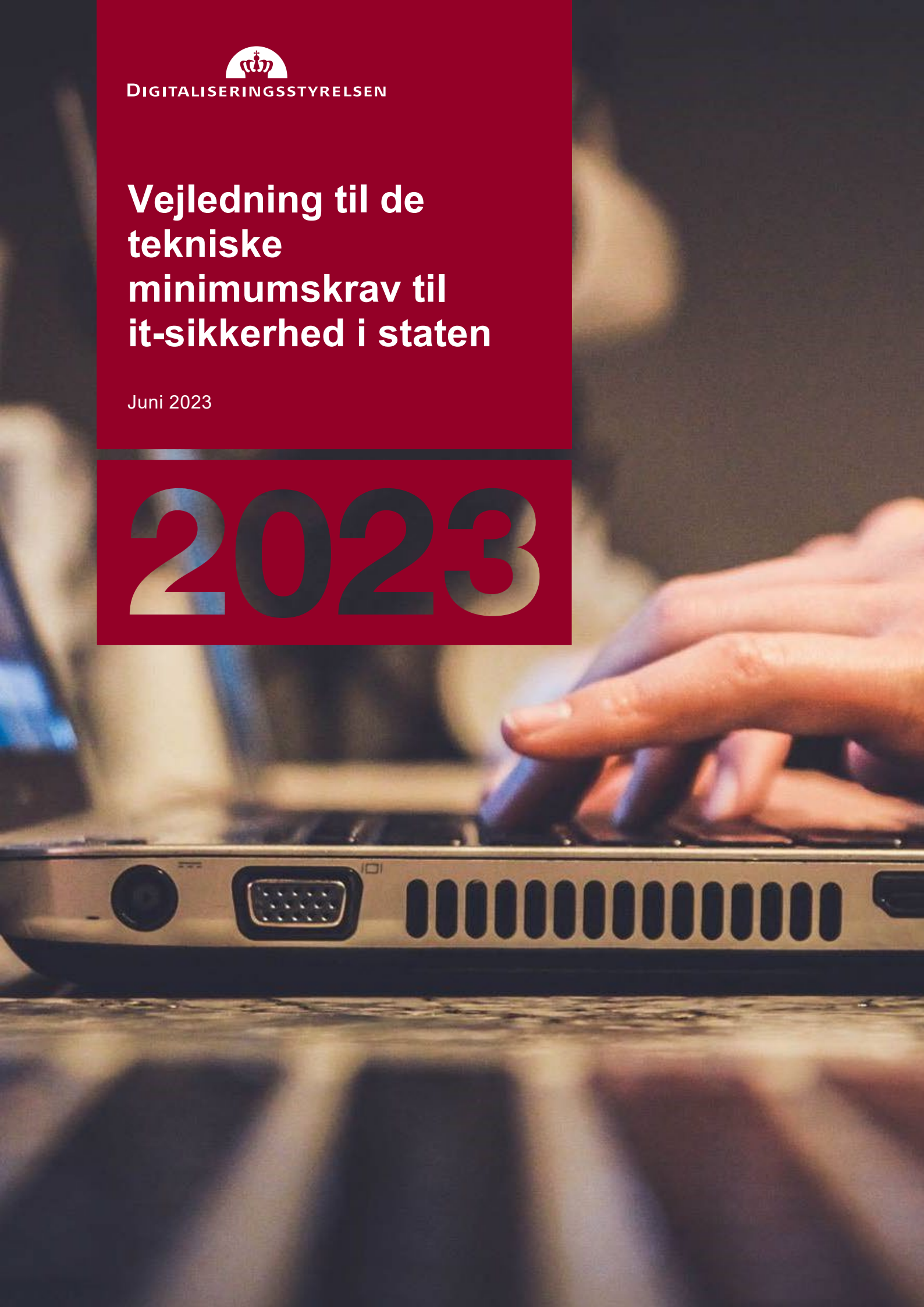
DIGITALISERINGSSTYRELSEN

Vejledning til de tekniske minimumskrav til it-sikkerhed i staten

Juni 2023

2023



Indhold

1. Indledning

Denne vejledning uddyber de tekniske minimumskrav til it-sikkerhed, som er obligatoriske at implementere for alle statslige myndigheder.

