DIGITALISERINGSSTYRELSEN

Notat

19. april 2022

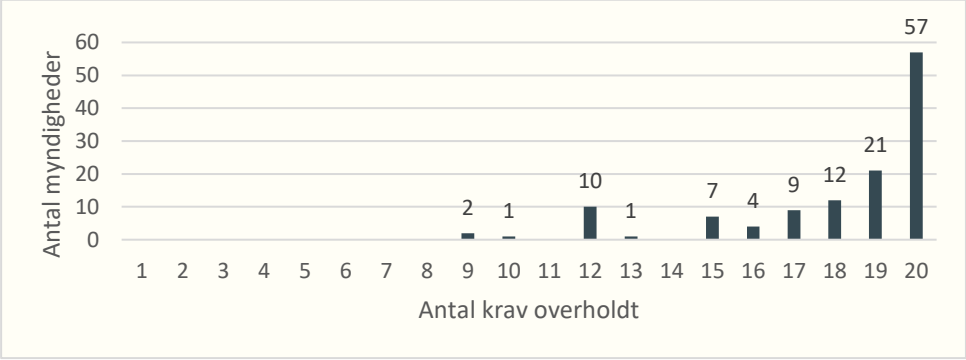
Efterlevelse af tekniske minimumskrav til sikkerheden i statslige myndigheder – 3. kvartal 2021

Det blev som led i den nationale cyber- og informationssikkerhedsstrategi i september 2019 besluttet, at de statslige myndigheder skal efterleve en række tekniske minimumskrav med henblik på at sikre et højt fælles sikkerhedsniveau i staten. De første 17 krav skulle være implementeret senest den 1. januar 2020, mens tre yderegere krav først trådte i kraft den 1. juli 2020. Kravene er alle ufravigelige.

Der er i hhv. Q3 2020 og Q1 2021 samt i Q3 2021 gennemført spørgeskemaundersøgelser om myndighedernes efterlevelse af kravene. Det fremgik af følgeteksten til spørgeskemaerne, at et krav kun kunne betragtes som efterlevet i tilfælde af "fuld" efterlevelse, altså hvor der ikke var nogle udeståender ift. implementeringen af kravet i den enkelte myndighed. Ved målingen i Q3 2021 er der alt modtaget 124 besvarelser fra myndigheder og institutioner på samtlige ministerområder. Enkelte myndigheder på Forsvarsministeriets område er undtaget pga. fortrolighed[1].

Resultaterne viser, at 57 (46 pct.) af myndighederne efterlever samtlige af de 20 krav. Det er en fremgang på ca. 10 procentpoint siden målingen i Q1 2021, hvor 45 myndigheder havde opnået fuld implementering. 109 myndigheder efterlever mindst 15 af kravene fuldt ud, hvilket svarer til 89 pct. Kun 3 (2 pct.) af myndighederne efterlever 10 af kravene eller færre. Der er i disse tilfælde tale om myndigheder med et kompliceret og/eller atypisk system-setup, som kun i begrænset omfang kan sammenlignes med resten af staten.

Figur 1: Antal myndigheder fordelt på antal krav som efterleves



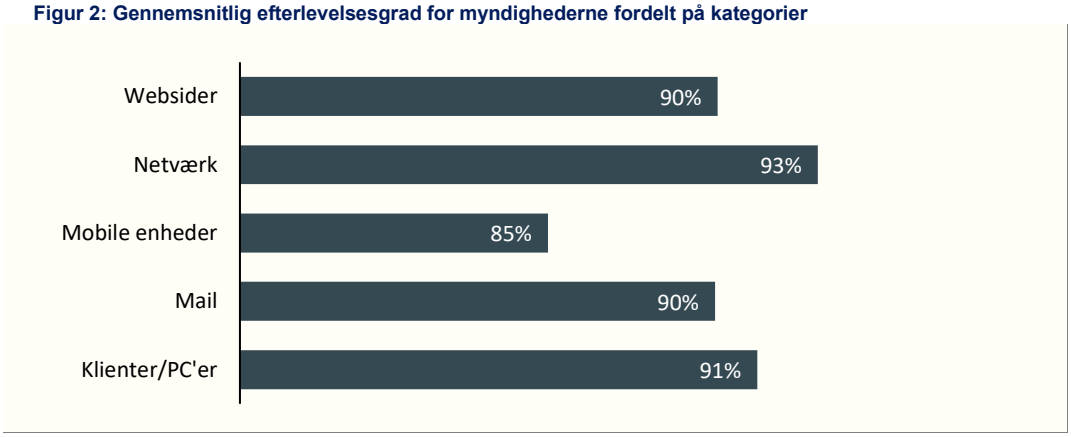
De nærmere resultater for hver af kravene, samt udviklingen i implementeringen heraf, gennemgås nedenfor.

