Anbefalinger om tekniske minimumskrav i kommuner 2023

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Anbefalingerne til tekniske minimumsstandarder er udarbejdet i samarbejde med en række kommuner. Formålet med anbefalingerne er, at det skal være et værktøj, der kan lette opgaven i den enkelte kommune med at vurdere, hvad der er et tilstrækkeligt minimumsniveau for sikkerhed i det tekniske udstyr. Yderligere er formålet med anbefalingerne, at de skal understøtte god beskyttelse af it-udstyr og netværk mod hackerangreb og malware. Og dermed at beskytte medarbejdere og borgeres oplysninger mod at blive kompromitteret eller misbrugt.
Minimumsstandarderne kan ligeledes anvendes til at sammenligne niveauet på egen it-infrastruktur mod et anbefalet minimumsniveau.
Det anbefales, at de tekniske minimumsstandarder forankres i kommunens ansvarlige udvalg for informationssikkerhed.

Om anbefalingerne

Dette dokument indeholder en række anbefalinger til minimumsstandarder for teknisk infrastruktur i kommuner. De tekniske minimumsstandarder for kommuner er udarbejdet i samarbejde med et antal kommuner.
Anbefalingerne er inspireret af, og tager udgangspunkt i, listen over tekniske minimumskrav til statslige myndigheder fra 2020 og er efterfølgende revideret efter opdatering af de statslige tekniske minimumskrav 2023.

Anbefalingerne tager afsæt i vejledninger fra Digitaliseringsstyrelsen, Center for Cybersikkerhed og Datatilsynet eller er udtryk for alment anerkendt best practice. De tekniske minimumsstandarder i kommuner består af en række anbefalinger, som kan give basis for god beskyttelse af kommunens it-infrastruktur og borgernes oplysninger. Anbefalingerne er minimumsstandarder, og kommuner bør således stadig foretage egne risikovurderinger og evt. implementere yderligere sikkerhedstiltag i relevant omfang. Det betyder f.eks. at for nogle kommuner kan det give mening at fravige enkelte af anbefalingerne, hvis man i kommunens tekniske opsætning imødekommer trusler på anden vis, end der er beskrevet i disse anbefalinger. Et eksempel på dette kunne være anbefalingen om at anvende minimum 6 cifre på adgangskode til mobiltelefoner, hvor en kommune påpegede, at nogle medarbejdere havde vagttelefoner, hvis eneste funktion og formål er at kunne modtage alarmopkald. I et sådan tilfælde, hvor der ikke kan tilgås personoplysninger på mobiltelefonen, kan man i kommunen argumentere for at fravige anbefalingen, eftersom den ikke er relevant for omtalte alarmtelefoner.

Hvordan anbefalingerne bruges

Det anbefales, at de tekniske minimumsstandarder forankres i kommunens ansvarlige udvalg for informationssikkerhed. Dette vil i mange kommuner være informationssikkerhedsudvalget, et digitaliseringsudvalg eller eventuelt hos it-chefen i kommunen. Af hensyn til en rettidig implementering anbefales det at fastsætte frister for implementering af de enkelte anbefalinger, som passer ind i kommunens forretnings- og indkøbsstrategi. Hvis kommunen benytter en leverandør eller et system, som gør at kommunen ikke kan leve op til en anbefaling, vil det være nærliggende at fastsætte implementeringsfristen ved

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

kontraktens udløb, så kommunen herefter kan benytte sig af en leverandør, som lever op til den givne anbefaling.
Kommunens tilslutning til anbefalingerne kan med fordel skrives ind i kommunens generelle informationssikkerhedspolitik, hvor andre it- og informationssikkerhedsmæssige retningslinjer ofte fremgår.

Mange kommuner vil allerede leve op til en lang række af anbefalingerne. De færreste kommuner vil dog være i mål med samtlige anbefalinger. Anbefalingerne kan således bruges af kommuner som en sigtelinje for, hvor man i kommunen bør arbejde sig hen inden for en kortere årrække med forbehold for evt. risikobaserede afvigelser fra anbefalingerne.

