Rapport (3. kvartal 2020)

25. juni 2021

Tekniske minimumskrav til sikkerheden i statslige myndigheder

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 fleste krav skulle være implementeret senest den 1. januar 2020, mens nogle få krav først trådte i kraft den 1. juli 2020. Kravene er alle ufravigelige.

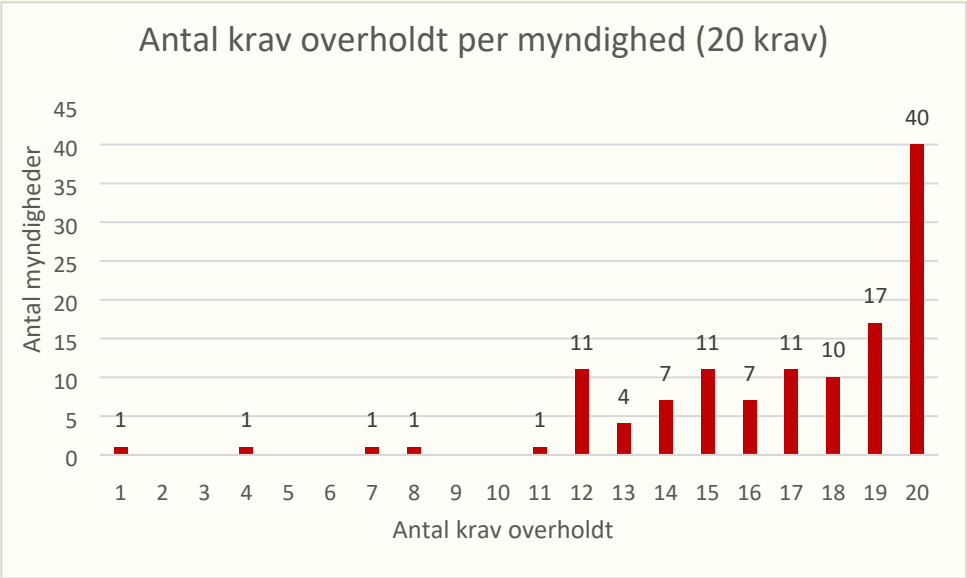
Der er i hhv. februar/marts og i august/september 2020 gennemført spørgeskemaundersøgelser om myndighedernes efterlevelse af kravene. Det fremgik af følgeteksten til spørgeskemaerne, at et krav kun kunne betragtes som efterlevet i tilfælde af "fuld" efterlevelse, altså hvor der ikke var nogle udeståender ift. implementeringen af kravet i den enkelte myndighed. Der blev ved målingen gennemført i august/september 2020 modtaget 123 besvarelser fra myndigheder og institutioner på samtlige ministerområder.

Resultaterne viser, at 40 (33 pct.) af myndighederne efterlever samtlige af de 20 krav, der trådte i kraft den 1. januar 2020, mens i alt 96 (78 pct.) efterlever mindst 15 af kravene. Kun 4 (3 pct.) af myndighederne efterlever 10 af kravene eller færre, og der er i disse tilfælde tale om myndigheder med et kompliceret og/eller atypisk systemsetup, som kun i begrænset omfang kan sammenlignes med resten af staten. I mange af de tilfælde, hvor et krav ikke efterleves, er det mindre udeståender, der forhindrer myndigheden i at være i mål. Derudover afventer et enkelt ministerområde med flere styrelser og institutioner overflytning til Statens IT, hvorefter en række krav som ikke overholdes pt. automatisk vil blive bragt i orden. Det vurderes derfor, at den reelle efterlevelse i dag er højere end på opfølgningstidspunktet, at kravene generelt efterleves af myndighederne, samt at efterlevelsen vil stige yderligere over det næste halve år.

Figur 2 illustrerer efterlevelsen per krav samt udviklingen siden 1. måling i 1. kvartal. Det fremgår, at myndighederne i høj grad efterlever de krav, der har til formål at sikre de enkelte arbejds-PCer og myndighedernes mail-kommunikation. I disse kategorier er det således kun kravet om brug af VPN, der efterleves af mindre end 88 pct. af myndighederne, og selv i de myndigheder, der ikke efterlever kravet fuldt ud, anvendes der i vidt omfang VPN ved adgang til interne systemer. Laveste grad af efterlevelse ses på krav, der angår den udadvendte sikring af mail og hjemmesider (DMARC, DNSSEC og https/TLS). Der er her tale om krav, som potentielt kræver opdatering af en stor mængde domæner og hjemmesider og hvor manglende implementering på bare et domæne betyder, at kravet som helhed ikke er overholdt. Det er vurderingen, at myndighederne ligeledes på dette område er i gang med disse projekter, samt at det i mange myndigheder er få udeståender, der gør, at kravet ikke fremstår som opfyldt. Der ses ligeledes en moderat stigning i efterlevelsen i forhold til målingen i 1. kvartal 2020.

