Ændringslog til de tekniske minimumskrav til it-sikkerhed

Juni 2023

Opdatering af de tekniske minimumskrav - juni 2023

De tekniske minimumskrav er i juni 2023 blevet opdateret til en 2024 version. Med opdateringen er der indført ni nye minimumskrav og foretaget ændringer af tre eksisterende krav. De overordnede ændringer er beskrevet nedenfor. Kravspecifikke ændringer fremgår af tabel 1.

Overordnede ændringer:

- Flere af kategoribeskrivelser er blevet opdateret, og der er udarbejdet en vejledning til kravene med henblik på at tydeliggøre kravenes omfang og afgrænsning.
- Der er tilføjet to nye kategorier: *passwords* og *interne it-systemer*.

Tabel 1: De nye minimumskrav samt væsentlige ændringer i forhold til efterlevelse

Nr[1].	Krav (ny formulering)	Væsentlige ændringer
Klienter/PCer		
1	Der skal implementeres firewall på alle klienter	Ingen ændringer.
2	Klienter skal benytte Always-On VPN fra eksterne net-værk	Ingen ændringer.
3	Klienters harddiske skal krypteres.	Ingen ændringer.
4	Der skal implementeres endpoint-beskyttelse på alle kli-enter.	Ingen ændringer.
5	Klienters OS og applikationer på klienten skal holdes sik-kerhedsopdateret	Ingen ændringer.
6	Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.	Ingen ændringer.
7	Klienter skal anvende det nyeste operativsystem.	Ingen ændringer.
Mail		
8	Der må kun anvendes godkendte mail-relays med auten-tifikation.	Ingen ændringer.
9	Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.	Ingen ændringer.

[1] Det gamle nummer fremgår i parentes, såfremt der er ændret i rækkefølgen.

10	Afsenders DMARC-politik skal overholdes ved modtagelse af indgående mail.	Kravet er nyt. Formålet med kravet er at reducere antallet af forfalskede mails, der modtages af en slutbruger ved at sikre, at afsenderdomænets eventuelle DMARC-politik overholdes.
Autentifikation		
11 (10)	Autentifikation til myndighedens systemer over internettet skal anvende flerfaktor-autentificering.	Kravet er justeret med en ny anvisning om, at engangskoder skal genereres lokalt og ikke må transmitteres til brugeren fx via SMS eller mail.
Password (ny kategori)		
12	Myndigheden skal sikre, at der ikke anvendes tidligere lækkede passwords.	Kravet er nyt. Formålet med kravet er at sikre, at uvedkommende ikke nemt kan kompromittere konti, fordi der anvendes passwords, der er offentligt kendt.
Mobile enheder		
13 (11)	Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation	Ingen ændringer.
14 (12)	MDM (Mobile Device Management) skal implementeres på alle mobile enheder.	Ingen ændringer.
15 (13)	Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret.	Ingen ændringer.
Logning (ny kategoribeskrivelse)		
16 (14)	Logning skal foretages på internetvendte tjenester og centrale interne it-systemer.	Kravet er opdateret, så det nu fremgår, hvilke logkilder der er omfattet, herunder hvilke logdata der skal opsamles. Der stilles desuden krav om, at alle logs skal anvende en fælles tidskilde og samme tidszone. Desuden skal de opsamlede logdata opbevares i minimum 12 måneder medmindre lovgivning på området tilsiger andet. For yderligere information henvises der til bilag 1 i kravoversigten.
Domænesikkerhed (ny kategoribeskrivelse)		
17	Internetvendte tjenester tilhørende myndigheden skal registreres under .dk-domæner.	Kravet er nyt. Formålet med kravet er at sikre genkendelighed for borgere, myndigheder og virksomheder i Danmark, og at statslige domæner er under national kontrol via DK-hostmaster. Dette sikrer eksempelvis, at ondsindede. .dk-domæner, der bruges til fx phishing, hurtigt kan nedtages.
18 (15)	DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.	Ingen ændringer.
19	Det skal sikres, at indgående mailgateways ligger i DNSSEC-signerede domæner.	Kravet er nyt. Formålet med kravet er sikre, at domæner, der håndterer mails på vegne af myndigheden, er DNSSEC-signerede. Signering af MX-recorden sikrer, at afsender af mails kryptografisk kan stole på, at de sender til de rette indgående mailgateways.
20	Der skal anvendes DANE for alle indgående mailgateways.	Kravet er nyt. Formålet med kravet er at tydeliggøre over for afsenderen, at myndigheden understøtter kryptering med henblik på at reducere risikoen for, at mails sendes ukrypteret.
21	Der skal foretages DNSSEC validering på svar på navneopslag.	Kravet er nyt. Formålet med kravet er at forhindre, at myndighedens ansatte eksempelvis sendes videre til falske hjemmesider. Ved at foretage DNSSEC-validring sikres det, at svar på navneopslag kommer fra domæneejeren og ikke er manipuleret undervejs.
22 (16)	Myndigheden skal anvende en Sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod adgang til kendte skadelige domæner.	Ingen ændringer.
23 (17)	DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden.	Ingen ændringer.

