DATATILSYNET

Fredericia Kommune
Gothersgade 20
7000 Fredericia
Danmark

Sendt med Digital Post

20. december 2022

J.nr. 2022-423-0314
Dok.nr. 546320
Sagsbehandler
Marie Louise Buch-Lassen

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Skriftligt tilsyn med Fredericia Kommunes modenhed på databeskyttelsesområdet 2022

1. Datatilsynets tilsyn

Datatilsynet fører tilsyn med enhver behandling af oplysninger, der er omfattet af databeskyttelsesforordningen, databeskyttelsesloven og anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, jf. databeskyttelseslovens § 27, stk. 1.

Som led i Datatilsynets løbende tilsynsvirksomhed, der bl.a. udøves gennem stikprøvekontrol, blev Fredericia Kommune den 30. august 2022 varslet om, at Fredericia Kommune var blevet udvalgt til planlagt tilsyn i henhold til databeskyttelseslovens § 29, stk. 1.

Tilsynet blev gennemført som et skriftligt tilsyn i form af en række spørgsmål (også kaldet "Tilsyn med organisationers modenhed på databeskyttelsesområdet 2022"), som også blev sendt til en række andre dataansvarlige (kommuner og regioner). Der er blevet gennemført i alt 55 skriftlige tilsyn.

Tilsynene har baggrund i Datatilsynets strategi om en mere data- og risikobaseret tilgang til vejledning og kontrol (https://www.datatilsynet.dk/Media/C/A/Tilsyn%20med%20effekt_data_og_risikobaseret_indsats.pdf). Formålet med tilsynene er bl.a., at Datatilsynet skal kunne foretage en overordnet vurdering af forskellige organisationers modenhed i forhold til databeskyttelse. Tilsynene tager udgangspunkt i en sammenligning af besvarelserne på tværs af ensartede dataansvarlige.

2. Datatilsynets bemærkninger

Datatilsynet har nu modtaget og behandlet de oplysninger, som Fredericia Kommune har givet Datatilsynet ved det skriftlige tilsyn.

Brevet her og den vedlagte rapport med bilag udgør Datatilsynets samlede tilbagemelding på besvarelsen af spørgsmålene og dermed på det skriftlige tilsyn.

Rapporten med bilag indeholder grafer, der illustrerer centrale tal fra tilsynets modenhedsanalyse vedrørende Fredericia Kommune og tilsvarende organisationer. I rapporten er benchmarking udført på den måde, at der sammenlignes på tværs af besvarelser fra lignende organisationer (kommuner over for kommuner og regioner over for regioner). Hensigten er at give Fre-

dericia Kommune mulighed for at vurdere eget modenhedsniveau i forhold til det gennemsnitlige modenhedsniveau for sammenlignelige organisationer.

Særligt om anbefalingerne

Rapporten indeholder ligeledes en række konkrete anbefalinger, som Datatilsynet, bl.a. på baggrund af besvarelsen, vurderer er særligt relevante for det videre arbejde med persondatasikkerhed i jeres organisation. Anbefalingerne er valgt ud fra en samlet, overordnet vurdering af jeres besvarelse, og der kan godt være flere områder, som organisationen med fordel kan arbejde yderligere med, selv om der ikke er vedlagt konkrete anbefalinger herom.

Det kan forekomme, at Datatilsynet har givet jeres organisation en eller flere anbefalinger vedrørende et emne, hvor Datatilsynet kan se ud fra besvarelsen, at jeres organisation allerede har beskrevet det påtænkte videre arbejde i fritekstfeltet. Datatilsynet har valgt alligevel at give den konkrete anbefaling som en bekræftelse på, at det er noget, jeres organisation bør arbejde videre med.

I den forbindelse vil Datatilsynet gerne tilbyde alle organisationer, der har været omfattet af tilsynet, to direkte kontaktpunkter (it-sikkerhedskonsulenter) i Datatilsynet, som kan kontaktes for råd og vejledning i forhold til at komme videre med de enkelte emner og anbefalinger. I finder navn og direkte nummer på it-sikkerhedskonsulenterne sidst i dette brev.

Det har været Datatilsynets ønske at give konkret og individuel vejledning i videst muligt omfang og så tæt på organisationernes arbejde med besvarelserne, som det har været muligt. På den måde vil det være muligt at arbejde videre internt i organisationen med drøftelser om, hvorvidt der bør indføres yderligere eller nye foranstaltninger for at nedbringe risici i forhold til de konkrete emner.

