DE TEKNISKE MINIMUMSKRAV FOR STATSLIGE MYNDIGHEDER 2024

Opdateret oktober 2024

Indholdsfortegnelse

Klienter/PC'er

Krav til Klienter/PC'er:

1. Der skal implementeres firewall på klienterne
Formålet med kravet er at sikre myndighedens klienter mod utilsigtet netværksadgang. Klientbaserede firewalls reducerer risikoen for at en kompromitter et klient kan bruges til at kompromittere andre klienter.

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.

3. Fysiske 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 forbrug på fortroligheden af data.

4. Der skal implementeres end point-beskyttelse på klienterne
Formålet med kravet er at opdage og forhindre, at vira og malware mv. afvikles på klienten.

5. Klienters OS og applikation er på klienten skal holdes sikkerhedsopdateret
Formålet med kravet er at lukke kendte sårbarheder på klienterne.

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.

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 de omfattede klienter.

ANVISNIGER

Kravene angår alle de stationære, bærbare og virtuelle computere, som har adgang til myndighedens interne systemer

1. Der skal implementeres firewall på klienterne

Kravet er opfyldt, hvis

1. der er implementeret firewall på de omfattede klienter hos myndigheden og
2. myndigheden aktivt har forholdt sig til nødvendig indgående og udgående trafik på klienten og
3. firewall politikken/konfigureringen kun tillader det, der er identificeret som nødvendigt jf. punkt 2.

2. Klienter skal benytte Always On VPN fra eksterne netværk

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.

3. Fysiske klienters harddiske skal krypteres

Kravet er opfyldt, hvis der er aktiveret fuld diskkryptering af det lokale faste lager på de omfattede klienter i myndigheden, typisk vha. indbygget funktionalitet i operativsystemet.

4. Der skal implementeres endpoint-beskyttelse på klienterne

Kravet er opfyldt, hvis der er installeret endpoint-beskyttelse med automatisk opdatering på de omfattede klienter hos myndigheden.

.

ANVISNIGER

Kravene angår alle de stationære, bærbare og virtuelle computere, som har adgang til myndighedens interne systemer

5. Klienters OS og applikationer på klienten skal afholdes sikkerhedsopdateret

Kravet er opfyldt, hvis

1. det anvendte operativsystem og applikationerne på klienten er under aktiv support (dvs. at der udgives sikkerhedsopdateringer, som adresserer kendte sårbarheder) 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.

6. Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter

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.

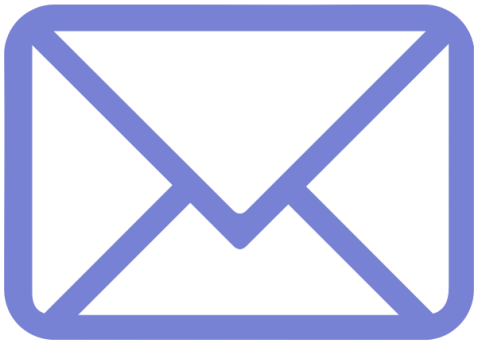
Softwarebaseret elevering af brugerens privilegier kan tillades, såfremt det teknisk er sikret, at det kun er den anmodede og godkendte aktivitet, der udføres med de eleverede privilegier. Administratorprivilegier skal således automatisk trækkes tilbage, når den pågældende aktivitet er udført. Brugerens øvrige aktiviteter, som fx mail- og internetbrug, skal fortsat udføres under brugerens almindelige brugerkonto uden specielle privilegier.

ANVISNIGER

Kravene angår alle de stationære, bærbare og virtuelle computere, som har adgang til myndighedens interne systemer

7. Klienter skal anvende det nyeste operativsystem

Kravet er opfyldt, hvis det anvendte operativsystem (OS) er en major release eller major update udgivet for mindre end 24 måneder siden.



Mail

Krav til Mail:

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.

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.

10. Afsenders DMARC-politik skal overholdes ved modtagelse
Formålet med kravet er at reducere antallet af forfalskede mails, der modtages af en slutbruger ved at sikre, at afsenderdomænets eventuelle DMARC-politik overholdes.

ANVISNIGER

Kravene angår mailkommunikation til og fra myndigheden

8. Der må kun anvendes godkendte mail-relays med autentifikation

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.

9. Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1. 2

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.

10. Afsenders DMARC-politik skal overholdes ved modtagelse

Kravet er opfyldt, hvis det sikres, at indgående mailgateways respekterer afsenderdomænets DMARC-politik, såfremt en sådan politik er publiceret af domæneejeren.

.

Autentifikation

Kravet til Autentifikation:

11. Autentifikation til myndighedens systemer over internettet skal anvende flerfaktor-autentificering
Formålet med kravet er at reducere risikoen for, at kompromitterede login-oplysninger kan anvendes af andre til at tilgå myndighedens it-systemer og data.