Selvom de kommunale tekniske minimumsstandarder er anbefalinger og ikke krav, er det vigtigt, at kommuner lever op til et minimum af teknisk sikkerhed, hvad enten man følger niveauet i disse anbefalinger, eller et niveau kommunen selv har fastlagt. Kommuner behandler mange forskellige typer af oplysninger om borgere og også meget følsomme oplysninger. Anbefalingerne vil derfor kunne vise en vej til, hvordan kommunen løbende kan investere i at opgradere it-infrastrukturen med nye sikkerhedsstandarder, så borgerne fortsat kan have tillid til, at kommuner behandler deres oplysninger med de fornødne sikkerhedsforanstaltninger.

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Ændringslog:

Version 1.0: 8. februar 2021

Version 1.1: 8. april 2021
To anbefalinger om Borger PC'er flyttet fra kategori 'Mail' til kategori 'Klienter/PCer'.

Version 2023: 25. oktober 2022
Versioneringen følger Digitaliseringsstyrelsens versionering af Statens tekniske minimumskrav.
Anbefalingerne er blevet nummereret, så de matcher de tilsvarende numre i Statens tekniske minimumskrav. Hvor der er et match med et statsligt krav, står nummeret som Sx og hvor det er en kommunal anbefaling, står nummeret som Kx.

Kategorierne Autentifikation og Logning er tilføjet. Kategorien Mobiltelefoner er erstattet af Mobile enheder og Websider er erstattet af Domæner. Anbefalingerne er grupperet efter de reviderede kategorier.
Krav om flerfaktor-autentificering erstatter tidligere krav 10 om flerfaktor på webmail.
Krav om at der ikke anvendes Flash på hjemmesider tilhørende kommunen er udgået.
Desuden er der sket mindre tekstændringer i uddybningsteksten på K5 og K16.

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Nr.	Klienter/PCer		
	Anbefaling	**Uddybning**	**Følger af**
S1	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
S2	Der skal benyttes en af kommunen stillet til rådighed VPN-løsning eller anden sikkerhedsteknologi, der tilgodeser krav til autentifikation af brugeren og kryptering af data til at tilgå kommunens systemer og ressourcer via arbejds-PC fra eksterne netværk.	Brug af VPN eller anden sikkerhedsteknologi skal sikre dataintegritet og fortrolighed og bl.a. modvirke man-in-the-middle angreb.	CFCS: It-sikkerhed på rejsen
S3	Alle harddiske på til medarbejdere udleverede enheder skal krypteres efter tidssvarende standard.	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 enhed.	CFCS: It-sikkerhed på rejsen
S4	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

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

S5	Klienter skal patches og opdateres regelmæssigt – både OS og applikationer.	Al software, der implementeres, bør være styret af en patch-management plan og omfattet af regelmæssig opdatering. Dette således at evt. sårbarheder hurtigst muligt bliver lukket, så systemet ikke kan udnyttes af offentlige tilgængelige exploits.	CFCS/DIGST: Cyberforsvar der virker
S6	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
S7	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
K1	For borger-PC'er gælder det, at tilslutning af eget udstyr skal blokeres fysisk og ved krav om administratortilladelse.	Her tænkes fx på PC'er, der opstillet på biblioteker eller andre offentlige steder med fri tilgængelighed for borgerne. Formålet er beskyttelse mod keyloggere eller anden skadelig software samt misbrug af kommunens systemer og ressourcer.	Best practice
K2	Der skal opsættes en politik for konfiguration af PC'er uden password (fx borger-PC'er), som tilgodeser brugernes sikkerhed i størst muligt omfang.	Borgere skal kunne være trygge ved at benytte kommunens opstillede PC'er. En fysisk sikret tynd klient, med et sikret OS, hvis virtuelle maskine nulstilles efter hver session, ville være idéelt.	Best practice