Særligt om tilbagemeldingen vedrørende de 20 tekniske minimumskrav

Spørgsmålene 14.1-14.20 har baggrund i de 20 tekniske minimumskrav til it-sikkerheden i statslige myndigheder, der som led i den nationale strategi for cyber- og informationssikkerhed 2022-2024 nu er blevet opdaterede, og som skal være implementeret af alle statslige myndigheder senest den 1. januar 2023.

De 20 tekniske minimumskrav har dannet grundlag for spørgsmålene, fordi kravene handler om generelle tekniske og organisatoriske foranstaltninger imod cyberangreb. Disse cyberangreb udgør ofte en trussel mod persondatasikkerheden, og flere af foranstaltningerne har længe været anbefalet generelt – ikke kun overfor statslige myndigheder.

Selv om kravene i udgangspunktet er rettet mod statslige myndigheder, har Datatilsynet valgt alligevel at lade dem indgå i spørgsmålene, fordi kravene må anses for at være udtryk for en form for *best practice*, og fordi flere af kravene allerede følger af eksisterende vejledninger, anbefalinger og praksis på området fra både Center for Cybersikkerhed, Digitaliseringsstyrelsen og Datatilsynet.

3. Afsluttende bemærkninger

Datatilsynet anser hermed det skriftlige tilsyn med Fredericia Kommune for afsluttet.

Det bemærkes imidlertid, at Datatilsynet i nogle tilfælde vil anmode om dokumentation, stille yderligere spørgsmål, iværksætte stikprøvekontrol, og/eller varsle opfølgende skriftlige eller fysiske tilsynsbesøg som opfølgning på denne besvarelse.

Det bemærkes også, at Datatilsynet – typisk hvis der måtte fremkomme nye oplysninger eller klager vedrørende Fredericia Kommune, eller hvis der modtages nye anmeldelser om brud på persondatasikkerheden – vil kunne lade oplysningerne i nærværende tilsynssag indgå i sagsbehandlingen, ligesom besvarelserne vil indgå i grundlaget for udarbejdelsen af Datatilsynets tilsynsplaner.

Sagen er imidlertid for indeværende at betragte som afsluttet.

Såfremt Datatilsynet måtte modtage anmodninger om aktindsigt i vedlagte materiale eller i tilsynssagen i øvrigt, vil Datatilsynet indhente en udtalelse fra jeres organisation. Dette særligt med henblik på at få belyst risikoen for, hvorvidt en udlevering af oplysningerne, herunder også oplysning om, hvilke anbefalinger, jeres organisation har modtaget, vil kunne kompromittere sikkerheden i jeres organisation.

Hvis ovenstående giver anledning til generelle spørgsmål, er Fredericia Kommune velkommen til at kontakte undertegnede telefonisk på 29 49 33 03.

Hvis ovenstående giver anledning til særlige spørgsmål vedrørende it-sikkerhedsretlige emner eller til anbefalingernes indhold, er jeres organisation også velkommen til at kontakte enten it-sikkerhedskonsulent, Anders Chemnitz, på telefon 29 49 33 09 eller it-sikkerhedskonsulent, Walther Starup-Jensen, på telefon 29 49 32 66.

Med venlig hilsen

Marie Buch-Lassen

Vedlagt: Rapport: ”*Tilsyn med organisationers modenhed på databeskyttelsesområdet 2022*” + bilag