[1] FKO, FE, FMI og BRS indgår ikke i opfølgningen.

De tekniske minimumskrav fordeler sig i fem forskellige kategorier:
1. Klienter/PC'er
2. Mail
3. Mobile enheder
4. Netværk
5. Websider

Den gennemsnitlige efterlevelsesgrad på tværs af alle 20 krav er 90 pct., hvilket betyder, at en myndighed i gennemsnit efterlever 18 ud af 20 krav. I figur 2 er den gennemsnitlige efterlevelsesgrad for myndighederne angivet for de fem kategorier. Kravene relateret til mobile enheder ligger som den eneste under gennemsnittet.

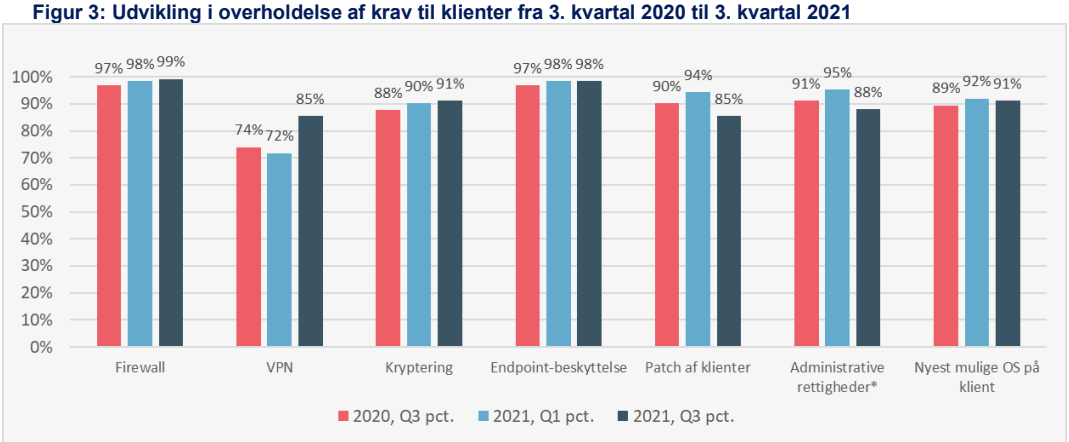
Figur 2: Gennemsnitlig efterlevelsesgrad for myndighederne fordelt på kategorier



Udviklingen i efterlevelsen af de tekniske minimumskrav

Klienter:
I figur 3 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "Klienter".

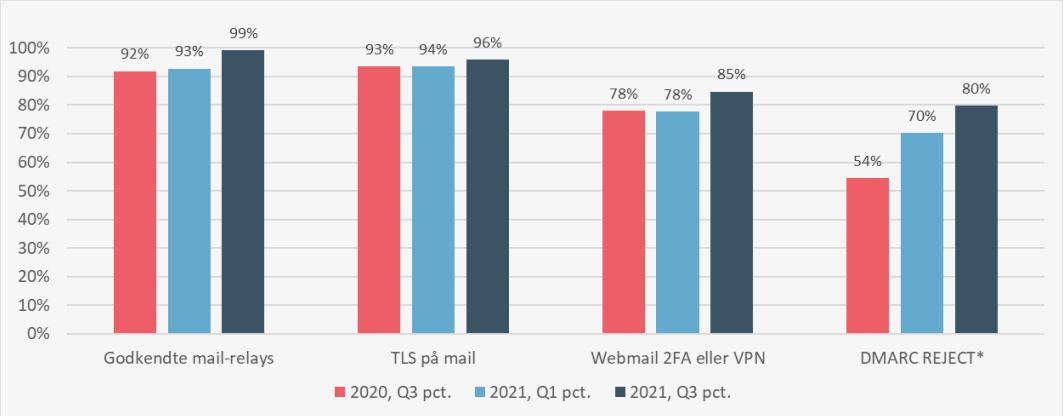
Figur 3: Udvikling i overholdelse af krav til klienter fra 3. kvartal 2020 til 3. kvartal 2021



Det ses, at implementeringen for klient-kravene grundlæggende er høj. Krav om brug af VPN er siden seneste måling gået frem med 13 procentpoint. Omvendt ses der et fald i efterlevelsesgraden på 9 procentpoint i andelen af myndigheder, der efterlever kravet om løbende patching. Faldet skyldes hovedsageligt, at et ministerområde, med en koncernfælles it-funktion, ikke har haft mulighed for at patche klienterne pga. hjemsendelse af medarbejdere som følge af COVID-19. Myndighederne rapporterer desuden, at de klienter og applikationer, som Statens IT har ansvar for, bliver patchet. Den lave efterlevelsesgrad skyldes primært, at nogle myndigheder ikke patcher enkelte tredjepartsapplikationer eller endnu ikke har fået gennemført deres transition til SIT.