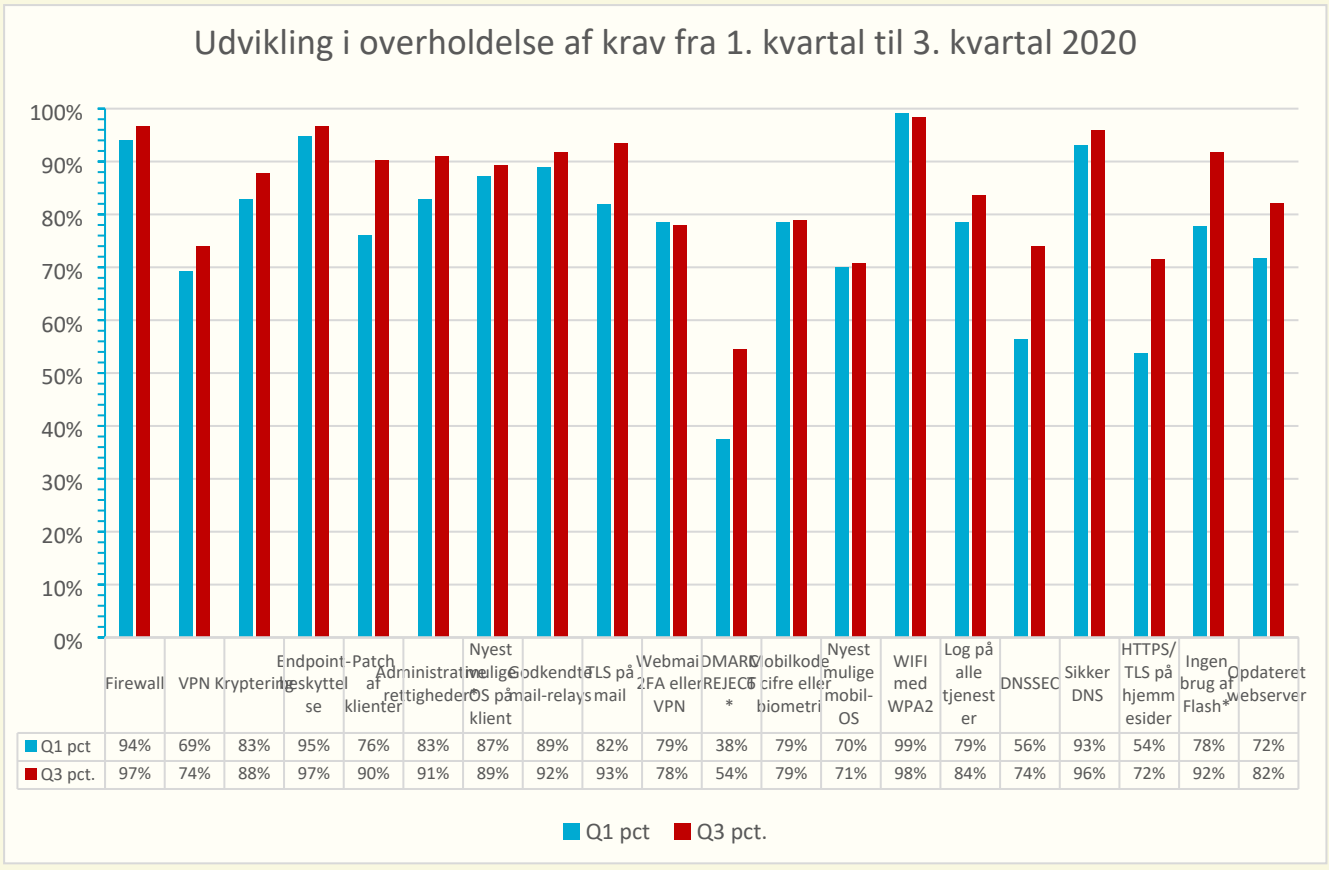
Figur 1

Antal tekniske minimumskrav overholdt per myndighed (20 krav) (3. kvartal 2020)