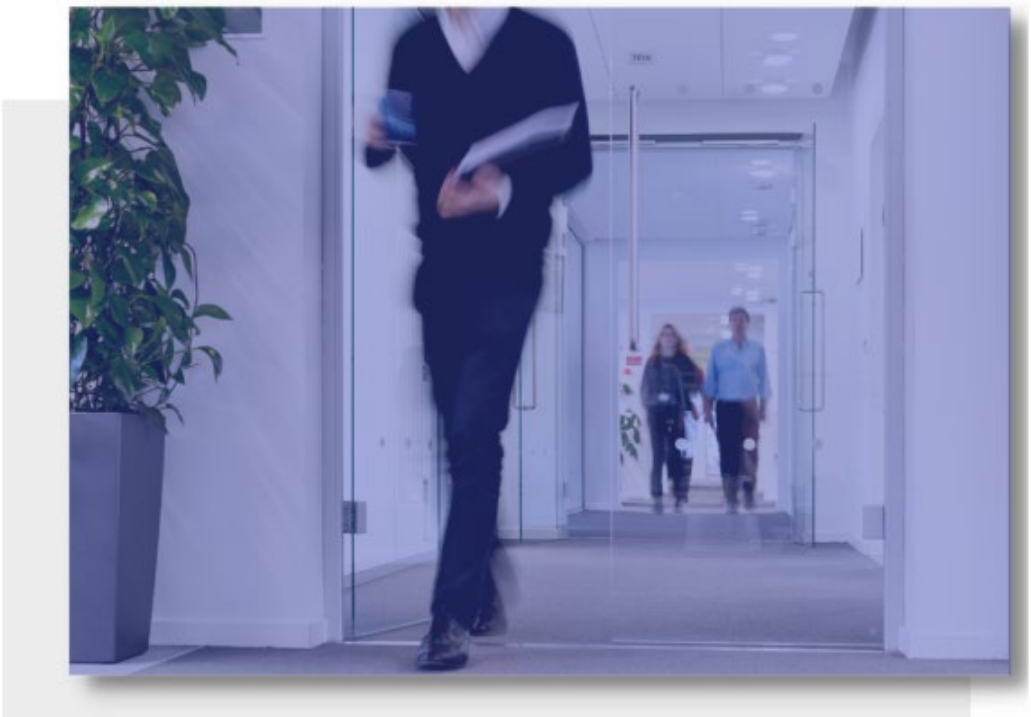
ANVISNIGER

Kravet angår de af myndighedernes it-systemer, som kan tilgås fra internettet, og hvor der logges på med myndighedens brugerkonti

11. Autentifikation til myndighedens systemer over internettet skal anvende flerfaktor-autentificering

Kravet er opfyldt, hvis

1. flerfaktor-autentifikation er påkrævet ved adgang til de af myndighedens it-systemer, som kan tilgås fra internettet og
2. flerfaktor-autentifikationen er baseret på brugerens brugernavn og to eller flere autentifikationstyper og
3. såfremt der identificeres på baggrund af en enhed eller biometri, skal brugerens identitet bekræftes og
4. såfremt der anvendes engangskoder skal disse koder genereres lokalt (på enheden) og må ikke transmitteres til brugeren, fx via SMS eller mail.



Password

Kravet til Password:

12. Myndigheden skal sikre, at der ikke anvendes tidligere lækkede passwords
Formålet med kravet er at sikre, at uvedkommende ikke nemt kan kompromittere konti, fordi der anvendes passwords, der er lækkede.