Tilsyn med organisationers modenhed på databeskyttelsesområdet 2022

Fredericia Kommune

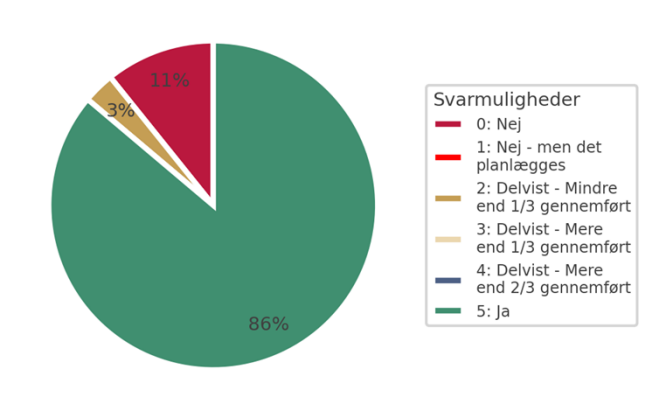
2022

DATATILSYNET

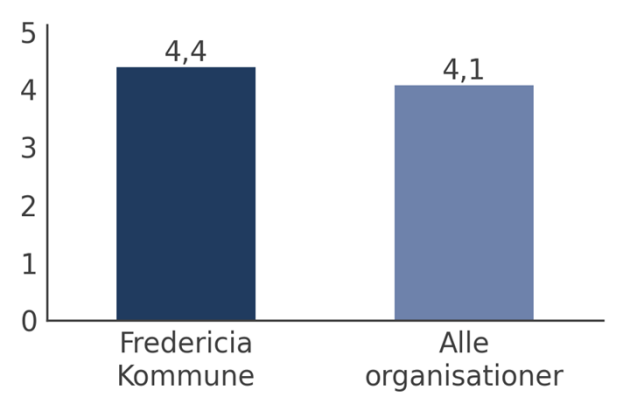
Fredericia Kommune

I det følgende afsnit finder du centrale tal fra Datatilsynets tilsyn med Fredericia Kommunes og tilsvarende organisationers modenhed på databeskyttelsesområdet – med særlig fokus på behandlingssikkerhed.

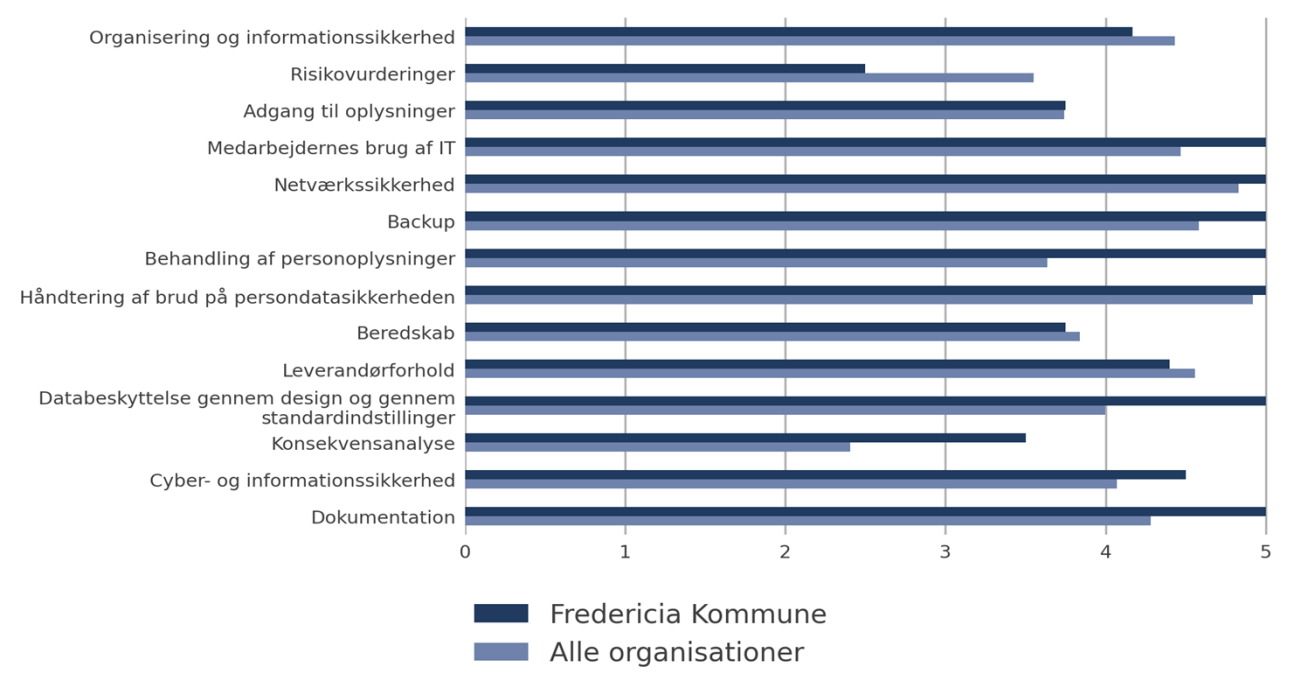
50 organisationer har været omfattet af tilsynet og besvaret 73 spørgsmål, og svarene herfra udgør datagrundlaget for de fremhævede resultater i denne rapport. De fremhævede svar er alle besvaret ud fra en svarskala fra 0-5, som er gengivet herunder. Når der nedenfor henvises til 'gennemsnit for tilsvarende organisationer', henvises der således til gennemsnittet af svarerne fra de 50 organisationer.



