De tekniske minimumskrav for statslige myndigheder 2023

De 20 tekniske minimumskrav til it-sikkerhed for statslige myndigheder blev i juni 2022 opdateret til en 2023-version. I november 2022 er der foretaget mindre præciseringer til et af kravene samt nogle af kategorierne. Kravene er ufravigelige for statslige myndigheder og skal sikre et fælles højt sikkerhedsniveau i staten. Implementering af kravene skal ske senest d. 1. januar 2023.

Nr.	Kravformulering	Formål	Anvisninger	Skal være implementeret den:	Brug for yderligere hjælp og vejledning?
	Klienter/PC'er: Kravene til klienter/PC'er angår de stationære og bærbare computere, der administreres af myndigheden.				
1	Der skal implementeres firewall på alle klienter.	Formålet med kravet er at sikre myndighedens klienter mod utilsigtet netværksadgang. Klientbaserede firewalls reducerer risikoen for at en kompromitteret klient kan bruges til at kompromittere andre klienter.	Kravet er opfyldt, hvis 1) der er implementeret firewall på alle klienter hos myndigheden og 2) myndigheden aktivt har forholdt sig til nødvendig indgående og udgående trafik på klienten og 3) firewallpolitikken/konfigureringen kun tillader det, der er identificeret som nødvendigt jf. punkt 2.	1. januar 2023	
2	Klienter skal benytte Always On VPN fra eksterne netværk.	Formålet med kravet er at modvirke man-in-the-middle angreb og sikre, at klientens trafik er omfattet af myndighedens øvrige sikkerhedstiltag. Ved brug af Always On VPN sikres det, at al internettrafik ledes gennem myndighedens egen it-infrastruktur.	Kravet er opfyldt, hvis 1) der anvendes Always On VPN, når klienten er koblet på netværk uden for myndighedens egen it-infrastruktur og 2) Always On VPN forbindes til myndighedens egen it-infrastruktur, således at al internettrafik går via myndigheden. Tidsbegrænset lokal netværksadgang kan tillades for at kunne anvende login-portaler på fremmed WiFi.	1. januar 2023	Læs mere i vejledningen "*Cybersikkerhed på rejsen*"
3	Klienters harddiske skal krypteres.	Formålet med kravet er at undgå kompromittering af data i forbindelse med tab eller tyveri af en klient. Fuld diskkryptering af det lokale faste lager på klienten reducerer risikoen for brud på fortroligheden af data.	Kravet er opfyldt, hvis der er aktiveret fuld diskkryptering af det lokale faste lager på alle klienter i myndigheden, typisk vha. indbygget funktionalitet i operativsystemet.	1. januar 2023	Læs mere i vejledningen "*Cybersikkerhed på rejsen*"
4	Der skal implementeres endpoint-beskyttelse på alle klienter.	Formålet med kravet er at opdage og forhindre, at vira og malware mv. afvikles på klienten.	Kravet er opfyldt, hvis der er installeret endpoint-beskyttelse med automatisk opdatering på alle klienter hos myndigheden.	1. januar 2023	Læs mere i vejledningen "*Reducer risikoen for ransomware*"
5	Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret	Formålet med kravet er at lukke kendte sårbarheder på klienterne.	Kravet er opfyldt, hvis 1) det anvendte operativsystem og applikationerne på klienten er under aktiv support (dvs. der udgives sikkerhedsopdateringer fra producenten) og 2) der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer at ikke-kritiske systemer opdateres inden for 30 dage, og at kritiske systemer opdateres hurtigst muligt inden da.	1. januar 2023	Læs mere i vejledningen "*Cyberforsvar der virker*"