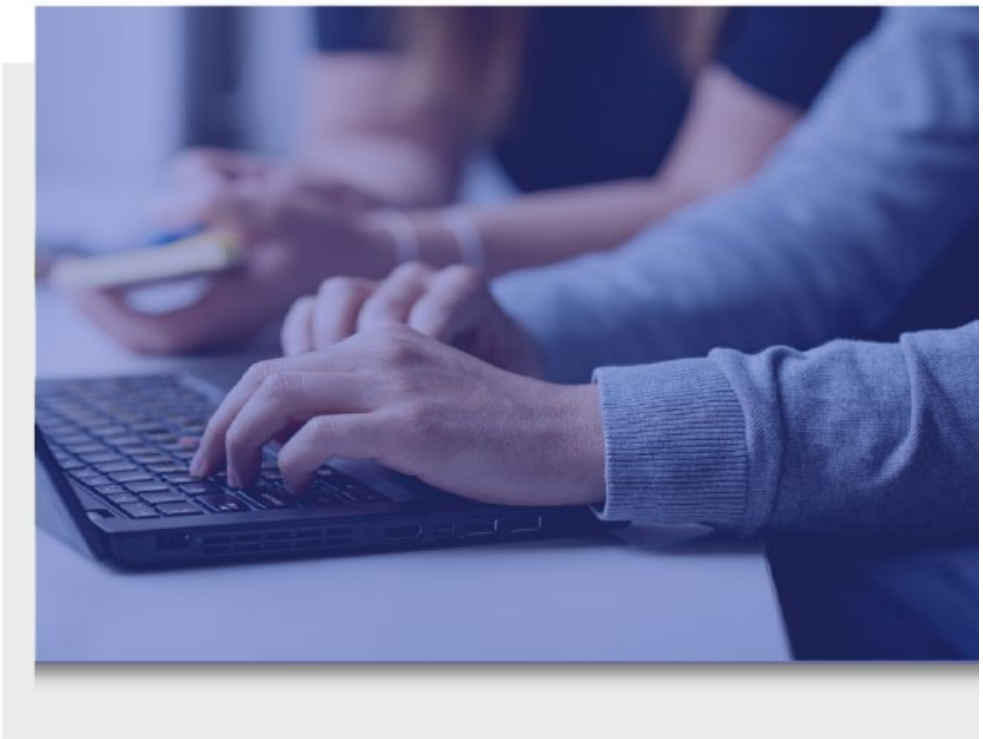
ANVISNIGER

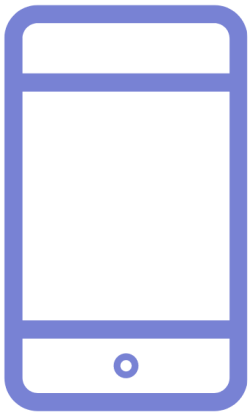
Kravet angår alle myndighedens brugerkonti, herunder konti udstedt til administratorer, it-systemer og services i centrale brugerdatabaser/autentifikationstjenester

12. Myndigheden skal sikre, at der ikke anvendes tidligere lækkede passwords

Kravet er opfyldt, hvis

1. der minimum én gang om måneden tjekkes op mod en liste over lækkede passwords og
2. brugerkonti, hvor der anvendes lækkede passwords, tvinges til at skifte password ved næste log-on og
3. kontoejere for it-systemer og servicekonti, der anvender lækkede passwords, orienteres med henblik på skift af password.





Mobile enheder

Krav til Mobile enheder:

13. 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.

14. MDM (Mobile Device Management) skal implementeres på alle mobile enheder
Formålet med kravet er at beskytte myndighedens data på mobile enheder med særlige sikkerhedstiltag.

15. 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.

ANVISNIGER

Kravet angår alle mobiltelefoner og tablets med app-baseret adgang til myndighedens data

13. Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation

Kravet er opfyldt, hvis der anvendes numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation for at få adgang til den mobile enhed.

14. MDM (Mobile Device Management) skal implementeres på alle mobile enheder

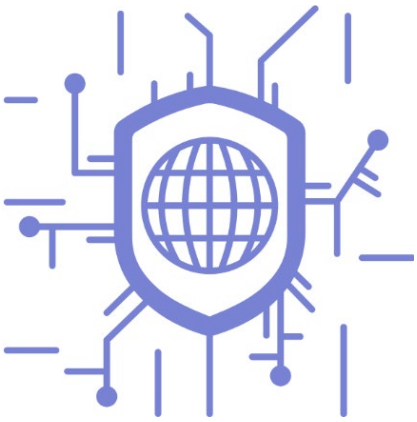
Kravet er opfyldt, hvis MDM-løsningen

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.

15. Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret

Kravet er opfyldt, hvis

1. operativsystemet er under aktiv support (dvs. at 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.



Logning

Kravet til Logning:

16. Logning skal foretages på internetvendte tjenester og centrale interne it-systemer
Formålet med kravet er at sikre de bedste forudsætninger for opdagelse og efterforskning af sikkerhedshændelser. Logningen skal ikke implementeres med formål om at monitorere brugeradfærd.

