Tilsyn med kommuners modenhed i forhold til grundlæggende behandlingssikkerhed

Ishøj Kommune

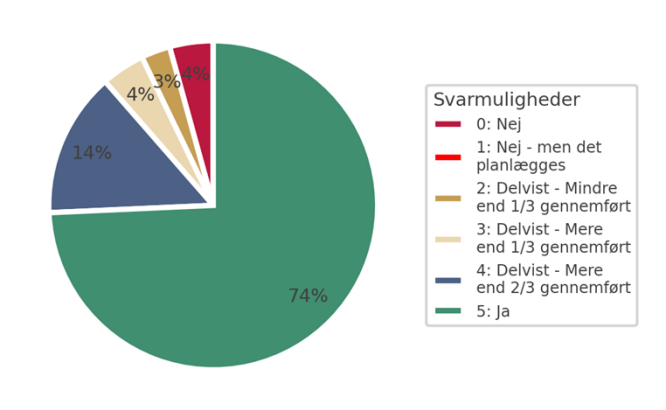
2024

DATATILSYNET

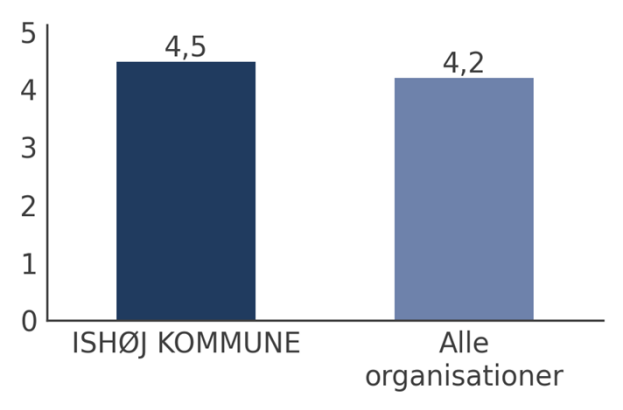
Ishøj Kommune

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

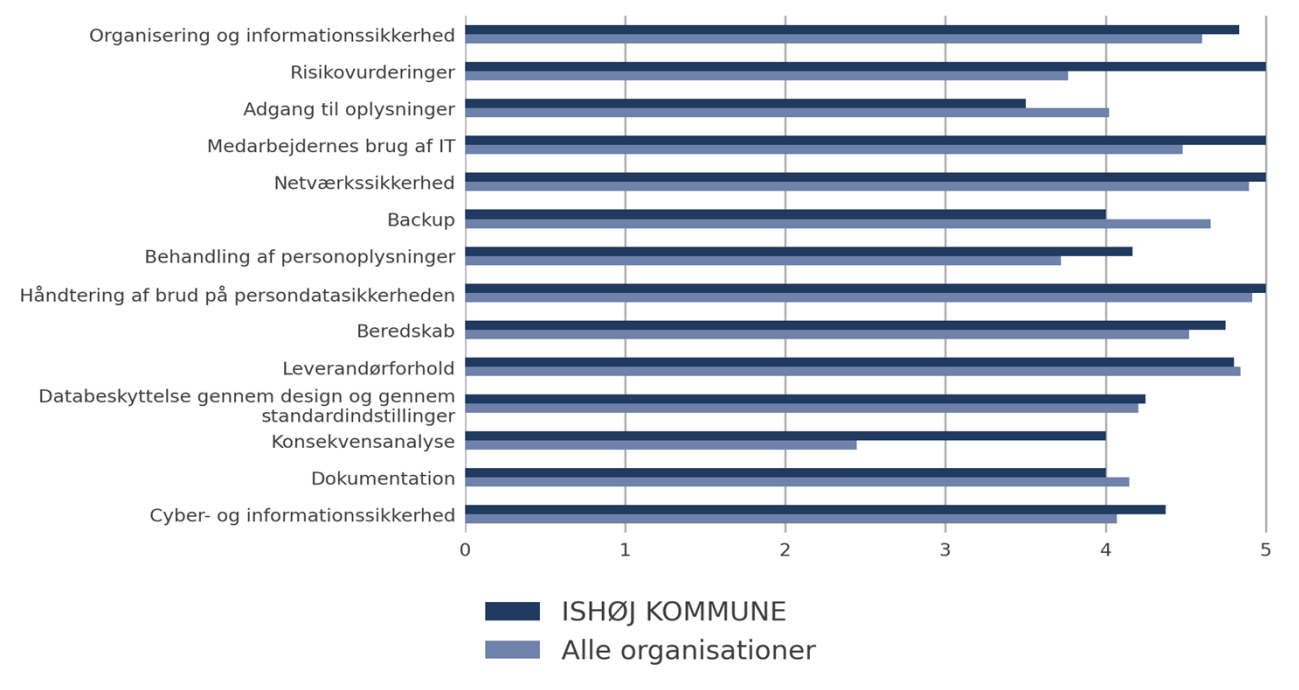
48 kommuner har været omfattet af tilsynet og besvaret 77 spørgsmål, og svarene herfra udgør datagrundlaget for de fremhævede resultater i denne rapport. De fremhævede svar er alle besvaret ud fra en svarskala fra 0-5, som er gengivet herunder. Når der nedenfor henvises til 'gennemsnit for tilsvarende organisationer', henvises der således til gennemsnittet af besvarelserne fra de 48 kommuner.