Netværk (ny kategoribeskrivelse)		
24 (18)	Myndighedens WiFI-netværk skal være krypteres med minimum WPA2.	Ændring af kategoribeskrivelsen betyder, at kryptering med minimum WPA2 skal anvendes på alle myndighedens trådede og trådløse netværk. Det omfatter derfor også myndighedens gæstenetværk. Der stilles krav om kryptering af gæstenetværket for at forhindre misbrug.
25	Gæstenetværk skal holdes adskilt fra myndighedens interne netværk.	Kravet er nyt. Formålet med kravet er at sikre, at trafik fra gæstenetværk ikke omgår eksisterende sikringstiltag, og at eventuel uønsket internettrafik fra gæstenetværk ikke påvirker myndighedens omdømme.
Internetvendte tjenester		
26 (19)	Software på myndighedens internetvendte tjenester skal holdes sikkerhedsopdateret	Ingen ændringer.
27 (20)	Adgang til myndighedens internetvendte tjenester skal ske over en krypteret forbindelse.	Ingen ændringer.
28	Internettilgængelige IP-adresser, ejet af myndigheden, skal scannes for tjenester.	Kravet er nyt. Formålet med kravet er at sikre, at kun det nødvendige og forventede er tilgængeligt over internettet.
Interne it-systemer (ny kategori)		
29	Software på specifikke interne infrastruktur-enheder og –tjenester skal holdes sikkerhedsopdateret.	Kravet er nyt. Formålet med kravet er, at kendte sårbarheder bliver lukket hurtigst muligt. Derfor skal software, der anvendes på omfattede infrastruktur-enheder og –tjenester være omfattet af regelmæssig sikkerhedsopdatering.

Opdatering af de tekniske minimumskrav - marts 2023

Der er foretaget mindre opdatering af de tekniske minimumskrav per 23. marts 2023. Ændringerne er nærmere beskrevet nedenfor.

Ændringer:

- I bilag 1 er konfigurationsparametre 15 ændret, da det ved en fejl har været angivet, at OCSP hæftning (stapling) var utilstrækkeligt, hvis værdien var sat til Off. Dette er nu ændret til *tilstrækkeligt.*

Opdatering af de tekniske minimumskrav - november 2022

Der er foretaget mindre opdatering af de tekniske minimumskrav per 24. november 2022. Ændringerne ændrer ikke på formål eller kravene til myndighederne. Der er udelukkende tale om præciseringer. Ændringerne er nærmere beskrevet nedenfor.

