DIGITALISERINGSSTYRELSEN

Tekniske minimumskrav – Status for 2. kvartal

Oktober 2022

2022

Indhold

Indledning

1. Indledning

Rapporten behandler resultatet af de statslige myndigheders implementering af de 20 tekniske minimumskrav til it-sikkerhed. Opfølgningen gælder for 2. kvartal 2022.

Som led i den nationale cyber- og informationssikkerhedsstrategi for 2018-2021 blev det besluttet, at de statslige myndigheder skulle efterleve en række tekniske minimumskrav med henblik på at sikre et højt fælles sikkerhedsniveau i staten.

Kravene er ufravigelige for de statslige myndigheder og har primært til formål at beskytte statslige it-arbejdspladser, herunder arbejdsnetværk og arbejdsstationer, mod ondsindede cyber- og informationssikkerheds-hændelser, for eksempel hackerangreb og spredning af malware. De første 17 krav skulle være implementeret senest den 1. januar 2020, mens tre ydergere krav først trådte i kraft den 1. juli 2020.

Tekniske minimumskrav – spørgeskema

Til brug for de løbende opfølgninger har Digitaliseringsstyrelsen udarbejdet et spørgeskema til at foretage målingen på de tekniske minimumskrav. På baggrund af en beskrivelse af opfyldelseskriteriet for hvert enkelt krav, angiver myndighederne om de efterlever de enkelte krav. Kravene fordeler sig på fem kategorier:

- Klienter/PC'er
- Mail
- Mobile enheder
- Netværk
- Websider

Det fremgår af følgeteksten til spørgeskemaerne, at et krav kun kan betragtes som efterlevet i tilfælde af "*fuld*" efterlevelse, altså hvor der ikke er nogen udeståender ift. implementeringen af kravet i den enkelte myndighed.

De seneste opfølgninger på myndighedernes efterlevelse har vist, at der er en forholdsvis høj grad af efterlevelse på tværs af staten, men at der fortsat er en del myndigheder, der ikke efterlever alle krav.

Resultater

- 2. kvartal 2022

2. Resultater

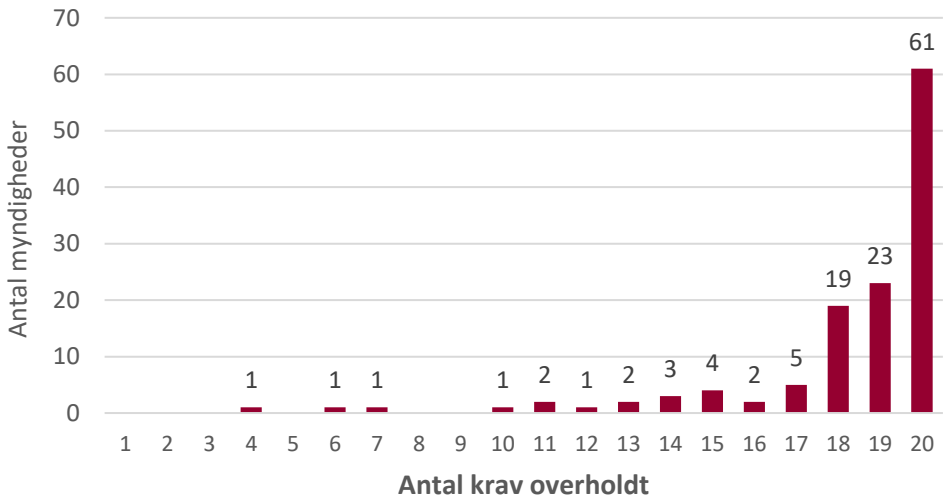
Opfølgningen viser en forholdsvis høj efterlevelse af kravene på tværs af staten. Der har dog været en begrænset forbedring i efterlevelsen sammenlignet med tidligere opfølgninger.

Der er i hhv. første og tredje kvartal af 2021 samt i andet kvartal 2022 foretaget opfølgning på, om myndighederne efterlever de tekniske minimumskrav. Ved denne måling er der modtaget 126 besvarelser fra myndigheder og institutioner på samtlige ministerområder.