Nr.	Kravformulering	Formål	Anvisninger	Skal være implementeret den:	Brug for yderligere hjælp og vejledning?
6	Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.	Formålet med kravet er at reducere risikoen for installation af malware eller anden kompromittering. Da størstedelen af malware kræver administrative rettigheder på klienten for at blive installeret eller afviklet, må administrative rettigheder ikke tildeles konti, der anvendes til andre aktiviteter.	Kravet er opfyldt, hvis 1) der er truffet organisatoriske foranstaltninger, med evt. teknisk understøttelse, der sikrer, at administrative rettigheder på klienterne tildeles en separat konto, der kun anvendes til aktiviteter, hvor den administrative rettighed er påkrævet og 2) medarbejdere, hvis primære jobfunktion ikke inkluderer administration af klienter, kun tildeles en separat konto med administrative rettigheder i en tidsbegrænset periode, og på baggrund af en dokumenteret godkendelse af et konkret behov. Ved fornyelse skal en ny godkendelse foretages og dokumenteres. Softwarebaseret elevering af brugerens privilegier kan tillades, såfremt det teknisk er sikret, at det kun er den anmodede og godkendte aktivitet, der udføres med de eleverede privilegier. Administratorprivilegier skal således automatisk trækkes tilbage, når den pågældende aktivitet er udført. Brugerens øvrige aktiviteter, som fx mail- og internetbrug, skal fortsat udføres under brugernes almindelige brugerkonto uden specielle privilegier.	1. januar 2023	Læs mere i vejledningen "*Cyberforsvar der virker*"
7	Klienter skal anvende det nyeste operativsystem.	Formålet med kravet er at sikre, at myndighedens klienter får gavn af de nyeste sikkerhedsfeatures. Da nyere operativsystemer ofte har et højere sikkerhedsniveau end ældre versioner, skal myndigheden anvende det nyeste operativsystem på alle klienter.	Kravet er opfyldt, hvis det anvendte operativsystem (OS) er en major release eller major update udgivet for mindre end 18 måneder siden.	1. januar 2023	Læs mere i vejledningen "*Cyberforsvar der virker*"
	Mail: Kravene til mails angår mailkommunikation til og fra myndigheden				
8	Der må kun anvendes godkendte mail-relays med autentifikation.	Formålet med kravet er at reducere risikoen for misbrug af mail-servere til spredning af malware og spam. Der må derfor kun anvendes mail-relays med autentifikation, som myndigheden har godkendt.	Kravet er opfyldt, hvis mail-relays, som tilhører eller anvendes af myndigheden, kun accepterer mails fra autentificerede brugere eller systemer. Hvor autentifikation ikke understøttes, skal mail kun accepteres fra positivlistede systemer/software.	1. januar 2023	
9	Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.	Formålet med kravet er at kryptere mailtrafikken med henblik på at sikre dataintegritet og fortrolighed. Med anvendelse af TLS 1.2 reduceres risikoen for, at mail-kommunikation bliver aflyttet undervejs i transmissionen over internettet.	Kravet er opfyldt, hvis 1) 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 2) alle relevante servere er sat op til at foretage tvungen kryptering (forced TLS) til statslige myndigheder og 3) TLS er konfigureret i henhold til bilag 1.	1. januar 2023	Læs mere i vejledningen "*Sikker brug af Transport Layer Security (TLS)*"
	Autentifikation: Kravet angår de af myndighedens it-systemer, som kan tilgås fra internettet, og hvor der logges på med myndighedens brugerkonti (typisk brugerens standardkonto).				
10	Autentifikation til myndighedens systemer over internettet skal anvende flerfaktor-autentificering[1].	Formålet med kravet er at reducere risikoen for, at kompromitterede login oplysninger kan anvendes af andre til at tilgå myndighedens systemer og data.	Kravet er opfyldt, hvis 1) fler-faktor autentifikation er påkrævet ved ekstern adgang til myndighedens data og 2) fler-faktor autentifikationen er baseret på brugerens brugernavn og to eller flere autentifikationstyper. Udstedelse af faktorer baseret på typerne "*har*" og "*er*" er baseret på bekræftet identitet eller en anden eksisterende flerfaktor-autentifikation.	1. januar 2023	Læs mere i vejledningen "Password-sikkerhed"

[1] I forbindelse med udarbejdelse af nye tekniske minimumskrav, vil kravet blive præciseret med en anvisning om, at engangskoder skal genereres lokalt og ikke skal transmitteres til brugeren, fx via SMS eller mail.