Figur 2

Udvikling i overholdelse af krav fra 1. kvartal til 3. kvartal 2020



	Firewall	VPN	Kryptering	Endpoint-beskyttelse	Patch af klienter	Administrative rettigheder	Nyest mulige OS på klient	Godkendte mail-relays	TLS på mail	Webmail 2FA eller VPN	DMARC REJECT*	Mobilkode cifre eller biometri	Nyest mulige mobil-OS	WIFI med WPA2	Log på alle tjenester	DNSSEC	Sikker DNS	HTTPS/ TLS på hjemmesider	Ingen brug af Flash*	Opdateret webserver
Q1 pct	94%	69%	83%	95%	76%	83%	87%	89%	82%	79%	38%	79%	70%	99%	79%	56%	93%	54%	78%	72%
Q3 pct.	97%	74%	88%	97%	90%	91%	89%	92%	93%	78%	54%	79%	71%	98%	84%	74%	96%	72%	92%	82%

Tabel 1 - Oversigt over tekniske minimumskrav

Klienter/Pcer	*Kravene til klienter/PC'er angår de stationære og bærbare computere, der almindeligvis anvendes i myndigheden med forbindelse med myndighedens arbejdsnetværk*
Der skal implementeres firewall på alle klienter	Kravet er opfyldt, hvis der er implementeret firewall på alle klienter hos myndigheden.
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.
Kryptering af harddiske	Kravet er opfyldt, hvis kryptering er aktiveret på alle klienter i myndigheden, typisk vha. indbygget funktionalitet i operativsystemet.
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.
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
Administrative rettigheder for brugere tildeles kun tidsbegrænset og med veldokumenterede behov (bemærk, at dette krav trådte i kraft 1. juli 2020)	Kravet er opfyldt, hvis der er truffet organisatoriske foranstaltninger med evt. teknisk understøttelse, der sikrer, at administrative rettigheder på klienter med adgang til myndighedens arbejdsnetværk kun tildeles tidsbegrænset og med veldokumenteret behov.
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*
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.
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 mhp. implementering af dette krav udarbejdet en liste over relevante domæner, mellem hvilke der skal kommunikeres forced TLS).
Webmail må kun anvendes udenfor myndighedens lokale netværk, hvis dette foregår vha 2FA eller via en direkte VPN-forbindelse til myndighedens netværk.	Kravet er opfyldt, hvis der er implementeret tekniske foransaltninger som sikrer, at webmail til myndighedens mail udelukkende kan anvendes efter to-faktor-autentificering eller brug af en direkte VPN-forbindelse til myndighedens netværk.

DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden. (bemærk, at dette krav trådte i kraft 1. juli 2020)	Kravet er opfyldt, hvis der er implementeret DMARC REJECT policy på alle domæner tilhørende myndigheden, herunder domæner, der ikke anvendes til at sende mails.
Mobile enheder	*Kravene til mobile enheder angår arbejdstelefoner, tablets og evt. andre lignende enheder, hvorfra der er adgang til myndighedens arbejdsnetværk og/eller fra hvilke, der kommunikeres på vegne af myndigheden*
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 vha. en adgangskode/PIN-kode på minimum 6 cifre eller vha. biometrisk identifikation.
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 evt. gæstenetværk uden adgang til myndighedens systemer*
WIFI på myndighedens arbejdsnetværk skal være krypteret med minimum WPA2	Kravet er opfyldt, hvis trådsløs adgang til myndighedens arbejdsnetværk er krypteret med minimum WPA2.
Krav om logning, log på alle systemer og tjenester på netværksservere	Kravet er opfyldt, hvis der er implementeret logning på infrastrukturkomponenter i overenstemmelse 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 evt. andre systemer, som udelukkende kan tilgås fra myndighedens interne netværk og som derfor er afskærmet fra det åbne internet.*
DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden	Kravet er opfyldt, hvis der er opsat DNSSEC på alle domænenavne tilhørende myndigheden.
Myndigheden skal anvende en sikker DNStjeneste 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.
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.
Der må ikke anvendes Flash på hjemmesider tilhørende myndigheden (bemærk, at dette krav trådte i kraft 1. juli 2020)	Kravet er opfyldt, hvis der ikke anvendes Flash-løsninger på nogen hjemmesider tilhørende myndigheden.
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.