ANVISNIGER

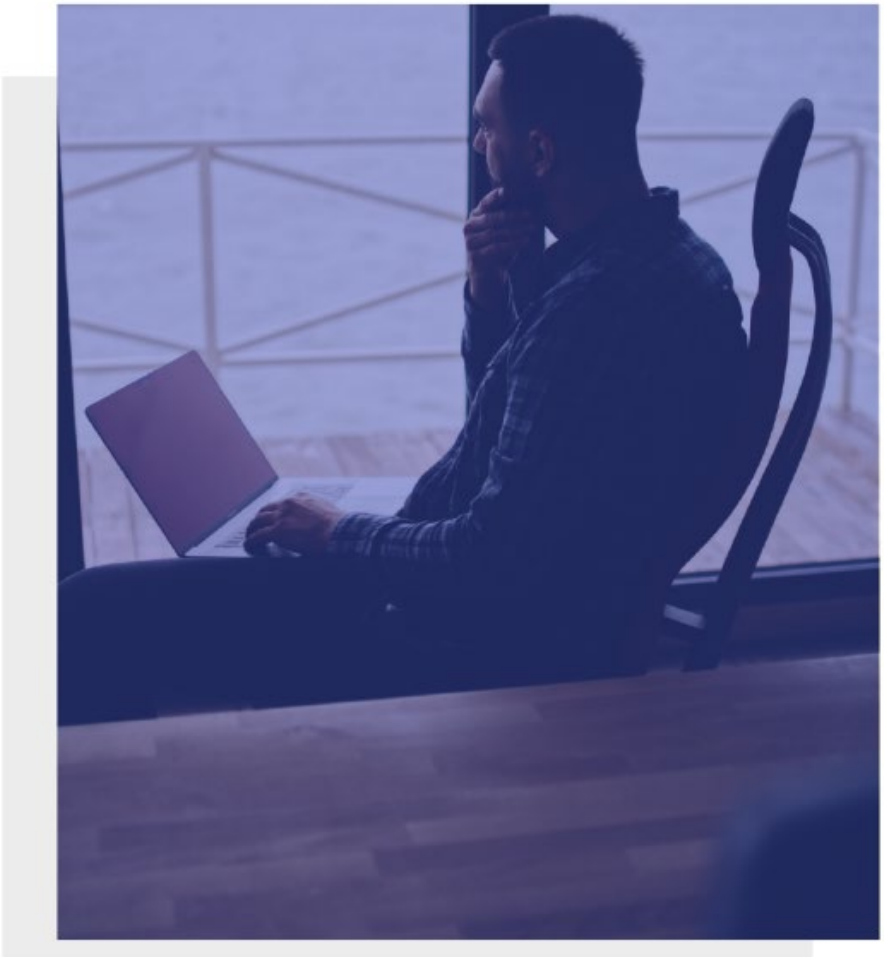
Kravet angår alle internetvendte tjenester og centrale interne it-systemer

16. Logning skal foretages på internetvendte tjenester og centrale interne it-systemer

Kravet er opfyldt, hvis

1. logning er implementeret på alle internetvendte tjenester og alle centrale interne it-systemer jf. bilag 1 og
2. alle logs anvender en fælles tidskilde og samme tidszone og
3. logs er sat til opbevaring i minimum 12 måneder med mindre lovgivning på området tilsiger andet.

Bilag 1 udgør en udtømmende liste over de internetvendte tjenester og centrale interne it-systemer, der er omfattet af kravet, herunder hvilke data der skal logges.



Domænesikkerhed

Krav til Domæne sikkerhed:

17. Internetvendte tjenester tilhørende myndigheden skal registreres under .dk-domæner
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. DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden
Formålet med kravet er 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.

19. Det skal sikres, at indgående mailgateways ligger i DNSSEC-signerede domæner
Formålet med kravet er at sikre, at domæner, der håndterer mails på vegne af myndigheden, er DNSSEC-signerede. Signering af MX-recorden sikrer, at afsender af mails kryptografisk stole på, at de sender til de rette indgående mailgateways.

20. Der skal anvendes DANE for alle indgående mailgateways
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 validering af DNSSEC-signerede svar på navneopslag
Formålet med kravet er at forhindre, at myndighedens ansatte eksempelvis sendes videre til falske hjemmesider. Ved at foretage DNSSEC-validering sikres det, at svar på navneopslag kommer fra domæneejeren og ikke er manipuleret undervejs.

22. 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 phishing-sider og hjemmesider med malware. Ved brug af en Sikker DNS-tjeneste filtreres navneforespørgsler på baggrund af automatisk opdaterede lister over domæner, der vurderes at være skadelige.

23. DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden
Formålet med kravet er at give mailmodtagere mulighed for at opdage forsøg på mail-spoofing, hvor en afsender udgiver sig for at være en anden. Ved at implementere DMARC på alle domæner reduceres risikoen for, at myndighedens domænenavne kan misbruges til udsendelse af phishing- eller spam-mails.

ANVISNINGER

Kravene angår myndighedens egne domæner og sikringer i forbindelse med myndighedens navneforespørgsler

17. Internetvendte tjenester tilhørende myndigheden skal registreres under .dk-domæner

Kravet er opfyldt, hvis

1. alle internetvendte tjenester tilhørende myndigheden er registreret under .dk-domæner, og
2. såfremt myndigheden ejer domæner under andre Top-level-domains (TLD's), skal trafik omdirigeres til.dk-domænet.

