FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

Januar 2022
– 9/2021

Rigsrevisionens beretning afgivet
til Folketinget med Statsrevisorernes
bemærkninger

5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden

9/2021

Beretning om

5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden

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 2022

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:

Statsrevisorerne fremsender med deres bemærkning Rigsrevisionens beretning til Folketinget og vedkommende minister.

Finansministeren, justitsministeren, sundhedsministeren, ministeren for fødevarer, landbrug og fiskeri samt klima-, energi- og forsyningsministeren 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 april 2022.

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 2021, som afgives i februar 2023.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

Karakterskala	
Positiv kritik	• finder det meget/særdeles positivt • finder det positivt • finder det tilfredsstillende/er tilfredse med
Kritik under middel	• finder det ikke helt tilfredsstillende
Middel kritik	• finder det utilfredsstillende/er utilfredse med • påpeger/understreger/henstiller/forventer • beklager/finder det bekymrende/foruroligende
Skarp kritik	• kritiserer/finder det kritisabelt/kritiserer skarpt/indskærper • påtaler/påtaler skarpt
Skarpeste kritik	• påtaler skarpt og henleder særligt Folketingets opmærksomhed på

Henvendelse vedrørende denne publikation rettes til:
Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

Yderligere eksemplarer kan købes ved henvendelse til:
Rosendahls Lager og Logistik
Vandtårnsvej 83A
2860 Søborg

Tlf.: 4322 7300
distribution@rosendahls.dk
www.rosendahls.dk

ISSN 2245-3008
ISBN trykt 978-87-7434-744-6
ISBN online 978-87-7434-745-3

Statsrevisorernes bemærkning

Beretning om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden

Statsrevisorerne og Rigsrevisionen har i en række beretninger over en længere årrække påpeget vigtigheden af, at statslige myndigheder har iværksat it-sikkerhedsmæssige foranstaltninger, der kan imødegå risici for cyberangreb og misbrug, fx uberettiget adgang til it-systemer samt hacker- og ransomwareangreb. Siden den 1. januar 2020 har alle statslige myndigheder skullet efterleve 17 tekniske krav til it-sikkerhed, hvortil der den 1. juli 2020 er føjet yderligere 3 krav, dvs. at staten skal efterleve 20 tekniske minimumskrav til it-sikkerhed.

Denne beretning handler om, hvorvidt 5 samfundsvigtige statslige myndigheder – Statens It (Finansministeriet), Kriminalforsorgen (Justitsministeriet), Sundhedsdatastyrelsen (Sundhedsministeriet), Energistyrelsen (Klima-, Energi- og Forsyningsministeriet) og Fødevarestyrelsen (Ministeriet for Fødevarer, Landbrug og Fiskeri) efterlevede de 20 minimumskrav i 2021. De 5 myndigheder er udvalgt, fordi de varetager samfundsvigtige opgaver og/eller håndterer følsomme oplysninger om borgerne.

Statsrevisorerne finder det utilfredsstillende, at hverken Statens It eller nogen af de 4 andre statslige myndigheder har efterlevet alle de tekniske minimumskrav til it-sikkerheden i staten, på trods af at de trådte i kraft for 1-1½ år siden. Sårbarhed i myndighedernes it-systemer, hjemmesider, mobiltelefoner og tablets har således medført øget risiko for cyberangreb og misbrug.

Statsrevisorerne

17. januar 2022

Henrik Thorup
Klaus Frandsen
Frank Aaen
Mette Abildgaard
Leif Lahn Jensen
Troels Lund Poulsen

Statsrevisorerne har hæftet sig ved disse undersøgelsesresultater:

- Sundhedsdatastyrelsen har efterlevet færrest minimumskrav (12 ud af de 20 minimumskrav), mens Energistyrelsen har efterlevet 15 krav, Kriminalforsorgen har efterlevet 16 krav, og Fødevarestyrelsen har efterlevet 17 krav. Statens It, som er professionel aktør og leverandør af it-ydelser til 19 ministerområder, har kun efterlevet 18 af de 20 minimumskrav.
- Ingen af myndighederne har levet op til minimumskravet om regelmæssig opdatering af mobile enheder, hvorved risikoen for uberettiget adgang og aflytning er øget.
- 4 ud af de 5 statslige myndigheder har haft handlingsplaner for implementering af minimumskrav, som de ikke efterlevede.
- Statens It har som leverandør af it-ydelser til Energistyrelsen og Fødevarestyrelsen sikret, at 13 ud af de 20 minimumskrav er efterlevet i styrelserne for de systemer, der er overdraget til Statens It. Af de krav, som styrelserne selv har været ansvarlige for, har Energistyrelsen kun efterlevet 3 ud af 7 krav, og Fødevarestyrelsen har efterlevet 5 ud af 8 krav.
- Statens It har ikke koordineret tilstrækkeligt med Fødevarestyrelsen og Energistyrelsen i forhold til krav 18, mens Energistyrelsen ikke har koordineret tilstrækkeligt med Statens It i forhold til krav 20.

Statsrevisorerne finder, at der er brug for, at Finansministeriet stiller sig i spidsen for vedvarende fokus på it-sikkerheden i staten.

Statsrevisorerne konstaterer, at 4 minimumskrav er upræcise og har givet anledning til fortolkning og tvivl om, hvordan man efterlever kravene. Statsrevisorerne skal derfor tilslutte sig Rigsrevisionens anbefaling om, at Finansministeriet konkretiserer og uddyber minimumskrav 6, 13, 15 og 18.

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 § 7. Finansministeriet, § 11. Justitsministeriet, § 16. Sundhedsministeriet, §. 24. Ministeriet for Fødevarer, Landbrug og Fiskeri og § 29. Klima-, Energi- og Forsyningsministeriet.

I undersøgelsesperioden har der været følgende ministre:

Finansministeriet:
Nicolai Wammen: juni 2019 -

Justitsministeriet:
Nick Hækkerup: juni 2019 -

Sundhedsministeriet:
Magnus Heunicke: juni 2019 -

Ministeriet for Fødevarer, Landbrug og Fiskeri:
Rasmus Prehn: november 2020 -
Mogens Jensen: juni 2019 - november 2020

Klima-, Energi- og Forsyningsministeriet:
Dan Jørgensen: juni 2019 -

Beretningen har i udkast været forelagt Finansministeriet, Justitsministeriet, Sundhedsministeriet, Ministeriet for Fødevarer, Landbrug og Fiskeri samt Klima-, Energi- og Forsyningsministeriet, hvis bemærkninger er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. Denne beretning handler om, hvorvidt 5 samfundsvigtige statslige myndigheder efterlever de 20 tekniske minimumskrav til it-sikkerheden. Beretningen bygger på it-revisioner, der er gennemført i perioden marts-september 2021.

2. De 20 tekniske minimumskrav til it-sikkerhed skal beskytte statslige arbejdspladser mod ondsindede cyber- og informationssikkerhedshændelser. Det kan fx være angreb fra ondsindede aktører, der gerne vil opnå adgang til fortrolige oplysninger eller fastlåse data for at få løsepenge. 17 krav har været ufravigelige siden den 1. januar 2020, og 3 krav har været ufravigelige siden den 1. juli 2020, dvs. at alle statslige myndigheder skal efterleve dem.

Ondsindet aktør
En ondsindet aktør betegner i denne beretning en person, der foretager en tilsigtet eller utilsigtet ulovlig handling ved fx i det skjulte at skaffe sig adgang til og/eller inficere andres it-systemer eller data. Dette kan både være en medarbejder, men også en helt ukendt person.

3. Cybertruslen mod statslige myndigheder vokser i takt med den øgede digitalisering af samfundet. Dette afspejles også i Center for Cybersikkerheds trusselsvurderinger. Cyberangreb er ikke ualmindelige, og flere statslige myndigheder er gennem tiden blevet udsat for dem. I oktober 2021 kom det bl.a. frem, at it-kriminelle havde snydt Høje Taastrup Kommune ved at overtage en institutionsleders mailkonto og anmode kommunens økonomiafdeling om at betale COVID-19-relaterede udgifter. Herudover havde de it-kriminelle opnået adgang til følsomme oplysninger om et ukendt antal borgere (fx cpr-numre, fagforeningsmæssige tilhørsforhold og helbredsoplysninger).

4. Opgaven med at efterleve de 20 tekniske minimumskrav til it-sikkerheden er særlig vigtig hos myndigheder, der varetager samfundsvigtige opgaver eller håndterer følsomme oplysninger om fx borgere. Det skyldes, at efterlevelse af minimumskravene er med til at give en basal it-sikkerhed, der bidrager til at beskytte de oplysninger og data, som myndighederne er ansvarlige for.

5. Denne undersøgelse omfatter Statens It (Finansministeriet), Kriminalforsorgen (Justitsministeriet), Sundhedsdatastyrelsen (Sundhedsministeriet), Energistyrelsen (Klima-, Energi- og Forsyningsministeriet) og Fødevarestyrelsen (Ministeriet for Fødevarer, Landbrug og Fiskeri). De 5 myndigheder er udvalgt, fordi de varetager samfundsvigtige opgaver og/eller håndterer følsomme oplysninger om borgere. Statens It er desuden udvalgt, fordi Statens It er leverandør af it-services til 19 ministerområder, herunder Energistyrelsen og Fødevarestyrelsen, og derfor skal efterleve nogle af minimumskravene på vegne af de statslige myndigheder, der er kunder hos Statens It.

6. Formålet med undersøgelsen er at vurdere, om de 5 samfundsvigtige myndigheder efterlever de 20 tekniske minimumskrav til it-sikkerheden. Vi har undersøgt:

- om den enkelte myndighed efterlever de tekniske minimumskrav, som myndigheden selv er forpligtet til at efterleve
- om Statens It og kunderne, her Energistyrelsen og Fødevarestyrelsen, efterlever de tekniske minimumskrav i henhold til den ansvarsdeling, der er aftalt mellem dem.

7. Rigsrevisionen har selv taget initiativ til denne undersøgelse juni 2021. Undersøgelsen bygger på 5 it-revisioner, der er gennemført i perioden marts-september 2021. De udvalgte myndigheder har efter de gennemførte it-revisioner haft mulighed for at arbejde med at efterleve eventuelle ikke-opfyldte minimumskrav.

For 4 af de 20 minimumskrav er formuleringen af kravet upræcis, og Rigsrevisionen har derfor til brug for undersøgelsen operationaliseret kravet.

Statens It er fagligt uenig i Rigsrevisionens tolkning af minimumskravene 13 og 18. Statens It finder, at Rigsrevisionen bliver normerende i udmøntningen af kravene og anlægger en skærpet tolkning, som ikke er tilgået Statens It fra anden side. Statens It er desuden ikke enig i Rigsrevisionens vurdering af den risiko, som er forbundet med manglende efterlevelse af de 2 krav.

Kriminalforsorgen har indvendt, at Kriminalforsorgen ikke fuldt ud deler Rigsrevisionens fortolkning af, hvad der udgør efterlevelse af de 20 tekniske minimumskrav. Kriminalforsorgen har oplyst, at de 20 tekniske minimumskrav ikke oprindeligt er udformet med henblik på at danne udgangspunkt for en it-revision, hvorfor det ifølge Kriminalforsorgen for nogle af kravenes vedkommende har været nødvendigt for Rigsrevisionen at konkretisere, hvad der skal til for, at kravene er opfyldt. Det betyder ifølge Kriminalforsorgen, at revisionskriterierne kan siges at tage udgangspunkt i de tekniske minimumskrav, men er blevet underlagt Rigsrevisionens fortolkning.

Energistyrelsen har bemærket, at beretningen ikke i tilstrækkelig grad beskriver proportioner i den manglende efterlevelse eller tager højde for gennemførte mitigerende tiltag, der kan minimere risikoen ved den manglende efterlevelse af de enkelte krav.

Det er Rigsrevisionens opfattelse, at efterlevelse af de 20 tekniske minimumskrav sikrer en basal it-sikkerhed. Da enkelte af kravene som nævnt ikke er præcist formuleret, har Rigsrevisionen operationaliseret kravene. Det drejer sig om krav 6, 13, 15 og 18. Operationaliseringen er sket ud fra en it-sikkerhedsmæssig synsvinkel og ud fra en best practice-betragtning. Rigsrevisionens operationalisering af kravene er beskrevet i afsnit 1.3 om revisionskriterier. I beretningen beskriver Rigsrevisionen, hvilke risici der er forbundet med ikke at efterleve kravene. De beskrevne risici tager bl.a. udgangspunkt i de risici, som er beskrevet sammen med kravene på sikkerdigital.dk, og i Rigsrevisionens dialog med Center for Cybersikkerhed.

Rigsrevisionen finder, at der ikke kan være en delvis efterlevelse af minimumskravene. Rigsrevisionen har imidlertid indarbejdet myndighedernes bemærkninger om eventuelle mitigerende foranstaltninger, eller hvis myndighederne har påpeget, at få ting udestår, førend de efterlever et minimumskrav.

Hovedkonklusion

Finansministeriet, Justitsministeriet, Sundhedsministeriet, Ministeriet for Fødevarer, Landbrug og Fiskeri og Klima-, Energi- og Forsyningsministeriet har ikke sikret, at de 5 udvalgte myndigheder efterlevede alle 20 tekniske minimumskrav til it-sikkerheden, da Rigsrevisionen foretog en revision af området i 2021. Det finder Rigsrevisionen utilfredsstillende, da de fleste af kravene skulle være implementeret den 1. januar 2020. Konsekvensen er, at myndighederne har haft sårbarheder i deres it-systemer og på deres mobiltelefoner og tablets, hvilket har medført en øget risiko for cyberangreb og misbrug.

Ingen af myndighederne efterlevede alle de tekniske minimumskrav på revisionstidspunktet
Sundhedsdatastyrelsen efterlevede 12 krav, Energistyrelsen efterlevede 15 krav, Kriminalforsorgen efterlevede 16 krav, og Fødevarestyrelsen efterlevede 17 krav. Statens It efterlevede heller ikke alle 20 krav, men kun 18 af kravene, selv om Statens It er en professionel aktør på området, hvis kerneopgave er at levere sikker it-drift og service til andre statslige myndigheder. Dette til trods for at de 20 minimumskrav trådte i kraft for 1-1½ år siden.

Energistyrelsen og Fødevarestyrelsen er kunder hos Statens It og er derfor ikke selv ansvarlige for at sikre, at de efterlever alle 20 minimumskrav. Energistyrelsen er selv ansvarlig for at sikre efterlevelse af 7 ud af de 20 krav, mens Fødevarestyrelsen er ansvarlig for at sikre efterlevelse af 8 ud af de 20 krav. Undersøgelsen viser, at Energistyrelsen alene efterlevede 3 ud af de 7 krav, mens Fødevarestyrelsen efterlevede 5 ud af de 8 krav.

Ingen af myndighederne efterlevede minimumskrav 13 om opdatering af mobile enheder. Når fx mobiltelefoner ikke opdateres regelmæssigt, øges risikoen for, at ondsindede aktører opnår adgang til fortrolige oplysninger eller lykkes med at overvåge myndigheden (fx ved at aflytte mobiltelefoner).

4 af myndighederne har handleplaner for implementering af de minimumskrav, som de ikke efterlevede. Statens It har oplyst, at Statens It vil udarbejde risikovurderinger, men at disse risikovurderinger ikke er gennemført endnu.

Statens It har sikret, at Energistyrelsen og Fødevarestyrelsen efterlevede størstedelen af de tekniske minimumskrav, men koordinationen mellem Statens It og myndighederne har været utilstrækkelig i forhold til 2 krav
Statens It skal i kraft af sin rolle som leverandør sikre, at 13 ud af 20 krav bliver efterlevet på vegne af Energistyrelsen og Fødevarestyrelsen, som er kunder hos Statens It. Undersøgelsen viser, at Statens It lever op til denne forpligtelse.

Energistyrelsen og Fødevarestyrelsen kan ud over de 13 minimumskrav indgå et samarbejde med Statens It om at sikre efterlevelse af yderligere 4 minimumskrav. Det kræver koordination mellem Statens It og myndighederne. Rigsrevisionen har fundet eksempler på, at Statens It ikke har koordineret tilstrækkeligt med Fødevarestyrelsen og Energistyrelsen i forhold til krav 18 om kryptering af kommunikation til hjemmesider, mens Energistyrelsen ikke har koordineret tilstrækkeligt med Statens It i forhold til krav 20 om regelmæssig opdatering af webservere.

Rigsrevisionen anbefaler, at Finansministeriet sikrer, at 4 af kravene konkretiseres og uddybes, så tvivl om, hvad der skal til, for at det enkelte krav efterleves, minimeres

Rigsrevisionen kan konstatere, at 4 af kravene kan fortolkes - og af myndighederne bliver fortolket - forskelligt på grund af upræcise formuleringer mv. Det gælder krav 6 om begrænset tildeling af lokaladministratorrettigheder, krav 13 om regelmæssig opdatering af mobile enheder, krav 15 om logning samt krav 18 om kryptering af kommunikation til hjemmesider.

1.2. Baggrund

8. De tekniske minimumskrav udspringer af den nationale strategi for cyber- og informationssikkerhed 2018-2021. Det fremgår af strategien, at der skal være et tilstrækkeligt minimumsniveau for håndtering af cyber- og informationssikkerhed i statslige myndigheder. For at udmønte dette initiativ blev der nedsat en arbejdsgruppe bestående af Digitaliseringsstyrelsen, Center for Cybersikkerhed, Politiets Efterretningstjeneste og Statens It, som udarbejdede forslag til minimumskrav. De krav – hvis effekt og resurseanvendelse blev vurderet rimelige – blev efterfølgende drøftet i styregruppen for den nationale strategi for cyber- og informationssikkerhed, hvorefter de blev endeligt vedtaget i efteråret 2019. Herefter blev det meldt ud til alle statslige myndigheder, at de skulle efterleve 17 minimumskrav fra den 1. januar 2020 og yderligere 3 krav fra den 1. juli 2020.