Resultaterne viser overordnet set følgende:

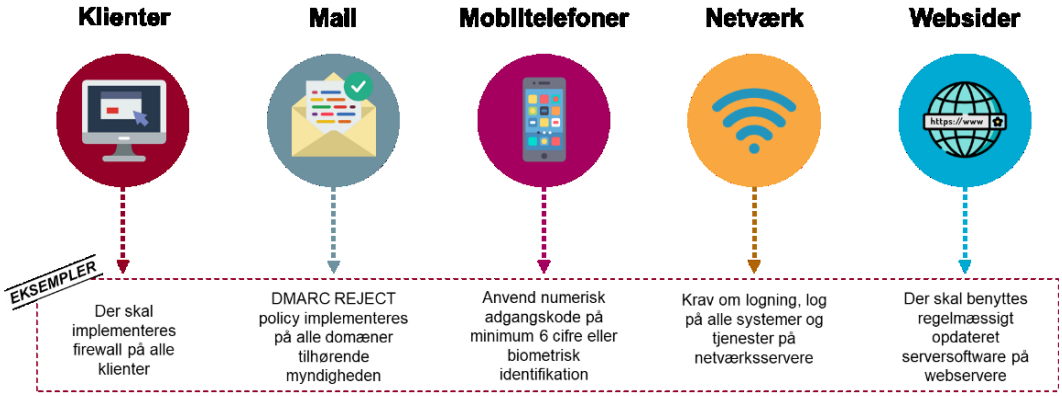
- 61 (48 pct.) af myndighederne efterlever samtlige 20 krav. Det er en fremgang på ca. 2 procentpoint siden målingen i tredje kvartal 2021, hvor 57 myndigheder havde opnået fuld implementering af kravene.
- 114 myndigheder efterlever mindst 15 af kravene, hvilket svarer til 90 pct.
- 3 myndigheder (2 pct.) efterlever mindre end 10 krav.

Figur 1: Antal myndigheder fordelt på antal krav, der efterleves.



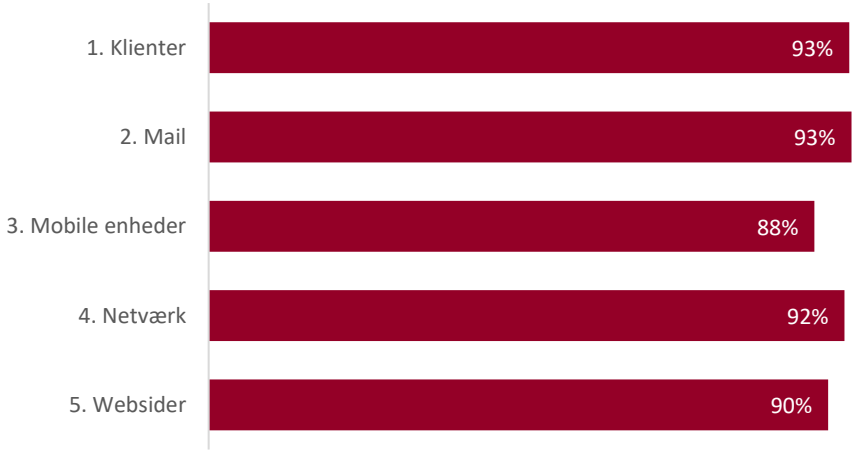
De 20 tekniske minimumskrav fordeler sig i fem forskellige kategorier jf. figur 2.

