DIGITALISERINGSSTYRELSEN

Tekniske minimumskrav – Status for 3. kvartal

November 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 3. 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 informationssikkerhedshændelser, for eksempel hacker-angreb 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

- 3. kvartal 2022

2. Resultater

Opfølgningen viser en forholdsvis høj efterlevelse af kravene på tværs af staten. Der har siden andet kvartal været en tilbagegang i efterlevelsen af kravene i kategorien Klienter, og en begrænset forbedring i efterlevelsen af de øvrige kategorier.

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

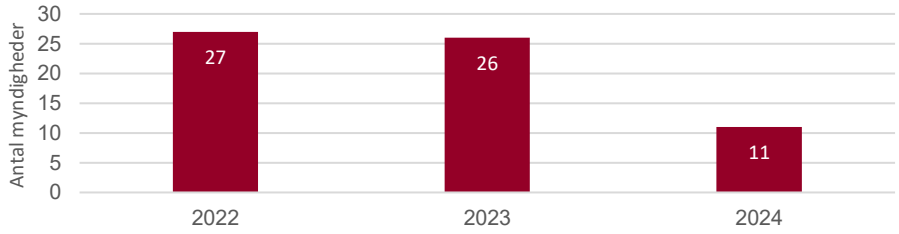
Resultaterne viser overordnet set følgende:

- 62 (49 pct.) af myndighederne efterlever samtlige 20 krav. Det er en myndighed mere sammenlignet med målingen i andet kvartal 2022, hvor 61 myndigheder efterlevede samtlige 20 krav.
- 105 (83 pct.) af myndighederne efterlever mindst 15 af kravene. Det er et fald på 7 procentpoint siden seneste måling.
- 4 myndigheder (3 pct.) efterlever mindre end 10 krav.

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

Ministerområderne har udarbejdet en handlingsplan, såfremt der er myndigheder på deres område, der ikke er i mål med alle 20 krav. I handlingsplanerne er der angivet en tidsplan for, hvornår de enkelte myndigheder forventer at være i mål med alle kravene. Disse forventninger er opsummeret i figur 2.

Figur 2: Myndighedernes målsætning vedr. efterlevelse af alle kravene

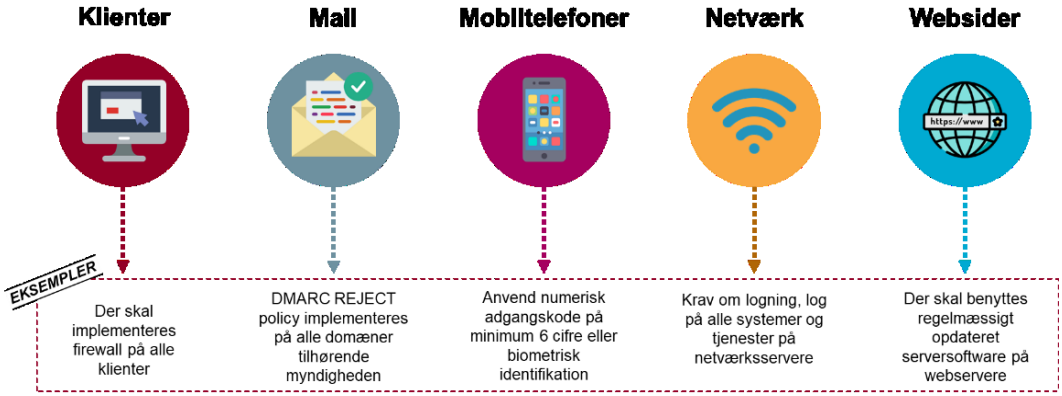


Som vist i figur 2, er der 53 myndigheder, der forventer at være i mål med efterlevelsen af alle 20 krav i 2023. Dog er der 11 myndigheder, som først forventer at kunne overholde alle kravene i 2024.

