7.1 Styr på informationssikkerhed i alle myndigheder

4. maj 2016

Aftalens indhold

En væsentlig forudsætning for den fremadrettede digitaliseringsindsats er, at borgere og virksomheder er trygge ved og har tillid til, at offentlige myndigheder håndterer følsomme oplysninger med fortrolighed og med respekt for sikkerheden. Det er derfor nødvendigt, at der opnås et tværgående højt sikkerhedsniveau, der samtidig balancerer hensyn til brugervenlighed og økonomi via en risikobaseret tilgang til informationssikkerhed. Tværgående erfaringsopsamling og koordination af parternes arbejde med informationssikkerhed bør ligeledes understøttes. Initiativet består af følgende indsatser:

- Alle myndigheder skal følge principperne i informationssikkerhedsstandarden ISO27001. For at understøtte indsatsen udarbejdes støtte til arbejde med og implementering af ISO27001.
- Alle offentlige myndigheder arbejder efter konkrete sikkerhedstiltag for at imødegå trusler om hacking. Center for Cybersikkerhed understøtter myndighedernes arbejde med sikkerhed, herunder udbredelse af "Top fire", der er forslag til konkrete sikkerhedstiltag.
- Alle offentlige myndigheder skal indberette større cybersikkerhedshændelser. Der skal findes en model, der sikrer myndighederne en smidig proces ved indberetning af sikkerhedsbrud
- Alle offentlige myndigheder stiller relevante sikkerhedsmæssige krav ved udbud og indgåelse af it-kontrakter fx som en del af løsningsarkitekturen. Myndighederne kan anvende Digitaliseringsstyrelsens klausulbibliotek som inspiration til deres it-kontrakter eller K04 efter dennes lancering.
- Digitaliseringsstyrelsen udarbejder i samarbejde med Justitsministeriet og Datatilsynet en vejledning i, hvordan offentlige myndigheder kan indarbejde krav, fx i design og videreudvikling af løsninger om *data protection by design* og *data protection by default*, der ventes med den kommende databeskyttelsesforordning.
- Der skal ske en løbende opfølgning på myndighedernes arbejde med informationssikkerhed i Forum for fællesoffentlig koordinering af informationssikkerhed. KL forestår opfølgningen i kommunerne, og Danske Regioner forestår opfølgningen i regionerne.

Organisering/tidsplan

Initiativet forankres i det eksisterende Forum for fællesoffentlig koordinering af informationssikkerhed, der afrapporterer til Styregruppen for digitaliseringsstrategien. Kommissoriet for forummet revideres i forbindelse hermed. Implementering af ISO27001 i staten fortsætter i regi af Statens informationssikkerhedsforum. Danske Regioner og KL understøtter regionernes og kommunernes arbejde med ISO-standarden og i forhold til behovet for den fremadrettede indsats. Allerede udarbejdet materiale fra DIGST stilles til rådighed til denne indsats.