1.1 Formål med kravene

De tekniske minimumskrav har til formål at sikre et fælles højt sikkerhedsniveau i staten. Kravene har bl.a. til formål at beskytte statslige it-arbejdspladser, herunder arbejdsnetværk og arbejdsstationer mod ondsindede cyber- og informationssikkerhedshændelser, fx hackerangreb og spredning af virus. Kravene sigter også mod at sikre borgere, virksomheder og myndigheder mod fx phishing, kompromittering af oplysninger og man-in-the-middle-angreb[1], hvorfor der stilles krav til myndighedernes internetvendte tjenester og krav om anvendelse af sikre internetstandarder.

Størstedelen af kravene følger af eksisterende vejledninger og anbefalinger på området fra Center for Cybersikkerhed, Digitaliseringsstyrelsen og Datatilsynet. De øvrige er udtryk for udbredt *'best practice'* på området for cyber- og informationssikkerhed.

1.2 Implementering af kravene

Det er obligatorisk for alle statslige myndigheder at implementere og sikre overholdelse af de til enhver tid gældende minimumskrav. Minimumskravene er ufravigelige, og myndighederne kan derfor ikke ud fra en risikobetragtning vælge at undtage udvalgte it-systemer, domæner eller lignende for overholdelse. Myndighederne er desuden forpligtet til at foretage egne risikovurderinger og implementere yderligere sikkerhedstiltag i relevant omfang. De tekniske minimumskrav til it-sikkerhed, formålsbeskrivelser for de enkelte krav, samt anvisninger for efterlevelse af kravene kan findes her[2].

For flere statslige myndigheder er den basale it-drift overdraget til Statens IT. Statens IT sikrer derfor overholdelse af flere af kravene for deres kunder. Efterlevelse af enkelte krav vil dog kræve en indsats både fra Statens IT og kunderne selv. Statens IT har udarbejdet et hjælpeark til myndighederne, der beskriver ansvarsfordelingen mellem kunderne og Statens IT. Der henvises til Statens IT, såfremt der er spørgsmål til den konkrete ansvarsfordeling.

---

[1] I et Man-in-the-middle (MITM) angreb har en tredjepart opnået adgang til kommunikationskanalen mellem to parter, og kan opsnappe eller manipulere indholdet.
[2] Det bemærkes, at der for klassificerede it-systemer gælder andre krav. For vejledning om krav til klassificerede systemer, kan sikkerhedsmyndighederne kontaktes på cfcs@cfcs.dk og pet@pet.dk.

2. Afgrænsning og uddybning

Dette kapitel beskriver den nærmere afgrænsning af minimumskravene.

De tekniske minimumskrav fordeler sig i 10 forskellige kategorier. For hver kategori er det beskrevet, hvad de underliggende krav gælder for. Denne opdeling og afgrænsning af kravene har til formål at tydeliggøre, hvad der er omfattet af kravene.

Kategori	Kategoribeskrivelser
Klienter/PC'er 	Kravene angår de stationære og bærbare computere, der administreres af myndigheden, og som har adgang til myndighedens almindelige it-infrastruktur og data.
Mail 	Kravene angår mailkommunikationen til og fra myndigheden.
Autentifikation 	Kravet angår de af myndighedens it-systemer, som kan tilgås fra internettet, og hvor der logges på med myndighedens brugerkonti (typisk brugerens standardkonto).
Password 	Kravet angår alle myndighedens brugerkonti, herunder konti udstedt til administratorer, it-systemer og services i centrale brugerdatabaser/autentifikationstjenester.
Mobile enheder 	Kravene angår mobiltelefoner og tablets med app-baseret adgang til myndighedens data.
Logning 	Kravet angår alle internetvendte tjenester og centrale interne it-systemer.
Domænesikkerhed 	Kravene til domænesikkerhed angår myndighedens egne domæner, og sikring i forbindelse med myndighedens navneforespørgsler.
Netværk 	Kravene angår myndighedens trådede og trådløse netværk.
Internetvendte tjenester 	Kravene angår alle tjenester, der kan tilgås fra internettet.
Interne it-systemer 	Kravet angår specifikke interne infrastruktur-enheder og -tjenester.