Det er tilladt at anvende andre TLD's uden omdirigering, hvis indholdet på disse tjenester primært er målrettet borgere, myndigheder og virksomheder uden for Danmark.

18. DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden

Kravet er opfyldt, hvis alle myndighedens domæner og delegerede subdomæner er DNSSEC-signerede.

19. Det skal sikres, at indgående mailgateways ligger i DNSSEC-signerede domæner

Kravet er opfyldt, hvis alle indgående mailgateways, der håndterer mails for myndigheden, ligger i DNSSEC-signerede domæner.

20. Der skal anvendes DANE for alle indgående mailgateways

Kravet er opfyldt, hvis myndigheden har publiceret gyldige TLSA-records for alle indgående mailgateways i domæner, der kan modtage mails.

ANVISNINGER

Kravene angår myndighedens egne domæner og sikringer i forbindelse med myndighedens navneforespørgsler

21. Der skal foretages validering af DNSSEC-signerede svar på navneopslag

Kravet er opfyldt, hvis alle svar på navneopslag DNSSEC-valideres.

22. Myndigheden skal anvende en Sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod adgang til kendte skadelige domæner

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.

23. DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden

Kravet er opfyldt, hvis

1. Der er implementeret DMARC med politikken ”reject” for alle myndighedens hoved- og subdomæner og
2. SPF (Sender Policy Framework) er implementeret for alle myndighedens hoved- og subdomæner og
3. DKIM (DomainKeys Identified Mail) er implementeret på alle hoveddomæner og på de subdomæner, der indgår i mailflow.

Netværk

Krav til netværk:

24. Myndighedens WiFi-netværk skal være krypteret med minimum WPA2
Formålet med kravet er at forhindre misbrug og aflytning af trafikken på myndighedens WiFi-netværk.

25. Gæstenetværk skal holdes adskilt fra myndighedens interne netværk
Formålet med kravet er at sikre, at trafik fra gæstenetværket ikke omgår eksisterende sikringstiltag, og at eventuel uønsket internettrafik fra gæstenetværket ikke påvirker myndighedens omdømme.

ANVISNIGER

Kravene angår myndighedens trådede og trådløse netværk

24. Myndighedens WiFi-netværk skal være krypteret med minimum WPA2

Kravet er opfyldt, hvis adgang til myndighedens WiFi-netværk er krypteret med minimum WPA2.

25. Gæstenetværk skal holdes adskilt fra myndighedens interne netværk

Kravet er opfyldt, hvis

1. gæstenetværket er logisk adskilt fra de interne netværk og
2. al trafik fra gæstenetværket betragtes og behandles som trafik fra internettet og
3. udgående trafik fra gæstenetværket skal anvende en anden IP-adresse end trafik fra myndighedens interne netværk.

Internetvendte tjenester

Krav til Internetvendte tjenester:

26. Software på myndighedens internetvendte tjenester skal holdes sikkerheds opdateret
Formålet med kravet er, at kendte sårbarheder, der kan udnyttes over internettet/fra internettet, bliver lukket hurtigst muligt. Derfor skal al software, der anvendes på myndighedens internetvendte tjenester, være omfattet af aktiv support og regelmæssige sikkerhedsopdateringer.

27. Adgang til myndighedens internetvendte tjenester skal ske over en krypteret forbindelse
Formålet med kravet er at sikre dataintegritet og fortrolighed samt forebyggelse af man-in-the-middle angreb.

28. Internettilgængelige IP-adresser, som myndigheden har brugsret over, skal scannes for tjenester
Formålet med kravet er, at sikre, at kun det nødvendige og forventede er tilgængeligt over internettet.

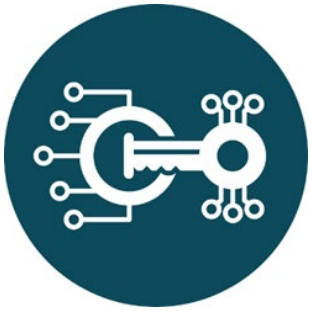
ANVISNIGER

Kravene angår de af myndighedens it-systemer, som kan tilgås fra internettet

26. Software på myndighedens internetvendte tjenester skal holdes sikkerhedsopdateret

Kravet er opfyldt, hvis

1. det anvendte software og eventuelle tredjepartsbiblioteker på internetvendte systemer, er under aktiv support (dvs. at der udgives sikkerhedsopdateringer, som adresserer kendte sårbarheder) 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.



27. Adgang til myndighedens internetvendte tjenester skal ske over en krypteret forbindelse

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.

28. Internettilgængelige IP-adresser, som myndigheder har brugsret over, skal scannes for tjenester

Kravet er opfyldt, hvis

1. der mindst én gang i kvartalet foretages en scanning af myndighedsbenyttede Internettilgængelige IP-adresser for internetvendte tjenester og
2. IP-rangen scannes for alle porte (0-65.535).