Figur 2: Eksempler på krav fordelt på de fem kategorier



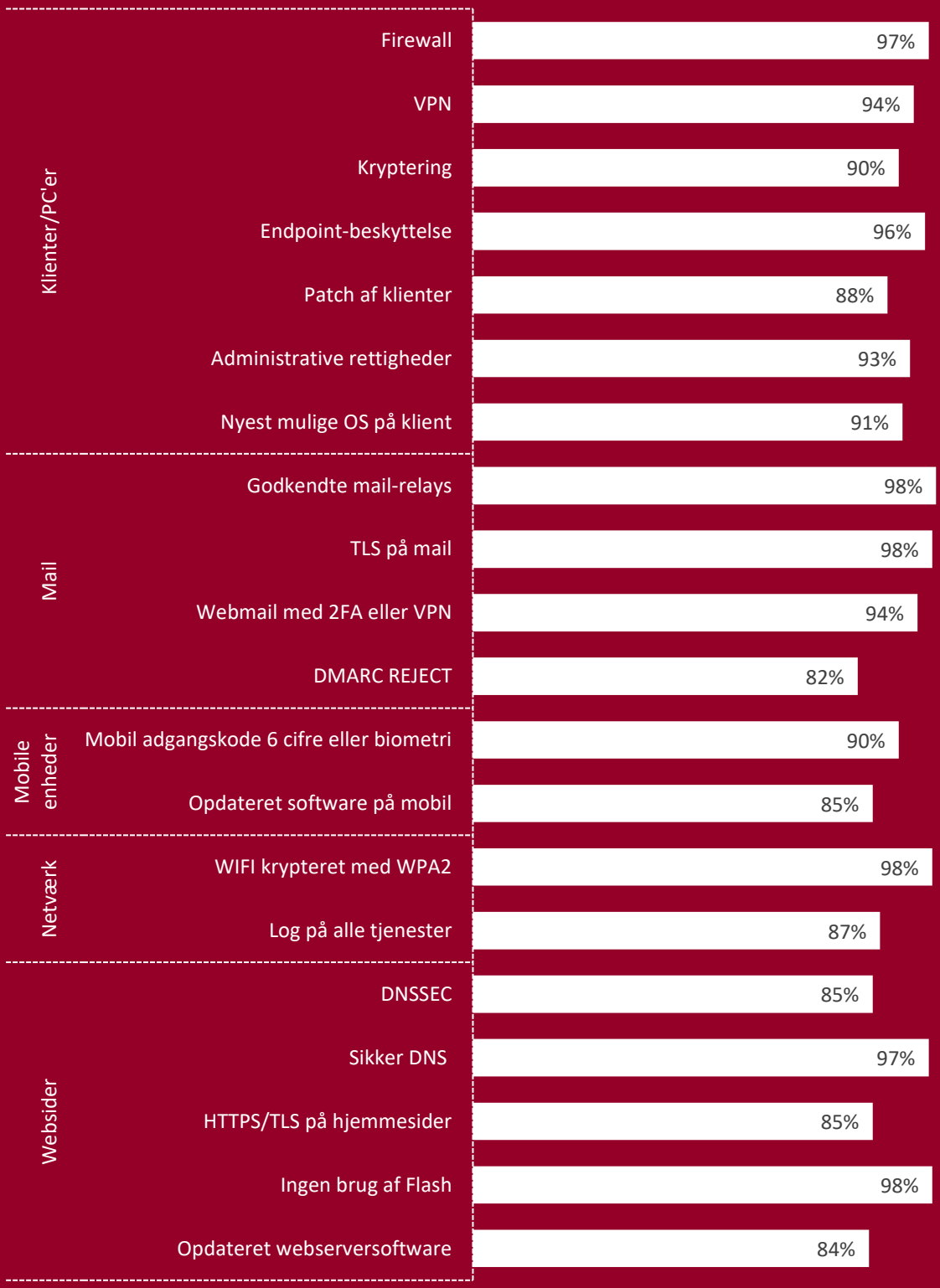
Den gennemsnitlige efterlevelsesgrad på tværs af alle 20 krav er ca. 91 pct., hvilket betyder, at en myndighed i gennemsnit efterlever 18 ud af 20 krav. I figur 3 er den gennemsnitlige efterlevelsesgrad for myndighederne angivet for de fem kategorier. Der ses generelt en høj efterlevelsesgrad af kravene for alle kategorierne. Kravene vedrørende mobile enheder og websider ligger som de eneste under gennemsnittet.