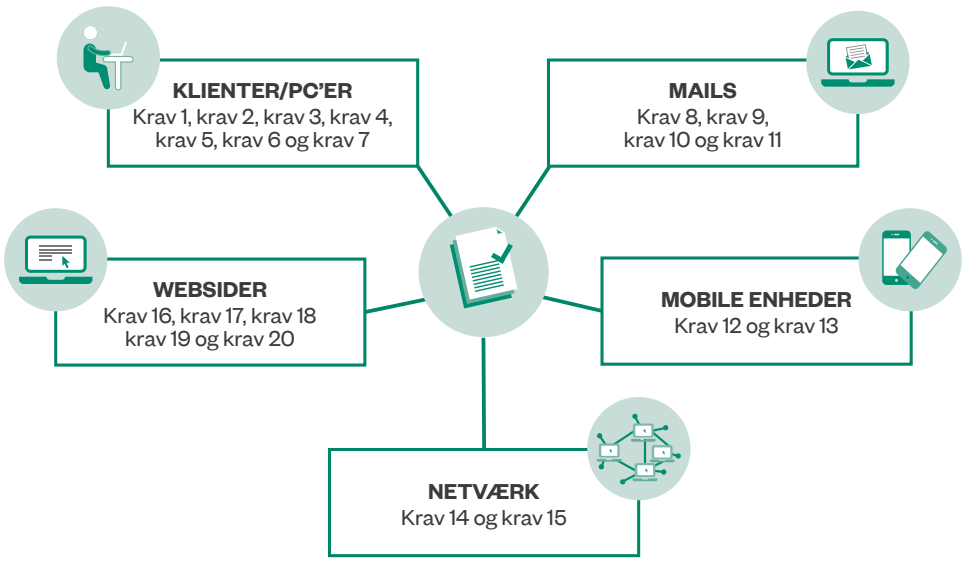
Styregruppen for den nationale strategi for cyber- og informationssikkerhed
Det er Finansministeriet (Digitaliseringsstyrelsen) og Forsvarsministeriet (Center for Cybersikkerhed), der varetager formandskabet for styregruppen. Herudover var Justitsministeriet, Klima-, Energi- og Forsyningsministeriet, Erhvervsministeriet, Transport- og Boligministeriet og Sundheds- og Ældreministeriet som medlemmer af styregruppen med til at godkende de 20 tekniske minimumskrav i 2019.

Det fremgår af Digitaliseringsstyrelsens hjemmeside, at det som udgangspunkt ikke er muligt at fravige kravene. Såfremt et krav undtagelsesvist ikke bliver efterlevet, skal myndigheden kunne redegøre for årsagen hertil samt for den forventede tidshorisont for implementering af kravet ud fra et *følg eller forklar*-princip. Rigsrevisionen kan bl.a. på den baggrund konstatere, at der er tale om ufravigelige minimumskrav, som de statslige myndigheder skal overholde.

De 20 tekniske minimumskrav

9. De 20 tekniske minimumskrav dækker en bred vifte af områder med betydning for it-sikkerheden. Det gælder områderne: klienter (fx pc og Mac), mails, mobile enheder (fx mobiltelefoner og tablets) samt netværk og websider. Figur 1 viser de forskellige områder, som er dækket af de 20 minimumskrav.

Figur 1
Områder, der er dækket af de 20 tekniske minimumskrav



Kilde: Rigsrevisionen.

10. Alle tekniske minimumskrav er baseret på etablerede anbefalinger, standarder eller best practice. Størstedelen af kravene er desuden understøttet af eksisterende vejledninger fra Center for Cybersikkerhed, Digitaliseringsstyrelsen og Datatilsynet. Digitaliseringsstyrelsen fremsendte på vegne af Digitaliseringsstyrelsen og Center for Cybersikkerhed en orientering om kravene til alle ministerier den 30. september 2019. Eftersom størstedelen af kravene har været best practice, inden de blev meldt ud som ufravigelige minimumskrav i 2019, burde de ikke have været ukendte for myndighederne.

De 20 minimumskrav og henvisninger til, hvad de følger af (fx specifikke vejledninger eller best practice), fremgår af sikkerdigital.dk, hvor de er tilgængelige for alle statslige myndigheder. Center for Cybersikkerhed har oplyst, at de statslige myndigheder skal følge kravene, da vejledningerne er udarbejdet uafhængigt og i flere tilfælde, inden de tekniske krav blev formuleret. Digitaliseringsstyrelsen har desuden udarbejdet en fortolkning af minimumskravene i et opfølgningsark, der er sendt til myndighederne. Digitaliseringsstyrelsen har understreget, at det alene er kravene, som de er formuleret på sikkerdigital.dk og med yderligere fortolkning i styrelsens opfølgningsark, der gælder som krav og ikke supplerende anbefalinger i eventuelle vejledninger. Det opfølgningsark, der var gældende på revisionstidspunktet, fremgår af bilag 2.

11. Denne beretning har efterlevelsen af de 20 minimumskrav som udgangspunkt, men de steder, hvor formuleringen af kravene ikke er tilstrækkeligt konkret, har Rigsrevisionen operationaliseret kravene. Et eksempel er krav 13, der omhandler, at myndighederne skal foretage regelmæssig opdatering af operativsystem og apps på mobile enheder. Her har Rigsrevisionen operationaliseret ordet *regelmæssigt* ud fra, hvad der giver mening i forhold til beskyttelseshensynet i kravet. Rigsrevisionen har imidlertid ikke defineret, hvilken efterlevelsesmetode eller teknologi en myndighed skal anvende for at efterleve et krav. Myndighederne har således en vis metodefrihed til at implementere kravet.

Vores operationalisering af de krav, der ikke er tilstrækkeligt konkrete, er beskrevet i afsnit 1.3 om revisionskriterier.

Tabel 1 viser de 20 krav og deres formål.

Tabel 1

De 20 tekniske minimumskrav og deres formål

Minimumskrav	Formål
Krav 1. Firewall Myndigheden skal implementere firewall på alle klienter.	Firewalls skal sikre mod utilsigtet adgang til arbejdsstationer. Ondsindet software forsøger typisk at sprede sig på tværs af systemer. Man kan begrænse denne spredning ved at indføre firewall.
Krav 2. VPN-løsning Myndigheden skal anvende en VPN-løsning til at gå på internettet via arbejds-pc fra eksterne netværk.	Brug af VPN-løsning skal bl.a. modvirke såkaldte man-in-the-middle-angreb, hvor ondsindede aktører får adgang til alt på en forbindelse (fx tekst og filer). Brug af VPN sikrer også mod, at data kan blive ændret af en ondsindet aktør.
Krav 3. Kryptering af harddiske Myndigheden skal sikre, at harddiske er krypterede.	Operativsystemet skal være sat op til at kryptere harddiske på den enkelte pc. Myndigheden kan herved undgå kompromittering af data i forbindelse med tab eller tyveri af pc'en.
Krav 4. End-point-beskyttelse Myndigheden skal implementere end-point-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter.	Kontinuerligt opdateret endpoint-beskyttelse sikrer, at kendte vira, malware mv. ikke kan afvikles på arbejdsstationen.
Krav 5. Regelmæssig opdatering af klienter Myndigheden skal sikre, at klienter opdateres regelmæssigt – både på operativsystem og applikationer.	Al software bør være omfattet af regelmæssig opdatering, så eventuelle sårbarheder lukkes hurtigst muligt. Herved minimerer myndigheden risikoen for, at ondsindede aktører udnytter kendte sikkerhedshuller.
Krav 6. Begrænset tildeling af lokaladministratorrettigheder Myndigheden skal kun tildele lokaladministratorrettigheder tidsbegrænset og med veldokumenterede behov.	Størstedelen af ondsindet software kræver lokaladministratorrettigheder på pc'en for at blive installeret. Myndigheden mindsker risikoen for installation af ondsindet software, hvis myndigheden tildeler lokaladministratorrettigheder tidsbegrænset og med veldokumenterede behov.
Krav 7. Sikkerhedsopdateret operativsystem Myndigheden skal sikre, at det anvendte operativsystem er så nyt som muligt og som minimum er supporteret med sikkerhedsopdateringer.	Nye operativsystemer har som udgangspunkt et højere sikkerhedsniveau end ældre versioner. Ældre operativsystemer, der ikke længere supporteres af producenten, modtager typisk ikke sikkerhedsopdateringer, når der opdages nye sårbarheder og exploits. Exploits er programkoder eller metoder til at udnytte en softwaresårbarhed eller en svag konfiguration af et system og på den måde forårsage en sikkerhedshændelse.
Krav 8. Godkendte mail-relays med autentifikation Myndigheden må kun anvende af myndigheden godkendte mail-relays med autentifikation.	Når myndigheden anvender af myndigheden godkendte mail-relays med autentifikation, øger det sikkerheden og mindsker risikoen for, at mail-servere misbruges til spam og spredning af ondsindet software. Myndigheden mindsker samtidig risikoen for, at ondsindede aktører lykkes med at udgive sig for at være myndigheden.
Krav 9. Kryptering af kommunikation med mail-protokoller Myndigheden skal sikre, at kommunikation med mail-protokoller er krypteret og anvender minimum TLS 1.2.	Brug af minimum TLS 1.2 reducerer risikoen for, at mail-kommunikation bliver aflyttet undervejs i transmissionen over internettet. Kryptering af mail-trafik skal desuden sikre, at data ikke læses eller bliver ændret af ondsindede aktører.

Tabel 1 (fortsat)

De 20 tekniske minimumskrav og deres formål

Minimumskrav	Formål
Krav 10. 2-faktor-autentifikation eller direkte VPN-forbindelse Myndigheden skal sikre, at webmail kun anvendes uden for myndighedens lokale netværk, hvis dette foregår ved hjælp af 2-faktor-autentifikation eller via en direkte VPN-forbindelse til myndighedens netværk.	Brug af 2-faktor-autentifikation eller direkte VPN-forbindelse skal forhindre, at ondsindede aktører får adgang til myndighedens mail ved tilslutning via usikre netværk (fx i lufthavne).
Krav 11. DMARC REJECT-policy på domæner Myndigheden skal implementere DMARC REJECT-policy på alle domæner tilhørende myndigheden.	DMARC er designet til at forhindre såkaldt mail-spoofing, hvor en afsender udgiver sig for at være en anden.
Krav 12. Adgangskode på min. 6 cifre eller biometrisk identifikation Myndigheden skal sikre, at der anvendes numerisk adgangskode på min. 6 cifre eller biometrisk identifikation.	Brug af numerisk adgangskode på min. 6 cifre eller biometrisk identifikation beskytter telefonen mod misbrug, hvis den tabes eller stjæles.
Krav 13. Regelmæssig opdatering af mobile enheder Myndigheden skal foretage regelmæssig opdatering af operativsystem og apps på mobile enheder.	Software på mobile enheder (fx mobiltelefoner og tablets) skal så vidt muligt opdateres, så snart leverandøren udgiver opdateringer. Myndigheden sikrer herved, at kendte sikkerhedshuller lukkes hurtigst muligt.
Krav 14. Kryptering af wi-fi på arbejdsnetværk Myndigheden skal sikre, at wi-fi på myndighedens arbejdsnetværk er krypteret med minimum WPA2.	Kryptering af wi-fi gør det vanskeligere for en ondsindet aktør at aflytte kommunikation på netværket.
Krav 15. Logning Myndigheden skal sikre logning, herunder log på alle systemer og tjenester på netværksservere.	Logning udgør en forudsætning for opdagelse og efterforskning af forskellige sikkerhedshændelser.
Krav 16. DNSSEC Myndigheden skal sikre, at DNSSEC tilknyttes alle domænenavne tilhørende myndigheden.	DNSSEC sikrer, at den *rigtige* side bliver vist, når der linkes til hjemmesiden. DNSSEC sikrer desuden, at medarbejdere og borgere kan stole på, at de tilgår den rigtige hjemmeside.
Krav 17. Beskyttelse mod skadelige hjemmesider Myndigheden skal anvende en sikker DNS-tjeneste eller implementere en anden løsning til beskyttelse mod skadelige hjemmesider.	En sikker DNS-tjeneste beskytter brugeren mod malware- og phishingsider ved at blokere for domæner, der er kendt som værende eller vurderes at være farlige.
Krav 18. Kryptering af kommunikation til hjemmesider Myndigheden skal sikre, at kommunikation til hjemmesider krypteres og anvender minimum TLS 1.2, dvs. der skal implementeres https på alle hjemmesider.	Kryptering af trafik til og fra hjemmesider skal sikre data mod at blive læst eller ændret af ondsindede aktører, herunder forebygge man-in-the-middle-angreb, hvor en ondsindet aktør får adgang til alt, hvad der foregår i trafikken (fx filer og tekst).
Krav 19. Flash Myndigheden må ikke anvende Flash på hjemmesider tilhørende myndigheden.	Brug af Flash i en webbrowser frarådes i forvejen, men udgør fortsat størstedelen af sårbarheder, der anvendes til at kompromittere en computer. Kompromittering sker gennem kørsel af skadelig Flash-kode.
Krav 20. Regelmæssig opdatering af webservere Myndigheden skal benytte regelmæssigt opdateret serversoftware på webservere.	Al software bør være omfattet af regelmæssig opdatering, så eventuelle sårbarheder lukkes hurtigst muligt. Myndigheden minimerer herved risikoen for, at ondsindede aktører udnytter kendte sikkerhedshuller.

Kilde: Rigsrevisionen, bl.a. på baggrund af oplysninger fra sikkerdigital.dk, der drives af Digitaliseringsstyrelsen og Erhvervsstyrelsen.

Rigsrevisionens tidligere undersøgelser af minimumskravene

12. Rigsrevisionen har i tidligere beretninger undersøgt områder af it-sikkerheden, der i dag er omfattet af de 20 tekniske minimumskrav. Fx er 4 af de 20 tiltag, som Rigsrevisionen undersøgte i beretningen om beskyttelse mod ransomwareangreb fra 2017, blevet en del af de 20 tekniske minimumskrav. Rigsrevisionens opfølgning på ransomwareberetningen i januar 2021 viste imidlertid, at 3 af de 4 undersøgte myndigheder endnu ikke var i mål med enkelte minimumskrav.

Rigsrevisionen har også tidligere påpeget vigtigheden af, at myndigheder fx sørger for systematisk sikkerhedsopdatering af programmer, at de logger færden i systemer, og at de begrænser tildelingen af administrative rettigheder til medarbejdere. Det har Rigsrevisionen fx berørt i *beretning om forebyggelse af hackerangreb* (2013), *beretning om statens behandling af fortrolige oplysninger om personer og virksomhede*r (2015), *beretning om adgangen til it-systemer, der understøtter samfundsvigtige opgaver* (2016), *beretning om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata* (2017) og *beretning om indsatsen for at undgå statsansattes besvigelser* (2020). Rigsrevisionen har således gennem tiden gjort opmærksom på forskellige forhold inden for it-sikkerhed, der i dag er indeholdt i de 20 tekniske minimumskrav.

Ansvarsdeling mellem Statens It og deres kunder

13. Alle statslige myndigheder skal efterleve de 20 tekniske minimumskrav. En række statslige myndigheder er imidlertid kunder hos Statens It, hvilket betyder, at de har overdraget ansvaret for den basale it-drift til Statens It. Statens It varetager således systemer for en række statslige myndigheder og har dermed et ansvar for at sikre, at disse systemer administreres i overensstemmelse med de tekniske minimumskrav.

Den konkrete ansvarsdeling mellem Statens It og deres kunder (herunder Energistyrelsen og Fødevarestyrelsen) er defineret af Statens It og er meldt ud i et hjælpeark i henholdsvis august 2020 og februar 2021. Heri fremgår det under hvert minimumskrav, hvad Statens It vil sikre på vegne af kunderne, og hvad kunderne selv skal være opmærksomme på at sikre. Fx fremgår det af hjælpearket, at kunden selv skal sørge for, at Mac-klienter efterlever minimumskravene, mens Statens It sørger for at efterleve minimumskrav for de klienter, som Statens It stiller til rådighed for kunderne.

Det fremgår således af hjælpearket, at efterlevelse af enkelte minimumskrav kræver både en indsats fra Statens It, men også fra kunderne, her Energistyrelsen og Fødevarestyrelsen.

14. I denne undersøgelse indgår Energistyrelsen og Fødevarestyrelsen, der begge er kunder hos Statens It. Det betyder, at de ikke selv har ansvaret for at efterleve alle 20 minimumskrav, men kun en del af kravene. De skal fx efterleve krav, som kræver en beslutning eller handling fra myndigheden selv, fx beslutningen om at tildele lokaladministratorrettigheder (minimumskrav 6). Herudover skal de efterleve krav angående de systemer, som de ikke har overdraget til Statens It. Myndighederne er selv ansvarlige for at sikre, at de systemer, der ligger uden for Statens It, bliver administreret i overensstemmelse med kravene.

Statens It

Statens It er en styrelse under Finansministeriet, som blev oprettet den 1. januar 2010. Ved oprettelsen blev 8 ministerområders it-driftsorganisationer fusioneret med henblik på at opnå højere kvalitet og lavere priser gennem harmonisering og stordriftsfordele. I dag leverer Statens It it-services til 19 ministerområder. Når en statslig myndighed overdrager den basale it-drift til Statens It, ressortoverføres ansvaret for denne drift og tilsynet hermed til Finansministeriet. Den statslige myndighed har fortsat ejerskab over sine systemer og derfor en række forpligtelser i forhold til at risikovurdere systemerne mv. En række af disse forpligtelser fremgår af bilag 1.