Nr.	Kravformulering	Formål	Anvisninger	Skal være implementeret den:	Brug for yderligere hjælp og vejledning?
	Mobile enheder: Kravene til mobile enheder angår mobiltelefoner og tablets med app-baseret adgang til myndighedens data.				
11	Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation	Formålet med kravet er at beskytte den mobile enhed mod misbrug, hvis den fx tabes eller stjæles.	Kravet er opfyldt, hvis der anvendes numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation for at få adgang til den mobile enhed.	1. januar 2023	Læs mere i vejledningen "*Råd om sikkerhed på mobile enheder*"
12	MDM (Mobile Device Management) skal implementeres på alle mobile enheder.	Formålet med kravet er at beskytte myndighedens data på mobile enheder med særlige sikkerhedstiltag.	Kravet er opfyldt, hvis MDM-løsningen: 1) sikrer, at de apps der må tilgå myndighedens data, leveres som 'managed apps' og 2) sikrer, at myndighedens data holdes adskilt fra øvrige data og 3) er i stand til at slette myndighedens data på enheden i tilfælde af bortkomst og 4) sletter myndighedens data automatisk ved maksimalt 10 fejlslagne loginforsøg og 5) afviser mobile enheder, der er rooted/jailbroken.	1. januar 2023	
13	Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret	Formålet med kravet er at sikre, at kendte sikkerhedshuller lukkes hurtigst muligt. Regelmæssig opdatering sikrer også, at myndighedens mobile enheder får gavn af de nyeste sikkerhedsfeatures.	Kravet er opfyldt, hvis 1) operativsystemet er under aktiv support (dvs. der udgives sikkerhedsopdateringer) og 2) seneste sikkerhedsopdateringer for operativsystem og 'managed apps' er installeret senest 30 dage efter udgivelse og 3) den mobile enhed er sat op til automatisk opdatering af alle installerede apps.	1. januar 2023	Læs mere i vejledningen "*Råd om sikkerhed på mobile enheder*"
	Logning: Kravene til logning angår alle systemer og tjenester på netværksservere.				
14	Krav om logning, log på alle systemer og tjenester på netværksservere[2]	Formålet med kravet er sikre de bedste forudsætninger for opdagelse af og efterforskning af sikkerhedshændelser. Logningen skal ikke implementeres med formål om at monitorere brugeradfærd.	Kravet er opfyldt, hvis der er implementeret logning på infrastrukturkomponenter i overensstemmelse med CFCS-vejledningen "*Logning – en del af et godt cyberforsvar*".	1. januar 2023	Læs mere i vejledningen "*Logning – en del af et godt cyberforsvar*"
	Domæner: Kravene til domæner angår alle domænenavne tilhørende myndigheden.				
15	DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.	Formålet med kravet at sikre, at domæneforespørgsler besvares af domæneejeren, og at svar ikke er manipuleret undervejs. Ved brug af DNSSEC kan klienter kryptografisk stole på, at de tilgår de rette systemer og tjenester hos myndigheden.	Kravet er opfyldt, hvis alle myndighedens domæner er DNSSEC-signerede.	1. januar 2023	

[2] Kravet er foreløbigt uændret. I forbindelse med udarbejdelse af nye tekniske minimumskrav, vil der blive sat øget fokus på logning, herunder også en justering af dette krav. Der henvises til ændringsloggen for yderligere.

Nr.	Kravformulering	Formål	Anvisninger	Skal være implementeret den:	Brug for yderligere hjælp og vejledning?
16	Myndigheden skal anvende en Sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod adgang til kendte skadelige domæner.	Formålet med kravet er at beskytte enheder på netværket mod at tilgå eksempelvis kendte phishingsider og hjemmesider med malware. Ved brug af en Sikker DNS-tjeneste filtreres navneforspørgsler på baggrund af automatisk opdaterede lister over domæner, der vurderes at være skadelige.	Kravet er opfyldt, hvis 1) myndigheden anvender en Sikker DNS-tjeneste, eller der er implementeret en anden løsning, som yder tilsvarende beskyttelse mod skadelige domæner og 2) løsningen er baseret på vedligeholdte negativlister, der opdateres automatisk.	1. januar 2023	
17	DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden.	Formålet med kravet er give mailmodtagere mulighed for at opdage forsøg på email-spoofing, hvor en afsender udgiver sig for at være en anden. Ved at implementere DMARC på alle domæner reduceres risikoen for myndighedens domænenavne kan misbruges til udsendelse af phishing- eller spam-mails.	Kravet er opfyldt, hvis: 1) DMARC er implementeret på alle myndighedens domæner og 2) DMARC politikken er sat til REJECT på alle myndighedens domæner og 3) SPF (Sender Policy Framework) og DKIM (DomainKeys Identified Mail) er implementeret på alle myndighedens domæner.	1. januar 2023	Læs mere i vejledningen "*Reducer risikoen for falske mails*"
	Netværk: Kravene til netværk angår myndighedens interne WiFi-netværk, men ikke evt. gæstenetværk uden adgang til myndighedens systemer.				
18	Myndighedens interne WiFI-netværk skal være krypteret med minimum WPA2.	Formålet med kravet er at forhindre aflytning ved at foretage kryptering af trafikken på interne WiFi-netværk.	Kravet er opfyldt, hvis trådløs adgang til myndighedens interne WiFi-netværk er krypteret med minimum WPA2.	1. januar 2023	
	Internetvendte tjenester: Kravene til internetvendte tjenester angår alle myndighedens tjenester, der kan tilgås fra internettet.				
19	Software på myndighedens internetvendte tjenester skal holdes sikkerhedsopdateret.	Formålet med kravet er at kendte sårbarheder bliver lukket hurtigst muligt. Derfor skal al software, der anvendes på myndighedens internetvendte tjenester, være omfattet af regelmæssig sikkerhedsopdatering.	Kravet er opfyldt, hvis 1) det anvendte software og eventuelle tredjepartsbiblioteker på internetvendte systemer, er under aktiv support (dvs. der udgives sikkerhedsopdateringer fra producenten) og 2) der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer, at ikke-kritiske systemer sikkerhedsopdateres inden for 30 dage, og at kritiske systemer sikkerhedsopdateres hurtigst muligt inden da.	1. januar 2023	Læs mere i vejledningen "*Cyberforsvar der virker*"
20	Adgang til myndighedens internetvendte tjenester, herunder hjemmesider, skal ske over en krypteret forbindelse.	Formålet med kravet er at sikre dataintegritet og fortrolighed samt forebyggelse af man-in-the-middle angreb.	Kravet er opfyldt, hvis alle myndighedens internetvendte tjenester kun kan anvendes over en krypteret forbindelse, herunder at: a) HTTP-tilgængelige tjenester automatisk omdirigerer til en HTTPS forbindelse og b) HTTPS-baserede tjenester kun understøtter TLS 1.2 eller højere og c) TLS krypterede forbindelser er baseret på konfigurationsparametrene i bilag 1.	1. januar 2023	Læs mere i vejledningen "*Sikker brug af Transport Layer Security (TLS)*"