Figur 3: Gennemsnitlig efterlevelsesgrad for myndighederne fordelt på kategorier



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

Myndighedernes efterlevelsesgrad fordelt på kravene
2. kvartal 2022

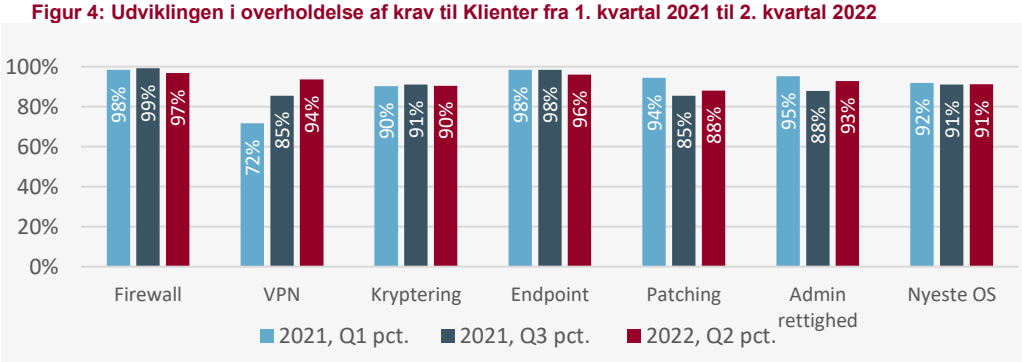


2.1 Udviklingen i implementeringen af minimumskravene

I dette kapitel vises udviklingen i andelen af myndigheder, der efterlever kravene for hver af de fem kategorier. Der er forskel på antallet af myndigheder, som har rapporteret ved de forskellige målinger. Det er derfor ikke præcis de samme myndigheder, der sammenlignes på tværs af de tre målinger.

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

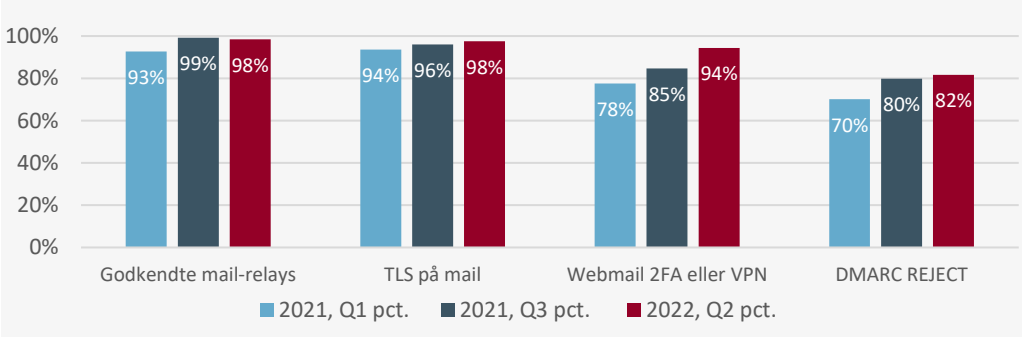
Figur 4: Udviklingen i overholdelse af krav til Klienter fra 1. kvartal 2021 til 2. kvartal 2022



Myndighederne har en grundlæggende høj efterlevelsesgrad af kravene vedrørende klienter. Kravet om brug af VPN er siden målingen i første kvartal 2021 steget med hele 22 procentpoint. Omvendt er der sket et fald i andelen af myndigheder, der efterlever kravet om løbende patching. Årsagen til den manglende efterlevelse er primært, at nogle myndigheder ikke patcher enkelte tredjepartsapplikationer eller endnu ikke har fået gennemført deres transition til Statens It. Myndighederne angiver også, at de klienter og applikationer, som Statens It har ansvar for, bliver patchet.