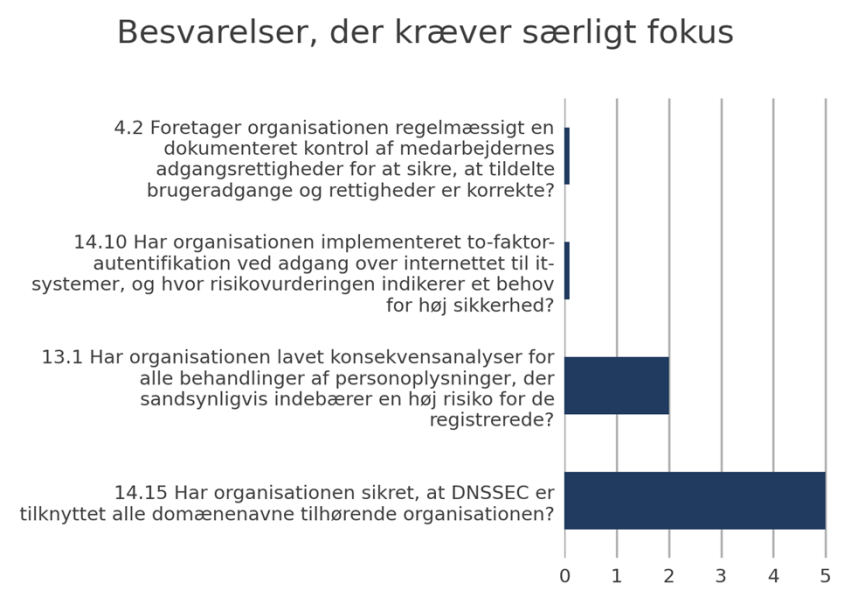
Figur 1 viser Fredericia Kommunes svar fordelt på svarmulighederne.



Figur 2 viser Fredericia Kommunes svargennemsnit sammenholdt med svargennemsnittet for tilsvarende organisation.



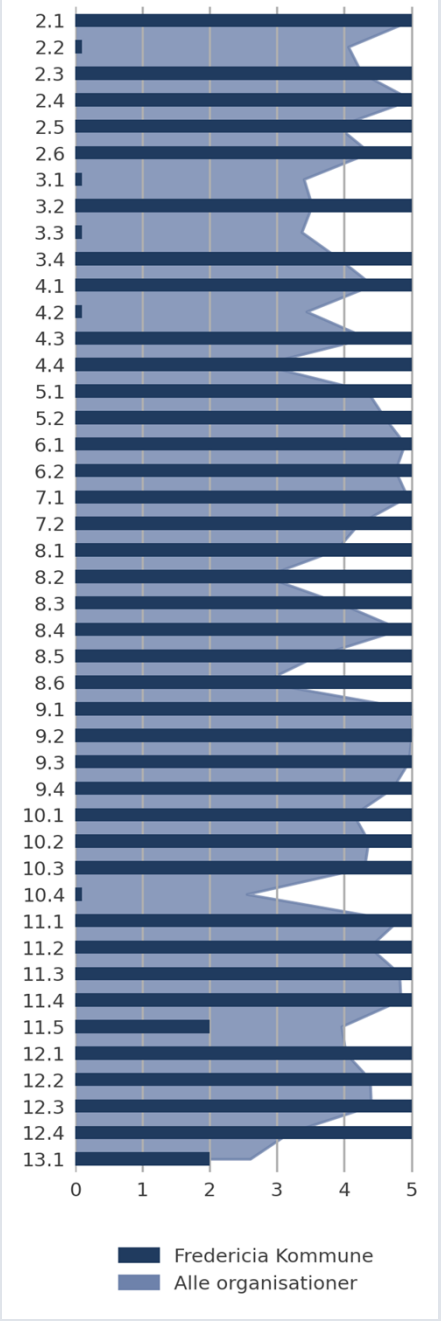
Figur 3 viser Fredericia Kommunes svargennemsnit på 14 udvalgte sikkerhedsområder sammenlignet med svargennemsnittet for tilsvarende organisationer.



Figur 4 viser de svar, hvor Fredericia Kommune enten har den laveste svarscore inden for egen besvarelse, eller hvor der på trods af en ellers høj svarscore alligevel har været anledning til at komme med en anbefaling ud fra en samlet vurdering af besvarelsen.