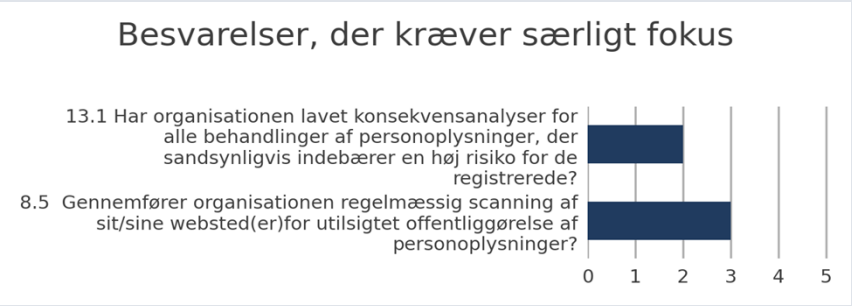
Figur 1 viser Ishøj Kommunes svar fordelt på svarmulighederne.



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



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

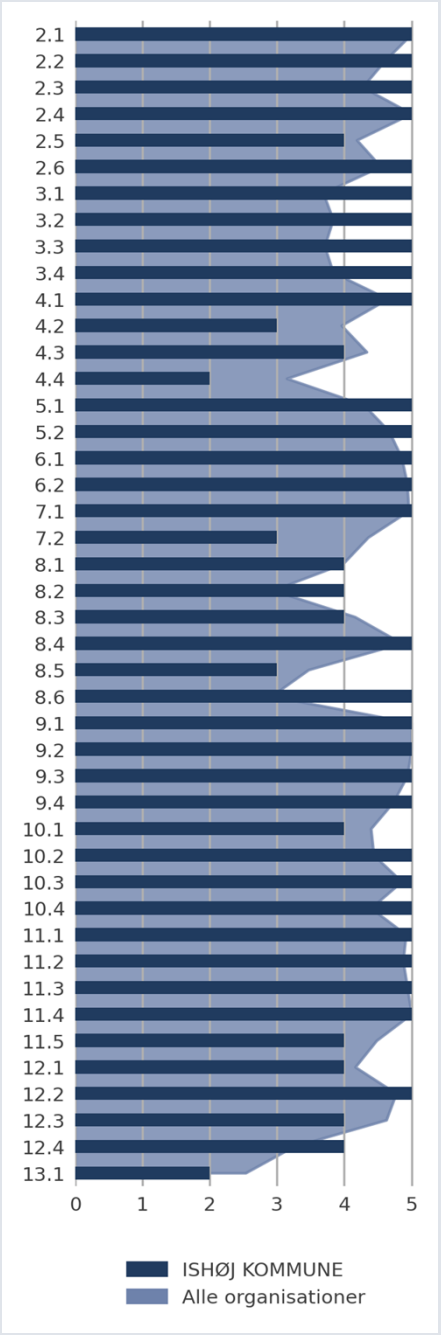


Figur 4 viser de svar, hvor Ishøj Kommune har den laveste svarscore sammenholdt med egne svar.

Datatilsynet har på baggrund af besvarelsen følgende 2 anbefalinger:

Se bilag

- Scanning af web
- Konsekvensanalyser (dækker 13.1-13.3)



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

DATATILSYNET

Se anbefalingerne i deres fulde længde i det vedlagte anbefalingsbilag.