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

Figur 5: Udviklingen i overholdelse af krav til Mail fra 1. kvartal 2021 til 2. kvartal 2022

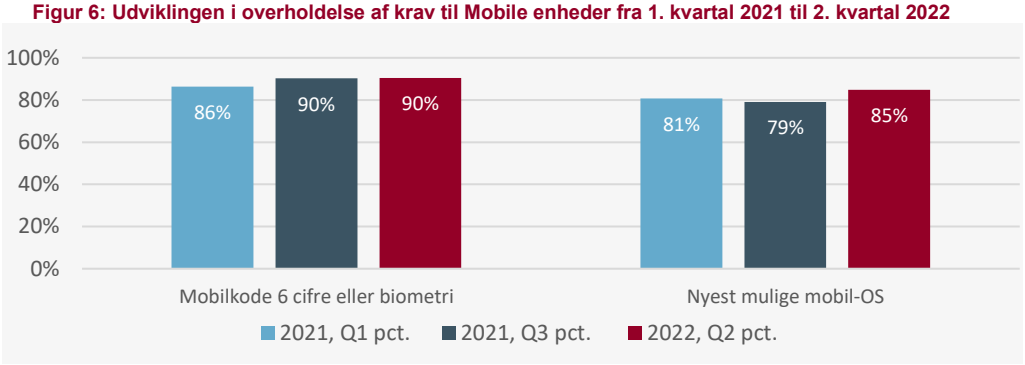


Generelt har myndighederne en høj efterlevelse af kravene vedrørende mail. For kravet om flerfaktor-autentificering (2FA) eller anvendelse af en VPN ved brug af webmail, er andelen af myndigheder, som efterlever kravet steget med 16 procentpoint siden opfølgningen i første kvartal 2021.

Der ses en lille fremgang i den samlede efterlevelsesgrad på kravet om opsætning af en DMARC REJECT policy på myndighedernes domæner. Siden seneste rapportering er flere myndigheder kommet i mål med kravet. Forklaringen på den begrænsede effekt er, at et ministerområde med en koncernfælles it-funktion, der tidligere har været i mål med kravet, har overtaget nogle nye domæner, der endnu ikke lever op til kravet. Det betyder, at flere myndigheder på dette ministerområde ikke længere efterlever kravet, hvilket trækker den samlede efterlevelsesgrad ned. Generelt angiver de myndigheder, der ikke efterlever kravet om DMARC, at der er opsat en DMARC politik på langt de fleste af deres domæner, hvorfor det er et fåtal af domæner, som udestår. Myndighederne har også konkrete planer for håndtering af domænerne og angiver, at de på sigt enten vil udfase dem eller overdrage dem til Statens It.

Mobile enheder:
I figur 6 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "*Mobile enheder*"

Figur 6: Udviklingen i overholdelse af krav til Mobile enheder fra 1. kvartal 2021 til 2. kvartal 2022



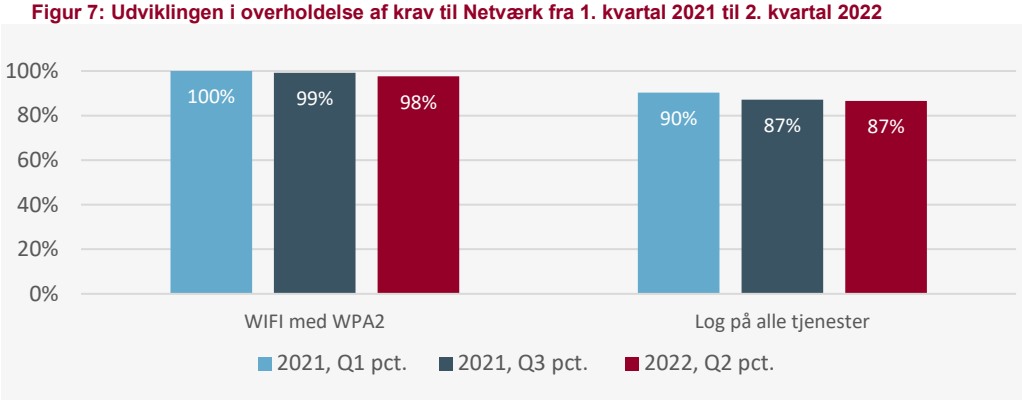
Andelen af myndigheder, der efterlever kravet om minimum 6 cifre eller biometrisk adgangskode på mobile enheder er uændret siden opfølgningen i tredje kvartal 2021. De myndigheder, som ikke efterlever kravet angiver, at de er i færd med at udrulle en MDM-løsning (Mobile Device Mangement). Andre myndigheder afventer afslutning af deres transition til Statens It, herunder implementering af Statens It's MDM-løsning. Det fremgår af rapporteringerne, at det i tilfælde af manglende efterlevelse ofte er relativt få mobile enheder, der ikke lever op til kravet om passwords på mobile enheder.