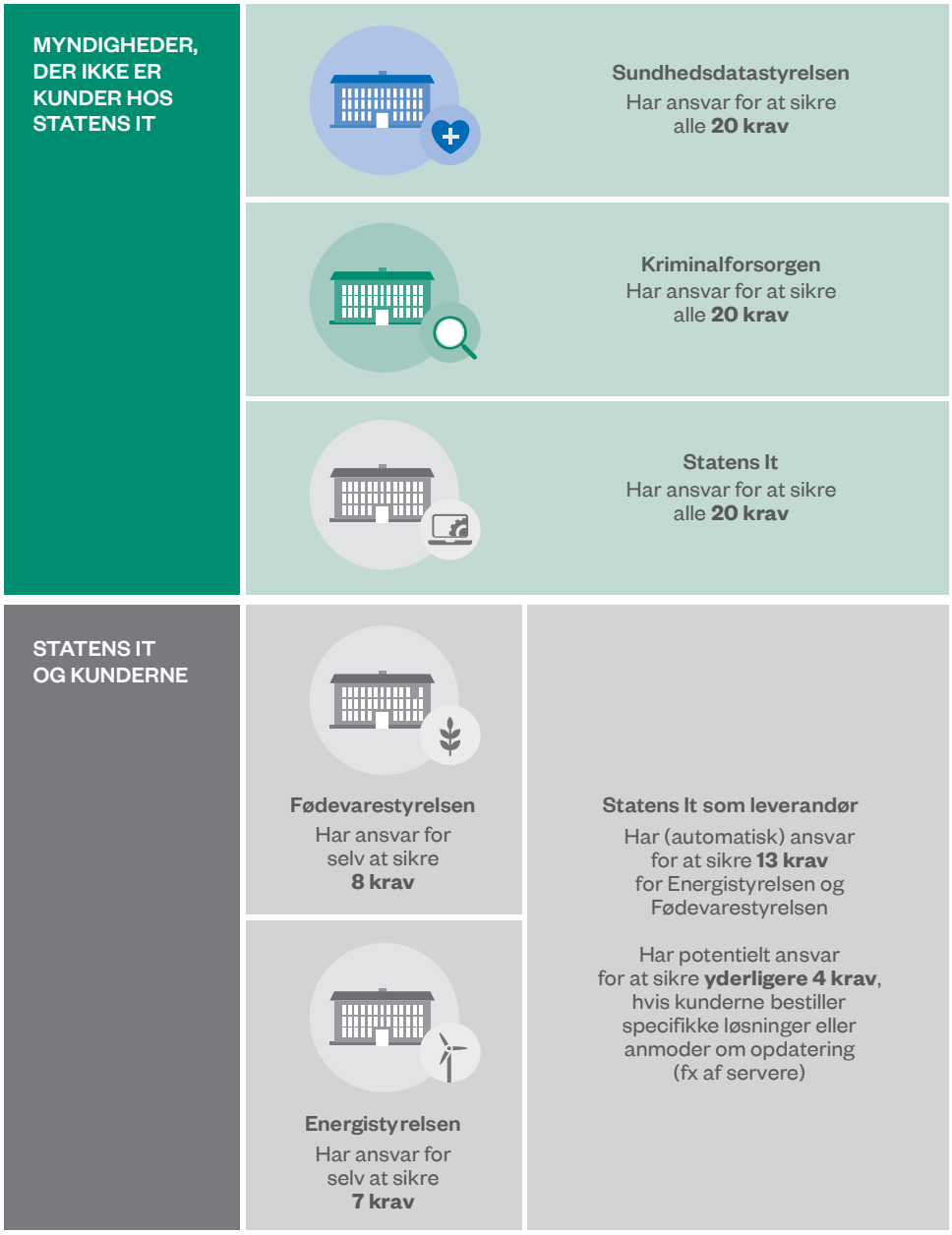
I denne undersøgelse har Statens It 2 roller. Den første rolle er som myndighed, der *i egen organisation* skal efterleve de tekniske minimumskrav. Den anden rolle er som leverandør af it-services til Energistyrelsen og Fødevarestyrelsen. Som nævnt er Statens It ansvarlig for at sikre, at de systemer, som Statens It varetager for Energistyrelsen og Fødevarestyrelsen, administreres i overensstemmelse med kravene. Statens It skal fx sikre, at der er implementeret firewall på de klienter, som Statens It stiller til rådighed for Fødevarestyrelsen (minimumskrav 1).

De 5 myndigheder i undersøgelsen

15. De 5 udvalgte myndigheder er Statens It, Kriminalforsorgen, Sundhedsdatastyrelsen, Energistyrelsen og Fødevarestyrelsen. Disse myndigheder har enten ansvar for at sikre alle 20 minimumskrav eller en del af minimumskravene. Det afhænger af, om de er kunder hos Statens It.

Figur 2 viser, hvor mange minimumskrav de 5 myndigheder er ansvarlige for at efterleve.

Figur 2
Myndigheder og antal krav



Note: Lægger man antallet af krav sammen i søjlerne for henholdsvis Statens It og kunderne (Energistyrelsen og Fødevarestyrelsen) summer antallet af minimumskrav ikke til 20. Det skyldes, at både Statens It og kunderne, dvs. Energistyrelsen og Fødevarestyrelsen, skal efterleve de samme minimumskrav. Statens It skal således efterleve disse krav i forhold til de systemer, som kunderne har overdraget til Statens It, mens kunderne skal efterleve de samme krav i forhold til de systemer, der ikke er overdraget til Statens It.

Kilde: Rigsrevisionen, bl.a. på baggrund af oplysninger fra Statens It.

Figur 2 indeholder 4 informationer, der er afgørende for at forstå de enkelte myndigheders ansvar.

Den første information er, at Statens It, Kriminalforsorgen og Sundhedsdatastyrelsen selv er ansvarlige for at efterleve alle 20 krav. Statens It skal her forstås som en selvstændig myndighed, der skal efterleve de tekniske minimumskrav *i egen organisation*. At disse myndigheder selv skal sikre alle 20 krav skyldes, at de ikke har overdraget it-driften og ressortansvaret til andre ministerier.

Den anden information er, at Energistyrelsen og Fødevarestyrelsen, der er kunder hos Statens It, selv er ansvarlige for at efterleve henholdsvis 7 og 8 krav. Ansvaret omfatter de systemer, der ikke er overdraget til Statens It, og krav, som kræver en beslutning eller handling fra Energistyrelsen og Fødevarestyrelsen.

Den tredje information er, at Statens It i kraft af sin rolle som leverandør skal sikre, at Energistyrelsen og Fødevarestyrelsen efterlever 13 minimumskrav. 4 af disse 13 krav overlapper med de 7 krav, som Energistyrelsen selv skal sikre efterlevelse af, og de 8 krav, som Fødevarestyrelsen selv skal sikre efterlevelse af. Derfor summer antallet af krav nederst i figuren (dvs. i den grå boks) ikke til 20.

Den fjerde information er, at Statens It samt Energistyrelsen og Fødevarestyrelsen kan indgå et samarbejde om at efterleve yderligere 4 krav. Det afhænger af, om myndighederne koordinerer. Fx fremgår det af hjælpearket, at kunderne, her Energistyrelsen og Fødevarestyrelsen, selv skal tage initiativ til at få opdateret serversoftware på de webservere, der ligger hos Statens It. Hvis myndighederne anmoder Statens It om denne opdatering, bliver det Statens It's ansvar at sikre, at opdateringen udføres.

1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier

16. Formålet med undersøgelsen er at vurdere, om de 5 udvalgte statslige myndigheder, nemlig Statens It, Kriminalforsorgen, Sundhedsdatastyrelsen, Energistyrelsen og Fødevarestyrelsen har sikret, at de efterlever de 20 tekniske minimumskrav til it-sikkerheden.

17. Første del af undersøgelsen handler om, hvorvidt de enkelte myndigheder efterlever de tekniske minimumskrav, som de selv er forpligtet til at efterleve. Vi lægger til grund, at myndigheder forvalter de systemer – som de selv er ansvarlige for – i overensstemmelse med de tekniske minimumskrav.

For at vurdere, om myndighederne efterlever kravene, undersøger vi, om myndighederne administrerer deres systemer i overensstemmelse med de enkelte krav. Kravene er således undersøgelsens revisionskriterier, dvs. det, som myndighederne skal leve op til. De 20 krav fremgår af tabel 1 og bilag 2.

18. Anden del af undersøgelsen handler om, hvorvidt Statens It og kunderne, her Energistyrelsen og Fødevarestyrelsen, efterlever de tekniske minimumskrav i henhold til den ansvarsdeling, der er aftalt mellem dem. Vi lægger til grund, at Statens It og kunderne lever op til den ansvarsbeskrivelse, der fremgår af et hjælpeark, som Statens It har sendt ud til kunderne i henholdsvis august 2020 og februar 2021. Af hjælpearket fremgår det, at Statens It automatisk skal sikre, at Energistyrelsen og Fødevarestyrelsen efterlever 13 minimumskrav for de systemer, der er overdraget til Statens It. Herudover fremgår det af hjælpearket, at Energistyrelsen og Fødevarestyrelsen kan henvende sig til Statens It vedrørende løsninger eller opdateringer, der medvirker til, at de 2 myndigheder kan efterleve yderligere 4 minimumskrav. Hvis Energistyrelsen og Fødevarestyrelsen retter henvendelse til Statens It, er Statens It ansvarlig for at bistå myndighederne med at efterleve kravene.

Automatisk
Betegnelsen automatisk betyder i denne undersøgelse, at Statens It skal håndtere de systemer, som Statens It varetager for Energistyrelsen og Fødevarestyrelsen, i overensstemmelse med de tekniske minimumskrav. Dvs. at Energistyrelsen og Fødevarestyrelsen ikke behøver at henvende sig til Statens It for at sikre efterlevelse.

For at vurdere, om Statens It og de 2 myndigheder efterlever minimumskravene i henhold til ansvarsdelingen, undersøger vi 3 forhold. For det første undersøger vi, om Statens It lever op til de 13 krav, som Statens It automatisk skal sikre på vegne af Energistyrelsen og Fødevarestyrelsen. For det andet undersøger vi, om Energistyrelsen og Fødevarestyrelsen har henvendt sig til Statens It vedrørende løsninger eller opdateringer, der kan medvirke til, at de efterlever yderligere 4 krav. For det tredje undersøger vi, om Statens It har sikret, at de bestilte løsninger eller opdateringer udføres i overensstemmelse med de tekniske minimumskrav.

Upræcise krav

19. Vi kan konstatere, at enkelte krav er formuleret upræcist, og vi har derfor været nødt til at operationalisere 4 specifikke krav. Vores operationalisering af kravene er sket ud fra en it-sikkerhedsmæssig synsvinkel og en best practice-betragtning. Vores operationalisering, herunder hvad vi lægger til grund, beskrives nedenfor.

Krav 6: Begrænset tildeling af lokaladministratorrettigheder

20. Krav 6 handler om, at myndigheden kun skal tildele lokaladministratorrettigheder tidsbegrænset og med veldokumenterede behov. Rigsrevisionen bemærker, at begreberne *tidsbegrænset* og *veldokumenterede behov* ikke er nærmere defineret i kravet. Det fremgår heller ikke af kravet, om myndigheder, der tildeler lokaladministratorrettigheder i forbindelse med en konkret jobfunktion (fx it-support) uden udløbsdato, falder ind under begrebet tidsbegrænset.

Digitaliseringsstyrelsen har oplyst, at styrelsen umiddelbart vurderer, at fx rettigheder, der er tildelt som følge af ansættelse i en konkret jobfunktion, hvor disse rettigheder er nødvendige for udførelsen af funktionen, kan betragtes som tidsbegrænsede, såfremt der er indført procedurer, som sikrer, at disse rettigheder trækkes tilbage, når den pågældende medarbejder ikke længere har den pågældende funktion.

Rigsrevisionen har endvidere forelagt Digitaliseringsstyrelsen, om en myndighed, der tildeler lokaladministratorrettigheder i forbindelse med en jobfunktion, ikke også løbende bør foretage en kompenserende kontrol af, om den pågældende medarbejder fortsat varetager sin oprindelige jobfunktion, dvs. stadig har et forretningsmæssigt behov for lokaladministratorrettighederne. Digitaliseringsstyrelsen har hertil oplyst, at det i flere tilfælde vil være fornuftigt at implementere kompenserende kontroller, men at der med krav 6 ikke stilles krav om kompenserende kontroller, og at der i kravet ikke er angivet en specifik periode for tildeling af rettigheder eller metode til, hvordan de skal administreres.

21. Det er Statens It's tolkning, at krav 6 vedrører *almindelige* brugere og dermed skal imødegå en tidligere udbredt praksis om, at *almindelige* brugere var lokaladministratorer og dermed selv kunne installere programmer på klient-pc'er – ligesom malware også let kunne installeres.

Rigsrevisionen bemærker, at Digitaliseringsstyrelsen har understreget, at det alene er kravene, som de er formuleret på sikkerdigital.dk og med yderligere fortolkning i styrelsens opfølgningsark, der gælder som krav. Se bilag 2 for opfølgningsark og formulering af kravene. Rigsrevisionen konstaterer med udgangspunkt heri, at det hverken fremgår af kravformulering eller opfølgningsark, at krav 6 (kun) er rettet mod *almindelige* brugere, og Rigsrevisionen finder derfor, at kravet også omfatter brugere, der er beskæftiget med specifikke opgaver, fx at yde it-support.

22. Rigsrevisionen lægger til grund for denne undersøgelse, at krav 6 er opfyldt, hvis lokaladministratorrettigheder bliver tildelt på baggrund af et forretningsmæssigt behov, dvs. hvis en medarbejder har behov for rettighederne til at udføre en bestemt opgave. Det kan fx være som led i sin jobfunktion som it-supporter. Rigsrevisionen lægger desuden til grund, at en jobfunktion kan udgøre en form for tidsbegrænsning.

Krav 13: Regelmæssig opdatering af mobile enheder
23. Hvad angår krav 13 om, at myndigheden skal foretage regelmæssig opdatering af operativsystem og apps på mobile enheder, lægger vi til grund, at software så vidt muligt skal opdateres, så snart leverandøren udgiver opdateringer, og at myndigheden ikke anvender versioner af operativsystemet, der indeholder kendte sårbarheder. Det har vi konkret operationaliseret som, at iPhone 6 eller ældre mobiltelefoner på revisionstidspunktet skulle være sikkerhedsopdateret til Apples version 12.5.1., mens iPhone 6s eller nyere mobiltelefoner skulle være sikkerhedsopdateret til Apples version 14.4.1. For Android-enheder var kravet minimum version 8 eller nyere.

Digitaliseringsstyrelsen har i et opfølgningsark til myndighederne om de 20 tekniske minimumskrav angivet, at kravet er opfyldt, hvis der er truffet tekniske og/eller organisatoriske foranstaltninger til at sikre regelmæssig opdatering af operativsystem (OS) og applikationer på mobile enheder. Såfremt myndighederne har anvendt denne løsning, finder Rigsrevisionen, at myndighederne bør følge op på, om de tekniske og/eller organisatoriske foranstaltninger også medfører, at der faktisk sker en regelmæssig opdatering af de mobile enheder. Center for Cybersikkerhed har i forbindelse med udarbejdelsen af denne beretning også oplyst, at såfremt medarbejdere pålægges at foretage opdateringerne, bør det verificeres, at dette finder sted.

Krav 15: Logning
24. Hvad angår krav 15 om, at myndigheden skal sikre logning, og hvor der ikke stilles krav om, hvor lang tid en log skal gemmes, lægger Rigsrevisionen i revisionskriteriet til grund, at 30 dage er for kort en periode at gemme en log i. Præciseringen udledes af, at Center for Cybersikkerhed – i den vejledning, som kravet følger af – skriver, at der ofte kan gå uger og måneder fra et angreb sker, til det bliver opdaget. Center for Cybersikkerhed har oplyst, at Center for Cybersikkerhed er enig i Rigsrevisionens vurdering, selv om kravet ikke nævner noget om, hvor længe logs skal opbevares.

Krav 18: Kryptering af kommunikation til hjemmesider
25. Hvad angår krav 18 om, at myndigheden skal sikre, at kommunikation til hjemmesider krypteres, og at der som minimum anvendes TLS 1.2, dvs. der skal implementeres https på alle hjemmesider, har Rigsrevisionen måttet operationalisere, hvad en hjemmeside er. Behovet for operationalisering skyldes, at der har været drøftelser med de reviderede om, hvad en hjemmeside reelt er. Rigsrevisionen definerer hjemmesider som alle internet-tilgængelige tjenester, der svarer på http- eller https-forespørgsler. Rigsrevisionen finder således, at selv om der kun er minimalt indhold på en hjemmeside, fx en placeholder, der viser, hvem der ejer hjemmesiden, så er hjemmesiden omfattet af kravet om kryptering.

Placeholder
En placeholder er en midlertidig information, som sættes ind på en hjemmeside, så den ikke fremstår tom. Det kan fx være et logo, et billede eller en angivelse af, hvem der ejer hjemmesiden.