Bilag 1

23. marts 2023

Afgrænsning af minimumskrav 9 og 20.

Nærværende bilag skal ses i sammenhæng med de tekniske minimumskrav til it-sikkerhed i staten. For krav 9 og 20 skal der tages udgangspunkt i beskrivelserne angivet i bilaget med henblik på at sikre, at kravene efterleves korrekt.

Krav 9: *Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.*
TLS krypterede forbindelser skal baseres på de konfigurationsparametre, der har status som enten "God" eller "Tilstrækkelig" jf. tabel 1.

Tabel 1: Oversigt over konfigurationsparametre

#	Emne for retningslinjer	Værdi	Status
1	TLS-versioner	TLS 1.3 TLS 1.2	God
		TLS 1.1 TLS 1.0	Bør udfases
		SSL 3.0 SSL 2.0 SSL 1.0	Utilstrækkelig
2	Algoritmer for - Nøgleudveksling	ECDHE	God
		DHE	Tilstrækkelig
		RSA	Bør udfases
		DH ECDH KRB5 NULL PSK SRP	Utilstrækkelig
3	Algoritmer for – Certifikat verifikation	ECDSA RSA	God
		DSS EXPORT-variants PSK Anon NULL	Utilstrækkelig
4	Algoritmer for - Bulk kryptering	AES-256-GCM ChaCha20-Poly1305 AES-128-GCM	God
		AES-256-CBC AES-128-CBC	Tilstrækkelig
		3DES-CBC	Bør udfases
		AES-256-CCM_833 AES-128-CCN_832 IDEA DES RC4 NULL	Utilstrækkelig

#	Emne for retningslinjer	Værdi	Status
5	Hash funktioner for – Nøgleudveksling	SHA-512 SHA-384 SHA-256	God
		Øvrige funktioner	Bør udfases
6	Hash funktioner for – Certifikat verifikation	SHA-512 SHA-384 SHA-256	God
		SHA-1 MD5	Utilstrækkelig
7	Hash funktioner for - Bulk kryptering	HMAC-SHA-512 HMAC-SHA-384 HMAC-SHA-256	God
		HMAC-SHA-1	Tilstrækkelig
		HMAC-MD5	Utilstrækkelig
8	RSA Nøglelængder	Mindst 3072	God
		2048-3071	Tilstrækkelig
		Mindre end 2048	Utilstrækkelig
9	Understøttet elliptisk kurver	secp384r1 secp256r1 x448 x25519	God
		secp224r1	Bør udfases
		Andre kurver	Utilstrækkelig
10	Understøttet ”finite field” grupper	ffdhe4096 (RFC 7919) ffdhe3072 (RFC 7919)	God
		Ffdhe2048 (RFC 7919)	Bør udfases
		Andre grupper	Utilstrækkelig
11	Komprimering	Ingen komprimering	God
		Application-level komprimering	Tilstrækkelig
		TLS-komprimering	Utilstrækkelig
12	Usikker genforhandling (Insecure renegotiation)	Off (eller N/A for TLS 1.3)	God
		ON	Utilstrækkelig
13	Klient-initierede genfor-handling (Client initiated renegotiation)	Off (eller N/A for TLS 1.3)	God
		ON	Utilstrækkelig
14	0-RTT	Off (eller N/A for TLS 1.3)	God
		ON	Utilstrækkelig
15	OCSP hæftning (stapling)	ON	God
		Off	Tilstrækkelig

Krav 20: *Adgang til myndighedens internetvendte tjenester, herunder hjemmesider, skal ske over en krypteret forbindelse.*
TLS krypterede forbindelser skal baseres på de konfigurationsparametre, der har status som enten ”*God*” eller ”*Tilstrækkelig*” jf. tabel 1 (se krav 9).