For kravet vedrørende regelmæssig opdatering af operativsystem på mobile enheder, ses en fremgang på 4 procentpoint siden opfølgningen i første kvartal 2021 og en fremgang på 6 procentpoint sammenlignet med opfølgningen i tredje kvar-

tal 2021. Fremgangen skyldes hovedsageligt, at flere myndigheder på et ministerområde er blevet omfattet af Statens It's MDM-løsning og dermed procedure omkring opdatering af telefoner. Størstedelen af de myndigheder, som ikke efterlever kravet, angiver her, at kravet forventes efterlevet, når deres egen MDM-løsning er implementeret, eller der er gennemført en transition til Statens It.

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

Figur 7: Udviklingen i overholdelse af krav til Netværk fra 1. kvartal 2021 til 2. kvartal 2022



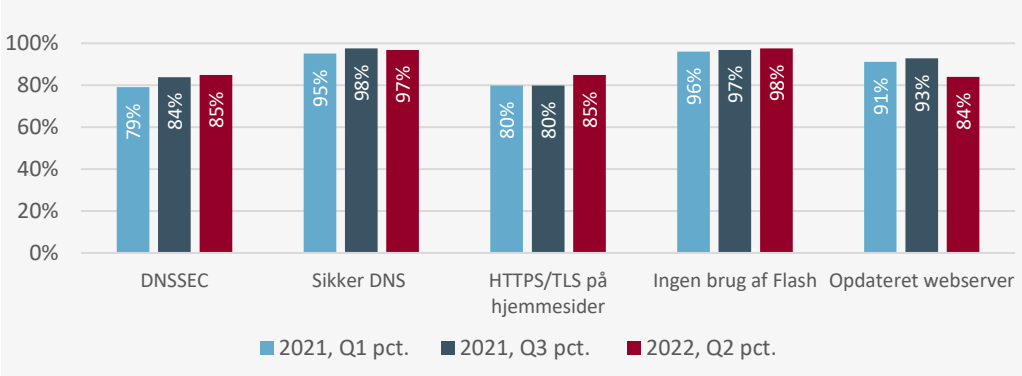
Der ses en meget høj efterlevelsesgrad for kravet vedrørende kryptering af myndighedens arbejdsnetværk med minimum WPA2. Der kan dog konstateres et mindre fald i efterlevelsen sammenlignet med de tidligere målinger. Faldet skyldes udelukkende, at der ved denne opfølgning indgår andre myndigheder, end dem som indgik i den seneste opfølgning. Da de nye myndigheder endnu ikke er i mål med kravet, påvirker det den samlede efterlevelsesgrad negativt. Disse myndigheder angiver, at et mindre lokalt netværk skal opdateres, førend kravet er overholdt.

Efterlevelsen for kravet vedrørende logning er uændret sammenlignet med den seneste opfølgning. Den primære forklaring herpå er også, at der ved denne opfølgning indgår nogle andre myndigheder, og at disse myndigheder ikke efterlever kravet. Ses der ikke på de samlede andele, men på de konkrete myndigheder, er der flere myndigheder, som siden seneste måling er kommet i mål med logningskravet. Denne positive effekt udlignes dog af de nye myndigheder, hvorfor der samlet set ikke kan ses en fremgang. De myndigheder, som ikke efterlever kravet, angiver, at der er igangsat konkrete projekter med henblik på at sikre efterlevelse fremover.