Center for Cybersikkerhed har oplyst, at de er enige med Rigsrevisionen i, at alle hjemmesider skal have implementeret https, også selv om der kun er indsat en placeholder på dem. Center for Cybersikkerhed fortolker således hjemmesider, som alle internet-tilgængelige tjenester med et visuelt indhold, der svarer på http- eller https-forespørgsler. Http-/https-baserede API'er, der ikke returnerer visuelt indhold, kan ifølge Center for Cybersikkerhed dårligt falde ind under begrebet hjemmeside, men bør ligeledes kun udveksle indhold over en https-krypteret forbindelse. Center for Cybersikkerhed har videre anført, at en blank hjemmeside eller en hjemmeside, hvor der er indsat en placeholder, vil kunne manipuleres undervejs, såfremt forbindelsen ikke er krypteret. En ondsindet aktør vil derfor have mulighed for at inkludere ondsindet indhold eller links dertil under myndighedens navn.

Metode

26. Undersøgelsen bygger på 5 it-revisioner, som Rigsrevisionens kontor for it-revision har gennemført i perioden marts-september 2021. Undersøgelsens resultater og konklusioner baserer sig på revisionsbeviser, som vi har indhentet via it-revisionerne. Vi har bl.a. gennemgået systemopsætninger og konfigurationer samt retningslinjer og politikker for tildeling af rettigheder og for opdatering af mobiltelefoner. Vi har taget udgangspunkt i systemværktøjer og udtaget stikprøver med henblik på at teste, om myndighederne har implementeret eller foretaget en række sikkerhedshandlinger, fx har sikret, at der anvendes numerisk adgangskode på min. 6 cifre eller biometrisk identifikation. En mere detaljeret gennemgang af vores metode fremgår af bilag 1.

27. Vi har holdt møder med Center for Cybersikkerhed og Digitaliseringsstyrelsen, der begge har været med til at udforme de tekniske minimumskrav. På møderne har vi bl.a. drøftet, hvilke sikkerhedsmæssige handlinger der skal til, for at en myndighed efterlever de tekniske minimumskrav. Drøftelserne har indgået i vores vurdering af, hvilke betingelser der skal være opfyldt for, at en myndighed kan siges at efterleve minimumskravene.

28. I vores vurdering af, om myndighederne efterlever kravene, lægger vi vægt på 2 forhold. Det første forhold er, at alle klienter (fx pc'er), mobile enheder, hjemmesider mv. skal leve op til minimumskravene. Det betyder, at hvis 1 pc ud af mange pc'er ikke er håndteret i overensstemmelse med et krav, vurderer vi, at myndigheden ikke efterlever kravet. Det skyldes, at kravene omfatter alle pc'er, hjemmesider mv. hos myndighederne, og derfor kan der ikke være en gradvis efterlevelse af kravene. Det andet forhold er, at vi ikke har vægtet de 20 krav indbyrdes, dvs. prioriteret nogle krav som mere væsentlige end andre. Det skyldes, at alle er minimumskrav, der bør være efterlevet.

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

Afgrænsning

30. Undersøgelsen omhandler 5 samfundsvigtige myndigheders efterlevelse af de 20 tekniske minimumskrav til it-sikkerheden. Vi har vurderet en myndighed som samfundsvigtig, hvis den er kendetegnet ved ét af følgende 2 forhold. Det første forhold er, at myndigheden råder over systemer, der understøtter vigtige opgaver. I denne undersøgelse råder størstedelen af myndighederne over systemer, der understøtter vigtige opgaver inden for energi, fødevarer, statslig it-drift og sundhed. Det andet forhold er, at myndigheden råder over følsomme oplysninger om borgere. I denne undersøgelse råder Sundhedsdatastyrelsen over sundhedsdata, mens Kriminalforsorgen råder over oplysninger om kriminalitet, efterforskning mv.

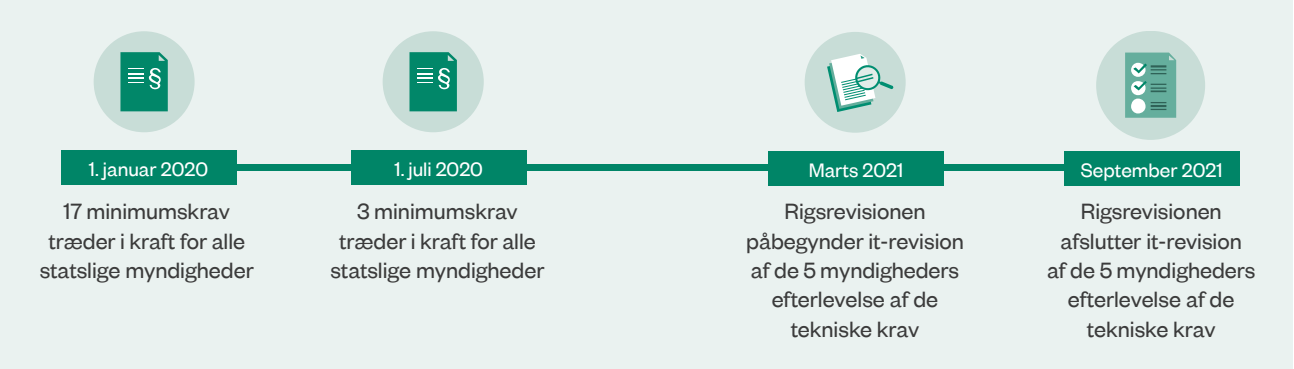
Med hensyn til Sundhedsdatastyrelsen som undersøgelsesområde har Sundhedsministeriet bemærket, at Rigsrevisionens revision i praksis har omfattet hele Sundhedsministeriets koncern, fordi Sundhedsdatastyrelsen er koncern it-funktion for hele ministerområdet med undtagelse af Lægemiddelstyrelsen. Sundhedsministeriet har videre oplyst, at styrelsens sundhedsdata imidlertid er beskyttet ud over den sikkerhed, som de 20 minimumskrav adresserer, samtidig med at en stor del af data håndteres i eksterne datacentre, der ligeledes har høje krav til sikkerhed. Rigsrevisionen har ikke undersøgt, om styrelsens sundhedsdata er beskyttet ud over den sikkerhed, som de 20 minimumskrav adresserer, da denne beretning omhandler myndighedernes efterlevelse af minimumskravene.

31. Efterlever en myndighed de 20 tekniske minimumskrav, vil det alt andet lige styrke den basale it-sikkerhed, men det er ikke i sig selv et udtryk for, at myndigheden har en høj it-sikkerhed. En høj it-sikkerhed kræver således mere end efterlevelsen af de 20 tekniske minimumskrav, og efterlevelsen af minimumskravene fritager ikke myndighederne for at foretage egne risikovurderinger og eventuelt implementere yderligere sikkerhedstiltag i relevant omfang for at beskytte data og systemer bedst muligt.

Vi har ikke undersøgt, om – eller i hvilken grad – de risici, som manglende efterlevelse af kravene medfører, kan udnyttes af ondsindede aktører, idet eventuelle mitigerende tiltag hos myndighederne ikke er blevet undersøgt.

32. Undersøgelsesperioden omfatter januar 2020 - september 2021. Perioden dækker fra, hvornår kravene skulle være efterlevet, til revisionstidspunktet, dvs. 1-1½ år efter frist for efterlevelse. 17 minimumskrav skulle være efterlevet fra den 1. januar 2020, og de sidste 3 krav fra den 1. juli 2020. Figur 3 viser undersøgelsesperioden.

Figur 3
Undersøgelsesperioden



Note: De 3 minimumskrav, som trådte i kraft den 1. juli 2020, var krav 6 om begrænset tildeling af lokaladministratorrettigheder, krav 11 om DMARC REJECT-policy på domæner og krav 19 om Flash.

Kilde: Rigsrevisionen.

Som det fremgår af figur 3, har vi afsluttet vores it-revision af de 5 myndigheders efterlevelse af minimumskravene i september 2021. Undersøgelsen tegner derfor et øjebliksbillede af myndighedernes efterlevelse af minimumskravene.

33. I bilag 1 er undersøgelsens metodiske tilgang beskrevet. Bilag 2 viser Digitaliseringsstyrelsens opfølgningsark til myndighederne. Bilag 3 viser myndighedernes efterlevelse af minimumskravene. Bilag 4 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. De 5 myndigheders efterlevelse af de 20 tekniske minimumskrav

34. Dette kapitel handler om, hvorvidt de 5 samfundsvigtige myndigheder har sikret, at de efterlever de 20 tekniske minimumskrav til it-sikkerheden. Vi har undersøgt:

- om den enkelte myndighed efterlever de tekniske minimumskrav, som myndigheden selv er forpligtet til at efterleve
- om Statens It og kunderne, her Energistyrelsen og Fødevarestyrelsen, efterlever de tekniske minimumskrav i henhold til den ansvarsdeling, der er aftalt mellem dem.

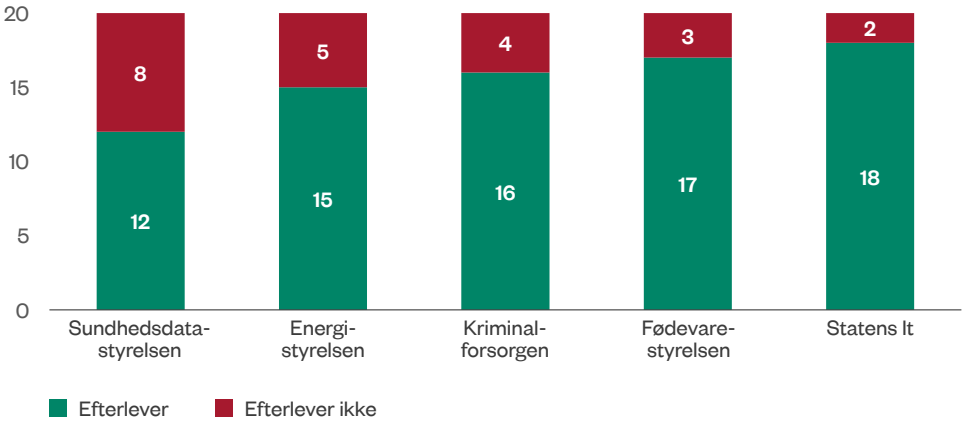
2.1. Myndighedernes eget ansvar

35. Vi har undersøgt, om de 5 myndigheder efterlever de tekniske minimumskrav, som de selv er forpligtet til at efterleve, dvs. hvor ansvaret ikke ligger hos Statens It eller er delt med Statens It.

I dette afsnit behandler vi udelukkende Statens It som en selvstændig myndighed, der *i egen organisation* skal sikre, at de 20 minimumskrav bliver efterlevet.

36. Figur 4 viser overordnet status for efterlevelsen af de 20 tekniske minimumskrav hos de 5 myndigheder. Bilag 3 indeholder en detaljeret oversigt over, hvilke minimumskrav de enkelte myndigheder efterlever.

Figur 4
Myndighedernes efterlevelse af de 20 minimumskrav på revisionstidspunktet



Kilde: Rigsrevisionen.

Det fremgår af figur 4, at ingen af de 5 myndigheder på revisionstidspunktet (sommer/efterår 2021) efterlever alle de tekniske minimumskrav til it-sikkerheden, selv om 17 minimumskrav skulle være efterlevet fra den 1. januar 2020, og de resterende 3 krav skulle være efterlevet fra den 1. juli 2020. Sundhedsdatastyrelsen efterlever 12 krav, Energistyrelsen efterlever 15 krav, Kriminalforsorgen efterlever 16 krav, mens Fødevarestyrelsen efterlever 17 krav, og Statens It efterlever 18 krav.

Energistyrelsens og Fødevarestyrelsens efterlevelse, som er vist i figuren, er et resultat af de 2 myndigheders egne indsatser og af Statens It's indsats som leverandør. I det følgende beskriver vi her i afsnit 2.1 alene de minimumskrav, som Energistyrelsen og Fødevarestyrelsen selv er ansvarlige for at efterleve, dvs. hvor Statens It ikke har en rolle, mens vi i afsnit 2.2 beskriver ansvarsdelingen og koordinationen med Statens It i forhold til at sikre, at en delmængde af minimumskravene efterleves.

Undersøgelsen viser, at Energistyrelsen selv har ansvar for at sikre 7 minimumskrav, mens Fødevarestyrelsen selv har ansvar for at sikre 8 minimumskrav. Energistyrelsen efterlever 3 ud af de 7 krav, og Fødevarestyrelsen efterlever 5 ud af de 8 krav. Bilag 3 indeholder en gennemgang af, hvilke minimumskrav Energistyrelsen og Fødevarestyrelsen selv har ansvar for at efterleve, herunder hvilke krav de ikke efterlever.

37. Vi har efter it-revisionerne informeret de 5 myndigheder om, hvilke minimumskrav der ikke er efterlevet. I forlængelse heraf har vi undersøgt, om de 5 myndigheder har en plan for implementeringen af de udestående krav.

Vi kan konstatere, at 4 ud af de 5 myndigheder har en plan for implementeringen af de krav, som de ikke efterlever. Statens It har oplyst, at Statens It i stedet for handleplaner vil udarbejde risikovurderinger, men at disse risikovurderinger ikke er gennemført endnu. Statens It har videre oplyst, at Statens It vil vurdere relevansen af en risikovurdering, når Statens It har haft en afklarende dialog med Digitaliseringsstyrelsen, der fastsætter reglerne på området.

Krav, alle myndigheder skal efterleve

38. Dette afsnit handler om efterlevelsen af de tekniske minimumskrav, som alle 5 myndigheder selv skal sikre efterlevelse af, dvs. at Energistyrelsen og Fødevarestyrelsen indgår for de krav, som de selv har ansvaret for.

39. Tabel 2 viser 5 krav, som én eller flere myndigheder ikke efterlever, og hvilke konsekvenser det har, når de ikke gør.

Tabel 2
Krav og konsekvenser: Alle 5 myndigheder

Minimumskrav	Myndigheder, der ikke efterlever	Konsekvenser
Krav 13. Regelmæssig opdatering af mobile enheder	●●●●● Alle 5 myndigheder	• Risiko for, at sikkerhedshuller udnyttes af ondsindede aktører, fx ved at de bryder ind og får adgang til data, eller ved at de installerer ondsindet software, som kan bruges til aflytning ved hjælp af en mobiltelefons kamera og mikrofon.
Krav 18. Kryptering af kommunikation til hjemmesider	●●●●● Statens It Sundhedsdatastyrelsen Energistyrelsen Fødevarestyrelsen	• Risiko for, at en ondsindet aktør får adgang til alt, hvad der foregår på forbindelsen (fx filer og tekst). • Risiko for, at myndighedens data kan blive ændret (dataintegritet), eller at andre kan få kendskab til fortrolige data.
Krav 11. DMARC REJECT-policy på domæner	●●●●● Kriminalforsorgen Sundhedsdatastyrelsen Energistyrelsen	• Risiko for, at en afsender udgiver sig for at være den pågældende myndighed, fx i mails til medarbejdere eller borgere.
Krav 8. Godkendte mail-relays med autentifikation	●●●● Energistyrelsen	• Risiko for kompromittering af mailsikkerheden, da ondsindede aktører kan udgive sig for at være myndigheden. • Risiko for, at mail-server kan misbruges til spredning af malware og spam.
Krav 20. Regelmæssig opdatering af webservere	●●●● Fødevarestyrelsen	• Risiko for, at ondsindede aktører udnyttet offentligt kendte sårbarheder i serversoftwaren.

● Angiver, hvor mange myndigheder der ikke opfylder kravet. ● Angiver, hvor mange myndigheder der opfylder kravet.

Note: Fødevarestyrelsen har ikke ansvar for at efterleve minimumskrav 8, da styrelsen anvender en løsning fra Statens It. Statens It's efterlevelse af minimumskrav 8 på vegne af Fødevarestyrelsen behandles i beretningens afsnit 2.2.

Energistyrelsens efterlevelse af minimumskrav 20 afhænger af, om Energistyrelsen anmoder Statens It om opdatering af webserve re. Dette forhold behandles i beretningens afsnit 2.2.

Kilde: Rigsrevisionen.

Det fremgår af tabel 2, at ingen af de 5 myndigheder efterlever minimumskrav 13, og at flertallet af myndighederne ikke efterlever minimumskrav 18 og 11. Energistyrelsen er desuden ikke i mål i med at efterleve minimumskrav 8, mens Fødevarestyrelsen ikke efterlever minimumskrav 20.

Manglende efterlevelse af minimumskrav 13: Regelmæssig opdatering af mobile enheder

40. Minimumskrav 13 omhandler, at myndigheden skal foretage regelmæssig opdatering af operativsystem og apps på mobile enheder, og at formålet er, at software så vidt muligt skal opdateres, så snart leverandøren udgiver opdateringer. Vi har derfor lagt til grund for undersøgelsen, at myndighederne ikke anvender versioner af operativsystemet, der indeholder kendte sårbarheder. Det har vi konkret operationaliseret til at:

- iPhone 6 eller ældre mobiltelefoner skulle på revisionstidspunktet være sikkerhedsopdateret til Apples version 12.5.1., mens iPhone 6s eller nyere mobiltelefoner skulle være sikkerhedsopdateret til Apples version 14.4.1. For Android-enheder var kravet minimum version 8 eller nyere.

Som det også fremgår af afsnittet om revisionskriterier, har Digitaliseringsstyrelsen i et opfølgningsark til myndighederne om de 20 tekniske minimumskrav angivet, at kravet er opfyldt, hvis der er truffet tekniske og/eller organisatoriske foranstaltninger til at sikre regelmæssig opdatering af operativsystem (OS) og applikationer på mobile enheder. Såfremt myndighederne har anvendt denne løsning, finder Rigsrevisionen, at myndighederne bør følge op på, om de tekniske og/eller organisatoriske foranstaltninger også medfører, at der faktisk sker en regelmæssig opdatering af de mobile enheder.