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Nr.	Mail		
	Anbefaling	**Uddybning**	**Følger af**
S8	Der må kun anvendes af kommunen godkendte mail-relays med autentifikation. Dette omfatter ikke godkendelse af kontraktuelle eksterne mail-servere.	Anvendelse af åbne mail relays kan kompromittere meddelelsessikkerheden. Ved kun at anvende af kommunen godkendte mail relays med autentifikation øges sikkerheden, og risikoen for misbrug af mail-server til spredning af malware og spam reduceres	Best practice
S9	Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2. Mellem offentlige myndigheder stilles krav om tvungen (forced) TLS ved udgående post, 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

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Nr.	Autentifikation		
	Anbefaling	**Uddybning**	**Følger af**
S10	Autentifikation til kommunens systemer over internettet skal anvende flerfaktor-autentificering	Skal reducere risikoen for, at kompromitterende login oplysninger kan anvendes af andre til at tilgå kommunens systemer og data	
K3	Alle platforme, hvor man logger på med kommunens legitimationsoplysninger (credentials) må kun anvendes udenfor kommunens lokale netværk, hvis dette foregår vha 2FA eller via en krypteret forbindelse (VPN, HTTPS el. tilsvarende) til kommunens netværk.	Skal forhindre adgang til kommunens oplysninger ved tilslutning via usikre netværk. Med VPN sikres en direkte og krypteret forbindelse ind i kommunens eget netværk.	Best practice

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Nr.	Mobile enheder		
	Anbefaling	**Uddybning**	**Følger af**
S11	Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation.	Krav om minimumlængde og anvendelse af numerisk kode eller biometrisk identifikation frem for andre typer adgangsgodkendelse beskytter telefonen mod misbrug, hvis den tabes/stjæles.	CFCS: Råd om sikkerhed på mobile enheder
S12	Der skal benyttes et MDM (Mobile Device Management) system til administration af kommunens mobile enheder.	Mulighed for administration og fjernstyring af kommunens enheder, fx sletning ved tab eller tyveri, men også styring af hvornår en enhed er compliant.	Best practice
S13	Operativsystem og apps på mobile enheder skal opdateres regelmæssigt. Kan enheden – fx pga. alder – ikke opdateres, skal den udskiftes.	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

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Nr.	Logning		
	Anbefaling	**Uddybning**	**Følger af**
S14	Der skal aktivt tages stilling til logning, log på alle systemer og tjenester på netværksservere i henhold til kommunens risikovurdering og best practice på området. Der stilles samme krav til eksterne leverandører.	Udgør en forudsætning for opdagelse og efterforskning af forskellige sikkerhedshændelser. Logningen skal ikke anvendes til overvågning af bruger-adfærd.	CFCS: Logning - en del af et godt cyberforsvar

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

	Domæner		
	Anbefaling	**Uddybning**	**Følger af**
S15	DNSSEC skal tilknyttes alle domænenavne tilhørende kommunen.	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 og CFCS: Sikker håndtering af domæner
S16	Kommunen 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 baseret på en automatisk vedligeholdt negativ liste.	Best practice
S17	DMARC REJECT policy implementeres på alle domæner tilhørende kommunen.	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 kommunens domæner.	CFCS: Reducer ri-sikoen for falske mails
K4	Indgående mailgateways skal respektere afsenders DMARC politik.	Skal sikre at egne brugere beskyttes mod forfalskede mails.	Best practice
K5	Indgående mailgateways skal være i en DNSSEC-beskyttet zone.	Skal sikre at DNSSEC-beskyttelse af egne domæner, ikke omgås ved anvendelse af trejde-parts mailgateways i andre domæner.	Best practice