Den nærmere afgrænsning af kravene gennemgås for hver kategori i de efterfølgende afsnit.

2.1 Klienter/PC'ere

Kravene til klienter angår de stationære og bærbare computere, der administreres af myndigheden, og som har adgang til myndighedens almindelige it-infrastruktur og data. Computere, som myndigheden har udleveret til eksterne konsulenter er derfor også omfattet. Kravene gælder uanset hvilket operativsystem, der anvendes på klienten. I det omfang, der i myndigheden anvendes computere til særlige brugssituationer, og der ikke fra disse kan opnås adgang til internettet, eller myndighedens almindelige it-infrastruktur og data, kan disse undtages fra kravene.

Det følger af kravene, at operativsystem (OS) og applikationer på klienten skal holdes sikkerhedsopdateret, og at operativsystemet skal være under aktiv support. Aktiv support betyder, at kendte sårbarheder adresseres/lukkes gennem frigivelse af sikkerhedsopdateringer. En applikation defineres som, *software der leverer funktionalitet til en bruger*. For at levere den funktionalitet, kan applikationen have medinstalleret og anvende forskellige komponenter. Komponenterne leverer i sig selv ikke aktivt nogen funktionalitet til brugeren (de anvendes ikke alene), og opdateres som udgangspunkt samtidig med applikationen. OS-specifikke komponenter vil oftest blive opdateret i forbindelse med opdatering af operativsystemet.

Det følger af kravene, at det anvendte OS skal være en major release eller major update udgivet for mindre end 18 måneder siden. Pr. 1. juli 2023 er følgende major releases/major updates for Microsoft Windows under 18 måneder gamle:

- Windows 11 – 22H2 (september 2022)
- Windows 10 - 22H2 (oktober 2022)

2.2 Mail

Kravene til mail angår mailkommunikationen til og fra myndigheden. Kravene gælder også, hvis mailkommunikationen eksempelvis varetages af en ekstern leverandør.

Det følger af kravene, at kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2. Det bemærkes, at ikke-krypteret kommunikation er tilladt i de tilfælde, hvor modtageren/afsenderen ikke understøtter kryptering. Dette er tilladt, da statslige myndigheder ikke kan afvise mails fra eksempelvis borgere. Hvis mails sendes mellem statslige myndigheder, skal der foretages tvungen kryptering.

Såfremt en mailafsender har valgt at implementere en DMARC-politik som et sikringstiltag, skal modtageren (myndigheden) overholde afsenderens DMARC-politik. Myndigheden skal derfor sikre, at de indgående mailgateways respekterer afsenderdomænets DMARC-politik, såfremt en politik er publiceret af afsenderen. Hvis en mailafsender får videresendt sine mails via en tredjepart, kan der ved fejlkonfiguration af DMARC-politikken hos afsenderen være risiko for, at en mail

fremstår som forfalsket, og derfor afvises af modtageren (myndigheden). Mailafsenderen vil typisk blive underrettet om, at mailen er blevet afvist. Risikoen herfor reduceres ved implementering af både SPF (Sender Policy Framework) og DKIM (DomainKeys Identified Mail) på afsenderdomænet.