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

Samlet oversigt over anbefalinger inden for grundlæggende behandlingssikkerhed

4.2. Periodisk kontrol af adgangsrettigheder
Læs om foranstaltningen "Periodisk kontrol af adgangsrettigheders aktualitet (datatilsynet.dk)" i Datatilsynets katalog over sikkerhedsforanstaltninger, som også henviser til Datatilsynets praksis på området.

Læs generelt om rettighedsstyring i vejledningen "Styr på rettighedsstyring (datatilsynet.dk)"

8.5-8.6 Scanning af web og e-mail
Læs om foranstaltningen "Styret og overvåget offentliggørelse af data (datatilsynet.dk)" i Datatilsynets katalog over sikkerhedsforanstaltninger, som også henviser til Datatilsynets praksis på området.

Læs også om "brud nr. 3 (datatilsynet.dk)" i Datatilsynets vejledende tekst om 10 typiske brud på persondatasikkerheden, som blandt andet omhandler fejl, der opstår, når data offentliggøres på en webside eller sendes med e-mail. Der henvises også til Datatilsynets praksis på området.

Se endvidere Datatilsynets vejledende tekst om "Kommuners offentliggørelse af oplysninger mv. i offentligt tilgængelige webarkiver (datatilsynet.dk)"

13.1-13.3 Konsekvensanalyser
Kommuner 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 kommunerne, som forudsættes efter databeskyttelsesforordningens artikel 32, men samtidig er der indikationer på, at mange kommuner ikke er nået lige så langt i arbejdet med konsekvensanalyser efter databeskyttelsesforordningens artikel 36. Det kan bl.a. betyde, at der sker behandlinger, hvor risikoen for de registrerede ikke er tilstrækkeligt adresseret.

På Datatilsynets hjemmeside er der forskelligt materiale om konsekvensanalyser, herunder vejledninger og skabeloner til gennemførelse af konsekvensanalyser. Materialet findes her Vejledningsmateriale om konsekvensanalyse (datatilsynet.dk)

14.10 Flerfaktorautentifikation (MFA)
Læs om foranstaltningen "Flerfaktor autentifikation (MFA) (datatilsynet.dk)" i Datatilsynets katalog over sikkerhedsforanstaltninger, som også henviser til Datatilsynets praksis på området.

14.15-14.17 Domænesikkerhed
For at minimere risikoen for, at kommunens hjemmesider eller mailadresser bliver brugt til it-kriminalitet, kan I følge disse anbefalinger:

- 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 her: Domænesikkerhed (cfcs.dk)
- 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. Yderligere forklaring kan læses her: Reducer risikoen for falske mails (cfcs.dk)
- Anvend DANE for alle indgående mailgateways. Det skal tydeliggøre overfor afsendere, at din organisation anvender kryptering. Derved kan risikoen for fremsendelse af ukrypterede e-mails reduceres. Se yderligere forklaring om DANE her: STARTTLS og DANE (sikkerpånettet.dk)

14.6 Administrative rettigheder
Læs om foranstaltningen "Minimering af privilegerede rettigheder (datatilsynet.dk)" i Datatilsynets katalog over sikkerhedsforanstaltninger, som også henviser til Datatilsynets praksis på området.

14.23 Scanning for sårbarheder
En organisation kan have et stort antal systemer og tjenester eksponeret mod internettet. For at bevare overblikket over dem og vide om de er tilstrækkeligt opdaterede, er det nødvendigt at scanne alle internettilgængelige IP-adresser jævnligt. På baggrund af scanningen er det vigtigt at vedligeholde en oversigt over, hvilke systemer og tjenester organisationen har eksponeret mod internettet. Der skal reageres, hvis der opdages en tjeneste, organisationen ikke selv har valgt at eksponere, eller hvis en scanning viser kendte sårbarheder.

DATATILSYNET

Tekniske minimumskrav for statslige myndigheder – basal informationssikkerhed i en digital forvaltning

1. Introduktion til bilaget

Spørgsmålene 14.1-14.24 i årets tilsyn med kommuners modenhed i forhold til grundlæggende behandlingssikkerhed er baseret på de tekniske minimumskrav til it-sikkerheden, som statslige myndigheder skulle have implementeret senest den 1. juli 2024. Flere af kravene har været gældende for statslige myndigheder siden 2020. Disse krav er opdateret som led i den nationale cyber- og informationssikkerhedsstrategi 2022-2024.

De 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.

