoppes eller begrænses	÷	÷	(✓)	÷

÷ Ikke opfyldt
(✓) Delvist opfyldt
✓ Opfyldt

Kilde: Rigsrevisionen.

BILAG 3. ORDLISTE

2-faktor login	2-faktor login ved webmailløsninger betyder, at medarbejderne skal validere deres identitet ved hjælp af 2 eller flere faktorer, når de logger på deres arbejdsmail udefra. Det er en kombination af noget, som brugeren ved (fx password), og noget, som brugeren har eller får (fx usb-nøgle eller en kode sendt til mobiltelefonen).
Afvikling	En afvikling kendetegner den proces, hvor et program åbnes og kører på computeren.
Antispam- og antivirusløsning	En opdateret og central antispam- og antivirusløsning frasorterer mistænkelige e-mails, der bliver sendt til institutionen. En sådan løsning kan medvirke til at forhindre e-mails med ransomware i at lande i medarbejderes indbakke.
Application white-listing-løsning	En systemunderstøttet liste over godkendte programmer, der må afvikles. En sådan liste vil medføre, at programmer, som ikke er på listen, ikke kan blive afviklet.
Arbejdsbetinget behov	Et arbejdsbetinget behov er, når en medarbejders kernefunktion omfatter afhjælpning af it-problemer, fx medarbejdere, som supporterer andre med it-driften. Dermed kan det ikke betegnes som et arbejdsbetinget behov, hvis institutionerne anvender software, der kræver lokaladministratorrettigheder.
Awareness-aktivitet	Aktiviteter, som har til formål at øge kendskabet til cybertrusler, herunder ransomware, blandt medarbejderne. Aktiviteterne har typisk været i form af oplysningskampagner, hvor institutionerne via bl.a. møder og informationsvideoer orienterer medarbejderne.
Backup	En sikkerhedskopi af data, så data ikke kun findes ét sted. Backuppen opdateres af dataejer i henhold til aftalte intervaller.
Blacklisting-løsning	En systemunderstøttet liste over programmer, der ikke må afvikles. En sådan liste vil medføre, at alle programmer, som er på listen, ikke kan blive afviklet.
Domænenavn	Domænenavnet afspejler typisk navnet på fx den institution, der råder over og anvender det.
Filserver	En central it-funktion, der opbevarer fildata, fx tekstbehandlings- og regnearksfiler.
Hacker	Betegner i denne beretning en ukendt og uautoriseret person, der foretager en ulovlig handling ved i det skjulte at skaffe sig adgang til og/eller inficere andres it-systemer eller data. Formålet med hacking og de anvendte metoder afhænger af de personer eller organisationer, der står bag, dvs. om det er fremmede stater, kriminelle organisationer eller individer, som på egen hånd misbruger en institutions svagheder.
IP-adresse	En slags telefonnummer, som fx kan identificere en computer, og som gør det muligt for en computer at finde og kommunikere med en anden computer, bl.a. i situationer, hvor data skal udveksles.
Kryptering/ dekryptering	En forvanskning af data foretaget ved hjælp af matematiske funktioner. Det betyder, at data ikke er læsbare, før de dekrypteres.
Logning	Registrering af oplysninger om anvendelse af og hændelser i institutionens it-systemer og data i en fil. Logning øger chancen for at kunne undersøge et angreb til bunds, fordi alle handlinger på institutionens systemer genererer et digitalt fingeraftryk, som kan opsamles i en log. Logning af konti med privilegerede rettigheder kan fx vise, om personer har logget sig på it-systemer, og hvad de har brugt rettighederne til.
Malware	En sammentrækning af de engelske ord *malicious software*. Malware er en fællesbetegnelse for ondsindede computerprogrammer, der gør skadelige eller uønskede handlinger på brugerens computer.

Privilegerede rettigheder	Rettigheder, der giver medarbejderen udvidet adgang til og kontrol med institutionens it-systemer og data. Hvis medarbejdere med privilegerede rettigheder kan tilgå e-mails, øger det risikoen for at blive ramt af ransomwareangreb.
Produktionsmiljø	Det it-mæssige arbejdsmiljø, som institutionens daglige arbejde udføres i, hvilket bl.a. er de computere og systemer, som medarbejderne arbejder ved eller med.
Ransomware	Ordet *ransomware* er en sammentrækning af det engelske ord for løsepenge *ransom* og *software*. Ransomware er skadelige programmer, der fjerner adgangen til data. Det sker typisk ved, at data bliver krypteret, så den ramte institution ikke kan tilgå dem. Hackere kræver løsepenge for at dekryptere data, så institutionen igen kan få adgang til dem.
Sandboxing-løsning	Sandboxing-løsninger øger beskyttelsen mod både kendte og ukendte skadelige filer, og hjemmesider bliver undersøgt og bremset, inden skaden sker. Sandboxing er en virksom beskyttelse, da denne teknologi kontrollerer, om filer og andet indhold fra hjemmesider er skadelige, før brugeren tilgår indholdet. Sandboxing modvirker derfor ransomware, som institutionens medarbejdere kommer i berøring med via internettet, fx via private e-mailløsninger.
SIEM-løsning	SIEM står for Security Information and Event Management. SIEM-løsninger betegner teknologier, der i realtid analyserer sikkerhedshændelser fra netværksenheder, programmer mfl.
Styresystem	Software, som styrer udvekslingen af data mellem fx computerens dele. Det kan anskues som computerens nervesystem, der forbinder mange elementer.
Tredjepartsprodukter	Typisk programmer udviklet af virksomheder, som leverer en service, fx tekstbehandling.