Datatilsynet har på baggrund af besvarelsen følgende 4 anbefalinger:

- 4.2 — Periodisk kontrol af adgangsrettigheder
- 13.1-13.3 — Konsekvensanalyser
- 14.10 — Flerfaktorautentifikation
- 14.15 - 14.17 — Domænesikkerhed



Figur 5 viser Fredericia Kommunes svar sammenlignet med svargennemsnittet for tilsvarende organisationer.

Anbefalingerne kan ses i fuld længde i rapportens bilag.

DATATILSYNET

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

20. december 2022

J.nr. 2022-423-0314
Dok.nr. 545274
MLB

Anbefalinger til Fredericia Kommune

4.2 Periodisk kontrol af adgangsrettigheder

For at undgå utilsigtede adgange til personoplysninger, bør jeres organisation have fokus på styring af brugeres adgangsrettigheder. Fejl i rettighedsstyring kan f.eks. opstå via brugerfejl (f.eks. kopiering af eksisterende adgangsrettigheder ved nyoprettelse) og pga. manglende handling, (f.eks. manglende opdatering af rettigheder ved ændringer i organisationen).
En kontrol kan omfatte én eller flere af følgende undersøgelser:

- Om de faktisk etablerede adgange er omfattet af en gældende autorisation
- Om adgange skulle være lukket tidligere grundet en tidsbegrænset/udløbet autorisation, fratrædelse, orlov eller andet
- Om autorisationerne er aktuelle – altså om alle godkendelser af adgange er nødvendige og bunder i et arbejdsbetinget behov
- Om der er er adgange, som ikke længere benyttes af den retmæssige bruger ("ghost accounts"), som burde være lukket

Datatilsynet har tidligere udtalt, at det er Datatilsynets opfattelse, at kravet om passende sikkerhed i databeskyttelsesforordningens artikel 32, stk. 1, normalt vil indebære, at den dataansvarlige løbende kontrollerer, om adgangsrettigheder til it-systemer er begrænset til de personoplysninger, som er nødvendige og relevante for den pågældende brugers arbejdsbetingede behov.

Det skyldes, at uanset hvor stringent organisationen styrer adgangsrettighederne, kan det gå galt mange steder i en sådan proces, der ofte involverer mange mennesker, og der vil derfor med al sandsynlighed være fejl, som kun opdages ved periodiske kontroller. Datatilsynet har en vejledning om rettighedsstyring på vej. Følg med på www.datatilsynet.dk
Se f.eks. praksis her

www.datatilsynet.dk:

https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jan/tilsyn-med-koege-kommunes-rettighedsstyring-i-aula

https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jan/tilsyn-med-gentofte-kommunes-rettighedsstyring-i-afdelings-og-funktionspostkasser

Se f.eks. en politianmeldelse:

https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/sep/region-midtjylland-indstillet-til-boede

13.1-13.3 Konsekvensanalyser

Kommuner og regioner er dataansvarlige for en række behandlingsaktiviteter, hvor der potentielt kan være en høj risiko for de registrerede. Den type af behandlingsaktiviteter kan give anledning til, at der skal udarbejdes en konsekvensanalyse for de registreredes rettigheder.
Det ser ud til, at der generelt arbejdes med de risikovurderinger i organisationerne, som forudsættes efter databeskyttelsesforordningens artikel 32, men samtidig er der indikationer på, at mange organisationer ikke er nået lige så langt i arbejdet med konsekvensanalyser efter databeskyttelsesforordningens artikel 36. Det kan betyde, at der sker behandlinger, hvor risikoen for de registrerede ikke er tilstrækkeligt adresseret.
Rådet for digital sikkerhed har udgivet en vejledning, der beskriver, hvordan arbejdet med at udføre konsekvensanalyser kan udføres. RfDS-vejledning-om-konsekvensanalyse-final-offentliggjort.pdf (digitalsikkerhed.dk)