Mail:
I figur 4 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "Mail".

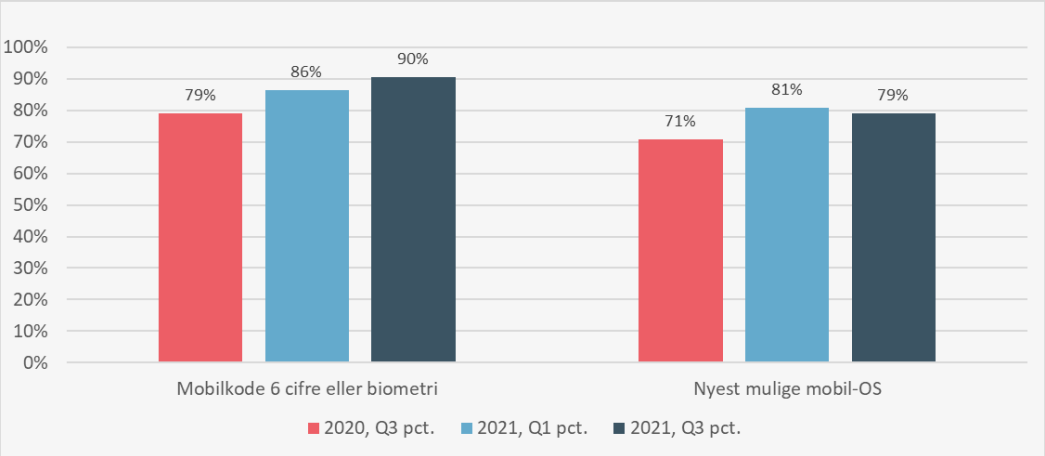
Figur 4: Udvikling i overholdelse af krav til mail fra 3. kvartal 2020 til 3. kvartal 2021



Kravene om godkendte mail-relays og TLS på mail er meget tæt på fuld implementering. Sammenlignet med tidligere målinger, ses der også en stigning i efterlevelsesgraden for kravet om 2-faktor-autentifikation eller VPN ved brug af webmail. Årsagen til den noget lavere efterlevelsesgrad skyldes primært, at et helt ministerområde på koncernniveau ikke efterlever kravet. Dette forventes dog håndteret i efteråret 2021. Endeligt ses der også en væsentlig fremgang i efterlevelsesgraden af kravet om opsætning af DMARC REJECT på myndighedernes domæner. Myndighederne, der ikke efterlever kravet, angiver, at dette vil blive håndteret af SIT, og at der i flere tilfælde er igangsat konkrete implementeringsprojekter.

Mobile enheder:
I figur 5 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "Mobile enheder".

Figur 5: Udvikling i overholdelse af krav til mobile enheder fra 3. kvartal 2020 til 3. kvartal 2021



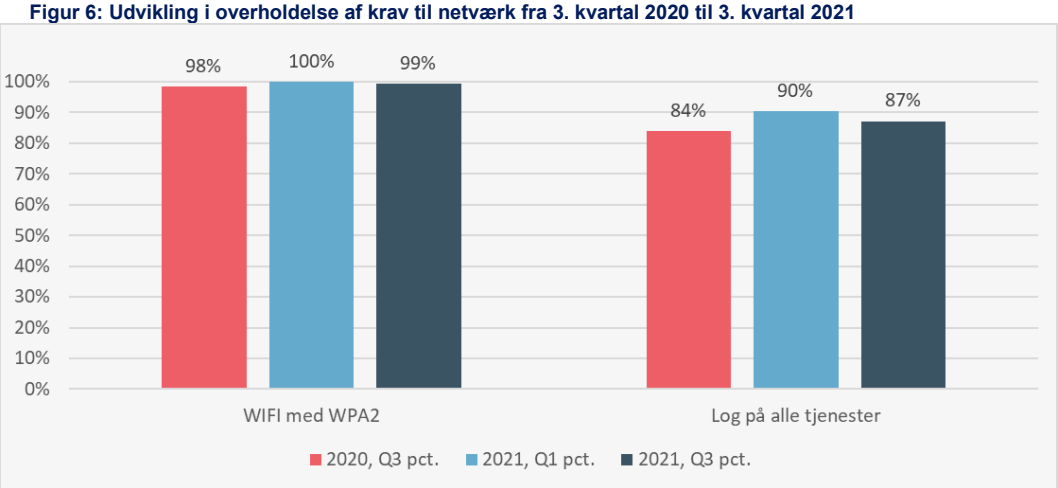
Krav om mobilkode på mindst 6 cifre eller brug af biometri efterleves af 90 pct. af myndighederne, og efterlevelsesgraden har været stigende ved de seneste målinger. Krav om brug af nyest mulige mobil-OS efterleves af ca. 80 pct., hvilket er lavere end ved målingen i Q1 2021. Faldet på ca. 2 procentpoint skyldes, at to myndigheder har ændret deres vurdering af, hvad der er tilstrækkelig ift. at efterleve kravet.