Websider

I figur 8 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "*Websider*"

Figur 8: Udviklingen i overholdelse af krav til Websider fra 1. kvartal 2021 til 2. kvartal 2022



For kravene vedrørende DNSSEC, Sikker DNS og ingen brug af Flash, er efterlevelsesgraden mere eller mindre uændret sammenlignet med seneste opfølgning fra tredje kvartal 2021. Sammenlignet med de tidligere opfølgninger er efterlevelsesgraden steget med 5 procentpoint for kravet om kryptering af hjemmesider. Omvendt er andelen af myndigheder, der efterlever kravet om regelmæssig opdatering af serversoftware på webservere faldet. Faldet skyldes bl.a., at enkelte myndigheder har ændret deres vurdering af, hvad der tilstrækkelig ift. at efterleve kravet, eller at myndighederne har fået ansvar for nye domæner, som endnu ikke lever op til kravet. Forklaringen skyldes til dels også, at der ved denne opfølgning, indgår nye myndigheder, som ikke har indgået i de tidligere opfølgninger. Disse nye myndigheder er ikke i mål med kravene, hvorfor den samlede efterlevelsesgrad påvirkes negativt.

Appendiks

3. Appendiks

De 20 tekniske minimumskrav og deres formål er angivet i tabel 1.

Tabel 1

De 20 tekniske minimumskrav og deres formål

Minimumskrav	Formål
Krav 1. Firewall Der skal implementeres firewall på alle klienter.	Firewalls skal sikre mod utilsigtet adgang til arbejdsstationer. Malware forsøger typisk at sprede sig på tværs af systemer, og ved at fjerne denne mulighed kan man begrænse denne spredning. Bør konfigureres så restriktivt som muligt.
Krav 2. VPN-løsning Der skal benyttes en af myndigheden stillet til rådighed VPN-løsning til at gå på internettet via arbejds-PC fra eksterne netværk.	Brug af VPN skal sikre dataintegritet og fortrolighed og bl.a. modvirke man-in-the-middle angreb.
Krav 3. Kryptering af harddiske Kryptering af harddiske.	For at undgå kompromittering af data i forbindelse med tab eller tyveri af PC, skal operativsystemet være sat op til at kryptere harddisken på den enkelte PC.
Krav 4. End-point beskyttelse Der skal implementeres endpoint-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter.	Anvendelse af kontinuerligt opdateret endpoint-beskyttelse sikrer, at kendte vira, malware mv. ikke kan afvikles på arbejdsstationen. De fleste endpoint protection-programmer kontrollerer ligeledes for anormal adfærd i applikationer.
Krav 5. Regelmæssig opdatering af klienter Klienter skal patches og opdateres regelmæssigt – både operativsystem og applikationer.	Al software der implementeres bør være omfattet af regelmæssig opdatering, således at evt. sårbarheder hurtigst muligt bliver lukket, så systemet ikke kan udnyttes af offentlige tilgængelige exploits.
Krav 6. Begrænset tildeling af lokaladministratorrettigheder Administrative rettigheder for brugere tildeles kun tidsbegrænset og med veldokumenterede behov.	Størstedelen af malware kræver administrative rettigheder på PCen for at blive installeret. For at hindre risikoen for spredning af malware, skal brugere derfor ikke have administrationsrettigheder med mindre, der er et dokumenteret forretningsmæssigt behov.
Krav 7. Sikkerhedsopdateret operativsystem Det anvendte operativsystem skal være så nyt som muligt, og skal som minimum være supporteret med sikkerhedsopdateringer.	Nyeste operativsystemer har, som udgangspunkt, et højere sikkerhedsniveau end ældre versioner. Operativsystemer som ikke længere supporteres af producenten modtager typisk ikke sikkerhedsopdateringer, når der opdages nye sårbarheder og exploits.