2.3 Autentifikation

Kravet angår autentifikation til de af myndighedens it-systemer, der kan tilgås fra internettet, og hvor der logges på med myndighedens brugerkonti (typisk brugerens standardkonto). Myndighedens brugerkonti skal her forstås som de interne konti, myndigheden har udstedt til egne ansatte og evt. konsulenter, så de kan tilgå myndighedens klienter, it-systemer og data. Kravet gælder ikke for de it-systemer, hvor eksterne brugere, fx myndigheder, borgere eller virksomheder logger ind for at tilgå egne data. Software-as-a-Service-løsninger, som myndigheden køber adgang til, er heller ikke omfattet af kravet, medmindre login er integreret (single sign-on el. lignende) med myndighedens egen autentifikationsplatform. Logges der på en SaaS-løsning med samme myndigheds-brugerkonti, som også giver adgang til myndighedens klienter, interne systemer og data, er løsningen fortsat omfattet af kravet. Det anbefales generelt, at der anvendes flerfaktor-autentifikation på alle de it-systemer, hvor det understøttes, uagtet om it-systemet ejes af myndigheden eller blot anvendes af myndighedens ansatte.

Flerfaktor-autentifikation er oftest karakteriseret ved, at en bruger får adgang med sit brugernavn og password suppleret med en eller flere autentifikationstyper. En type kan eksempelvis være noget brugeren *har*, fx et nøglekort eller noget bruger *er*, fx et fingeraftryk også kaldet biometrisk identifikation. Det er afgørende, at der uanset valg af autentifikationstype sker en bekræftelse af brugerens identitet, så det sikres, at et nøglekort eksempelvis udstedes til den rette person. Det følger derfor også af kravet, at myndigheden skal sikre, at en faktor ikke kan udstedes til uvedkommende, der måtte have opnået kendskab til personens brugernavn og password.

Såfremt autentifikationsmetoden gør brug af engangskoder, skal disse genereres lokalt og må ikke transmitteres til brugeren, fx via SMS eller mail. Årsagen hertil er, at koder sendt på denne måde kan opsnappes og anvendes til at kompromittere et log-on. Nedenfor er der angivet eksempler på autentifikationsmetoder, der kan anvendes:

- Kodevisere eller mobil applikationer, der genererer en tidsbegrænset engangskode på enheden (TOTP-koder).
- Engangskoder, der er udleveret fysisk til brugeren, fx et nøglekort.
- Mobilapplikationer, der anmoder om bekræftelse/godkendelse ved loginforsøg.
- Sikkerhedsnøgler, der er udleveret fysisk til brugeren, fx en USB-sikkerhedsnøgle.
- Biometri som fingeraftryk eller ansigtsgenkendelse.

2.4 Password

Kravet angår alle myndighedens brugerkonti, herunder konti udstedt til administratorer, it-systemer og services i centrale brugerdatabaser/autentifikationstjenester. Kravet gælder kun for myndighedens egne it-systemer. Eksterne it-systemer, som myndigheden anvender, fx Software-as-a-Service-løsninger, er altså ikke omfattet af kravet.

Overholdelse af kravet kan eksempelvis ske via et værktøj eller script, der sammenligner hashværdien for myndighedens anvendte passwords op mod en liste over lækkede passwords[3]. Hvis der er match mellem de to lister, skal den pågældende bruger underrettes jf. kravets anvisninger. En oversigt over lækkede passwords kan eksempelvis findes hos Have I Been Pwned[4]. Myndighederne kan overveje at supplere listen med en lokal liste over svage passwords eksempelvis "myndighedensnavn123".

2.5 Mobile enheder

Kravene til mobile enheder angår mobiltelefoner og tablets med app-baseret adgang til myndighedens data. Kravene gælder uafhængigt af, om disse data tilgås fra myndighedsudleverede enheder eller fra private enheder. Såfremt en applikation tilgår internettilgængelige data efter forudgående login og data ikke efterfølgende gemmes på telefonen, stilles der ikke krav om implementering af en MDM-løsning (Mobile Device Management) på den mobile enhed. Kravet omfatter ikke mobile enheder, der udelukkende anvendes til internetadgang, telefoni, SMS-beskeder osv. Der stilles dog krav om MDM på den mobile enhed, hvis der fra enheden eksempelvis er adgang til myndighedens interne it-systemer, fx mailsystem eller lignende.