Interne it-systemer

Kravet til interne it-systemer:

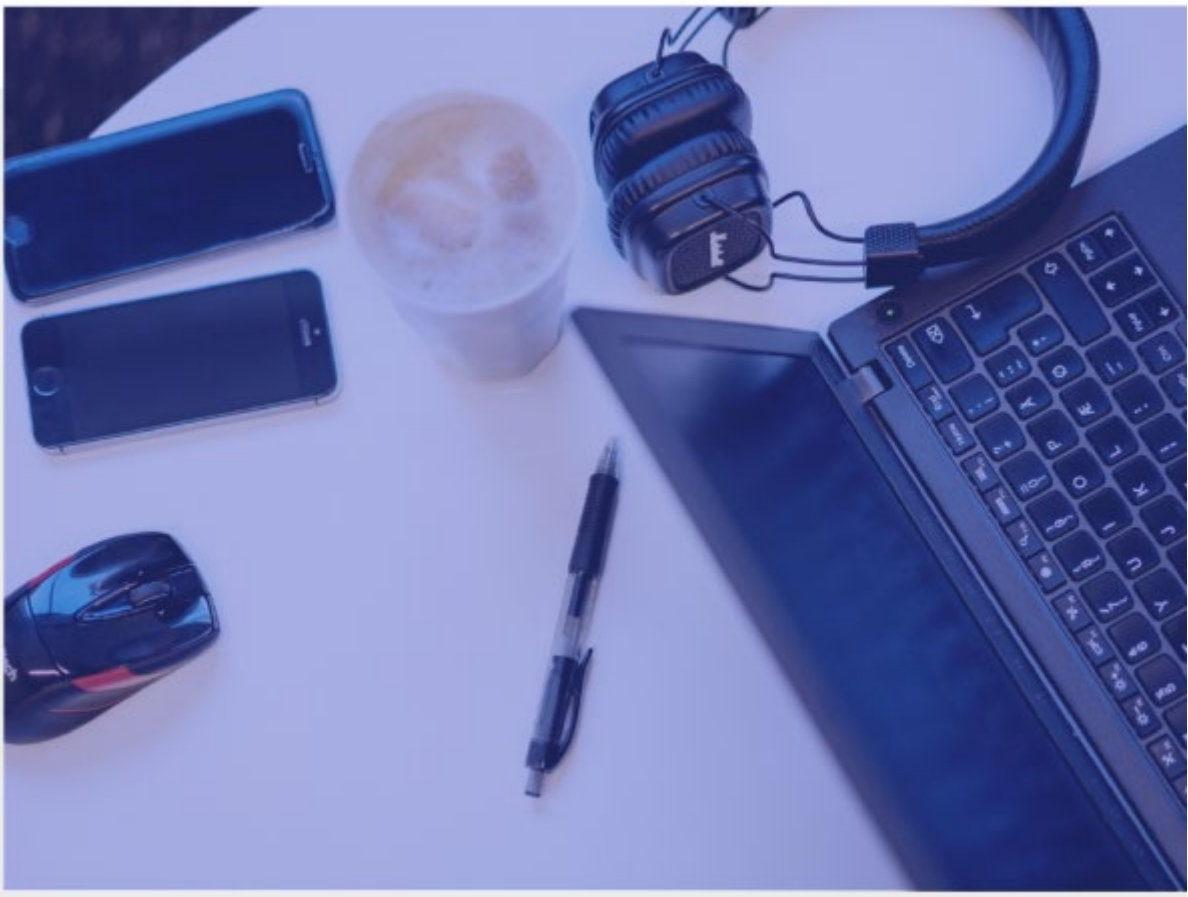
29. Software på specifikke interne infrastruktur-enheder og -tjenester skal holdes sikkerhedsopdateret
Formålet med kravet er, at kendte sårbarheder bliver lukket hurtigst muligt. Derfor skal software, der anvendes på omfattede infrastruktur-enheder og -tjenester være omfattet af regelmæssig sikkerhedsopdatering.

ANVISNIGER

Kravene angår specifikke interne infrastruktur-enheder og -tjenester

29. Software på specifikke interne infrastruktur-enheder og -tjenester skal holdes sikkerhedsopdateret

Kravet er opfyldt, hvis der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer, at omfattede infrastruktur-enheder og –tjenester sikkerhedsopdateres inden for 90 dage jf. bilag 1.



BILAG 1

Afgrænsning af minimumskrav 9, 16 og 27 og 29

Nærværende bilag skal ses i sammenhæng med de tekniske minimumskrav til it-sikkerhed i staten. For krav 9, 16, 27 og 29 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 og 2.

Tabel 1: Konfigurationsparametre TLS 1.2.