Samlet set angiver myndighederne forskellige årsager til, at de ikke overholder kravet, bl.a. at der endnu ikke er etableret en teknisk løsning, der kan understøtte overholdelsen, eller at myndighederne er i gang med en migrering til Statens It, hvorfor de har udskudt implementering til efter migreringen.

Efterlevelsesgraden forventes derfor at stige ved næste måling, når flere af myndighederne har gennemført deres migrering til Statens It.

Netværk:
I figur 6 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "Netværk".

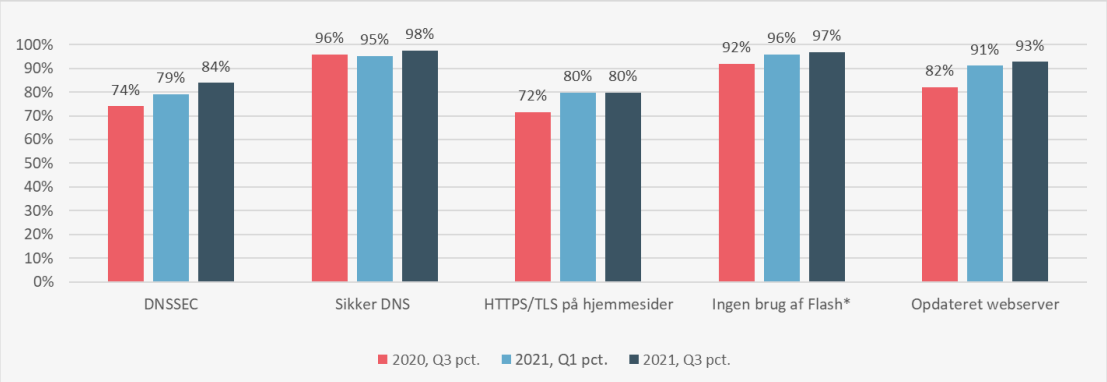
Figur 6: Udvikling i overholdelse af krav til netværk fra 3. kvartal 2020 til 3. kvartal 2021



Der ses en meget høj efterlevelsesgrad på de krav, der angår sikring af netværk. Alle med undtagelse af én myndighed rapporterer, at de har sikring på deres WIFI med WPA2, mens 87 pct. har implementeret den nødvendige logning. Myndighederne, der ikke efterlever logningskravet angiver, at der logges på infrastrukturkomponenterne, hvorfor manglerne primært skyldes, at der ikke logges på enkelte fagsystemer eller at logningen disse steder er mangelfuld. Et ministerområde angiver, at der for en del af deres underliggende myndigheder ikke har været foretaget logning på netværksserverne siden marts 2021. Ministerieret angiver, at dette er ved at blive håndteret.

Websider:
I figur 7 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "Websider".

Figur 7: Udvikling i overholdelse af krav til websider fra 3. kvartal 2020 til 3. kvartal 2021



Grundlæggende er der en høj efterlevelsesgrad for kravene relateret til kategorien "Websider", og efterlevelsesgraden har også været stigende sammenlignet med de tidligere målinger. Den laveste efterlevelsesgrad ses på kravet om at implementere TLS 1.2 (https) på alle hjemmesider/domæner. Der er her tale om et krav, der skal implementeres individuelt på hvert enkelt af myndighedens domæner/hjemmesider. I de fleste tilfælde er det få hjemmesider/domæner, der udestår, for at opnå fuld implementering. Hovedparten af myndighederne har også igangsat projekter mhp. at efterleve kravene, enten gennem implementering eller ved udfasning af ældre websider.