Krav 8. Godkendte mail-relays med autentifikation Der må kun anvendes af myndigheden godkendte mail-relays med autentifikation.	Anvendelse af åbne mail relays kan kompromittere meddelelsessikkerheden. Ved kun at anvende af myndigheden godkendte mail relays med autentifikation øges sikkerheden, og risikoen for misbrug af mail-server til spredning af malware og spam reduceres.
Krav. 9. Kryptering af kommunikation med mail-protokoller 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 modtageren understøtter det.	Kryptering af mailtrafik skal sikre dataintegritet og fortrolighed. Med anvendelse af TLS 1.2 reduceres risikoen for, at mail-kommunikation bliver aflyttet undervejs i transmissionen over internettet.
Krav 10. To-faktor-autentifikation eller direkte VPN-forbindelse Webmail må kun anvendes uden for myndighedens lokale netværk, hvis dette foregår vha. 2FA eller via en direkte VPN-forbindelse til myndighedens netværk.	Skal forhindre adgang til myndighedens e-mail ved tilslutning via usikre netværk. Med VPN sikres en direkte og krypteret forbindelse ind i myndighedens eget netværk.
Krav 11. DMARC-REJECT-policy på domæner DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden.	DMARC er et valideringssystem designet til at forhindre såkaldt email-spoofing, hvor en afsender udgiver sig for at være en anden. Løsningen giver også en god mitigering mod afsendelse af spam fra myndighedens domæner.
Krav 12. Adgangskode på min. 6 cifre eller biometrisk identifikation Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation.	Krav om minimumlængde og anvendelse af numerisk kode eller biometrisk identifikation frem for andre typer adgangsgodkendelse beskytter telefonen mod misbrug, hvis den tabes/stjæles.
Krav 13. Regelmæssig opdatering af mobile enheder Operativsystem og apps på mobile enheder skal opdateres regelmæssigt.	Mobiltelefoners software skal så vidt muligt opdateres, så snart leverandøren udgiver opdateringer. Derved sikres, at kendte sikkerhedshuller lukkes hurtigst muligt.
Krav 14. Kryptering af wi-fi på arbejdsnetværk. WiFi på myndighedens arbejdsnetværk skal være krypteret med WPA2.	Kryptering af WiFi gør det vanskeligere for en angriber, at "aflytte" kommunikation på netværket. WPA2 er sikrere end WPA og bør være standardvalget.
Krav 15. Logning Krav om logning, log på alle systemer og tjenester på netværksservere.	Udgør en forudsætning for opdagelse og efterforskning af forskellige sikkerhedshændelser. Logningen skal ikke anvendes til overvågning af brugeradfærd.
Krav 16. DNSSEC DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.	DNSSEC er en ekstra sikkerhedsservice, man kan tilknytte sit domænenavn. Med DNSSEC kan man være sikker på, at den rigtige side bliver vist, når der bliver linket til ens hjemmeside, og når den direkte URL-adresse bliver brugt. Klienter kan dermed kryptografisk stole på, at de tilgår det rette domæne.

Krav 17. Beskyttelse mod skadelige hjemmesider Myndigheden skal anvende en Sikker DNS-tjeneste eller implementere 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 Kommunikation til hjemmesider skal krypteres og anvende minimum TLS 1.2, dvs. der skal implementeres HTTPS på alle hjemmesider.	Kryptering af trafik til og fra hjemmesider skal sikre dataintegritet og fortrolighed, herunder forebygge man-in-the-middle angreb.
Krav 19. Flash Der må ikke anvendes Flash på hjemmesider tilhørende myndigheden.	Flash er et plugin, som tidligere har været bredt anvendt til at tilbyde avanceret eksempelvis grafisk funktionalitet og spil på hjemmesider. Anvendelse af Flash i en web-browser frarådes i forvejen, men udgør fortsat størstedelen af sårbarheder, der anvendes til at kompromittere en PC gennem kørsel af skadelig flash-kode. Flash når end-of-life i 2020 og modtager herefter ikke flere opdateringer
Krav 20. Regelmæssig opdatering af webservere Der skal benyttes regelmæssigt opdateret serversoftware på webservere.	Al software der implementeres bør være omfattet af regelmæssig opdatering, således evt. sårbarheder hurtigst muligt bliver lukket for offentligt tilgængelige exploits mv.

digst.dk