#	Emne for retningslinjer	Værdi	Status
1	TLS versioner	TLS 1.2	Tilstrækkelig
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_8 AES-128-CCM_8 IDEA DES RC4 NULL	Utilstrækkelig
5	Hash funktioner for – Nøgleudveksling	SHA-512 SHA-384 SHA-256	God
		Øvrige funktioner	Bør udfases
6	Hash funktioner for –	SHA-512	God

	Certifikat verifikation	SHA-384 SHA-256	
		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)	Tilstrækkelig
		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	God
		On	Utilstrækkelig
13	Klient-initierede genforhandling (Client initiated renegotiation)	Off	God
		On	Utilstrækkelig
14	0-RTT	Off	God
		On	Utilstrækkelig
15	OCSP hæftning (stapling)	ON	God
		Off	Tilstrækkelig

Tabel 2: Konfigurationsparametre TLS 1.3.

#	Emne for retningslinjer	Værdi	Status
1	TLS versioner	TLS 1.3	God
2	Algoritmer for – Nøgleudveksling	ECDHE	God
		DHE	Tilstrækkelig
3	Algoritmer for – Certifikat verifikation	ECDSA RSA	God
4	Algoritmer for – Bulk kryptering	AES-256-GCM ChaCha20-Poly1305 AES-128-GCM	God
		AES-256-CBC AES-128-CBC	Tilstrækkelig
5	Hash funktioner for – Nøgleudveksling	SHA-512 SHA-384 SHA-256	God
6	Hash funktioner for – Certifikat verifikation	SHA-512 SHA-384 SHA-256	God
7	Hash funktioner for – Bulk kryptering	HMAC-SHA-512 HMAC-SHA-384 HMAC-SHA-256	God
8	RSA Nøglelængder	Mindst 3072	God
		2048-3071	Tilstrækkelig
		Mindre end 2048	Utilstrækkelig
9	Understøttet elliptisk kurver	secp512r1 secp384r1 secp256r1 x448 x25519	God
10	Understøttet ”finite field” grupper	ffdhe4096 (RFC 7919) ffdhe3072 (RFC 7919)	Tilstrækkelig
		ffdhe2048 (RFC 7919)	Bør udfases
11	OCSP hæftning (stapling)	ON	God
		Off	Tilstrækkelig

Krav 16: *Logning skal foretages på internetvendte tjenester og centrale interne it-systemer.*

De internetvendte tjenester og centrale interne it-systemer, der er omfattet af kravet, fremgår af tabel 3. Disse tjenester og it-systemer er udvalgt, da de udgør ofte efterspurgte logkilder og –data i forbindelse med efterforskning af it-sikkerhedshændelser.

Andre logkilder og yderligere logdata kan være relevante, så tabellen angiver blot, hvad der som minimum skal logges. Hvis enkelte datapunkter ikke kan tilvejebringes i de anvendte tjenester eller it-systemer, bør tilsvarende logdata søges tilvejebragt fra andre logkilder.

For at sikre at aktiviteter kan sammenkædes, er det vigtigt at der anvendes en fælles tidskilde og samme tidszone på tværs af logkilder. CFCS anbefaler, at der anvendes UTC. Kravet angiver ikke, at logs skal opbevares online, blot at den angivne logning foretages, og at logdata kan tilvejebringes for den påkrævede periode.

Tabel 3: Oversigt over tjenester og it-systemer, herunder hvad der skal logges og med hvilket formål. Logning skal foretages såfremt disse tjenester og it-systemer anvendes.

Tjenester og it-systemer	Hvad skal logges?	Formål
Rekursive DNS-servere	• Tid • Forespørgers IP-adresse • Forespørgsel med indhold og svar returneret.	Logdata viser hvilke enheder der har foretaget hvilke navneopslag, og hvilket svar de modtog. Dette kan afsløre malware-infektion, kommunikation med hackeres kontrol-infrastruktur mv.
DHCP-servere	• Tid • Tildelt IP-adresse • Forespørgers MAC-adresse • Hostnavn	Logdata viser hvilke enheder der har haft en given IP-adresse tildelt, på et givent tidspunkt. Dette er nødvendigt for korrelation med andre logdata, når der anvendes DHCP.
Firewalls	• Tid • Afsender/modtager-IP-adresse • Port • Beslutning (såsom forbindelsen blev afvist, godkendt, lukket etc.) • Datastørrelser på sessionens trafik.	Logdata viser hvilken trafik der er accepteret eller afvist til/fra internettet og mellem interne netværk. Afvist trafik kan afsløre rekognoscering, forsøg på uautoriseret bevægelse mellem netværk, forsøg på omgåelse af blokering baseret på afsender-IP mv. Logning i forbindelse med DDoS/DoS angreb kan begrænses til at logge den initiale blokering af de enkelte IP-adresser.
Autentifikationsservere	• Tid • Eventtype • Kontonavn • Forespørgers IP-adresse • Forespørgers hostnavn (hvis modtaget) • Beslutning (resultat af autentifikationsforsøg).	Logdata viser autentifikationsforsøg, herunder succesfulde og fejlede loginforsøg. Dette kan afsløre kompromittering af konti eller tjenester, forsøg på brute-force angreb eller password-spraying mv.