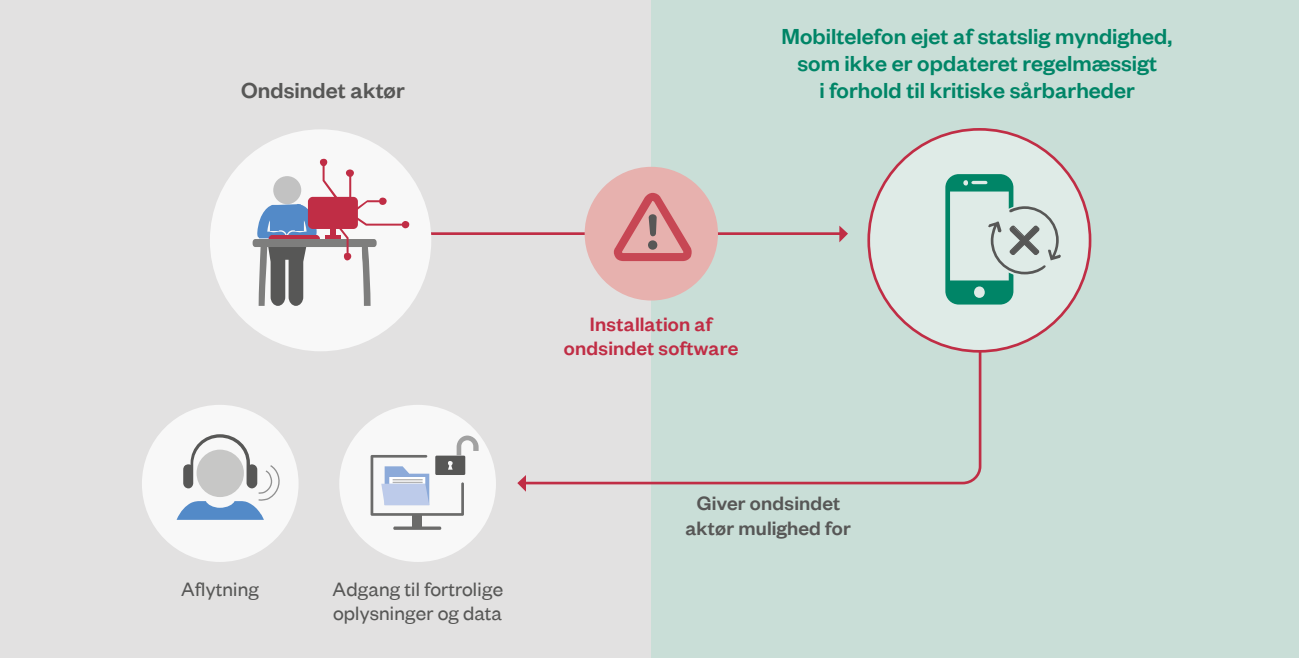
41. Vores undersøgelse viser, at ingen af myndighederne efterlever minimumskrav 13, da alle 5 myndigheder har mobile enheder, der ikke er opdaterede, og dermed har software, der indeholder kendte sikkerhedshuller eller sårbarheder. Vi kan således konstatere, at kun en mindre andel af enhederne var blevet opdateret til version 14.4.1 fra Apple, som lukker en kendt og kritisk sårbarhed.

42. Statens It har oplyst, at Statens It ikke deler Rigsrevisionens opfattelse af, at det skulle udgøre en sikkerhedsrisiko at anvende iPhones og iPads, der anvender IOS-versioner ældre end version 14 (fx iPhone 6), når blot de ældre versioner af operativsystemet er opdateret til senest frigivne version fra Apple (fx version 12.5.1.). Statens It bemærker i den sammenhæng, at det ikke fremgår af de tekniske minimumskrav, at man skal anvende det seneste operativsystem (p.t. IOS 15) frigivet fra producenten, men det blot fremgår, at: *"Mobiltelefoners software skal så vidt muligt opdateres, så snart leverandøren udgiver opdateringer"*.

Rigsrevisionen bemærker, at Statens It hverken lever op til Rigsrevisionens operationalisering eller Statens It's egen fortolkning af minimumskrav 13. Statens It havde på revisionstidspunktet 16 ud af 79 aktive iPhone 6, der ikke var blevet sikkerhedsopdateret til version 12.5.1. Undersøgelsen viste endvidere, at Statens It kun havde 118 ud af 328 iPhone 6s eller nyere mobiltelefoner, der var blevet opdateret til version 14.4.1, som lukker en kendt sårbarhed, og som på revisionstidspunktet var senest frigivne sikkerhedsopdatering for iPhone 6s eller nyere mobiltelefoner. Statens It havde desuden 33 Android-enheder, hvoraf 1 ikke var supporteret med sikkerhedsopdateringer.

43. Figur 5 viser, at en ondsindet aktør kan udnytte sikkerhedshuller i enten operativsystemet eller i apps på en mobiltelefon, og herved få mulighed for aflytning via mobiltelefonen eller opnå adgang til fortrolige oplysninger.

Figur 5
Cyberangreb på en mobiltelefon ejet af myndigheden



Kilde: Rigsrevisionen.

44. Statens It har oplyst, at Statens It's data enten kan tilgås via en statsligt udleveret tjenestetelefon eller ved at tillade, at private telefoner tilgår data. I begge tilfælde sker adgang til data via en såkaldt Mobile Device Management-løsning (MDM-løsning). Rigsrevisionen kan konstatere, at Statens It's data således tilgås via en app på mobiltelefonen. Undersøgelsen viser ligeledes, at Energistyrelsen, der er kunde hos Statens It, anvender samme MDM-løsning til at kryptere arbejdsinformationer.

Rigsrevisionen bemærker, at MDM-løsninger mindsker risikoen for, at sikkerhedshuller i operativsystem kan udnyttes og dermed kompromittere det data, som ligger i appen, men at appen ikke krypterer indhold, som ligger uden for appen, fx mobiltelefonens mikrofon, sms-beskeder mv., og derfor er regelmæssig sikkerhedsopdatering af mobiltelefoner nødvendig. Rigsrevisionen bemærker desuden, at formålet med kravet er, at kendte sikkerhedshuller lukkes hurtigst muligt.

Statens It har videre oplyst, at Statens It ikke har opsat MDM til at tvangsopdatere alle telefoner, da denne funktion ifølge Statens It ikke er mulig. Statens It bemærker, at det kun er muligt at få telefonen til at undersøge, om der er opdateringer, og notificere brugeren herom. Hertil kommer, at funktionaliteten kræver, at telefonen er i såkaldt supervised mode, hvilket for privatejede telefoner ikke er en mulighed. Statens It har oplyst, at Statens It vil styrke awareness om behov for opdatering ved at udnytte en funktionalitet, der gør, at alle telefoner i Statens It's MDM-løsning vil give brugeren en daglig mail om at opdatere telefonen. Dette gælder også for private telefoner, som er i Statens It's MDM-løsning. Ifølge Statens It vil gevinsten dog være marginal risikomæssigt.

Endelig har Statens It oplyst, at formålet med kravet – at beskytte data – i dag er opfyldt med anvendelsen af MDM. Rigsrevisionen bemærker, at formålet med krav 13 er følgende: *"Mobiltelefoners software skal så vidt muligt opdateres, så snart leverandøren udgiver opdateringer. Derved sikres, at kendte sikkerhedshuller lukkes hurtigst muligt"*. Formålet fremgår af senest opdaterede kravliste af 30. november 2019, som ligger på sikkerdigital.dk, som bl.a. drives af Digitaliseringsstyrelsen. Rigsrevisionen finder derfor ikke, at formålet med kravet er opfyldt ved, at Statens It anvender en MDM-løsning.

45. Energistyrelsen har oplyst, at tvungen sikkerhedsopdatering ikke er en aktiveret funktionalitet i Statens It's MDM-løsning, og at Energistyrelsen derfor via styrelsens intranet har gjort sine brugere opmærksomme på, at mobiltelefonerne skal opdateres regelmæssigt.

Rigsrevisionen finder, som nævnt ovenfor og jf. afsnittet om revisionskriterier, at såfremt medarbejdere pålægges at foretage opdateringerne, bør myndigheden følge op på, at opdateringerne finder sted.

46. Kriminalforsorgen har oplyst, at der i vejledningen, som ligger til grund for krav 13, er nævnt 3 mulige løsninger til at holde mobile enheder opdaterede. De 3 løsninger bliver kaldt *god*, *bedre* og *bedst*. Løsningen *god* har centraladministrationens embedsfolk som målgruppe, mens *bedre* og *bedst* kræver, at myndighedens it-afdeling kontrollerer, at kritiske opdateringer installeres eller håndhæver installation gennem en MDM-løsning. Kriminalforsorgen har i sine retningslinjer vedrørende databeskyttelse og informationssikkerhed beskrevet, at medarbejderne skal opdatere mobile enheder, når der udgives nye opdateringer, dvs. en løsning, som Kriminalforsorgen har oplyst er i overensstemmelse med løsningen *god* i vejledningen.

Mobile Device Management (MDM)
En MDM-løsning gør det muligt at styre mobile enheder centralt fra ét system, fx vil en it-afdeling med denne løsning kunne nægte en medarbejder adgang til sin mobiltelefon, indtil vedkommende installerer en opdatering. En MDM-løsning indeholder desuden muligheden for, at medarbejderen kun kan tilgå arbejdsmail via en app (fx Capsule). Denne app kan kryptere indhold i de apps, der styres via MDM, fx arbejdsmail, selv om mobiltelefonen ikke er regelmæssigt opdateret. Appen krypterer dog ikke indhold, som ligger uden for appen, fx mobiltelefonens mikrofon, sms-beskeder mv.

Den vejledning, som Kriminalforsorgen henviser til i forhold til krav 13, er udarbejdet af Center for Cybersikkerhed. Vejledningen hedder "Råd om sikkerhed på mobile enheder" og er fra november 2018. Vejledningen beskriver bl.a. 3 niveauer (*god*, *bedre* og *bedst*) for mobilsikkerhed.

Rigsrevisionen bemærker, at det er kravteksten, som er gældende, og ikke de vejledninger, som kravet følger af. Rigsrevisionen vurderer desuden, at løsningen *god* ikke er tilstrækkelig for Kriminalforsorgen, idet Kriminalforsorgen råder over følsomme oplysninger om borgere og dermed bør gøre mere for at sikre, at mobile enheder opdateres regelmæssigt. Det er, jf. afsnittet om revisionskriterier, både Rigsrevisionens og Center for Cybersikkerheds vurdering, at såfremt medarbejdere pålægges at foretage opdateringerne, bør myndigheden følge op på, at opdateringerne finder sted.

Rigsrevisionen kan konstatere, at Kriminalforsorgen på revisionstidspunktet havde 321 Apple-enheder, hvoraf kun 30 enheder anvendte version 14.4.1. Desuden havde Kriminalforsorgen 186 Android-enheder, hvoraf 13 ikke var supporteret med sikkerhedsopdateringer. Rigsrevisionen konstaterer, at det øger risikoen for, at sikkerhedshuller på mobile enheder kan udnyttes og dermed give direkte adgang til data fra fx Kriminalforsorgens arbejdsmail. Det er således Rigsrevisionens vurdering, at Kriminalforsorgens retningslinjer ikke er tilstrækkelige til at sikre efterlevelse af krav 13, da retningslinjerne ikke har ført til regelmæssig opdatering af mobile enheder. Rigsrevisionen finder desuden, at Kriminalforsorgens løbende opfølgning er mangelfuld.

47. Rigsrevisionen må generelt konstatere, at efterlevelsen af krav 13 er vanskelig for myndighederne, bl.a. fordi der ofte, sådan som de mobile enheder anvendes i dag, findes indhold af både arbejdsmæssig og privat karakter på de mobile enheder – hvilket giver udfordringer i forhold til, hvad og hvordan en myndighed kan/må kontrollere.

Rigsrevisionen anbefaler derfor, at Finansministeriet sikrer, at det overvejes, hvordan krav 13 skal udformes for at give den sikkerhed, der er tiltænkt.

Manglende efterlevelse af minimumskrav 18: Kryptering af kommunikation til hjemmesider

48. Minimumskrav 18 omhandler, at kommunikation til hjemmesider skal krypteres og anvende minimum TLS 1.2, dvs. der skal implementeres https på alle hjemmesider. Rigsrevisionen har i den henseende måttet operationalisere, hvad en hjemmeside er, da der ikke har været enighed med bl.a. Statens It herom. Rigsrevisionen definerer hjemmesider som alle internet-tilgængelige tjenester, der svarer på http- eller https-forespørgsler. Rigsrevisionen finder således, at selv blanke hjemmesider eller hjemmesider med minimalt indhold (fx en placeholder der viser, hvem der ejer domænet) skal have implementeret https.

49. Undersøgelsen viser, at 4 ud af de 5 myndigheder ikke efterlever minimumskrav 18, og at der er forskellige årsager hertil.

Statens It og Sundhedsdatastyrelsen efterlever den del af kravet, der omhandler brug af TLS 1.2., men begge myndigheder har hjemmesider, hvor https ikke er slået til. Vi kan konstatere, at begge myndigheder har nogle hjemmesider, der tilsyneladende ikke anvendes, men samtidig ikke er tomme for indhold, da der er indsat en placeholder på dem.

TLS 1.2
Transport Layer Security (TLS) er en protokol, der muliggør kryptering af følsomme oplysninger i forbindelse med datakommunikation over internetprotokollen (fx via internettet og lokalnet). Herudover sikrer kryptering data mod uønsket ændring under transporten (dataintegritet).

Http/https
Http er den protokol, der anvendes til at sende hjemmesider over internettet.

Https er den protokol, der krypterer data på hjemmesider, der sendes over internettet. Https forhindrer dermed, at data bliver opfanget og ændret af en ondsindet aktør.

I forhold til hjemmesiderne med placeholdere, har Statens It oplyst, at Statens It på vegne af kunderne og for egen organisation administrerer et antal domæner, som ikke er i aktivt brug på internettet. Skrives domænenavnet, når man en ukrypteret side, som viser, at domænet ejes af Statens It, og der er et link til Statens It's officielle hjemmeside. Ifølge Statens It er der således intet beskyttelsesværdigt indhold på siden. Statens It har anført, at de hjemmesider, som kritiseres for manglende overholdelse, alle er *tomme hjemmesider uden indhold*, og at der på revisionstidspunktet eller efterfølgende ikke har været konstateret hjemmesider med kundernes data, som ikke var beskyttet.

Rigsrevisionen bemærker, at en hjemmeside, hvor der er indsat en placeholder, vil kunne manipuleres undervejs, såfremt forbindelsen ikke er krypteret. En ondsindet aktør vil derfor have mulighed for at inkludere ondsindet indhold eller links dertil under myndighedens navn. Denne sårbarhed er Center for Cybersikkerhed enig med Rigsrevisionen i. Rigsrevisionen bemærker desuden, at hvis en hjemmeside ikke er helt tom (fx har en placeholder), vil der kunne ligge andre aktive sider, som ikke er direkte synlige, men som potentielt kan indeholde fortrolige oplysninger, og som uden implementering af https vil blive sendt u-krypteret over internettet.

Center for Cybersikkerhed har desuden oplyst, at alle internet-tilgængelige tjenester med et visuelt indhold, der svarer på http- eller https-forespørgsler, bør have implementeret https. Det samme gælder http/https-baserede API'er, der ikke returnerer visuelt indhold. På den baggrund er Rigsrevisionen ikke enig med Statens It i, at der er tale om tomme hjemmesider uden indhold.

50. Undersøgelsen viser videre, at Energistyrelsen og Fødevarestyrelsen ikke efterlever minimumskrav 18 i forhold til hjemmesider, som ligger hos en anden leverandør end Statens It. En stikprøve har vist, at Energistyrelsen ikke har sikret TLS 1.2. på 10 hjemmesider. En stikprøve hos Fødevarestyrelsen har vist, at styrelsen ikke har implementeret https på 5 hjemmesider, og desuden har 1 hjemmeside, der ikke overholder kravet om tvungen TLS 1.2.

51. Rigsrevisionen anbefaler – i lyset af uklarheden om, hvad en hjemmeside er – at Finansministeriet sikrer, at begrebet *hjemmeside* defineres, så der ikke er tvivl om indholdet i krav 18.

Manglende efterlevelse af minimumskrav 11: DMARC REJECT-policy på domæner

52. 3 ud af de 5 myndigheder har ikke implementeret DMARC REJECT-policy på alle domæner, som myndighederne ejer. De 3 myndigheder er Kriminalforsorgen, Sundhedsdatastyrelsen og Energistyrelsen. Det muliggør, at en udefrakommende afsender kan udgive sig for at være myndigheden i mails til medarbejdere eller borgere, fx udgive sig for at være chef eller direktør og anmode medarbejdere om at betale fakturaer uretmæssigt eller udlevere fortrolige oplysninger.

DMARC REJECT-policy
Opsætning af en DMARC REJECT-policy sikrer, at ondsindede mails med forfalsket afsenderadresse kan identificeres og eventuelt blokeres hos modtageren.

Energistyrelsen har oplyst, at Rigsrevisionens revision viser, at det er 2 ud af 58 domæner, hvor DMARC REJECT-policy ikke var blevet implementeret korrekt. Rigsrevisionen kan konstatere, at kravet omfatter alle domæner, hvorfor kravet ikke er efterlevet, selv om langt størstedelen af Energistyrelsens domæner har fået implementeret DMARC REJECT-policy.