Det følger af kravene, at operativsystem (OS) og applikationer på enheden skal holdes sikkerhedsopdateret, og at operativsystemet skal være under aktiv support. Aktiv support betyder, at kendte sårbarheder adresseres/lukkes gennem frigivelse af sikkerhedsopdateringer.

2.6 Logning

Kravet til logning angår alle myndighedens internetvendte tjenester og centrale interne it-systemer. I kravoversigtens bilag 1 fremgår en liste over de internetvendte

---

[3] Hashing er en matematisk envejsfunktion, der udregner en unik værdi på baggrund af noget data. Da det er en envejsfunktion, kan hash-værdien ikke anvendes til at udregne det oprindelige data. Hash-værdier anvendes eksempelvis til at tjekke, at filers indhold ikke er blevet ændret eller til at gemme en sikker repræsentation af et password.

[4] https://haveibeenpwned.com/

tjenester og centrale interne it-systemer, der er omfattet af kravet, herunder hvilke data, der skal logges.

Myndigheden skal sikre, at kravet også overholdes for de af myndighedens it-systemer, der driftes hos en ekstern leverandør. Såfremt it-systemet driftes hos en ekstern leverandør, gælder kravet kun for den it-infrastruktur, der indgår i leverandørens leverancer ift. det konkrete it-system. Hvis myndigheden eksempelvis får hostet en hjemmeside hos en ekstern leverandør, skal der foretages logning i overensstemmelse med kravets anvisninger på webserverne og den understøttende infrastruktur, fx den firewall, der beskytter webserverne. Kravet omfatter altså kun de centrale it-systemer hos leverandøren, som direkte indgår i leverancerne ift. det konkrete system.

Software-as-a-Service-løsninger, som myndigheden køber adgang til, er ikke omfattet af kravet. Der stilles ikke krav om central opsamling eller monitorering/overvågning af logdata. Der stilles heller ikke krav om, at logs skal opbevares online.

2.7 Domænesikkerhed

Kravene til domænesikkerhed angår myndighedens egne domæner, og sikring i forbindelse med myndighedens navneforespørgsler. Det indebærer bl.a., at myndighedens internetvendte tjenester skal registreres under .dk-domæner. Der kan anvendes andre landekoder end .dk, hvis domænet er passivt eller trafik til disse domæner omdirigeres til .dk-domænet. Det kan eksempelvis være relevant, hvis en myndighed af kommunikationsmæssige årsager vil fastholde et nuværende domænenavn, eller hvis myndigheden har opkøbt det samme eller et lignende domænenavne under et andet top-level domain af hensyn til at minimere risikoen for misbrug. Internetvendte tjenester, hvor indholdet primært er målrettet borgere, myndigheder eller virksomheder uden for Danmark, er ikke omfattet af kravet. Det kunne eksempelvis være en hjemmeside, hvor informationen primært er målrettet borgere i Grønland eller på Færøerne, eller en hjemmeside til brug for internationalt samarbejde med andre myndigheder i fx EU.

Det følger af kravene, at DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden. Hvis myndighedens indgående mail håndteres af en tredjepart, skal myndigheden endvidere sikre, at det domæne, som tredjeparten anvender, ligger i DNSSEC-signerede domæner.

2.8 Netværk

Kravene angår myndighedens trådede og trådløse netværk. Det følger af kravene, at myndighedens WiFi-netværk skal være krypteret med minimum WPA2. For at reducere risikoen for misbrug, gælder kravet om WPA2 også for myndighedens gæstenetværk.