Selvom kravene som udgangspunkt er rettet mod statslige myndigheder, har Datatilsynet ladet dem indgå i tilsynet, da de må anses for at være udtryk for best practice, og i mange tilfælde allerede følger af gældende praksis fra Datatilsynet og vejledninger, anbefalinger og standarder på området for relevante myndigheder og instanser som f.eks. Center for Cybersikkerhed, Digitaliseringsstyrelsen, Datatilsynet, NIST Cyber Security Framework mv. Flere af disse foranstaltninger har længe været anbefalet generelt – og således ikke kun overfor statslige myndigheder.

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.

En oversigt over kommunens svar samt procentangivelse for JA-svar for de øvrige kommuner omfattet af ”Tilsyn med kommuners modenhed i forhold til grundlæggende behandlingssikkerhed 2024” er vedlagt som bilag.

Tabel 1 – Oversigt over kommunens svar samt procentangivelse for JA - svar for øvrige kommuner omfattet af ”Tilsyn med kommuners modenhed i forhold til grundlæggende behandlingssikkerhed 2024”.

Tabellen i bilaget om de tekniske minimumskrav omhandler de tekniske minimumskrav for statslige myndigheder (spørgsmål 14.1-14.24). Tabellen sidestiller den enkelte kommunes svar med den andel af kommuner, der har svaret ”Ja” til hvert spørgsmål om de tekniske minimumskrav for statslige myndigheder. 48 kommuner har været adspurgt, og andelen af kommuner, der har svaret ”Ja” er i forhold til de 48 adspurgte kommuner. Kommuner som har svaret ”Ved ikke” eller ”Ikke relevant” udgår af sammenligningen.

SPØRGSMÅL	PROCENT JA-SVAR	ORGANISATIONENS SVAR
14.1 Har organisationen en firewall på alle klienter?	73%	Ja
14.2 Har organisationen på samtlige klienter gennemtvunget anvendelsen af Always On VPN fra eksterne netværk.	50%	Nej
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?	98%	Ja
14.4 Har organisationen implementeret end-point-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter?	96%	Ja
14.5 Har organisationen etableret en proces, der sikrer, at alle klienters operativsystemer og applikationer holdes sikkerhedsmæssigt opdateret?	98%	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.	70%	Ja
14.7 Har organisationen sikret, at alle pc'er anvender nyeste operativsystem?	77%	Ja
14.8 Har organisationen sikret, at der kun anvendes godkendte mail-relays med autentifikation?	89%	Ja
14.9 Har organisationen sikret, at forsendelse af e-mail sendt via internettet eller andre netværk, som ikke er under den dataansvarliges kontrol, altid sker krypteret minimum med TLS 1.2?	94%	Ja
14.10 Har organisationen implementeret to-faktor-autentifikation ved adgang over internettet til it-systemer, og hvor risikovurderingen indikerer et behov for høj sikkerhed?	70%	Ja
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.	94%	Ja
14.12 Har organisationen implementeret MDM (Mobile Device Management) på alle mobile enheder?	69%	Nej

SPØRGSMÅL	PROCENT JA-SVAR	ORGANISATIONENS SVAR
14.13 Har organisationen sikret, at operativsystemer og apps på mobile enheder så vidt muligt er opdateret, så snart leverandøren udgiver opdateringer?	83%	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?	65%	Nej
14.15 Har organisationen sikret, at DNSSEC er tilknyttet alle domænenavne tilhørende organisationen?	71%	Ja
14.16 Anvender organisationen en Sikker DNS-tjeneste eller anden løsning, som beskytter organisationens brugere mod kendte skadelige websteder?	92%	Ja
14.17 Har organisationen implementeret DMARC REJECT-policy på alle domæner tilhørende organisationen?	75%	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?	85%	Ja
14.20 Krypterer organisationen al kommunikation til organisationens tjenester, hvor data transmitteres via internettet og andre netværk, som ikke er under den dataansvarliges kontrol, og denne kryptering er altid TLS 1.2 eller bedre?	91%	Ja
14.21 Anvender organisationen DANE på alle indgående mailgateways?	33%	Ja
14.22 Har organisationen adskilt gæstenetværk fra interne netværk?	100%	Ja
14.23 Scanner organisationen for tjenester på internettilgængelige IP-adresser?	88%	Ja
14.24 Holder organisationen software på kritiske infrastruktur-enheder og -tjenester opdateret?	94%	Ja