Ændringer:

- Anvisningerne for krav 6 er præciseret således, at 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.
- Det er præciseret i kategoribeskrivelsen for kategorien "Autentifikation", at kravet vedrørende autentifikation kun angår de af myndighedens it-systemer, som kan tilgås fra internettet, og hvor der logges på med myndighedens brugerkonti (typisk standardkonto).
- Krav 19 og 20 om hhv. sikkerhedsopdatering af software og kryptering af internetvendte tjenester, herunder hjemmesider, er flyttet fra kategorien "Netværk" til en ny kategori kaldet *Internetvendte tjenester*. Kravene til internetvendte tjenester angår alle tjenester, der kan tilgås fra internettet, eksempelvis myndighedens fagsystemer og hjemmesider.

Reviderede tekniske minimumskrav - juni 2022

De tekniske minimumskrav er opdateret per 29. juni 2022. De overordnede og kravspecifikke ændringer fremgår nedenfor.

Overordnede ændringer:

- Kategorierne *Autentifikation, Logning* og *Domæner* er tilføjet. Alle kategorier indeholder en definition af, hvad de underliggende krav angår.

- Der er på baggrund af en ØU-sag fra januar 2022 indført to nye minimumskrav om hhv. 1) flerfaktor-autentificering og 2) anvendelse af en MDM-løsning. Krav om flerfaktor-autentificering erstatter tidligere krav 10 om flerfaktor på webmail.
- De væsentligste ændringer er foretaget til anvisningerne for de enkelte krav. De specifikke ændringer for de enkelte krav fremgår af tabel 2.

Tabel 2: De nye minimumskrav samt væsentlige ændringer i forhold til efterlevelse

