Tekniske minimumskrav til it-sikkerheden hos statslige myndigheder

Krav	Formål	Følger af	Skal være implementeret den:
Klienter/PCer			
Der skal implementeres firewall på alle klienter.	Firewalls skal sikre mod utilsigtet adgang til arbejdsstationer. Malware forsøger typisk at sprede sig på tværs af systemer, og ved at fjerne denne mulighed kan man begrænse denne spredning. Bør konfigureres så restriktivt som muligt.	Best practice	1. januar 2020
Der skal benyttes en af myndigheden stillet til rådighed VPN-løsning til at gå på internettet via arbejds-PC fra eksterne netværk.	Brug af VPN skal sikre dataintegritet og fortrolighed og bl.a. modvirke man-in-the-middle angreb	CFCS: It-sikkerhed på rejsen	1. januar 2020
Kryptering af harddiske	For at undgå kompromittering af data i forbindelse med tab eller tyveri af pc, skal operativsystemet være sat op til at kryptere harddisken på den enkelte PC.	CFCS: It-sikkerhed på rejsen	1. januar 2020
Der skal implementeres endpoint-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter.	Anvendelse af kontinuerligt opdateret endpoint-beskyttelse sikrer at kendte vira, malware mv. ikke kan afvikles på arbejdsstationen. De fleste endpoint protection-programmer kontrollerer ligeledes for anormal adfærd i applikationer.	CFCS: Reducér risikoen for ransomware	1. januar 2020
Klienter skal patches og opdateres regelmæssigt – både OS og applikationer	Al software der implementeres bør være omfattet af regelmæssig opdatering, således at evt. sårbarheder hurtigst muligt bliver lukket, så systemet ikke kan udnyttes af offentlige tilgængelige exploits.	CFCS/DIGST: Cyberforsvar der virker	1. januar 2020
Administrative rettigheder for brugere tildeles kun tidsbegrænset og med veldokumenterede behov	Størstedelen af malware kræver administrative rettigheder på PCen for at blive installeret. For at hindre risikoen for spredning af malware, skal brugere derfor ikke have administrationsrettigheder med mindre, der er et dokumenteret forretningsmæssigt behov.	CFCS/DIGST: Cyberforsvar der virker	1. juli 2020
Det anvendte operativsystem skal være så nyt som muligt, og skal som minimum være supporteret med sikkerhedsopdateringer	Nyeste operativsystemer har, som udgangspunkt, et højere sikkerhedsniveau end ældre versioner. Operativsystemer som ikke længere supporteres af producenten modtager typisk ikke sikkerhedsopdateringer, når der opdages nye sårbarheder og exploits.	CFCS/DIGST: Cyberforsvar der virker	1. januar 2020
Mail			
Der må kun anvendes af myndigheden godkendte mail-relays med autentifikation	Anvendelse af åbne mail relays kan kompromittere meddelelsessikkerheden. Ved kun at anvende af myndigheden godkendte mail relays med autentifikation øges sikkerheden, og risikoen for misbrug af mail-server til spredning af malware og spam reduceres	Best practice	1. januar 2020
Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2. Mellem statslige myndigheder stilles krav om tvungen (forced) TLS, mens der til øvrige skal sendes TLS, hvis modtager understøtter det.	Kryptering af mailtrafik skal sikre dataintegritet og fortrolighed. Med anvendelse af TLS 1.2 reduceres risikoen for, at mail-kommunikation bliver aflyttet undervejs i transmissionen over internettet.	Datatilsynet: Transmission af personoplysninger via e-mail	1. januar 2020
Webmail må kun anvendes udenfor myndighedens lokale netværk, hvis dette foregår vha 2FA eller via en direkte VPN-forbindelse til myndighedens netværk.	Skal forhindre adgang til myndighedens e-mail ved tilslutning via usikre netværk. Med VPN sikres en direkte og krypteret forbindelse ind i myndighedens eget netværk.	CFCS: It-sikkerhed på rejsen	1. januar 2020

DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden.	DMARC er et valideringssystem designet til at forhindre såkaldt email-spoofing, hvor en afsender udgiver sig for at være en anden. Løsningen giver også en god mitigering mod afsendelse af spam fra myndighedens domæner.	CFCS: Reducer risikoen for falske mails	1. juli 2020
Mobiltelefoner			
Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation	Krav om minimumlængde og anvendelse af numerisk kode eller biometrisk idenfikation frem for andre typer adgangsgodkendelse beskytter telefonen mod misbrug, hvis den tabes/stjæles.	CFCS: Råd om sikkerhed på mobile enheder	1. januar 2020
Operativsystem og apps på mobile enheder skal opdateres regelmæssigt	Mobiltelefoners software skal så vidt muligt opdateres, så snart leverandøren udgiver opdateringer. Derved sikres, at kendte sikkerhedshuller lukkes hurtigst muligt.	CFCS: Råd om sikkerhed på mobile enheder	1. januar 2020
Netværk			
WIFI på myndighedens arbejdsnetværk skal være krypteret med minimum WPA2	Kryptering af WiFi gør det vanskeligere for en angriber, at "aflytte" kommunikation på netværket. WPA2 er sikrere end WPA og bør være standardvalget.	Best practice	1. januar 2020
Krav om logning, log på alle systemer og tjenester på netværksservere	Udgør en forudsætning for opdagelse og efterforskning af forskellige sikkerhedshændelser. Logningen skal ikke anvendes til overvågning af brugeradfærd.	CFCS: Logning - en del af et godt cyberforsvar	1. januar 2020
Websider			
DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden	DNSSEC er en ekstra sikkerhedsservice, man kan tilknytte sit domænenavn. Med DNSSEC kan man være sikker på, at den rigtige side bliver vist, når der bliver linket til ens hjemmeside, og når den direkte URL-adresse bliver brugt. Klienter kan dermed kryptografisk stole på, at de tilgår det rette domæne.	Best practice	1. januar 2020
Myndigheden skal anvende en sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod skadelige hjemmesider	En sikker DNS-tjeneste beskytter brugeren mod malware- og phishingsider ved at blokere for domæner, der er kendt som værende eller vurderes at være farlige.	Best practice	1. januar 2020
Kommunikation til hjemmesider skal krypteres og anvende minimum TLS 1.2, dvs. der skal implementeres https på alle hjemmesider	Kryptering af trafik til og fra hjemmesider skal sikre dataintegritet og fortrolighed, herunder forebygge man-in-the-middle angreb.	Best practice	1. januar 2020
Der må ikke anvendes Flash på hjemmesider tilhørende myndigheden	Flash er et plugin, som tidligere har været bredt anvendt til at tilbyde avanceret eksempelvis grafisk funktionalitet og spil på hjemmesider. Anvendelse af Flash i en web-browser frarådes i forvejen, men udgør fortsat størstedelen af sårbarheder, der anvendes til at kompromittere en computer gennem kørsel af skadelig flash-kode. Flash når end-of-life i 2020 og modtager herefter ikke flere opdateringer.	Best practice	1. juli 2020
Der skal benyttes regelmæssigt opdateret serversoftware på webservere	Al software der implementeres bør være omfattet af regelmæssig opdatering, således evt. sårbarheder hurtigst muligt bliver lukket for offentligt tilgængelige exploits mv.	CFCS/DIGST: Cyberforsvar der virker	1. januar 2020