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Nr.	Netværk		
	Anbefaling	**Uddybning**	**Følger af**
S18	WIFI på kommunens 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. Det kan med fordel yderligere tilstræbes, at alle enheder tilgår netværket med 802.1x.	Best practice
S19	Der skal benyttes regelmæssigt opdateret serversoftware på web- og andre servere.	Al software der implementeres bør være omfattet af regelmæssig opdatering, således evt. sårbarheder hurtigst muligt bliver lukket for offentligt tilgængelige exploits mv. Det er sværere at definere for Open Source operativsystemer, hvilket evt. kan løses ved en positivliste over godkendt software.	CFCS/DIGST: Cyberforsvar der virker
S20	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 og CFCS: Sikker brug af TLS
K6	Al netværksadgang skal være behørigt segmenteret.	Der skal være særligt fokus på kabelstik, som offentligheden har adgang til, fx i åbne rådhuse, på skoler og institutioner. Det kan med fordel yderligere tilstræbes, at alle enheder tilgår netværket med 802.1x.	Best practice

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Nr.	Diverse		
	Anbefaling	**Uddybning**	**Følger af**
K7	Der skal være adgangskontrol for fysisk adgang til rum med følsomme oplysninger eller udstyr såsom servere, netværksudstyr, der håndterer intern trafik mv.	Døre skal være aflåst for uvedkommende, hvor det har relevans. Der kan findes inspiration til sikring i standarden "EN/ISO 17065"	ISO 27001
K8	Ekstern adgang til eksempelvis konsulenter skal tildeles tidsbegrænset og kun til og med opgavens ophør. Den eksterne adgang skal kun inkludere adgang til relevante systemer/services ift. den konkrete opgaveløsning.	Eksterne brugere skal benytte multifaktor autentifikation hvor muligt og kun have tidsbegrænset adgang til det nødvendige.	Best practice
K9	Passwords skal udformes, opdateres og opbevares i overensstemmelse med CFCS anbefalinger.	At medarbejdere ikke benytter usikre kodeord og at brugeroplysninger ikke kan tilgås af utilsigtede.	CFCS: Vejledning i passwordsikkerhed
K10	Videokameraer skal være beskyttet med ikke-default password og skal være koblet på et sikkert netværk med adgangsbegrænsning.	Adgang til optagelser skal være velafgrænset. Der skal defineres bruger/password på videokameraer samt optagelser. Det skal tilstræbes at forhindre mulighed for fysisk manipulation af kameraerne. Fysisk placering af eventuelle visningsskærme skal overvejes med henblik på, hvem der kan se dem.	Best practice
K11	Internet-of-Things enheder skal være beskyttet med ikke-default password og skal være koblet på et behørigt segmenteret netværk.	IoT-enheder har potentiale til at være en stor sikkerhedsrisiko, der kan agere springbræt for et angreb på kommunens netværk, systemer og ressourcer. Behørig segmentering er et vigtigt element for at beskytte ressourcer.	Best practice

Dato: 31. oktober 2022

E-mail: JELA@kl.dk
Direkte: 3370 3227

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

K12	Der skal tages backup af vigtige data og systemkonfigurationer.	Sikrer at data og systemer kan genskabes ved utilsigtet sletning eller ændring. Bør ske i henhold til en godkendt backuppolitik, testes regelmæssigt, og beskyttes mod manipulation af eksempelvis ransomwareaktører.	Best practice
K13	Hjemmesider bør sikres mod angrebsteknikker i OWASP Top 10.	Sikrer mod kompromittering via oftest anvendte angrebsteknikker.	https://owasp.org/www-project-top-ten/
K14	Alle hjemmesider bør anvende sikre HTTP headers.	X-Frame-Options kan beskytte mod "click-jacking". X-Content-Type-Option nosniff kan beskytte mod "MIME confusion attacks". Content-Security-Policy kan beskytte mod "cross-site scripting (XSS)".	Best practice
K15	Alle hjemmesider skal implementere en HSTS header.	Beskytter mod MITM angreb, ved at sikre at brugere kun tilgår HTTPS-beskyttede hjemmesider med HTTPS, uden at forlade sig på redirection fra HTTP der kan kompromitteres.	Best practice