Manglende efterlevelse af minimumskrav 8: Godkendte mail-relays med autentifikation

53. Energistyrelsen efterlever ikke krav 8, da styrelsen ikke har sikret, at der kun anvendes mail-relays med autentifikation godkendt af Energistyrelsen. Energistyrelsen har oplyst, at der er tale om 1 ud af 58 domæner og subdomæner. Rigsrevisionen kan konstatere, at kravet omfatter alle domæner og har til formål at forhindre, at ondsindede aktører udgiver sig for at være Energistyrelsen i mails. Kravet skal også forhindre, at mailserveren kan misbruges til at sprede ondsindet software og spam.

Manglende efterlevelse af minimumskrav 20: Regelmæssig opdatering af webservere

54. Fødevarestyrelsen efterlever ikke minimumskrav 20, da styrelsen ikke har sikret regelmæssig opdatering af webservere. Rigsrevisionen kan konstatere, at manglende efterlevelse af kravet medfører en risiko for, at ondsindede aktører udnytter offentligt kendte sårbarheder i softwaren på webserveren.

Særligt vedrørende minimumskrav 6: Begrænset tildeling af lokaladministratorrettigheder

55. Minimumskrav 6 omhandler, at myndigheden kun skal tildele lokaladministratorrettigheder tidsbegrænset og med veldokumenterede behov.

Undersøgelsen viser, at alle 5 myndigheder efterlever krav 6, da de har tildelt lokaladministratorrettigheder til specifikke jobfunktioner, fx inden for it-support, som alle har et forretningsmæssigt behov for rettighederne. Rigsrevisionen lægger ved vurderingen til grund, at en jobfunktion kan udgøre en form for tidsbegrænsning. Rigsrevisionen kan endvidere konstatere, at alle 5 myndigheder opretter separate konti til de medarbejdere, der er it-supportere, og dermed har fået tildelt lokaladministratorrettigheder i forbindelse med deres jobfunktion. Rigsrevisionen vurderer, at brug af en separat konto til lokaladministratorrettigheder mindsker risikoen for utilsigtede hændelser.

56. Rigsrevisionen kan imidlertid konstatere, at det ikke fremgår tydeligt af krav 6, hvad der ligger i henholdsvis *tidsbegrænset* og *veldokumenterede behov*, ligesom der heller ikke i formuleringen af kravet tages stilling til, om lokaladministratorrettighederne tildeles ad hoc eller til medarbejdere med jobfunktioner, der kræver lokaladministratorrettigheder (fx it-support).

Digitaliseringsstyrelsen har oplyst, at styrelsen umiddelbart vurderer, at fx rettigheder, der er tildelt som følge af ansættelse i en konkret jobfunktion, hvor disse rettigheder er nødvendige for udførelsen af funktionen, kan betragtes som tidsbegrænsede, såfremt der er indført procedurer, som sikrer, at rettighederne trækkes tilbage, når den pågældende medarbejder ikke længere har den pågældende funktion.

Rigsrevisionen kan videre konstatere, at Digitaliseringsstyrelsen har angivet, at det alene er kravene, som de er formuleret på sikkerdigital.dk og med yderligere fortolkning i styrelsens opfølgningsark, der gælder som krav. Det fremgår af opfølgningsarket (bilag 2), at kravet er opfyldt, hvis der er truffet organisatoriske foranstaltninger med eventuel teknisk understøttelse, der sikrer, at administrative rettigheder på klienter med adgang til myndighedens arbejdsnetværk kun tildeles tidsbegrænset og med veldokumenteret behov.

Rigsrevisionen anbefaler på den baggrund, at Finansministeriet bør sikre, at krav 6 præciseres, så det tydeligt fremgår, hvad der udgør en tidsbegrænsning og et veldokumenteret behov, herunder hvilke medarbejdere kravet omfatter. Rigsrevisionen anbefaler endvidere, at Finansministeriet overvejer, om der i de tilfælde, hvor en medarbejder anvender adgangen som led i sin jobfunktion, bør stilles krav om, at myndighederne skal supplere med en kompenserende kontrol, fx udføre regelmæssig kontrol af brugerens rettigheder og kontrollere brugerens handlinger ved at gennemgå en log.

57. Undersøgelsen viser, at Statens It har en serviceportal, som både Statens It og Energistyrelsen og Fødevarestyrelsen anvender, når der skal tildeles lokaladministratorrettigheder. Rigsrevisionen kan konstatere, at det systemmæssigt ikke er muligt at definere en udløbsperiode for de lokaladministratorrettigheder, der tildeles til interne brugere (dvs. myndighedernes egne medarbejdere). Det er udelukkende eksterne brugere (fx konsulenter udefra), der systemmæssigt kan oprettes tidsbegrænset. Rigsrevisionen finder, at Statens It burde have etableret en bedre systemunderstøttelse af tildeling af lokaladministratorrettigheder, da Statens It er statens interne it-driftsorganisation, som servicerer 19 ministerområder.

Krav, som de myndigheder, der ikke er kunder hos Statens It, skal efterleve

58. Statens It, Kriminalforsorgen og Sundhedsdatastyrelsen er ikke kunder hos Statens It. Derfor har de ansvar for at efterleve en række minimumskrav, som Energistyrelsen og Fødevarestyrelsen ikke har.

Tabel 3 viser de krav, som alene Statens It, Kriminalforsorgen og Sundhedsdatastyrelsen har ansvar for at sikre. Tabellen viser, hvilke krav de 3 myndigheder ikke efterlever, og hvilke konsekvenser det kan have.

Tabel 3

Krav og konsekvenser: Myndigheder, der ikke er kunder hos Statens It

Minimumskrav	Myndigheder, der ikke efterlever	Konsekvenser ved ikke at efterleve krav
Krav 5. Regelmæssig opdatering af klienter	●●● Kriminalforsorgen Sundhedsdatastyrelsen	• Risiko for, at en ondsindet aktør udnytter kendte sårbarheder i applikationer til at kompromittere data.
Krav 7. Sikkerhedsopdateret operativsystem	●●● Kriminalforsorgen Sundhedsdatastyrelsen	• Myndigheden har et lavere sikkerhedsniveau, fordi kendte sikkerhedshuller ikke bliver lukket. Det øger risikoen for, at en ondsindet aktør udnytter kendte sårbarheder i operativsystemet.
Krav 10. 2-faktor-autentifikation eller direkte VPN-forbindelse	●●● Sundhedsdatastyrelsen	• Hvis en medarbejder hos myndigheden er koblet på et netværk uden 2-faktor-autentifikation eller VPN (fx et netværk i lufthavnen), er der risiko for, at andre på samme netværk kan opsnappe alt, hvad medarbejderen foretager sig (fx læse med i mails på skærmen eller få adgang til medarbejderens webadresse, brugernavn og password) og kan tiltvinge sig adgang som medarbejderen.
Krav 15. Logning	●●● Sundhedsdatastyrelsen	• Risiko for, at loggen ikke kan anvendes til opdagelse og efterforskning af forskellige sikkerhedshændelser. • Risiko for, at logdata kan manipuleres eller slettes, hvis loggen ikke er beskyttet.
Krav 16. DNSSEC	●●● Sundhedsdatastyrelsen	• Risiko for, at den *rigtige* hjemmeside ikke bliver vist, når der linkes til hjemmesiden. • Medarbejder eller borger kan ikke stole på, at den rette hjemmeside tilgås.

● Angiver, hvor mange myndigheder der ikke opfylder kravet. ● Angiver, hvor mange myndigheder der opfylder kravet.

Kilde: Rigsrevisionen.

Det fremgår af tabel 3, at Sundhedsdatastyrelsen ikke efterlever nogen af de 5 minimumskrav, der er listet i tabellen, mens Kriminalforsorgen ikke efterlever minimumskrav 5 og 7. Statens It efterlever alle krav i tabellen, hvorfor Statens It ikke er nævnt under de enkelte krav.

Manglende efterlevelse af minimumskrav 5: Regelmæssig opdatering af klienter
59. Kriminalforsorgen og Sundhedsdatastyrelsen efterlever ikke krav 5. Hos Sundhedsdatastyrelsen er det kun 1 applikation, der ikke er regelmæssigt opdateret, og styrelsen har dermed opdateret alle øvrige applikationer.

Manglende efterlevelse af minimumskrav 7: Sikkerhedsopdateret operativsystem
60. Kriminalforsorgen og Sundhedsdatastyrelsen efterlever ikke minimumskrav 7.

Sundhedsdatastyrelsen – der i alt har 4.309 klienter – havde ved begyndelsen af vores it-revision 273 klienter, der ikke var supporteret med sikkerhedsopdateringer. Sundhedsdatastyrelsen har i forbindelse med revisionen afviklet en del af disse klienter, og der udestod i august 2021 afvikling af 73 klienter.

Kriminalforsorgen – der i alt har 3.747 klienter – havde ved begyndelsen af vores it-revision 5 klienter med et forældet operativsystem, der ikke kunne sikkerhedsopdateres. Da Rigsrevisionen afsluttede sin it-revision af Kriminalforsorgen i sommeren 2021, havde Kriminalforsorgen afviklet 4 af disse klienter, og der udestod kun håndtering af 1 klient. Det er Rigsrevisionens vurdering, at selv denne ene klient udgør en sikkerhedsrisiko, da en ondsindet aktør kan tiltvinge sig adgang til netværk og systemer, hvis aktøren formår at udnytte de kendte sårbarheder, som klientens software har. Flere cyberangreb sker i dag ved, at ondsindede aktører gør brug af automatiseret scanning for sikkerhedshuller, og dermed kan selv få klienter med forældet software blive et sikkerhedsmæssigt problem for en myndighed.

Manglende efterlevelse af minimumskrav 10: 2-faktor-autentifikation eller direkte VPN-forbindelse
61. Sundhedsdatastyrelsen efterlever ikke minimumskrav 10, da styrelsen ikke anvender 2-faktor-autentifikation til at tilgå webmail, når brugeren ikke er på styrelsens netværk. Det betyder, at hvis en medarbejder fra Sundhedsdatastyrelsen logger på via offentlige netværk, fx i en lufthavn eller på et hotel, er der risiko for, at andre på samme netværk kan opsnappe alt, hvad medarbejderen foretager sig. Det kan fx være at læse med i mails på skærmen eller få adgang til medarbejderens webadresse, brugernavn og password og bruge dem til at tiltvinge sig adgang til Sundhedsdatastyrelsens systemer, som var man den pågældende medarbejder.

Manglende efterlevelse af minimumskrav 15: Logning
62. Sundhedsdatastyrelsen efterlever ikke minimumskrav 15, da styrelsen ikke har sikret tilstrækkelig logning (herunder log på alle systemer og tjenester) på netværksservere.

Vi vurderer, at Sundhedsdatastyrelsens logning ikke er tilstrækkelig af 2 årsager. Den første årsag er, at Sundhedsdatastyrelsen anvender et logningssystem (en såkaldt SIEM-løsning), der opsamler logs fra mange af Sundhedsdatastyrelsens forskellige systemer. Vi kan konstatere, at loggen ikke har været beskyttet i tilstrækkelig grad, da de medarbejdere, der administrerede diverse systemer, også havde fuld adgang til SIEM-løsningen. Der har således ikke været en tilstrækkelig funktionsadskillelse, og dermed har medarbejdere potentielt kunnet manipulere eller helt slette logs fra SIEM-løsningen. Sundhedsdatastyrelsen har oplyst, at styrelsen nu har begrænset de adgange, som medarbejderne havde til SIEM-løsningen.

SIEM-løsning
SIEM (Security Information and Event Management) er en løsning, der leverer overvågning, sporing og alarmering af sikkerhedshændelser eller hændelser inden for et it-miljø.

Den vejledning, Rigsrevisionen henviser til i forhold til minimumskrav 15, er udarbejdet af Center for Cybersikkerhed. Vejledningen hedder "Logning – en del af et godt cyberforsvar" og er fra november 2020.

Den anden årsag er, at der logges data fra netværksudstyr, som ikke sendes til SIEM-løsningen, og som kun gemmes i 30 dage. Det fremgår af den vejledning fra Center for Cybersikkerhed, som minimumskrav 15 følger af, at der ofte kan gå uger og måneder, fra et angreb sker, til det bliver opdaget. Det er Rigsrevisionens vurdering, at 30 dage er for kort en periode at gemme en log i, da det mindsker sandsynligheden for, at loggen kan anvendes til at opklare eventuelle sikkerhedshændelser.

63. Rigsrevisionen anbefaler, at Finansministeriet sikrer, at det fremgår af kravet, hvor længe en log – som minimum – bør gemmes.

Manglende efterlevelse af minimumskrav 16: DNSSEC
64. Sundhedsdatastyrelsen efterlever ikke minimumskrav 16, da styrelsen ikke har tilknyttet DNSSEC på alle domænenavne tilhørende myndigheden.

Vi udtog en stikprøve på 6 domæner og kunne konstatere, at halvdelen af domænerne ikke havde konfigureret og aktiveret DNSSEC. Vi kan konstatere, at manglende implementering af DNSSEC på Sundhedsdatastyrelsens domæner medfører en risiko for, at de *rigtige* hjemmesider ikke bliver vist, når der linkes til hjemmesiderne. Medarbejdere eller borgere kan heller ikke være sikre på, at de rette hjemmesider tilgås hos Sundhedsdatastyrelsen.

65. Sundhedsdatastyrelsen har oplyst, at styrelsen har nedbragt antallet af domæner uden DNSSEC. Sundhedsdatastyrelsen har videre oplyst, at styrelsen er i gang med at afvikle de sidste domæner uden DNSSEC.

Status fra myndighederne efter afslutningen af it-revisionerne
66. Sundhedsministeriet har i november 2021 oplyst, at Sundhedsdatastyrelsen nu har implementeret DMARC REJECT på alle domæner (minimumskrav 11). Desuden har styrelsen oplyst, at multifaktor-autentifikation var implementeret på hele ministerområdet primo november 2021 (minimumskrav 10).

I september 2021 påbegyndte Sundhedsministeriets koncern transitionen af den basale it-drift til Statens It, og ministeriet har oplyst, at Statens It som leverandør fremover vil have medansvar for at opfylde nogle af minimumskravene.

Sundhedsministeriet har videre oplyst, at den manglende implementering af minimumskravene skal ses i lyset af coronapandemien, hvor det har været afgørende for ministeriet at prioritere en række it-udviklingsprojekter med meget kort varsel for at håndtere epidemien.

67. Fødevarestyrelsen har oplyst, at styrelsen nu efterlever minimumskrav 18 og 20 og arbejder videre for med tiden at efterleve minimumskrav 13.

68. Energistyrelsen har oplyst, at styrelsen nu har implementeret https og tvungen TLS 1.2. på alle styrelsens hjemmesider.

69. Rigsrevisionen har ikke efterprøvet myndighedernes oplysninger, da de er fremkommet, efter revisionerne er afsluttet.

Resultater

Undersøgelsen viser, at ingen af myndighederne på revisionstidspunktet efterlevede alle de minimumskrav til it-sikkerheden, som de var forpligtet til at efterleve. Det finder Rigsrevisionen utilfredsstillende, idet de fleste af kravene skulle være implementeret den 1. januar 2020.

På revisionstidspunktet var billedet dette: Sundhedsdatastyrelsen efterlever 12 krav, Energistyrelsen 15 krav, Kriminalforsorgen 16 krav, mens Fødevarestyrelsen efterlever 17 krav. Statens It efterlever heller ikke alle 20 krav, selv om Statens It er en professionel aktør på området, hvis kerneopgave er at levere sikker it-drift og service til andre statslige myndigheder. Statens It efterlever 18 ud af de 20 krav.

Energistyrelsen og Fødevarestyrelsen, der er kunder hos Statens It, har ikke ansvar for at sikre efterlevelse af alle 20 krav, da en del af kravene bliver dækket af Statens It eller i samarbejde med Statens It. Undersøgelsen viser, at Energistyrelsen kun efterlever 3 ud af de 7 krav, styrelsen selv er ansvarlig for, mens Fødevarestyrelsen efterlever 5 ud af 8 krav.

Undersøgelsen viser, at manglende efterlevelse er særligt udbredt i forhold til 3 specifikke minimumskrav. Der er således ingen af de 5 myndigheder, der efterlever minimumskrav 13 om regelmæssig opdatering af mobile enheder. Når fx mobiltelefoner ikke opdateres regelmæssigt, øges risikoen for, at ondsindede aktører opnår adgang til fortrolige oplysninger eller lykkes med at overvåge myndigheden (fx ved at aflytte mobiltelefoner).

4 ud af de 5 myndigheder opfylder heller ikke minimumskrav 18 om kryptering af kommunikation til hjemmesider. Herudover har 3 ud af de 5 myndigheder ikke implementeret DMARC REJECT-policy på alle domæner, og efterlever derfor ikke krav 11. Det muliggør, at en udefrakommende aktør kan udgive sig for at være myndighederne i mails til medarbejdere eller borgere, fx udgive sig for at være chef og anmode medarbejdere om at betale fakturaer uretmæssigt eller om at udlevere fortrolige oplysninger.

Undersøgelsen viser generelt, at 4 af minimumskravene på grund af upræcise formuleringer mv. kan fortolkes – og bliver fortolket – forskelligt. Det drejer sig om krav 6 om begrænset tildeling af lokaladministratorrettigheder, krav 13 om regelmæssig opdatering af mobile enheder, krav 15 om logning og krav 18 om kryptering af kommunikation til hjemmesider. Rigsrevisionen anbefaler, at Finansministeriet sikrer, at disse krav konkretiseres og uddybes, så tvivl om, hvad der skal til for, at de enkelte krav efterleves, minimeres.