14.10 Flerfaktorautentifikation (MFA)

For at undgå uautoriseret adgang til personoplysninger og angreb, som f.eks. ransomware-angreb, skal login, som er tilgængeligt fra internettet, (eventuelt også interne login) være styrket med flerfaktorautentifikation.
Det er desværre relativt udbredt, at medarbejdere genbruger passwords flere steder, herunder også det password, som medarbejderne bruger til at logge på arbejdskontoen. Derfor kan et login, der kun er baseret på dette password, være sårbart.
En velvalgt, yderligere login-faktor kan sænke sandsynligheden for misbrug betydeligt.
I Center for Cybersikkerheds vejledning om passwords gives der gode råd til implementering af effektiv flerfaktorautentifikation. -vejledning-passwordsikkerhed-2020.pdf (cfcs.dk)
Se f.eks. praksis her

www.datatilsynet.dk:

https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jun/datatilsynet-har-udtalt-alvorlig-kritik-af-at-designbysi-ikke-har-levet-op-til-kravet-om-fornoedne-sikkerhedsforanstaltninger-i-gdpr

https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-udtaler-kritik-og-giver-to-paabud-til-eg-digital-welfare-aps

14.15-14.17 Domænesikkerhed

For at undgå, at organisationens hjemmesider eller mailadresser bliver brugt til it-kriminalitet, er der nogle anbefalinger, som jeres organisation kan følge:

- Skab overblik over alle de domæner, som din organisation råder over. Det er en udbredt misforståelse, at domænesikkerhed kun er nødvendigt for ”hoved-domænet”.
- Implementér en procedure, der sikrer, at alle fremtidige indkøb af domæner godkendes og indstilles med den ønskede domænesikkerhed.
- Sørg for, at DNSSEC aktiveres for alle organisationens domæner. Derved reduceres sandsynligheden for, at organisationens domæner kan misbruges, f.eks. til angreb hvor it-kriminelle forsøger at stjæle brugernavne og adgangskoder. Se yderligere forklaring på f.eks. https://www.dk-hostmaster.dk/da/dnssec.
- Sæt DMARC op på alle organisationens domæner. Den største sikkerhed opnås ved at sætte DMARC til REJECT. I den forbindelse er det vigtigt, at organisationens SPF og DKIM record er sat korrekt op, og at SPF record indstilles, så den fortæller, hvis et givent domæne slet ikke sender mails. Korrekt opsætning kan reducere sandsynligheden for, at organisationens mailadresser eller domæner misbruges til f.eks. phishing. Derudover styrker det også legitimiteten af de mails, der sendes fra organisationens domæner. Se yderligere forklaring på f.eks. https://www.dk-hostmaster.dk/da/dmarc.

DATATILSYNET

20. december 2022

J.nr. 2022-423-0314
Dok.nr. 544855
GWA

De 20 minimumskrav til statslige myndigheder – basal informationssikkerhed i en digital forvaltning

1. Introduktion til bilaget

Spørgsmålene 14.1-14.20 i årets Tilsyn med organisationers modenhed har baggrund i de 20 tekniske minimumskrav til it-sikkerheden i statslige myndigheder, der som led i den nationale strategi for cyber- og informationssikkerhed 2022-2024 nu er blevet opdaterede, og som skal være implementeret af alle statslige myndigheder senest den 1. januar 2023.

De 20 tekniske minimumskrav har dannet grundlag for spørgsmålene, fordi kravene handler om generelle tekniske og organisatoriske foranstaltninger imod cybertrusler og i vidt omfang overlapper med tilsvarende krav til persondatasikkerheden. Flere af disse foranstaltninger har længe været anbefalet generelt – ikke kun overfor statslige myndigheder. Rigsrevisionen skriver bl.a. i sin beretning af 2021 om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden[1]:

”*De 20 tekniske minimumskrav skal beskytte statslige arbejdspladser mod ondsindede cyber- og informationssikkerhedshændelser. Cybertruslen mod statslige myndigheder vokser i takt med den øgede digitalisering af samfundet. Dette afspejles også i Center for Cybersikkerheds trusselsvurderinger.*

Opgaven med at efterleve de 20 tekniske minimumskrav til it-sikkerheden er særlig vigtig hos myndigheder, der varetager samfundsvigtige opgaver eller håndterer følsomme oplysninger om fx borgere. Det skyldes, at efterlevelse af minimumskravene er med til at give en basal it-sikkerhed, der bidrager til at beskytte de oplysninger og data, som myndighederne er ansvarlige for”.

Spørgsmålene er besvaret med Ja/Nej, fordi delvis implementering normalt ikke hjælper meget på sikkerheden. Når det drejer sig om cyber- og informationssikkerhed, er det ofte ”det svageste led, der bestemmer styrken af kæden”. Hvis en ondsindet person først er kommet forbi et "lag i sikkerheden", fx en brugers pc, og næste angrebspunkt er det interne netværk, så hjælper det ikke, at alle andre brugeres pc'er var bedre beskyttet.