Resultaterne fordelt på de overordnede kategorier

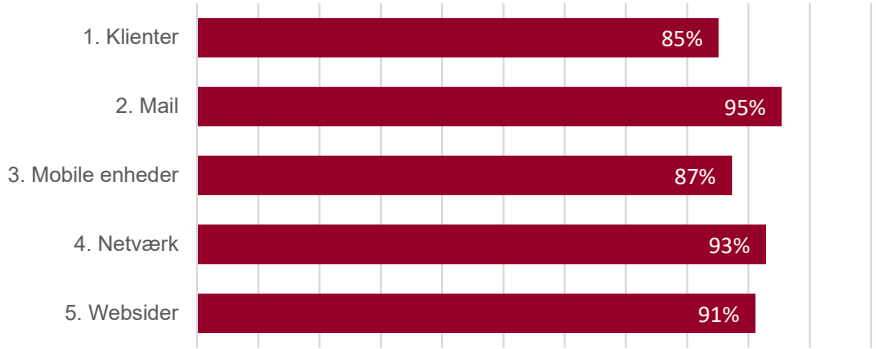
De 20 tekniske minimumskrav fordeler sig i fem forskellige kategorier jf. figur 3.

Figur 3: Eksempler på krav fordelt på de fem kategorier



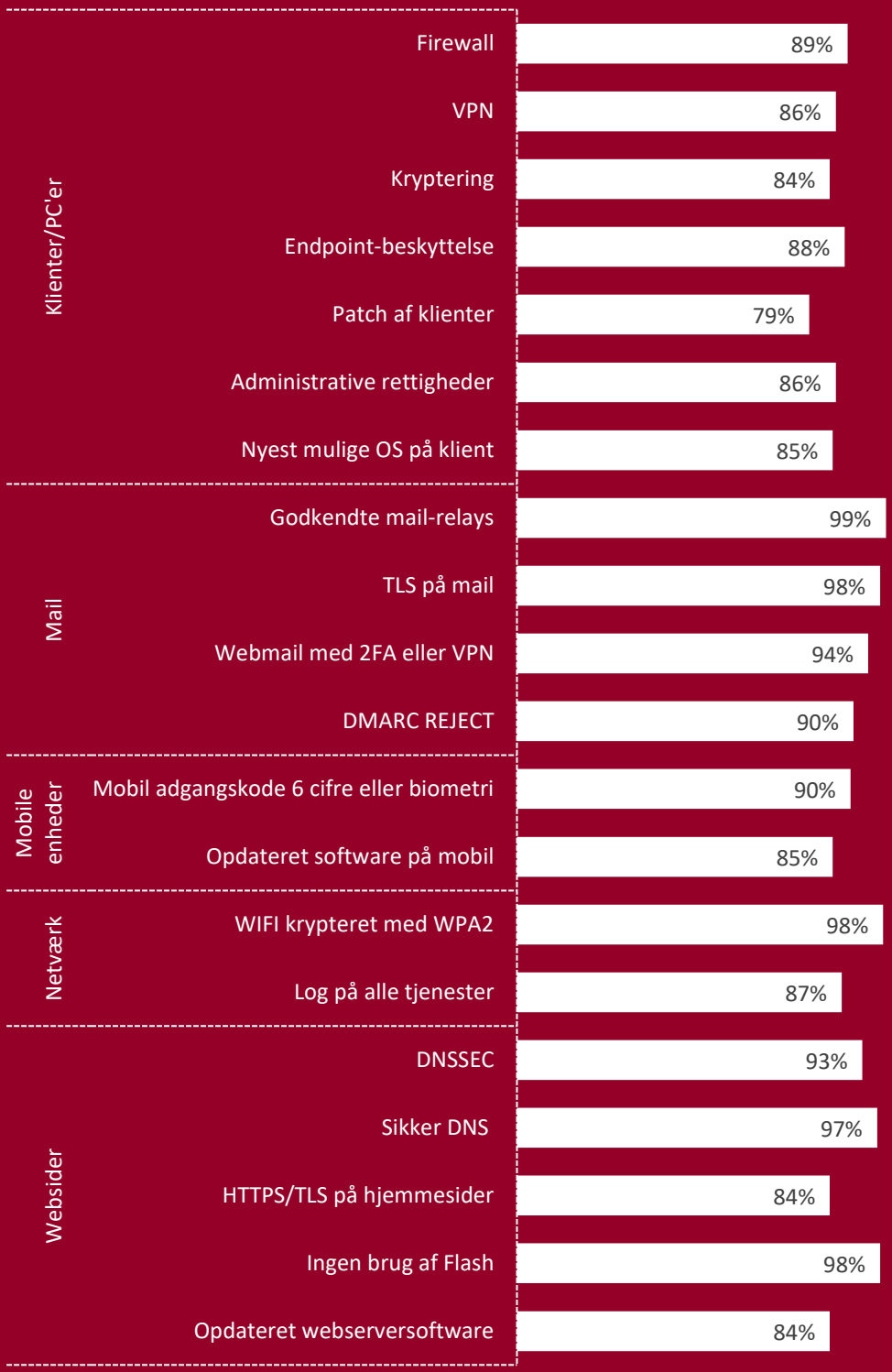
Den gennemsnitlige efterlevelsesgrad på tværs af alle 20 krav er ca. 90 pct., hvilket betyder, at en myndighed i gennemsnit efterlever 18 ud af 20 krav. I figur 4 er den gennemsnitlige efterlevelsesgrad for myndighederne angivet for de fem kategorier. Der ses generelt en høj efterlevelsesgrad af kravene for alle kategorierne. Kravene vedrørende klienter og mobile enheder ligger som de eneste under gennemsnittet.