Rigsrevisionen anbefaler endvidere, at Statens It etablerer en bedre systemunderstøttelse af tildeling af lokaladministratorrettigheder i den serviceportal, som både Statens It og kunderne anvender, når der skal tildeles lokaladministratorrettigheder.

2.2. Delt ansvar mellem Statens It og kunderne

70. Vi har undersøgt, om Statens It og kunderne, i dette tilfælde Energistyrelsen og Fødevarestyrelsen, efterlever en række minimumskrav i henhold til den ansvarsdeling, der er aftalt mellem dem.

Statens It's efterlevelse af 13 krav

71. Der er 13 tekniske minimumskrav, som Statens It automatisk skal efterleve på vegne af Energistyrelsen og Fødevarestyrelsen. Automatisk betyder, at Statens It skal efterleve disse krav, uden at Energistyrelsen og Fødevarestyrelsen anmoder herom. Tabel 4 viser, om Statens It automatisk sikrer efterlevelse af de 13 krav.

Tabel 4
Statens It's efterlevelse af 13 krav

Område	Minimumskrav	Statens It's efterlevelse
Klienter/pc'er	Krav 1. Firewall	●
	Krav 2. VPN-løsning	●
	Krav 3. Kryptering af harddiske	●
	Krav 4. End-point-beskyttelse	●
	Krav 5. Regelmæssig opdatering af klienter	●
	Krav 7. Sikkerhedsopdateret operativsystem	●
Mail	Krav 8. Godkendte mail-relays med autentifikation	●
	Krav 9. Kryptering af kommunikation med mail-protokoller	●
	Krav 11. DMARC REJECT-policy på domæner	●
Netværk	Krav 14. Kryptering af wi-fi på arbejdsnetværk	●
	Krav 15. Logning	●
Websider	Krav 16. DNSSEC	●
	Krav 17. Beskyttelse mod skadelige hjemmesider	●

● Krav opfyldt.

Kilde: Rigsrevisionen.

Det fremgår af tabel 4, at Statens It efterlever de 13 minimumskrav på vegne af Energistyrelsen og Fødevarestyrelsen for de systemer, der er overdraget til Statens It.

Koordination mellem Statens It og Energistyrelsen og Fødevarestyrelsen

72. Energistyrelsen og Fødevarestyrelsen kan indgå et samarbejde med Statens It om efterlevelsen af yderligere 4 minimumskrav. De 4 krav ligger ud over de 13 krav, som Statens It automatisk skal sikre, jf. ovenfor.

Samarbejdet om at efterleve de 4 krav kan foregå ved, at Energistyrelsen eller Fødevarestyrelsen enten bestiller specifikke løsninger eller opdateringer hos Statens It. Såfremt Energistyrelsen og Fødevarestyrelsen tager initiativ til dette, bliver Statens It ansvarlig for at sikre, at de bestilte løsninger eller opdateringer virker i overensstemmelse med de 4 krav. Anmoder Energistyrelsen og Fødevarestyrelsen ikke Statens It om et bidrag, bliver Statens It ikke ansvarlig for at sikre, at disse krav efterleves.

73. Vi har undersøgt, i hvilket omfang de 2 styrelser har bestilt løsninger eller opdateringer vedrørende minimumskravene hos Statens It, og om Statens It effektuerer løsningerne eller opdateringerne i overensstemmelse med kravene.

Samarbejde vedrørende krav 10: 2-faktor-autentifikation eller direkte VPN-forbindelse
74. Energistyrelsen og Fødevarestyrelsen har bestilt 2-faktor-autentifikation hos Statens It, som er en løsning, der bidrager til efterlevelse af minimumskrav 10.

Samarbejde vedrørende krav 12: Adgangskode på min. 6 cifre eller biometrisk identifikation
75. Energistyrelsen har tilkøbt en løsning hos Statens It, der sikrer, at adgangskoden er min. 6 cifre på mobile enheder. Undersøgelsen viser, at Statens It har sikret en sådan opsætning. Fødevarestyrelsen anvender ikke Statens It's mobilløsning, og derfor er Statens It ikke forpligtet til at bistå Fødevarestyrelsen med at efterleve minimumskrav 12. Fødevarestyrelsen har imidlertid sikret, at styrelsen efterlever minimumskrav 12, jf. bilag 3.

Samarbejde vedrørende krav 18: Kryptering af kommunikation til hjemmesider
76. Undersøgelsen viser, at Statens It ikke har sikret, at Fødevarestyrelsen og Energistyrelsen efterlever minimumskrav 18, herunder at der skal implementeres https på alle hjemmesider.

Ifølge det hjælpeark, som Statens It har kommunikeret ud til sine kunder, skal Energistyrelsen og Fødevarestyrelsen bestille https til hjemmesider, der hostes af Statens It. Vores undersøgelse viser, at Statens It har registreret 4 domænenavne for Energistyrelsen og 1 domænenavn for Fødevarestyrelsen. Registreringerne er foretaget på baggrund af anmodninger fra begge styrelser. Registrering af et domænenavn sikrer brugsretten til domænet. Undersøgelsen viser dog, at Statens It af egen drift har konfigureret webservere og indsat placeholdere på de 5 domænenavne. Ved at konfigurere webservere og indsætte placeholdere på et domæne vil domænet fungere som en hjemmeside, der ikke er helt tom. Rigsrevisionen kan konstatere, at hverken Energistyrelsen eller Fødevarestyrelsen har anmodet Statens It om at indsætte placeholdere, og derfor har styrelserne ikke nødvendigvis haft kendskab til, at der var en aktiv webserver på deres domæne, og at hjemmesiderne derfor skulle have implementeret https.

Domænenavn
Et domænenavn er den unikke genvej til en IP-adresse. Et domænenavn kan bl.a. bruges til nemt at finde en hjemmeside eller en mail-server, så man ikke behøver at kende IP-adressen på fx webserveren.

Fødevarestyrelsen har oplyst, at deres hjemmeside ikke havde et indhold, hvorfor styrelsen ikke har anmodet Statens It om at implementere https. I forbindelse med vores undersøgelse har Fødevarestyrelsen bedt Statens It om at nedlægge domænet, efter det har eksisteret i knap 4 år.

Energistyrelsen har oplyst, at styrelsen ikke har anmodet Statens It om at indsætte en placeholder på de 4 hjemmesider, men blev bekendt med placeholderne i forbindelse med et oprydningsarbejde i foråret 2020. Energistyrelsen har oplyst, at styrelsen i forbindelse med oprydningsarbejdet konstaterede, at der var https på de 4 hjemmesider. Rigsrevisionen kunne dog på revisionstidspunktet i 2021 konstatere, at de 4 hjemmesider ikke havde https.

Rigsrevisionen finder samlet set, at minimumskrav 18 ikke har været efterlevet, da der ikke har været implementeret https på hjemmesiderne.

Samarbejde vedrørende krav 20: Regelmæssig opdatering af webservere
77. Undersøgelsen viser, at Energistyrelsen ikke har sikret, at minimumskrav 20 efterleves. Det skyldes, at styrelsen ikke har anmodet om opdatering af webservere hos Statens It. Rigsrevisionen finder derfor, at Statens It ikke har reel mulighed for at bidrage til efterlevelsen af dette krav. Manglende efterlevelse af kravet medfører en risiko for, at ondsindede aktører udnytter offentligt kendte sårbarheder i softwaren på webserveren. Energistyrelsen er enig i Rigsrevisionens vurdering, men har oplyst, at der har været en løbende dialog med Statens It om dette efterslæb. Rigsrevisionen konstaterer, at opdateringerne ikke har fundet sted regelmæssigt, og finder derfor, at Energistyrelsen fremadrettet bør sikre, at styrelsen får anmodet Statens It om opdateringer. Fødevarestyrelsen har selv været ansvarlig for at sikre efterlevelse af dette minimumskrav. Det fremgår af både tabel 2 og bilag 3, at styrelsen ikke har sikret efterlevelse af krav 20.

Resultater

Undersøgelsen viser, at Statens It har sikret, at Energistyrelsen og Fødevarestyrelsen efterlever 13 tekniske minimumskrav for de systemer, der er overdraget til Statens It.

Undersøgelsen viser, at Energistyrelsen og Statens It har koordineret, at Energistyrelsen yderligere efterlever krav 10 om 2-faktor-autentifikation og krav 12 om adgangskode på min. 6 cifre eller biometrisk identifikation. Energistyrelsen har imidlertid ikke anmodet Statens It om at opdatere webservere, der ligger hos Statens It, hvorfor Statens It ikke har kunnet bistå Energistyrelsen med at efterleve minimumskrav 20. Rigsrevisionen finder, at Energistyrelsen fremadrettet bør sikre, at styrelsen får anmodet Statens It om opdatering af webservere.

Undersøgelsen viser videre, at Statens It og Fødevarestyrelsen har koordineret, at Fødevarestyrelsen efterlever minimumskrav 10 om 2-faktor-autentifikation. Fødevarestyrelsen har modsat Energistyrelsen fravalgt løsningen hos Statens It i forhold til at sikre krav 12 om adgangskode på min. 6 cifre eller biometrisk identifikation. Fødevarestyrelsen har imidlertid selv sørget for at efterleve dette krav.

Endelig viser undersøgelsen, at der ikke har været en tilstrækkelig koordinering mellem Statens It og henholdsvis Energistyrelsen og Fødevarestyrelsen i forhold til at sikre minimumskrav 18 om kryptering af kommunikation til hjemmesider. Statens It hoster 5 hjemmesider for henholdsvis Energistyrelsen og Fødevarestyrelsen, som ikke er tomme for indhold og derfor bør have https. Da Statens It har placeret indholdet på hjemmesiderne, har kunderne ikke været bekendt med behovet for https, og Rigsrevisionen finder derfor, at Statens It burde have implementeret https eller sikret, at der ikke var en aktiv webserver på domænerne.

Rigsrevisionen, den 6. januar 2022

Lone Strøm

/Peder Juhl Madsen

Bilag 1. Metodisk tilgang

Formålet med undersøgelsen er at vurdere, om 5 udvalgte samfundsvigtige myndigheder efterlever 20 tekniske minimumskrav til it-sikkerheden. Derfor har vi undersøgt følgende:

- om den enkelte myndighed efterlever de tekniske minimumskrav, som myndigheden selv er forpligtet til at efterleve
- om Statens It og kunderne, her Energistyrelsen og Fødevarestyrelsen, efterlever de tekniske minimumskrav i henhold til den ansvarsdeling, der er aftalt mellem dem.

I undersøgelsen indgår Statens It (under Finansministeriet). Statens It leverer it-services til 19 ministerområder. Statens It er udvalgt, fordi Statens It varetager systemer for andre ministerområder og skal sikre, at driften af systemerne sker i overensstemmelse med de tekniske minimumskrav. Desuden indgår Kriminalforsorgen (under Justitsministeriet). Kriminalforsorgen indgår, fordi myndigheden behandler følsomme oplysninger om borgere (fx inden for efterforskning og strafbare handlinger). Sundhedsdatastyrelsen (under Sundhedsministeriet) indgår ligeledes, fordi styrelsen behandler følsomme oplysninger i form af sundhedsdata, men også fordi styrelsen har ansvar for at it-understøtte det strategiske sundhedsberedskab og Sundhedsministeriets it-infrastruktur. Et brud på it-sikkerheden hos Sundhedsdatastyrelsen kan derfor være af samfundskritisk karakter. Vi har udvalgt Sundhedsdatastyrelsen som undersøgelsesområde, men i praksis har vores revision omfattet hele Sundhedsministeriets koncern, fordi Sundhedsdatastyrelsen er koncern-it-funktion for hele ministerområdet (med undtagelse af Lægemiddelstyrelsen). Endelig indgår 2 myndigheder, der har overdraget den basale it-drift til Statens It og dermed har ansvar for at sikre færre minimumskrav end myndigheder, der ikke benytter sig af Statens It's services. Det er Energistyrelsen (under Klima-, Energi- og Forsyningsministeriet) og Fødevarestyrelsen (under Ministeriet for Fødevarer, Landbrug og Fiskeri). Begge styrelser varetager samfundsvigtige opgaver. Energistyrelsen varetager opgaver i relation til energisektoren, som er udpeget som en samfundskritisk sektor i den nationale strategi for cyber- og informationssikkerhed 2018-2021. Fødevarestyrelsen varetager opgaver relateret til fødevaresektoren, som Politiets Efterretningstjeneste har udpeget som en sektor, der leverer kritiske ydelser til samfundet.

Undersøgelsen omhandler perioden januar 2020 - september 2021. Perioden dækker fra, hvornår kravene skulle være efterlevet til ca. 1-1½ år efter fristen for efterlevelse. 17 minimumskrav skulle være efterlevet fra den 1. januar 2020, og yderligere 3 krav fra den 1. juli 2020. De udvalgte myndigheder har således haft tid til at få implementeret de tekniske minimumskrav.

Undersøgelsen bygger på 5 it-revisioner, som Rigsrevisionens kontor for it-revision har gennemført i perioden marts-september 2021. Der foreligger på den baggrund it-revisionsrapporter og underliggende substansrevision. It-revisionerne består primært af virtuelle møder med myndighederne på grund af COVID-19-situationen, og kun Sundhedsdatastyrelsen er aflagt et fysisk revisionsbesøg.

It-revisionerne består bl.a. af en gennemgang af systemværktøjer, systemopsætninger og konfigurationer. Herudover har vi gennemgået lister over operativsystemer (både for klienter, servere og mobile enheder) og dokumentation for sikkerhedsopdateringer mv. Vi har endvidere gennemgået bl.a. retningslinjer og politikker for tildeling af rettigheder og af beslutningsgrundlag for log-opsamling. Der er desuden udtaget stikprøver med henblik på at efterprøve, om myndighederne har implementeret eller foretaget en række tekniske foranstaltninger fx sikret, at der anvendes numerisk adgangskode på min. 6 cifre eller biometrisk identifikation, og om myndighederne anvender DMARC, TLS 1.2., Flash og DNSSEC. De indsamlede data omfatter bl.a. datauddræk, skærmbilleder og skriftligt materiale (fx myndighedernes retningslinjer).

Ud over it-revisionerne har vi holdt møder med Center for Cybersikkerhed og Digitaliseringsstyrelsen, som begge har været ansvarlige for at udforme de 20 tekniske minimumskrav til it-sikkerheden. På møderne har vi drøftet baggrunden for de tekniske minimumskrav, herunder hvordan enkelte krav skal forstås. Vi har bl.a. drøftet hyppigheden af opdateringer med Center for Cybersikkerhed, herunder at sikkerhedsopdateringer bør gennemføres min. hver 30. dag, medmindre der er tale om kritiske opdateringer.

Center for Cybersikkerhed har oplyst, at ikke alle krav er direkte understøttet af tidligere udgivne anbefalinger, og anbefalingerne er ikke nødvendigvis formuleret enslydende med de senere aftalte tekniske minimumskrav.

Kvalitetssikring

Denne undersøgelse er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos den reviderede samt ledelsesbehandling og sparring på forskellige tidspunkter i undersøgelsesforløbet med chefer og medarbejdere i Rigsrevisionen.

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

- Statens It's hjælpeark til kunderne, der beskriver ansvarsdelingen mellem Statens It og kunderne i forhold til at efterleve de 20 tekniske minimumskrav. Hjælpearkene er fra henholdsvis august 2020 og februar 2021.
- Vejledninger, som de tekniske minimumskrav følger af (fx *Cyberforsvar der virker*, *Reducér risikoen for ransomware* og *Råd om sikkerhed på mobile enheder*).
- Vejledning om tilsynet med Statens It fra december 2017.
- National strategi for cyber- og informationssikkerhed 2018-2021.
- Notat om baggrunden for de tekniske minimumskrav udarbejdet af Center for Cybersikkerhed og Digitaliseringsstyrelsen.
- Myndighedernes retningslinjer og politikker for tildeling af rettigheder og for opdateringer.

Formålet med gennemgangen af dokumenterne har bl.a. været at undersøge, om de udvalgte myndigheder efterlever de 20 tekniske minimumskrav, herunder om Statens It og kunderne efterlever kravene i henhold til den ansvarsdeling, der er aftalt mellem dem.

Ansvarsdeling mellem Statens It og myndighederne (kunderne)

Statens It har fastlagt ansvarsdelingen i et hjælpeark, som Statens It har sendt ud til kunderne i henholdsvis august 2020 og februar 2021. De 2 hjælpeark fra Statens It er stort set identiske, bortset fra at Statens It i februar 2021 angiver, at kunderne selv skal sikre minimumskrav 4 for Mac-klienter. Vi har lagt den seneste udmelding fra februar 2021 til grund for vores vurdering af, om Statens It og kunderne efterlever minimumskravene i henhold til den aftalte ansvarsdeling.

