Ministeriet for
Samfundssikkerhed
og Beredskab

Dato: 20-05-2025
Sagsnr.: 2025 - 1155
Akt-id.: 6221

Besvarelse af spørgsmål nr. 84 (alm. del) fra Udvalget for Digitalisering og IT

Hermed sendes besvarelse af spørgsmål nr. 84 (alm. del), stillet af Folketingets Udvalg for Digitalisering og IT den 24. april 2025.

Torsten Schack Pedersen

Slotsholmsgade 12
1218 København K

mssb@mssb.dk

Spørgsmål nr. 84 (alm. del) fra Folketingets Udvalg for Digitalisering og IT:
Statslige myndigheder skal følge den internationale standard for informationssikkerhed (ISO27001). I forlængelse heraf, bedes ministeren redegøre for myndighedernes overvejelser om indkøb og implementering af it-systemer, herunder mere specifikt: Hvordan bliver der i udviklingen og i kravene til leverandøren taget højde for, at de it-systemer, der udvikles eller anskaffes, lever op til de krav til it-sikkerhed, der gælder i staten?

Spørger:
Udvalget v. Lisbeth Bech-Nielsen (SF).

Svar:
Ministeriet for Samfundssikkerhed og Beredskab har til brug for besvarelsen af spørgsmålet indhentet et bidrag fra Styrelsen for Samfundssikkerhed, der har oplyst følgende:

"I regi af den nationale strategi for cyber- og informationssikkerhed 2018-2021, er det besluttet, at der årligt skal gennemføres målinger af statslige myndigheders ISO 27001-implementering med henblik på at understøtte fremdrift i implementeringen. Den nationale strategi for cyber- og informationssikkerhed for 2022-2024 har videreført tiltaget, ligesom der ved denne strategi også blev indført krav til halvårlig opfølgning på de tekniske minimumskrav. Derudover er der en række specifikke krav i forbindelse med outsourcing af samfundskritiske it-systemer.

Fra 1. juli 2025 bliver myndighederne ligeledes forpligtet til at efterleve sikkerhedsforanstaltningerne i NIS 2-loven, som med bestemmelserne om forsyningskædesikkerhed (§ 6, stk. 1, nr. 4) og sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af it-systemer (§ 6, stk. 1, nr. 5) skærper fokus på netop dette.

ISO 27001-standarden er i sig selv en ledelsesstandard, som er med til at opstille de krav til risikostyring, processer og dokumentation, der skal sikre, at en organisations sikkerhed har det rette niveau. Det indgår som en del af standarden, at den enkelte organisation skal holde styr på efterlevelsen af juridiske, lovmæssige, regulatoriske og kontraktlige krav, ligesom standarden indeholder en række foranstaltninger angående informationssikkerhed i leverandørforhold,

håndtering af informationssikkerhed i leverandøraftaler og styring af informationssikkerhed i forsyningskæden.

Det er, inden for rammerne af ovennævnte krav, op til den enkelte myndighed, hvordan den i praksis tilrettelægger arbejdet med it-sikkerhed i forbindelse med indkøb og implementering af it-systemer hos eksterne leverandører. ISO 27001-standardens underliggende kontroller kan være med til at strukturere dette arbejde, og myndighederne kan i øvrigt få hjælp og inspiration hertil gennem en række forskellige vejledninger fra Styrelsen for Samfundssikkerhed, som er tilgængelige på hjemmesiden sikkerdigital.dk. Blandt disse vejledninger er en vejledning om cybersikkerhed i leverandørforhold samt et opslagsværk med ISO 27001-krav omskrevet til kontraktbestemmelser, som myndighederne kan anvende direkte. Derudover foreligger de tekniske minimumskrav til it-sikkerheden i staten, som ligeledes indgår i udbud og kontrakter med leverandører. Det er minimumskrav, som leverandører *skal* kunne efterleve.

Det bemærkes, at Styrelsen for Samfundssikkerhed arbejder på en fremadrettet model for opfølgning på efterlevelsen af ISO 27001 og de tekniske minimumskrav, som skal sammentænkes med den kommende tilsynsførelse med de statslige myndigheder i forbindelse med NIS 2, med henblik på at sikre mest mulig sammenhæng i og effektiv opfølgning på it-sikkerhedskrav til statslige myndigheder."