Figur 4: Gennemsnitlig efterlevelsesgrad for myndighederne fordelt på kategorier



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

Andelen af myndigheder som efterlever de enkelte minimumskrav for tredje kvartal 2022

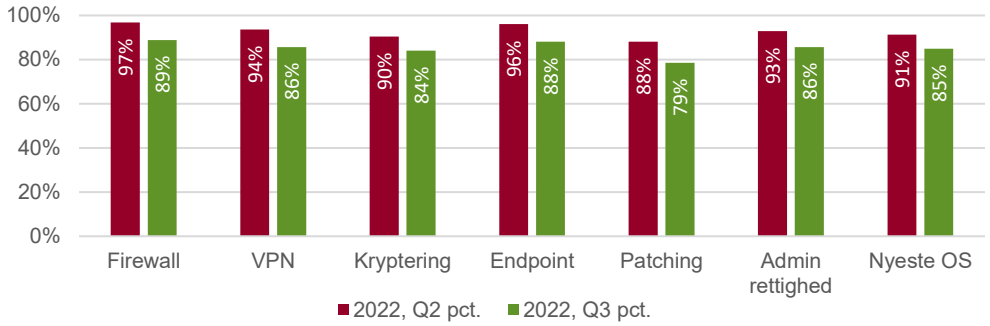


2.1 Udviklingen i implementeringen af minimumskravene

I dette kapitel vises udviklingen i andelen af myndigheder, der efterlever kravene for hver af de fem kategorier. Til at illustrere udviklingen er der foretaget en sammenligning fra andet og tredje kvartal i 2022. Det er de samme myndigheder, der indgår i begge målinger.

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

Figur 5: Udviklingen i overholdelse af krav til Klienter fra 2. kvartal 2022 til 3. kvartal 2022