1 Beretning om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden (rigsrevisionen.dk)

Sammenligningsgrundlag: 'Tilsvarende organisationer' er samtlige kommuner omfattet af Tilsyn med organisationers modenhed 2022.

Tabel 1 Oversigt over organisationens svar samt procentangivelse for JA-svar for samtlige tilsvarende organisationer omfattet af Tilsyn med organisationers modenhed 2022

SPØRGSMÅL	PROCENT JA-SVAR	ORGANISATIONENS SVAR
14.1 Har organisationen en firewall på alle klienter?	86%	Ja
14.2 Har organisationen på samtlige klienter gennemtvunget anvendelsen af Always On VPN fra eksterne netværk.	56%	Ja
14.3 Har organisationen forhindret, at brugere af bærbare computere (herunder smartphones) uforvarende kan lagre personoplysninger lokalt på enheden, eller er der alternativt implementeret kryptering af harddiske og/eller filsystemer på samtlige computere, hvor det er muligt for brugeren at lagre lokalt?	80%	Ja
14.4 Har organisationen implementeret end-point-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter?	100%	Ja
14.5 Har organisationen etableret en proces, der sikrer, at alle klienters operativsystemer og applikationer holdes sikkerhedsmæssigt opdateret?	96%	Ja
14.6 Har organisationen sikret, at almindelige brugerkonti ikke tildeles administrative rettigheder til klienter? Hvis enheden er en smartphone, er der enten samme begrænsning, eller behandlingen af personoplysninger i særlige apps er effektivt beskyttet imod indflydelse fra andre apps på samme enhed.	84%	Ja
14.7 Har organisationen sikret, at alle pc'er anvender nyeste operativsystem?	82%	Ja
14.8 Har organisationen sikret, at der kun anvendes godkendte mail-relays med autentifikation?	88%	Ja
14.9 Har organisationen sikret, at forsendelse af e-mail sendt via internettet eller andre netværk, som	90 %	Ja

SPØRGSMÅL	PROCENT JA-SVAR	ORGANISATIONENS SVAR
ikke er under den dataansvarliges kontrol, altid sker krypteret minimum med TLS 1.2?		
14.10 Har organisationen implementeret to-faktor-autentifikation ved adgang over internettet til it-systemer, og hvor risikovurderingen indikerer et behov for høj sikkerhed?	64 %	Nej
14.11 Har organisationen en skriftlig politik for valg af adgangskoder? For mobiltelefoner og lignende er der krav om numerisk adgangskode på min. 6 cifre eller biometrisk identifikation.	78 %	Nej
14.12 Har organisationen implementeret MDM (Mobile Device Management) på alle mobile enheder?	78%	Ja
14.13 Har organisationen sikret, at operativsystemer og apps på mobile enheder så vidt muligt er opdateret, så snart leverandøren udgiver opdateringer?	78%	Ja
14.14 Har organisationen sikret en logning fra alle it-systemer og tjenester på netværksservere, som gør det muligt at opdage og efterforske sikkerhedshændelser, samt sikret at denne log opbevares længe nok?	57 %	Ja
14.15 Har organisationen sikret, at DNSSEC er tilknyttet alle domænenavne tilhørende organisationen?	60%	Ja
14.16 Anvender organisationen en Sikker DNS-tjeneste eller anden løsning, som beskytter organisationens brugere mod kendte skadelige websteder?	88 %	Ja
14.17 Har organisationen implementeret DMARC REJECT-policy på alle domæner tilhørende organisationen?	70 %	Ja
14.18 Har organisationen sikret, at all Wi-Fi på organisationens arbejdsnetværk er krypteret med minimum WPA2?	100 %	Ja
14.19 Har organisationen sikret, at alle eksterne webservere så vidt muligt er opdaterede, så snart producenten udgiver opdateringer?	80 %	Ja
14.20 Krypterer organisationen al kommunikation til organisationens tjenester, hvor data transmitteres via internettet og andre netværk, som ikke er under den	88%	Ja

SPØRGSMÅL	PROCENT JA-SVAR	ORGANISATIO-NENS SVAR
dataansvarliges kontrol, og denne kryptering er altid TLS 1.2 eller bedre?		