Nr.	Krav (ny formulering)	Væsentlige ændringer
Klienter/PCer		
1	Der skal implementeres firewall på alle klienter.	Det er præciseret, at myndigheden aktivt skal forholde sig til nødvendig indgående og udgående trafik og kun tillade det, der er identificeret som nødvendigt.
2	Klienter skal benytte Always-On VPN fra eksterne netværk.	Kravet er ændret, så internetadgang fra eksterne net skal ske via VPN til myndighedens netværk, og ikke tillades via tredje-parts VPN. Kravet kan ikke længere efterleves gennem politikker, men kræver en teknisk løsning, der sikrer Always-On VPN. Det er præciseret, at tidsbegrænset lokalnetværksadgang kan tillades for at kunne anvende login-portaler på fremmede WiFi.
3	Klienters harddiske skal krypteres.	Ingen ændringer.
4	Der skal implementeres endpoint-beskyttelse på alle klienter.	Ingen ændringer.
5	Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret.	Kravet er ændret, så det kun omhandler sikkerhedsopdateringer og ikke brug af nyeste OS version. Det er præciseret, at ikke-kritiske systemer skal opdateres inden for 30 dage og at kritiske systemer skal opdateres hurtigst muligt.
6	Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.	Kravet er omformuleret for at tydeliggøre, at administrative rettigheder ikke må tildeles almindelige brugerkonti. IT-administratorer/supportere der i forvejen anvender separate administratorkonti til at udføre administrative aktiviteter, er dermed ikke længere omfattet af kravet om, at deres rettigheder skal være tidsbegrænset.
7	Klienter skal anvende det nyeste operativsystem.	Kravet er ændret, så det kun omhandler brug af nyeste OS version, og ikke sikkerhedsopdateringer. For at opfylde kravet, skal det anvendte operativsystem (OS) være en major release eller major update udgivet for mindre end 18 måneder siden.
Mail		
8	Der må kun anvendes godkendte mail-relays med autentifikation.	Det er præciseret, at hvis autentifikationen ikke understøttes, skal mail kun accepteres fra godkendte systemer/software.
9	Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.	Kravet er ændret, således at TLS krypterede forbindelser skal baseres på konfigurationsparametre "God" og "Tilstrækkelig", som angivet i bilag 1.
~~10~~	Webmail må kun anvendes udenfor myndighedens lokale netværk, hvis dette foregår vha 2FA eller via en direkte VPN-forbindelse til myndighedens netværk. (**ikke længere et krav**)	Dette krav er udgået og erstattet af de to krav om hhv. VPN (2) og autentifikation (10).
Autentifikation		
10	Autentifikation til myndighedens systemer over internettet skal anvende flerfaktor autentificering (**nyt krav**).	Kravet er nyt, og erstatter tidligere krav 10 om brug af flerfaktor på webmail. Kravet angår alle de systemer, der kan tilgås over internettet, og hvor der logges på med myndighedens brugerkonti. Flerfaktor autentificeringen skal baseres 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. For yderligere vejledning henvises der til CFCS vejledning *Passwordsikkerhed.* 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.	Krav (ny formulering)	Væsentlige ændringer
Mobile enheder		
11	Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation.	Ingen ændringer.
12	MDM (Mobile Device Management) skal implementeres på alle mobile enheder (**nyt krav**).	Kravet er nyt. MDM-løsningen skal sikre, at mobile enheder med app-baseret adgang til myndighedens data kan underlægges sikkerhedspolitiker, herunder sikre adskillelse af myndighedsdata fra øvrige data på enheden og give mulighed for sletning af myndighedens data på enheden i tilfælde af bortkomst. Løsningen skal være sat op til at håndtere 'managed apps', afvise enheder der er rooted/jailbroken og slette myndighedens data automatisk ved maksimalt 10 fejlslagne loginforsøg.
13	Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret	Begrebet "regelmæssigt" er præciseret således, at de seneste sikkerhedsopdateringer for OS og 'managed apps', skal være installeret senest 30 dage efter udgivelse. Derudover skal telefonen være sat op til automatisk opdatering af alle installerede apps.
Logning		
14	Krav om logning, log på alle systemer og tjenester på netværksservere.	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. Kravet forventes at blive udbygget med en konkret anvisning om, hvor længe logs på centrale interne it-systemer og internetvendte tjenester som minimum skal opbevares. Det bemærkes i den forbindelse, at Center for Cybersikkerhed anbefaler, at logs opbevares i minimum 13 måneder.
Domæner		
15	DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.	Ingen ændringer.
16	Myndigheden skal anvende en Sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod adgang til kendte skadelige domæner.	Det er præciseret, at Sikker DNS-løsningen skal være baseret på vedligeholdte negativlister, der opdateres automatisk.
17	DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden.	Kravet er præciseret, så det specifikt fremgår, at DMARC REJECT skal baseres på både SPF (Sender Policy Framework) og DKIM (DomainKeys Identified Mail) på alle myndighedens domæner.
Netværk		
18	Myndighedens interne WiFi-netværk skal være krypteret med minimum WPA2.	Arbejdsnetværk er ændret til myndighedens interne WiFi-netværk, for at tydeliggøre at kravet eksempelvis ikke gælder for gæstenetværk, der er isoleret fra myndighedens internetvendte it-systemer og tjenester.
19	Software på myndighedens internetvendte tjenester skal holdes sikkerhedsopdateret.	Det er præciseret at det anvendte software og eventuelle tredjepartsbiblioteker, skal være under aktiv support (dvs. der udgives sikkerhedsopdateringer til det fra producenten). Derudover skal det sikres, at ikke-kritiske systemer sikkerhedsopdateres inden for 30 dage, og at kritiske systemer sikkerhedsopdateres hurtigst muligt inden da.
20	Adgang til myndighedens internetvendte tjenester, herunder hjemmesider, skal ske over en krypteret forbindelse.	Kravet omfatter nu alle myndighedens internetvendte tjenester og ikke kun hjemmesider. Derudover er der underliggende anvisninger til, at HTTP-tilgængelige tjenester automatisk skal omdirigere til en HTTPS forbindelse. TLS krypterede forbindelser skal baseres på konfigurationsparametre "God" og "Tilstrækkelig", som angivet i bilag 1.
Websider		
21	Der må ikke anvendes Flash på hjemmesider tilhørende myndigheden (**ikke længere et krav**)	Kravet er udgået, da Flash ikke længere understøttes. Kravet vurderes derfor ikke længere at være relevant at stille.