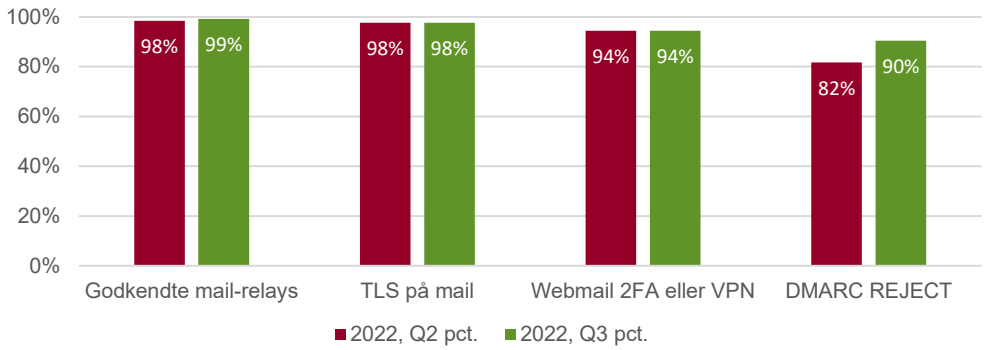


Sammenlignet med målingen fra 2. kvartal ses et fald i efterlevelsesgraden for alle kravene under kategorien klienter. Årsagen til faldet skyldes hovedsageligt, at et en myndighed med en koncernfælles it-funktion ikke længere efterlever kravene, hvorfor flere myndigheder ikke længere overholder kravene. Den manglende efterlevelse skyldes primært, at myndigheden er blevet opmærksom på, at kravene ikke var overholdt for et mindre antal computere i koncernen. Myndigheden har igangsat en række aktiviteter for at sikre overholdelse af kravet. Myndigheden har også plan om at indføre løbende kontroller, så det sikres, at implementeringen sker korrekt.

Andre myndigheder begrunder den manglende efterlevelse med, at de 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 6 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "*Mail*".

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

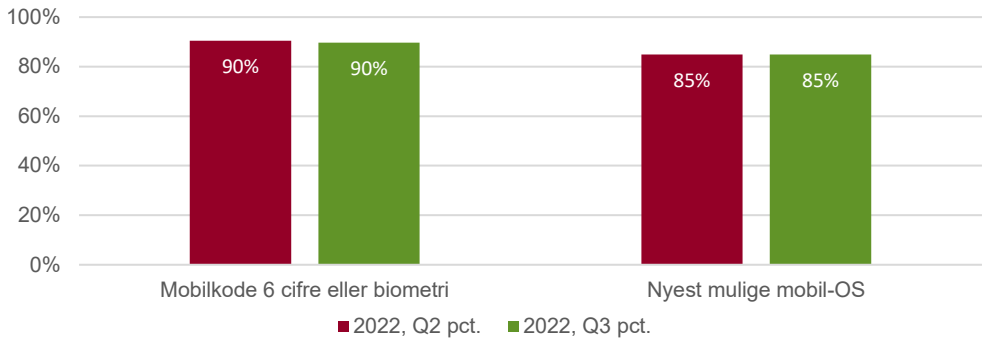


Generelt har myndighederne en høj efterlevelse af kravene vedrørende mail. For kravet om flerfaktor-autentificering (2FA), anvendelse af en VPN ved brug af webmail, eller godkendte mail-relays er efterlevelsen fortsat høj og uændret. For kravet om DMARC REJECT er andelen af myndigheder, som efterlever kravet steget med 8 procentpoint siden opfølgningen i andet kvartal 2022. Forklaringen på fremgangen er primært, at et ministerområde med en koncernfælles it-funktion, er kommet i mål med kravet siden afrapporteringen i andet kvartal 2022.

Generelt angiver de myndigheder, der ikke efterlever kravet om DMARC REJECT, at der er opsat en DMARC REJECT-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 7 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "*Mobile enheder*"

Figur 7: Udviklingen i overholdelse af krav til Mobile enheder fra 2. kvartal 2022 til 3. kvartal 2022