2.9 Internetvendte tjenester

Kravene til internetvendte tjenester angår alle myndighedens tjenester, der kan tilgås fra internettet. Det kan eksempelvis være myndighedens hjemmesider eller it-systemer, som er tilgængelige over internettet. Interne systemer, som ikke kan tilgås direkte fra internettet, er ikke omfattet af kravene under denne kategori. Det kan eksempelvis være fagsystemer, interne printerservere o.l. Såfremt der alene via VPN kan skabes forbindelse til et fagsystem over internettet, betragtes dette også som internt, og er altså ikke omfattet af kravene til internetvendte tjenester.

Ifølge kravene til internetvendte tjenester, skal det bl.a. sikres, at software på myndighedens internetvendte tjenester er under aktiv support. Aktiv support betyder, at kendte sårbarheder adresseres/lukkes gennem frigivelse af sikkerhedsopdateringer. Ved anvendelse af open-source-software betragtes det som værende under aktiv support, såfremt der løbende udgives sikkerhedsopdateringer, der adresserer kendte sårbarheder.

Det er den software, som de pågældende tjenester afhænger af, og som kan "rammes" over internettet, der er omfattet af kravet. Det kan fx være firewalls, webservere, databaser og CMS'er o.l., som anvendes. Kravet gælder som minimum for al software, hvor en sårbarhed kan udnyttes fra internettet. Funktionalitet, der er slået fra, eller hvor en sårbarhed i softwaren ikke kan udnyttes fra internettet er ikke omfattet af kravet. I tilfælde af at en sårbarhed i et bagvedliggende system kan udnyttes via en internetvendt tjeneste (som set med log4j), betragtes det bagvedliggende system som værende omfattet af kravet. Noget software kan have medinstalleret forskellige komponenter fx tredjepartsbiblioteker, der er integrerede i den samlede softwarepakke. Disse komponenter vil typisk blive sikkerhedsopdateret, som en del af sikkerhedsopdateringen af den software, de indgår i. Såfremt sikkerhedsopdateringer til disse underliggende komponenter indgår i sikkerhedsopdatering af den samlede softwarepakke, er de ikke selvstændigt omfattet af anvisningen om opdatering inden for 30 dage. I alle tilfælde anbefales det, at myndighederne sikrer rettidig sikkerhedsopdatering af anvendt software på internetvendte tjenester.

Ved anvendelse af egenudviklet software, betragtes en sikkerhedsopdatering som frigivet, når den er færdigtestet af myndigheden selv. Fra det tidspunkt, hvor softwaren er færdigtestet, har myndigheden 30 dage til at få opdateringen installeret.

Det følger også af kravene til internetvendte tjenester, at der minimum hvert kvartal skal foretages en portscanning af myndighedsejede internettilgængelige IP-adresser. Der stilles ikke krav om, at der foretages sårbarhedsscanning af de afdækkede internetvendte tjenester, men udelukkende at tjenesterne afdækkes. Dette giver myndigheden kendskab til angrebsfladen, hvilket har til hensigt at kunne sikre, at alle de eksponerede tjenester, som minimum overholder de øvrige tekniske minimumskrav.

Scanning af IP-adresser tilhørende leverandører eller andre tredjeparter er ikke omfattet af kravet, men det anbefales, at der ved kontraktindgåelse eller ved fornyelse af en eksisterende kontrakt indarbejdes krav om løbende scanninger af relevante IP-adresser.

2.10 Interne it-systemer

Kravet angår specifikke interne infrastruktur-enheder og -tjenester, som eksempelvis mail- og navneservere, firewalls, softwareudrulningssystemer og PAM-systemer. I tilfælde af overlap mellem krav 26 og 29, eksempelvis ved en mailserver der kan tilgås fra både internettet og fra myndighedens interne netværk, vil anvisningerne i krav 26 være gældende.

Begreberne "tjenester", "servere", "platforme" og "systemer" dækker i denne sammenhæng over den software, der stiller den givne funktionalitet til rådighed. I nogle tilfælde sikkerhedsopdateres disse sammen med det underliggende operativsystem, og i andre tilfælde sikkerhedsopdateres de separat. Kravet gælder kun for den software, der udstiller den givne funktionalitet, men myndighederne anbefales ligeledes at sikkerhedsopdatere det underliggende operativsystem rettidigt.

For nogle typer af omfattede enheder gælder det, at sikkerhedsopdateringer foretages i firmware, frem for i software. I disse tilfælde er sikkerhedsopdateringer af firmwaren omfattet af kravet.

Myndigheden skal sikre, at kravet overholdes, hvis driften af de interne systemer forestås af en ekstern leverandør. Kravet gælder i dette tilfælde kun for den it-infrastruktur, der indgår i leverandørens leverancer ift. det konkrete it-system. Hvis myndigheden eksempelvis har sin mailserver hos en ekstern leverandør, skal myndigheden sikre, at leverandøren overholder kravets anvisninger for mailserveren og den it-infrastruktur, der understøtter serveren. Software-as-a-Service-løsninger, som myndigheden køber adgang til, er ikke omfattet af kravet.

Opfølgning på kravene

3. Opfølgning på kravene

Dette kapitel beskriver, hvordan der foretages opfølgning på kravene.

3.1 Digitaliseringsstyrelsens opfølgning

Flere gange årligt gennemfører Digitaliseringsstyrelsen en spørgeskemaundersøgelse af myndighedernes efterlevelse af kravene. Med udgangspunkt i de beskrevne anvisninger for hvert krav, skal myndigheden selv vurdere, hvorvidt kravene er implementeret. Det fremgår af spørgeskemaet, at et krav kun kan betragtes som efterlevet i tilfælde af "*fuld*" efterlevelse, altså, hvor der ikke er nogle udeståender ift. implementering af kravet i den enkelte myndighed.

De myndigheder, som ikke er i mål med alle kravene, skal udarbejde en handlingsplan. De enkelte ministerområder har ansvar for at indsamle myndighedernes handlingsplaner i én samlet handlingsplan for ministerområdet. Den samlede handlingsplan for ministerområdet vil sammen med en samlet status for efterlevelsen af kravene på tværs af staten blive forelagt regeringen.

Digitaliseringsstyrelsens kontor for cyber- og informationssikkerhed kan kontaktes, såfremt der er spørgsmål til fortolkning af kravene.

3.2 Kontrol af udvalgte krav

Til kontrol af udvalgte krav kan myndighederne evt. anvende værktøjet sikkerpånettet.dk, der scanner for en række teknologier inden for kategorierne domænesikkerhed, mail og netværk, herunder om der anvendes kryptering på et vist niveau, om der er implementeret DMARC på domæneniveau mv.

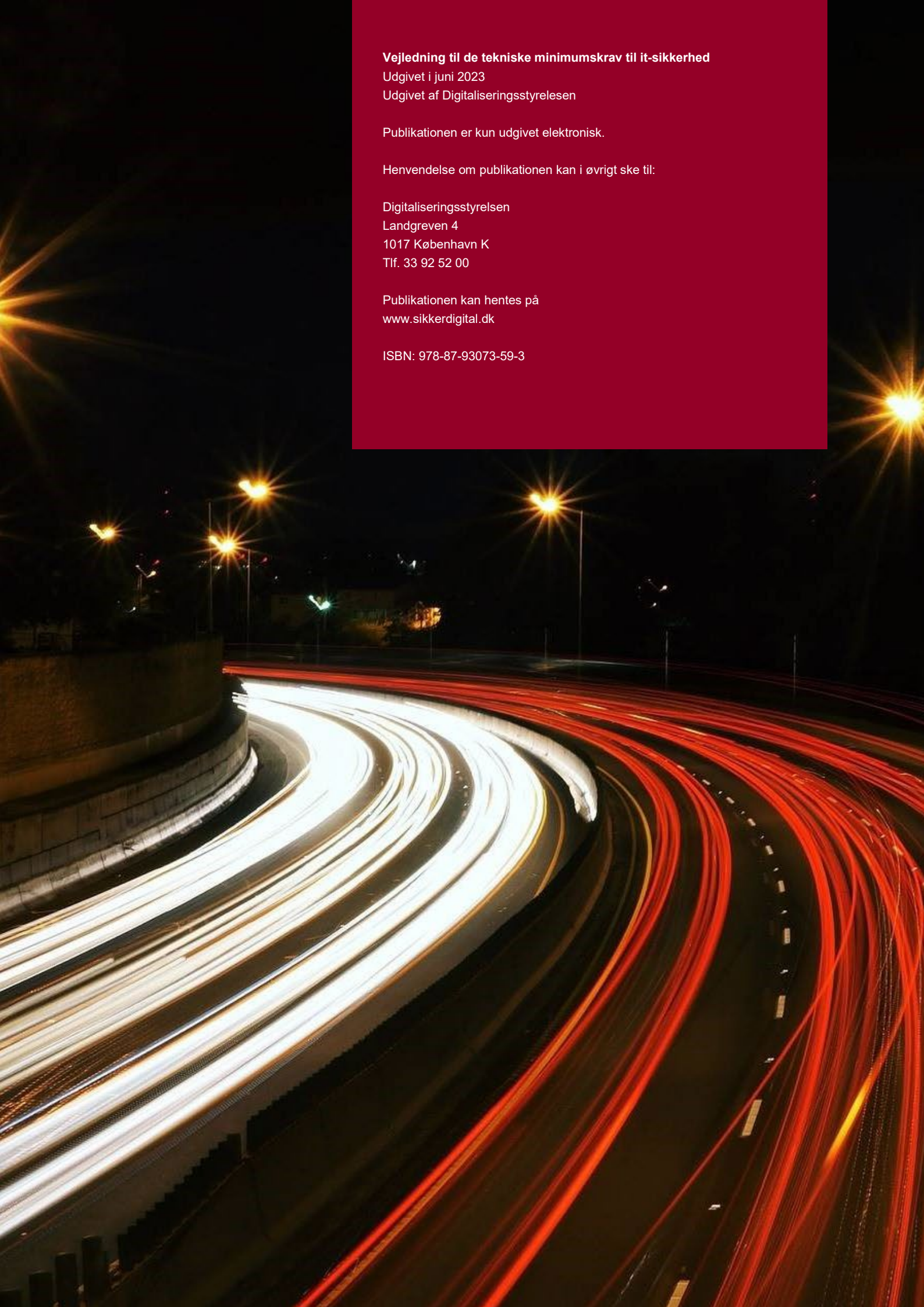
Værktøjet scanner for flere sikringstiltag og standarder end der stilles krav til, ligesom der er krav, hvis efterlevelse der ikke direkte kan scannes for. Værktøjet vil dog stadig kunne bekræfte korrekt efterlevelse af omfattede krav. Myndigheder med spørgsmål til værktøjets testresultater, kan kontakte Center for Cybersikkerhed for uddybning og rådgivning.

Vejledninger på området

4. Vejledninger på området

I dette kapitel henvises til øvrige vejledninger på området.

Kategori	Relevante vejledninger
1. Klienter/PC'er	• Cybersikkerhed på rejsen • Reducer risikoen for ransomware • Cyberforsvar der virker
2. Mail	• Sikker brug af Transport Layer Security (TLS)
3. Autentifikation	• Password-sikkerhed
4. Password	
5. Mobile enheder	• Råd om sikkerhed på mobile enheder
6. Logning	• Logning – en del af et godt cyberforsvar
7. Domænesikkerhed	• Reducer risikoen for falske mails • Domænesikkerhed
8. Netværk	• Ingen henvisninger.
9. Internetvendte tjenester	• Cyberforsvar der virker • Sikker brug af Transport Layer Security (TLS)
10. Interne tjenester	• Ingen henvisninger.



Vejledning til de tekniske minimumskrav til it-sikkerhed
Udgivet i juni 2023
Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk.

Henvendelse om publikationen kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
www.sikkerdigital.dk

ISBN: 978-87-93073-59-3