Routere, der blokerer for trafik	• Tid • Afsender/modtager-IP-adresse • Port • Beslutning (såsom forbindelsen blev afvist, godkendt, lukket etc.).	Logdata viser hvilken trafik der er accepteret eller afvist mellem netværk. Afvist trafik kan afsløre rekognosceringsforsøg, forsøg på uautoriseret bevægelse mellem netværk, forsøg på omgåelse af blokering baseret på afsender-IP mv. Logning i forbindelse med DDoS/DoS angreb kan begrænses til logning af den initiale blokering af de enkelte IP-adresser.
Klient-VPN gateways	• Tid • Klientens IP-adresse • Brugernavn • Tildelt IP-adresse • Fejlede og godkendte logins.	Logdata viser godkendt og afvist fjernadgang for brugere (f.eks. ved hjemmearbejde, rejse mv.), og hvilken IP-adresse deres klienter var tildelt under fjernadgangen. Dette kan afsløre forsøg på kompromittering af fjernadgang, og anvendes til korrelation med andre logdata.
Web proxy	• Tid • Klientens IP-adresse • Metode (f.eks. GET, POST, etc.) • URIs • Returkode.	Logdata viser udgående internettrafik på vegne af myndighedens klienter (forward proxy). Dette kan afsløre malware-infektion, kommunikation med hackeres kontrol-infrastruktur, eksfiltrering af data mv.
Antivirus/-malware-systemer	• Tid • Handling (f.eks. karantæne, blokering etc.) • Proces/filnavn/aktivitet der forårsager event.	Logdata viser hændelser der har foranlediget en handling af antimalware-systemet. Dette kan afsløre phishing og andre kompromitteringsforsøg, og eksempelvis afsløre tidlige tegn på et forestående ransomware-angreb.
Ind- og udgående mailgateways	• Tid • Afsender/modtager e-mailadresser, • Hostnavn og IP-adresse på afsender-/modtagergateways • Emne • Størrelse på besked • Navne på vedhæftede filer.	Logdata viser ind- og udgående mails og relevant information om disse. Dette kan afsløre phishing-angreb, eksfiltrering af data mv.
Internetvendte webservere eller webservices (fx hjemmesider, API, MQ og andre HTTPS-baserede tjenester).	• Tid • Afsenderens eksterne IP-adresse • Metode (f.eks. GET, POST, etc.) • URIs, • Returkode • User-agent • Antal bytes	Logdata viser indgående webtrafik og relevant information herom. Dette kan afsløre kompromittering af brugerkonti, anvendt software/tredjepartskomponenter, tilgængeligt indhold mv.

Øvrige internetvendte tjenester (f.eks. SFTP, SSH etc.).	• Tid • Afsenderens eksterne IP-adresse • Aktivitet relevant for den pågældende tjeneste (f.eks. godkendt/afvist login, up-/download af filer, udførte kommandoer etc.).	Logdata viser anvendelse af internetvendte tjenester. Dette kan afsløre kompromittering af brugerkonti, anvendt software/tredjepartskomponenter, tilgængeligt indhold, konfigurationsindstillinger mv. Hvilken aktivitet der er relevant at logge for den enkelte tjeneste afhænger af tjenestens karakter, og er derfor ikke udspecificeret her. Myndigheden skal dog have taget stilling hertil.

Krav 27: *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 og 2 (se krav 9).

Krav 29: *Software på specifikke interne infrastruktur-enheder og –tjenester skal holdes opdateret.*

Kravet angår specifikke interne infrastruktur-enheder og –tjenester. Software på disse interne infrastruktur-enheder og -tjenester er omfattet af kravet, såfremt de anvendes af myndigheden:

- Centrale autentifikationstjenester (fx domain controllere, LDAP, MFA, RADIUS mv.)
- Mailservere
- Navneservere (rekursive og autoritative)
- DHCP-servere
- Filservere
- Printservere
- Loadbalancers
- Firewalls, og routere der blokerer for trafik
- Proxyservere
- Hypervisors/virtualiseringsplatforme
- Antivirus- og malwaresystemer
- Backupservere
- IM, VoIP og Videokonferenceservere
- Softwareudrulningssystemer (fx Configuration Manager)
- Lognings- og monitoreringssystemer
- MDM-servere
- PAM-systemer