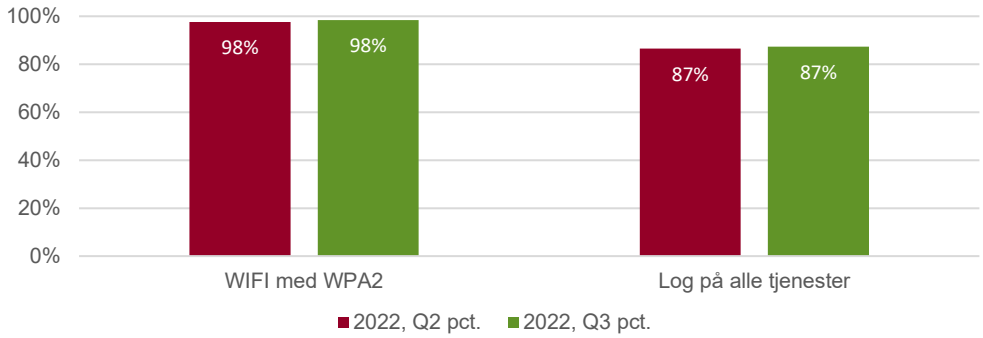


Andelen af myndigheder, der efterlever kravet om minimum 6 cifre eller biometrisk adgangskode på mobile enheder er uændret siden opfølgningen i andet kvartal 2022. Myndighederne er fortsat i færd med at udrulle en MDM-løsning (Mobile Device Mangement) med henblik på teknisk understøttelse af kravene. 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 er efterlevelsen også uændret siden andet kvartal 2022. Størstedelen af de myndigheder, som ikke efterlever kravet angiver, at kravet forventes efterlevet, når deres egen MDM-løsning er implementeret, eller der er gennemført en transition til Statens It.

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

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



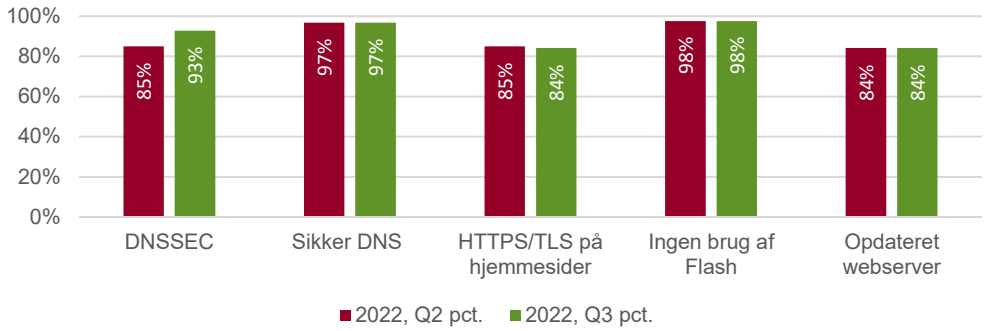
Der ses en meget høj efterlevelsesgrad for kravet vedrørende kryptering af myndighedens arbejdsnetværk med minimum WPA2. Der er en enkelt myndighed mere der er kommet i mål med kravet siden opfølgningen i andet kvartal 2022. De myndigheder der ikke er i mål med kravet angiver, at et mindre lokalt netværk skal opdateres, førend kravet er overholdt.

Efterlevelsen for kravet vedrørende logning er uændret sammenlignet med den seneste opfølgning. Siden andet kvartal 2022 er enkelte myndigheder kommet i mål med implementering af kravet, samtidig med at andre myndigheder ikke længere efterlever kravet. Det samlede antal af myndigheder der efterlever kravet, er derfor uændret. For de myndigheder der ikke længere er i mål med kravet, er årsagen en igangværende udrulning af log-værktøjer, eller fordi myndighederne afventer Statens It.

Websider

I figur 9 vises udviklingen i andelen af myndigheder, der efterlever kravene for kategorien "*Websider*"

Figur 9: Udviklingen i overholdelse af krav til Websider fra 1. kvartal 2021 til 2. kvartal 2022



For kravet vedrørende DNSSEC er der sket en stigning på 8 procentpoint i efterlevelsen af kravet. Stigningen skyldes især, at en myndighed med en koncernfælles it-funktion nu efterlever kravet, hvorved flere myndigheder også er nået i mål. For kravene vedrørende Sikker DNS, ingen brug af Flash og opdateret webserver, er efterlevelsesgraden uændret sammenlignet med seneste opfølgning fra andet kvartal 2022.

Omvendt er andelen af myndigheder, der efterlever kravet om HTTPS/TLS på hjemmesider faldet med 1 procentpoint. Årsagen hertil er, at en enkelt myndighed står overfor to mindre opgraderinger af et enkelt system. Når opgraderingen er gennemført, vil myndigheden overholde kravet.

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