DIGITALISERINGSSTYRELSEN

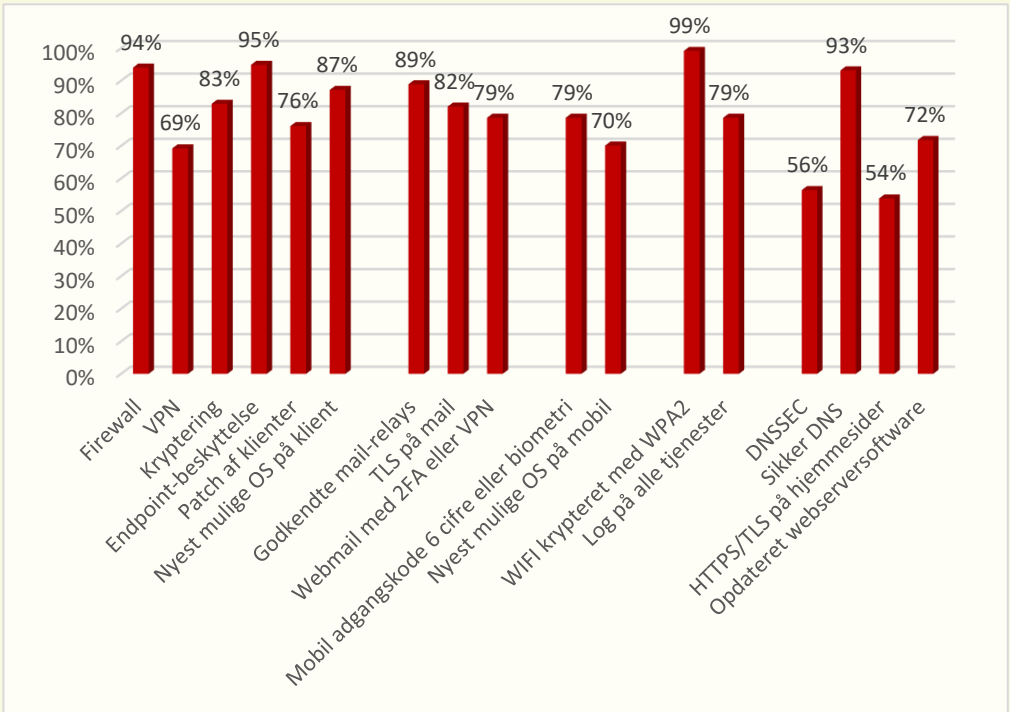
Faktaark

Myndighedernes efterlevelse af de tekniske minimumskrav til sikkerheden i statslige myndigheder – 1. kvartal 2020

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. 17 af kravene skulle være implementeret senest den 1. januar 2020, mens yderligere 3 krav skulle være implementeret den 1. juli 2020. Kravene er alle ufravigelige.

Digitaliseringsstyrelsen gennemførte i februar/marts 2020 en opfølgning på myndighedernes daværende efterlevelse af kravene. Opfølgningen blev gennemført i form af en spørgeskemaundersøgelse, hvor myndighederne skulle forholde sig til efterlevelsen af de enkelte krav i myndigheden. Det fremgik af følgeteksten til spørgeskemaet, 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. Der blev modtaget 117 besvarelser fra myndigheder og institutioner på samtlige ministerområder. Følgende figurer viser resultaterne af målingen af efterlevelsen af de 17 krav, der trådte i kraft 1. januar 2020.

Figur 1
Tekniske minimumskrav - procent implementeret 1. kvartal 2020



Figur 2
Tekniske minimumskrav - antal implementeret 1. kvartal 2020

Krav	Antal implementeret	Procent implementeret
Klienter/Pcer		
Der skal implementeres firewall på alle klienter	110	94%
Der skal benyttes en af myndigheden stillet til rådighed VPN-løsning til at gå på internettet via arbejds-PC fra eksterne netværk.	81	69%
Kryptering af harddiske	97	83%
Der skal implementeres endpoint-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter.	111	95%
Klienter skal patches og opdateres regelmæssigt – både OS og applikationer	89	76%
Det anvendte operativsystem skal være så nyt som muligt, og skal som minimum være supporteret med sikkerhedsopdateringer	102	87%
Mail		
Der må kun anvendes af myndigheden godkendte mail-relays med autentifikation	104	89%
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.	96	82%
Webmail må kun anvendes udenfor myndighedens lokale netværk, hvis dette foregår vha 2FA eller via en direkte VPN-forbindelse til myndighedens netværk.	92	79%
Mobile enheder		
Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation	92	79%
Operativsystem og apps på mobile enheder skal opdateres regelmæssigt	82	70%
Netværk		
WIFI på myndighedens arbejdsnetværk skal være krypteret med minimum WPA2	116	99%
Krav om logning, log på alle systemer og tjenester på netværksservere	92	79%
Websider		
DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden	66	56%
Myndigheden skal anvende en sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod skadelige hjemmesider	109	93%
Kommunikation til hjemmesider skal krypteres og anvende minimum TLS 1.2, dvs. der skal implementeres https på alle hjemmesider	63	54%
Der skal benyttes regelmæssigt opdateret serversoftware på webservere	84	72%

De enkelte krav er nærmere beskrevet på https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav