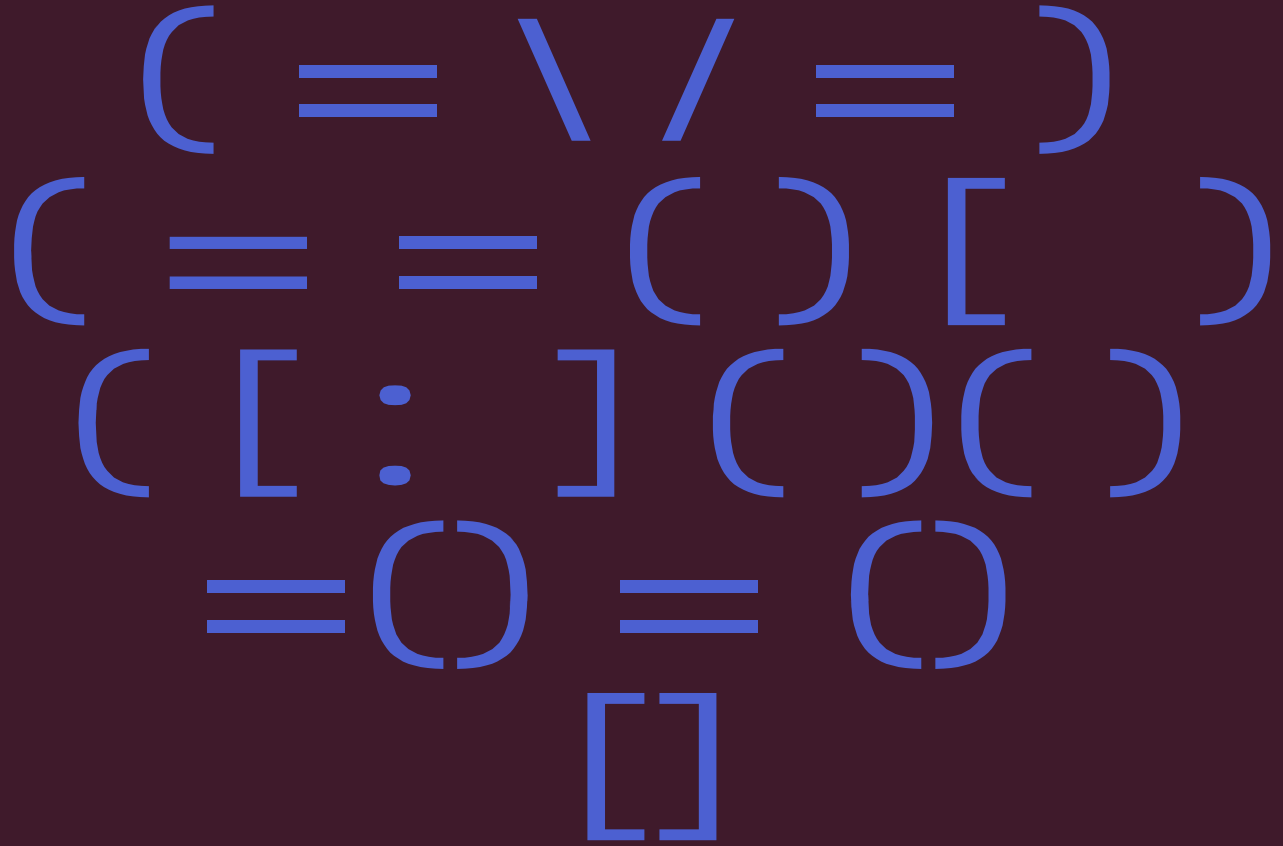
Digitaliseringsstyrelsen

Vejledning til de tekniske minimumskrav til it-sikkerhed i staten



Juni 2024

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,

[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.

der beskriver ansvarsfordelingen mellem kunderne og Statens It. Der henvises til Statens It, såfremt der er spørgsmål til den konkrete ansvarsfordeling.

Læsevejledning

Overordnet

- Minimumskravene er inddelt i kategorier. Hvert krav skal læses inden for rammerne af den kategori, det tilhører.
- Denne vejledning uddyber omfanget af kravene for hver kategori med henblik på at klæde myndighederne bedre på til at forstå og i sidste ende implementere minimumskravene.
- Det er derfor vigtigt, at I som myndigheder orienterer jer i de specifikke definitioner, afgrænsninger og forbehold, der gælder for de forskellige kategorier.
- I vejledningen gives fiktive eksempler, der har til formål at tydeliggøre afgrænsningen for de enkelte kravkategorier.

Gennemgående begreber

- **It-infrastruktur** er en samlebetegnelse for alle de it-systemer og enheder der understøtter leveringen af en organisations tjenester til dens medarbejdere, brugere mv., herunder netværk, servere osv.
- **Tjenester** er it-systemer eller software, der leverer en bestemt funktionalitet til medarbejdere, borgere eller til andre systemer. Tjenester kan omfatte alt fra webservere og databaser til mailservere samt cloud-baserede tjenester.
- **Internetvendte tjenester** omfatter alle de tjenester, som kan tilgås fra internettet, herunder VPN-gateways, hjemmesider, og andre webbaserede tjenester. Ofte er der tale om systemer, som af myndigheden stilles til rådighed for eksterne brugere fx borgere eller virksomheder, men også systemer målrettet myndighedens egen medarbejdere er omfattet, hvis de kan tilgås direkte fra internettet.
- **Interne it-systemer** er it-systemer eller tjenester, som ikke kan tilgås direkte fra internettet. Disse benyttes typisk kun af myndighedens egne medarbejdere, eller indgår i organisationens interne it-infrastruktur.
- **Software-as-a-Service**, ofte forkortet SaaS, omfatter webbaserede og -hostede tredjepartstjenester, og hvor adgangen til softwaren købes på abonnementsbasis.

2. Afgrænsning og uddybning

Dette kapitel beskriver den nærmere afgrænsning af minimumskravene.

De tekniske minimumskrav fordeler sig i ti 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
1. Klienter/PC'er 	Kravene til klienter angår alle de stationære, bærbare og virtuelle computere, som har adgang til myndighedens interne it-systemer.
2. Mail 	Kravene til mails angår e-mailkommunikationen til og fra myndigheden.
3. Autentifikation 	Kravet angår de af myndighedens it-systemer, som kan tilgås fra internettet, og hvor der logges på med myndighedens brugerkonti (typisk brugerens standardkonto).
4. Password 	Kravet angår alle myndighedens brugerkonti, herunder konti udstedt til administratorer, it-systemer og services i centrale brugerdatabaser/autentifikationstjenester.
5. Mobile enheder 	Kravene til mobile enheder angår mobiltelefoner og tablets med app-baseret adgang til myndighedens data.
6. Logning 	Kravet til logning angår alle internetvendte tjenester og centrale interne it-systemer.
7. Domænesikkerhed 	Kravene til domænesikkerhed angår myndighedens egne domæner, og sikring i forbindelse med myndighedens navneforespørgsler.
8. Netværk 	Kravene til netværk angår myndighedens trådede og trådløse netværk.
9. Internetvendte tjenester 	Kravene til internetvendte tjenester angår alle tjenester, der kan tilgås fra internettet.
10. Interne it-systemer 	Kravet angår specifikke interne infrastrukturenheder og -tjenester.

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

2.1 Klienter/PC'er

Kravene til klienter angår alle de stationære, bærbare og virtuelle computere, som har adgang til myndighedens interne systemer. Computere, som myndigheden har udleveret til eksterne konsulenter, er derfor også omfattet. Kravene gælder uanset hvilket operativsystem, der anvendes på klienten. Virtuelle klienter er også omfattet af kravene i det omfang, det teknisk er muligt at implementere kravene. Eksempelvis gælder kravet om harddiskkryptering ikke for virtuelle klienter, da disse ikke er udsat for samme risiko for tab eller tyveri som en fysisk computer.

Kravene gælder ikke pc'er uden adgang til myndighedens interne systemer, der ikke er administreret af myndigheden, og som kun kan opnå adgang til myndighedens internetvendte it-infrastruktur og data via fx virtuelle klienter eller webadgang.

Kravene omfatter pc'er, der kan danne VPN-forbindelse til myndighedens netværk. Fysiske klienter der kun kan opnå adgang til myndighedens interne systemer via virtuelle desktops, Remote Desktop Protocol (RDP) eller lignende, er ikke i sig selv omfattet af kravene.

I det omfang, der i myndigheden anvendes computere til særlige brugssituationer, og der ikke fra disse kan opnås adgang til myndighedens interne systemer, kan disse undtages fra kravene.

Eksempler

Scenarie 2.1A

En styrelse har to computere, som kun er tilsluttet styrelsens gæstenetværk. I det tilfælde er de to enheder ikke omfattet af kravene til klienter, da de ikke har adgang til myndighedens interne systemer.

Scenarie 2.1B

En styrelse tillader deres medarbejdere, at arbejde hjemmefra på medarbejderens private pc via webmail og internetadgang til VDI eller virtualiserede applikationer. Medarbejdernes pc'er kan ikke kobles på styrelsens interne netværk hverken med kabel, trådløst eller via VPN. I dette tilfælde er medarbejdernes pc'er ikke omfattet af kravene til klienter. Bemærk, at webmail og VDI/virtualiserede applikationer er omfattet af kravene om autentifikation og internetvendte tjenester.

For at efterleve kravet om implementering af endpoint-beskyttelse på klienter er det tilstrækkeligt at indføre antivirus med automatisk opdatering.

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.

2.2 Mail

Kravene til mail angår e-mailkommunikationen til og fra myndighedens domæner. Dette gælder også, når en myndighed eksempelvis bruger en ekstern leverandør til at sende mails på vegne af myndigheden, hvor afsenderadressen anvender et af myndighedens domæner. Hvor det derimod fremgår klart og tydeligt, at kommunikationen foregår ved en tredjepart, der ikke kan forveksles med myndigheden, er denne ikke omfattet af kravene til mail. Myndigheden bør dog under alle omstændigheder overveje, hvordan kommunikation via tredjepart foregår mest hensigtsmæssigt med hensyn til sikkerhed og troværdighed for både afsender og modtager.

Eksempler

Scenarie 2.2A

En styrelse benytter sig af en Software-as-a-Service-løsning til at udarbejde og udsende spørgeskemaer til andre myndigheder. Der udsendes en invitation til myndigheder om at besvare styrelsens spørgeskema via mail. Mailen fremsendes ikke fra styrelsens eget maildomæne, men derimod fra spørgeskemaleverandørens. I dette tilfælde er kommunikationen således ikke omfattet af kravene til mail. Styrelsen bør overveje, om det er hensigtsmæssigt, at de ikke selv fremstår som afsender, da modtagere kan opfatte spørgeskemaet som spam eller forsøg på phishing.

Scenarie 2.2B

En styrelse benytter sig af en ekstern leverandør til masseudsendelse af et nyhedsbrev fra styrelsens eget maildomæne. Da styrelsen fremstår som afsender af nyhedsbrevet er kommunikationen omfattet af kravene til mail.

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 i fx AD). Myndighedens brugerkonti defineres som *de interne konti, myndigheden har udstedt til egne ansatte og eventuelle 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 eller 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 eksempel-

vis 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 mobilapplikationer, 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 ansatte, eksterne konsulenter, administratorer, it-systemer og services i centrale brugerdatabaser/autentifikationstjenester, fx AD. For Statens It-kunder vil det blandt andet være B- og X-konti.

Kravet gælder kun for myndighedens egne it-systemer. Kravet omfatter derimod ikke separate passwords til eksterne it-systemer, som myndigheden anvender, fx sociale medier, Software-as-a-Service-løsninger, eller enkeltstående systemer, hvor der anvendes andre login end medarbejdernes hovedkonto, eksempelvis MitID Erhverv.

Eksempler

Scenarie 2.4A

Medarbejderne i en styrelse benytter sig af en tredjepartsløsning til at tilgå oplysninger om myndighedens aktiviteter på sociale medier. I dette tilfælde er myndighedens medarbejdere eksterne brugere af systemet, de logger ikke ind med deres almindelige brugerkonto, der kan give adgang til myndighedens interne systemer. Login til denne løsning er derfor ikke omfattet af kravet til password.

Scenarie 2.4B

En styrelse benytter sig af en cloudleverandør til deres mailløsning. Login til cloudleverandøren er AD-integreret med styrelsens on-premise AD. Passwords til mailløsningen er derfor 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 downloades fra Have I Been Pwned[4], hvilket har den fordel, at myndigheden kan føre kontrol på eget system uden at dele myndighedens anvendte passwords med tredjeparter.[5] Det tillader, at myndigheden kan overveje at supplere listen med en lokal liste over svage passwords eksempelvis ”myndighedensnavn123”.

2.5 Mobile enheder

Kravene til mobile enheder angår medarbejderes samt eventuelle konsulenters 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

---

[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/

[5] Se også Pwned Passwords Downloader: https://github.com/HaveIBeenPwned/PwnedPasswords-Downloader

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.

Der kan være tilfælde, hvor den mobile enhed ikke har adgang til data, fordi den holdes slukket i en længere periode, fx som følge af orlov. I disse tilfælde er kravet ikke gældende, mens telefonen er slukket. Opdateringen skal dog ske umiddelbart efter, at telefonen/enheden igen tændes.
Boks

Eksempler

Scenarie 2.5A

En myndighed stiller et appbaseret system til rådighed, der giver borgere mulighed for at tjekke personlige sundhedsdata over mobilen. I dette tilfælde er der ikke tale om myndighedens data, da systemet udelukkende giver adgang til borgerens egne data, og da kompromittering af login ikke i sig selv kan give adgang til myndighedens interne systemer. Borgernes mobiler er derfor ikke omfattet af kravene til mobile enheder.

Scenarie 2.5B

En medarbejder i et ministerium tager orlov i seks måneder. Som følge heraf slukker vedkommende sin arbejdstelefon i hele perioden. Da vedkommende igen vender tilbage til arbejdspladsen, tænder medarbejderen telefonen og installerer de foreliggende sikkerhedsopdateringer. I denne situation efterleves kravet om sikkerhedsopdateringer af mobile enheder.

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 tjenester og centrale interne it-systemer, der er omfattet af kravet, samt hvilke data der som minimum 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 i forhold til 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 af 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 delegerede subdomæner, samt sikring i forbindelse med myndighedens navneforespørgsler. Det indebærer blandt andet, 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.

Eksempler

Scenarie 2.7A

Styrelsen.dk er Styrelsens domæne og er signeret med en gyldig DNSSEC-signatur. Hjemmesiden lever derfor op til krav 18 om DNSSEC.

Scenarie 2.7B

Www.styrelsen.dk er en DNSSEC-signeret CNAME record, der peger på en leverandørs domæne uden DNSSEC-signering. Da det endelige domænenavn tilhører leverandøren, og ikke myndigheden, lever myndigheden fortsat op til krav 18 om DNSSEC.

DMARC skal være sat op med "p=reject". En record på hoveddomænet vil som udgangspunkt nedarves til alle subdomæner.

SPF skal være sat op med "-all". En *-record på hoveddomænet skal bruges til at beskytte subdomæner mod at blive anvendt til spoofing. For at sikre korrekt funktionalitet, kan det være nødvendigt at oprette specifikke SPF-records på subdomæner, der indgår i mailflow. På hoveddomæner, der ikke indgår i mailflow, oprettes tomme SPF-records, dvs. hvor der ikke angives IP-adresser eller andre domæner ("v=spf1; -all").

DKIM-records skal være sat op med korrekte selektorer og nøgler på alle hoved- og subdomæner, der indgår i mailflow, og tilhørende mailservere sættes op til at DKIM-signere udgående mails. På hoveddomæner, der ikke indgår i mailflow, oprettes tomme DKIM-records, dvs. uden nøgle ("v=DKIM1; p=").

SPF- og DKIM-records bør til enhver tid kun afspejle det aktuelle og anvendte mailflow. Der skal således løbende saniteres i forældede records.

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, it-systemer eller applikationer, som er tilgængelige over internettet. Kravet gælder for alle internettilgængelige tjenester, uagtet om de stilles til rådighed for eksterne slutbrugere eller kun benyttes af myndighedens egne medarbejdere.

Eksempler

Scenarie 2.9A

En styrelse benytter sig af en tredjepartsløsning til hjemmesidesøgning, der indgår som en integreret del af setuppet for et af styrelsens internetvendte hjemmeside. I dette tilfælde er det myndighedens eget ansvar at sikre, at leverandøren af tredjepartsløsningen efterlever kravene for internetvendte tjenester.

Interne systemer, som ikke kan tilgås direkte fra internettet, er ikke omfattet af kravene under denne kategori. 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 blandt andet 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 og lignende, 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. 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. Med myndighedens internettilgængelige IP-adresser menes *public* IP-adresser, som myndigheden har brugsret på, og som kan opnås forbindelse til fra internettet. Cloud- og hosting-udbydere er som udgangspunkt ikke omfattet af kravet, selvom det anbefales, at disse også scannes regelmæssigt.

For opfyldelse af kravet er det tilstrækkeligt at scanne alle porte for TCP, men det tilrådes også at scanne de mest anvendte UDP-porte, selvom det ikke er omfattet af kravet.

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.

Eksempler

Scenarie 2.9B

En styrelse er kunde hos Statens It. Statens It har tildelt styrelsen en række public IP-adresser, der anvendes til et internetvendt system, som blandt andet tilgås af borgere. Da der er tale om Statens Its IP-adresser, er det Statens Its ansvar at scanne disse IP-adresser.

Scenarie 2.9C

En styrelse har selv brugsret over en række IP-adresser, som styrelsen blandt andet benytter til at udstille styrelsens hjemmeside på egne webservere. En række af styrelsens IP-adresser er ikke i brug. Styrelsen skal scanne alle IP-adresser, styrelsen har brugsret over, for at leve op til kravet.

Scenarie 2.9D

En styrelse får driftet sin hjemmeside hos en tredjepartsleverandør på leverandørens egen infrastruktur og på IP-adresser, leverandøren stiller til rådighed. Det er en anbefaling, at styrelsen stiller krav til leverandøren om scanning af IP-adresser, men der er ikke krav herom.

2.10 Interne it-systemer

Kravet angår specifikke interne infrastrukturenheder 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 af 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 i forhold til 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 samt digitale kompetencer kan kontaktes, såfremt der er spørgsmål til fortolkning af kravene.

3.2 Kontrol af udvalgte krav

Til kontrol af udvalgte krav kan myndighederne eventuelt anvende værktøjet sikkerpånettet.dk, der scanner for en række sikringstiltag og standarder 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. 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 2024
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