Ud over den ansvarsdeling, som Statens It har kommunikeret ud til kunderne i forhold til minimumskravene, er forpligtelserne for Finansministeriet og kunderne defineret ved, at kunderne har ressortoverført den basale it-drift til Statens It. Ressortoverførelsen betyder også, at tilsynsforpligtelsen ligger hos Finansministeriet. Tilsynsforpligtelsen er nærmere beskrevet i Finansministeriets vejledning om tilsyn med Statens It fra 2017. Det fremgår af vejledningen, hvad Finansministeriet har ansvar for, og hvilket ansvar der påhviler kunden. Kundens ansvar er beskrevet i det følgende:

For det første skal kunden udarbejde en risikovurdering af sine it-systemer og vurdere, om der er behov for særlige sikkerhedsforanstaltninger, der ligger ud over Statens It's standardsikkerhedsniveau. Hvis kunden vurderer, at et system kræver særlige sikkerhedsforanstaltninger, skal myndigheden stille krav til Statens It om etablering af den ønskede sikkerhedsforanstaltning. Det skal medføre en aftale mellem kunden og Statens It om, hvordan de særlige krav imødekommes af Statens It, og hvordan Statens It bl.a. afrapporterer leverancen. Kunden skal på baggrund af afrapporteringen fra Statens It vurdere, om de særlige sikkerhedsforanstaltninger er gennemført som aftalt, og anvende afrapporteringen som et led i sin leverandørstyring. Hvis der er indgået en særskilt aftale mellem Statens It og kunden for et system, der kræver særlige sikkerhedsforanstaltninger, skal kunden specificere tilsynet herom i kontrakten med Statens It. Finansministeriets tilsyn omfatter ikke særlige krav stillet af kunderne, herunder om Statens It overholder afrapporteringen, og det er derfor udelukkende kundens ansvar at føre tilsyn med de områder, der er berørt af særskilte aftaler.

For det andet er kunden forpligtet til at læse den årlige tilsynsrapport fra Finansministeriet og vurdere relevansen af eventuelle risici fremhævet i tilsynsrapporten. Tilsynsrapporten omhandler kun de områder af driftsmodellerne, som Finansministeriet (jf. vejledningen) fører tilsyn med. Tilsynsrapporten dækker ligeledes kun forhold, som hører under Statens It's standard sikkerhedsniveau.

For det tredje har kunden mulighed for at deltage i relevante kundefora, som Statens It stiller til rådighed. Desuden har kunden mulighed for at komme med forslag til områder, som bør inddrages i Finansministeriets tilsyn. Det er dog udelukkende op til Finansministeriet at beslutte, hvilke områder der skal gennemgås i løbet af året.

Finansministeriets tilsynsrapport omhandler ikke de 20 minimumskrav eksplicit, og kunderne modtager derfor ikke en afrapportering på, om Statens It efterlever de tekniske minimumskrav på vegne af kunderne. Statens It har som nævnt beskrevet ansvarsdelingen mellem Statens It og kunderne i forhold til de tekniske minimumskrav, og vores undersøgelse tager udgangspunkt i denne ansvarsdeling.

Møder

Vi har holdt møder med:

- Statens It
- Kriminalforsorgen
- Sundhedsdatastyrelsen
- Fødevarestyrelsen
- Energistyrelsen
- Digitaliseringsstyrelsen
- Center for Cybersikkerhed.

Formålet med møderne har været at undersøge de udvalgte myndigheders efterlevelse af de 20 tekniske minimumskrav til it-sikkerheden. På møder med Digitaliseringsstyrelsen og Center for Cybersikkerhed har vi drøftet, hvordan enkelte minimumskrav skal forstås, og hvad der ligger til grund for en basal it-sikkerhed.

Stikprøver

I forbindelse med it-revisionerne har vi stikprøvevist testet, om myndighedernes løsninger er konfigureret, så de overholder de tekniske minimumskrav til it-sikkerheden. Vi har bl.a. udtaget stikprøver for at undersøge, om myndighederne har:

- implementeret krav til adgangskode på min. 6 cifre eller biometrisk identifikation på mobile enheder
- VPN-adgang til netværk
- foretaget kryptering af harddiske på klienter
- opdateret operativsystemer og applikationer
- anvendt 2-faktor-autentifikation til at tilgå webmail uden for myndighedens lokale netværk
- krypteret wi-fi med minimum WPA2
- implementeret DMARC REJECT på domæner
- foretaget kryptering af arbejdsnetværk
- konfigureret og aktiveret DNSSEC
- sikret, at der ikke anvendes Flash på hjemmesider.

På grund af COVID-19-situationen har vi gennemført størstedelen af revisionen ved hjælp af virtuelle møder i stedet for fysiske revisionsbesøg. Det har i et vist omfang begrænset vores mulighed for at udvælge stikprøver, da vi ikke har kunnet tilgå fysiske arbejdspladser. Vi har i stedet foretaget enkelte stikprøver gennem virtuelle møder fx påset, at mødedeltageres mobiltelefoner kræver numerisk adgangskode på min. 6 cifre eller biometrisk identifikation. Hvad angår minimumskrav 10, har vi ikke haft mulighed for at påse, om mødedeltagere anmodes om SMS-kode ved login til webmail via en privat pc (2-faktor-autentifikation). Det skyldes, at revisionen er udført virtuelt, hvorfor vi ikke har kunnet påse, at mødedeltagerne rent faktisk modtager en SMS-kode. Vi har efterfølgende modtaget skærmbilleder som dokumentation herfor.

Resten af vores stikprøver har imidlertid ikke været påvirket af COVID-19-situationen. Det gælder fx test af, om der er implementeret DMARC REJECT og DNSSEC på domæner, da disse tests kan udføres uden fysiske revisionsbesøg. Vi har i den forbindelse indhentet lister over alle domænenavne hos de enkelte myndigheder, som vi har anvendt til at udvælge vores stikprøver. Ud over at have udvalgt domæner ud fra et tilfældighedsprincip har vi lokaliseret domæner, som er meget anvendt, og domæner, som er mindre anvendt. Vi har udvalgt en række af disse for at undersøge, om der kunne være forskel i implementeringen af sikkerhedstiltag afhængig af, hvor meget domænerne bliver anvendt.

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. Digitaliseringsstyrelsens opfølgningsark til myndighederne (1. kvartal 2021)

Tabel A

Efterlevelse af tekniske minimumskrav til it-sikkerheden i statslige myndigheder

Krav	Beskrivelse
Klienter/pc'er	**Kravene til klienter/pc'er angår de stationære og bærbare computere, der almindeligvis anvendes i myndigheden med forbindelse med myndighedens arbejdsnetværk**
1. Der skal implementeres firewall på alle klienter.	Kravet er opfyldt, hvis der er implementeret firewall på alle klienter hos myndigheden.
2. Der skal benyttes en af myndigheden stillet til rådighed VPN-løsning til at gå på internettet via arbejds-pc fra eksterne netværk.	Kravet er opfyldt, hvis der stilles en VPN-løsning til rådighed på medarbejdernes arbejds-pc'er, og det gennem tekniske foranstaltninger (fx Always-On) eller politikker sikres, at der anvendes VPN, når pc'en er koblet på internettet uden for myndighedens eget netværk.
3. Kryptering af harddiske.	Kravet er opfyldt, hvis kryptering er aktiveret på alle klienter i myndigheden, typisk ved hjælp af indbygget funktionalitet i operativsystemet.
4. Der skal implementeres endpoint-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter.	Kravet er opfyldt, hvis der er installeret endpoint-beskyttelse med automatisk opdatering på alle klienter hos myndigheden.
5. Klienter skal patches og opdateres regelmæssigt – både OS og applikationer.	Kravet er opfyldt, hvis der er truffet tekniske og/eller organisatoriske foranstaltninger til at sikre regelmæssig opdatering og patching af OS og applikationer på klienter.
6. Administrative rettigheder for brugere tildeles kun tidsbegrænset og med veldokumenterede behov.	Kravet er opfyldt, hvis der er truffet organisatoriske foranstaltninger med eventuel teknisk understøttelse, der sikrer, at administrative rettigheder på klienter med adgang til myndighedens arbejdsnetværk kun tildeles tidsbegrænset og med veldokumenteret behov.
7. Det anvendte operativsystem skal være så nyt som muligt og skal som minimum være supporteret med sikkerhedsopdateringer.	Kravet er opfyldt, hvis det anvendte operativsystem fortsat er supporteret med sikkerhedsopdateringer, og hvis det af myndigheden vurderes at være nyest mulige udgave af pågældende system under hensyntagen til myndighedens systemmiljø og fagapplikationer.
Mail	**Kravene til mails angår mailkommunikation til/fra myndigheden**
8. Der må kun anvendes af myndigheden godkendte mail-relays med autentifikation.	Kravet er opfyldt, hvis internettilgængelige mail-relays, som tilhører eller anvendes af myndigheden, kun accepterer mails fra autentificerede brugere eller systemer.
9. Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2. Mellem statslige myndigheder stilles krav om tvungen (forced) TLS, mens der til øvrige skal sendes TLS, hvis modtager understøtter det.	Kravet er opfyldt, hvis alle mail-servere, hvorigennem der kommunikeres til, og fra myndigheden er sat op til at kryptere mails med TLS 1.2, såfremt modtager understøtter det (opportunistisk TLS), *og* hvis alle relevante servere er sat op til at foretage tvungen kryptering (forced TLS) til statslige myndigheder. (Statens It har med henblik på implementering af dette krav udarbejdet en liste over relevante domæner, mellem hvilke der skal kommunikeres (forced TLS)).
10. Webmail må kun anvendes uden for myndighedens lokale netværk, hvis dette foregår ved hjælp af 2-faktor-autentifikation eller via en direkte VPN-forbindelse til myndighedens netværk.	Kravet er opfyldt, hvis der er implementeret tekniske foranstaltninger, som sikrer, at webmail til myndighedens mail udelukkende kan anvendes efter 2-faktor-autentificering eller brug af en direkte VPN-forbindelse til myndighedens netværk.
11. DMARC REJECT-policy implementeres på alle domæner tilhørende myndigheden.	Kravet er opfyldt, hvis der er implementeret DMARC REJECT-policy på alle domæner tilhørende myndigheden, herunder domæner, der ikke anvendes til at sende mails.

Tabel A (fortsat)

Efterlevelse af tekniske minimumskrav til it-sikkerheden i statslige myndigheder

Krav	Beskrivelse
Mobile enheder	**Kravene til mobile enheder angår arbejdstelefoner, tablets og eventuelle andre lignende enheder, hvorfra der er adgang til myndighedens arbejdsnetværk og/eller fra hvilke, der kommunikeres på vegne af myndigheden**
12. Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation.	Kravet er opfyldt, hvis det teknisk og/eller organisatorisk sikres, at mobile enheder kun kan tilgås ved hjælp af en adgangskode/PIN-kode på minimum 6 cifre eller ved hjælp af biometrisk identifikation.
13. Operativsystem og apps på mobile enheder skal opdateres regelmæssigt.	Kravet er opfyldt, hvis der er truffet tekniske og/eller organisatoriske foranstaltninger til at sikre regelmæssig opdatering af OS og applikationer på mobile enheder.
Netværk	**Kravene til netværk angår myndighedens interne arbejdsnetværk, men ikke eventuelle gæstenetværk uden adgang til myndighedens systemer**
14. Wi-fi på myndighedens arbejdsnetværk skal være krypteret med minimum WPA2.	Kravet er opfyldt, hvis trådløs adgang til myndighedens arbejdsnetværk er krypteret med minimum WPA2.
15. Krav om logning, log på alle systemer og tjenester på netværksservere.	Kravet er opfyldt, hvis der er implementeret logning på infrastrukturkomponenter i overensstemmelse med CFCS-vejledningen "Logning – en del af et godt cyberforsvar".
Websider	**Kravene til websider angår alle myndighedens eksternt rettede websider og domæner, men ikke intranet og eventuelle andre systemer, som udelukkende kan tilgås fra myndighedens interne netværk, og som derfor er afskærmet fra det åbne internet**
16. DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.	Kravet er opfyldt, hvis der er opsat DNSSEC på alle domænenavne tilhørende myndigheden.
17. Myndigheden skal anvende en sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod skadelige hjemmesider.	Kravet er opfyldt, hvis myndigheden anvender en sikker DNS-tjeneste, eller hvis der er implementeret en anden løsning, som yder tilsvarende beskyttelse mod skadelige hjemmesider.
18. Kommunikation til hjemmesider skal krypteres og anvende minimum TLS 1.2, dvs. der skal implementeres https på alle hjemmesider	Kravet er opfyldt, hvis det teknisk er sikret, at myndighedens hjemmesider kun kan anvendes med TLS 1.2-kryptering eller højere. Kravet betragtes *ikke* som opfyldt, hvis der samtidig er mulighed for fallback til TLS 1.1, 1.0, SSL 3 eller SSL2.
19. Der må ikke anvendes Flash på hjemmesider tilhørende myndigheden	Kravet er opfyldt, hvis der ikke anvendes Flash-løsninger på nogen hjemmesider tilhørende myndigheden.
20. Der skal benyttes regelmæssigt opdateret serversoftware på webservere	Kravet er opfyldt, hvis der er truffet tekniske og/eller organisatoriske foranstaltninger til at sikre regelmæssig opdatering af serversoftware på webservere, der anvendes af myndigheden.

Note: Tabellen er et udsnit af Digitaliseringsstyrelsens opfølgningsark, som ud over de illustrerede kolonner indeholder kolonner til myndighedernes selvevaluering af, om de opfylder kravene.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Digitaliseringsstyrelsen.

Bilag 3. Myndighedernes efterlevelse

Tabel a
Myndighedernes efterlevelse

		Ikke kunder hos Statens It			Kunder hos Statens It	
		Statens It	**Kriminal-forsorgen**	**Sundheds-data-styrelsen**	**Energi-styrelsen**	**Fødevare-styrelsen**
Krav 1.	Firewall	●	●	●	IR	IR
Krav 2.	VPN-løsning	●	●	●	IR	IR
Krav 3.	Kryptering af harddiske	●	●	●	IR	IR
Krav 4.	End-point-beskyttelse	●	●	●	IR	IR
Krav 5.	Regelmæssig opdatering af klienter	●	●	●	IR	IR
Krav 6.	Begrænset tildeling af lokaladministratorrettigheder	●	●	●	●	●
Krav 7.	Sikkerhedsopdateret operativsystem	●	●	●	IR	IR
Krav 8.	Godkendte mail-relays med autentifikation	●	●	●	●	IR
Krav 9.	Kryptering af kommunikation med mail-protokoller	●	●	●	●	(●)
Krav 10.	2-faktor-autentifikation eller direkte VPN-forbindelse	●	●	●	IR	IR
Krav 11.	DMARC REJECT-policy på domæner	●	●	●	●	●
Krav 12.	Adgangskode på min. 6 cifre eller biometrisk identifikation	●	●	●	IR	●
Krav 13.	Regelmæssig opdatering af mobile enheder	●	●	●	●	●
Krav 14.	Kryptering af wi-fi på arbejdsnetværk	●	●	●	IR	IR
Krav 15.	Logning	●	●	●	IR	IR
Krav 16.	DNSSEC	●	●	●	IR	IR
Krav 17.	Beskyttelse mod skadelige hjemmesider	●	●	●	IR	IR
Krav 18.	Kryptering af kommunikation til hjemmesider	●	(●)	●	●	●
Krav 19.	Flash	●	●	●	(●)	●
Krav 20.	Regelmæssig opdatering af webservere	●	●	●	IR	●
Antal minimumskrav som myndigheden efterlever		**18/20**	**16/20**	**12/20**	**3/7**	**5/8**

● = Krav ikke opfyldt. ● = Krav opfyldt. (●) = Myndigheden er først begyndt at opfylde minimumskravet i forbindelse med vores it-revision i perioden marts-september 2021. IR = Ikke relevant, fordi myndigheden ikke har et ansvar i forhold til det pågældende minimumskrav, eller fordi der er et delt ansvar med Statens It. Resultaterne vedrørende det delte ansvar med Statens It er beskrevet i beretningens afsnit 2.2.

Note: Hvad angår krav 10, er revisionsbeviset begrænset på grund af virtuel revision.

Kilde: Rigsrevisionen.

Bilag 4. Ordliste

2-faktor-autentifikation	2-faktor-autentifikaton betyder, at medarbejderne skal validere deres identitet ved hjælp af 2 faktorer, når de logger på udefra. Det er en kombination af noget, som brugeren ved (fx password), og noget som brugeren har eller får (fx token eller en kode sendt som SMS til brugerens mobiltelefon).
App	Forkortelse for applikation, som dækker over et computerprogram. De mest anvendte apps til kontorbrug er fx mail, webbrowsere, tekstbehandlingsprogrammer og regneark.
Cyberangreb	Hændelser, hvor en ondsindet aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Cyberangreb kan også være hændelser, hvor data og systemer helt ødelægges.
Kryptering	En proces, der via matematiske funktioner omdanner den oprindelige data til data, der er ulæselig for tredjepart.
Log/logning	Registreringer af hændelser, der foretages i myndighedens it-systemer.
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.
Ondsindet aktør	Betegner i denne beretning en person, der foretager en tilsigtet eller utilsigtet ulovlig handling ved fx i det skjulte at skaffe sig adgang til og/eller inficere andres it-systemer eller data. Dette kan både være en medarbejder, men også en helt ukendt person. Formålet med de ondsindede handlinger afhænger af, hvilken person der står bag, dvs. om vedkommende er fra en fremmed stat, fra en kriminel organisation, eller er et individ, som på egen hånd misbruger en myndigheds sårbarheder.
Operativsystem	Det grundlæggende system, der styrer computeren og giver mulighed for at afvikle applikationer.
Ransomware	Ordet 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 myndighed eller virksomhed ikke kan tilgå dem. Ondsindede aktører kræver løsepenge for at dekryptere data, så institutionen igen kan få adgang til data.
SIEM-løsning	SIEM står for Security Information and Event Management. SIEM-løsninger bruges til at opsamle logs centralt fra ét eller flere it-systemer hos myndighederne. SIEM-løsninger kan fx anvendes til at analysere hændelser på tværs af myndigheden.
VPN-løsning	En Virtuel Private Network (VPN)-løsning er en krypteret forbindelse over internettet fra en enhed til et netværk. Den krypterede forbindelse bidrager med at sikre, at data transmitteres sikkert. Det forhindrer uautoriserede personer i at overvåge trafikken over internettet.