Ministeriet for Fødevarer, Landbrug og Fiskeri

Folketingets Forsvarsudvalg

København, den 24. juni 2014
Sagsnr.: 26337
Dok.nr.: 686239

Fødevareministerens besvarelse af spørgsmål nr. 264 (FOU alm. del) stillet den 26. maj 2014 efter ønske fra Troels Lund Poulsen (V)

Spørgsmål nr. 264:
"I det forsvarsministeren på et åbent samråd i Forsvarsudvalget den 23. maj 2014 om cybersikkerhed opfordrede udvalget til at spørge de enkelte ministre om, hvad der gøres for at beskytte sig imod cybertrusler, bedes ministeren redegøre for, hvad der er gjort eller vil blive gjort indenfor ministerens ansvarsområde m.h.t. at beskytte it-systemer og fortrolige data samt m.h.t. at sikre sig imod hackerangreb, jf. statsrevisorernes beretning 3/2013 om forebyggelse af hackerangreb, hvor statsrevisorerne bl.a. udtaler foruroligelse over utilstrækkelig beskyttelse mod cybertrusler i en række undersøgte statslige virksomheder."

Svar:
Fødevareministeriets koncern har løbende fokus på at opretholde og udbygge sikkerhedsforanstaltninger for at beskytte it-systemer og fortrolige data samt m.h.t. at sikre sig imod hackerangreb.

Som følge af Rigsrevisionens beretning til Statsrevisorerne om forebyggelse af hackerangreb udarbejdede Center for Cybersikkerhed under Forsvarets Efterretningstjeneste og Digitaliseringsstyrelsen en vejledning om cybersikkerhed, navngivet 'Cyberforsvar der virker' fra december 2013.

Af vejledningen fra Center for Cybersikkerhed og Digitaliseringsstyrelsen fremgår en køreplan for et godt cyberforsvar. Af vejledningen fremgår forskellige skridt samt følgende fire konkrete sikringstiltag:

- Udarbejd positivliste over applikationer af godkendte programmer, for at forhindre kørsel af ondsindet eller uønsket software
- Opdatér programmer med seneste sikkerhedsopdateringer, højrisiko inden for to dage
- Opdatér operativ-systemet med seneste sikkerhedsopdateringer, højrisiko inden for to dage. Undgå Windows XP eller tidligere
- Begræns antallet af brugerkonti med domæne- eller lokaleadministratorrettigheder.

Ministeriet for Fødevarer, Landbrug og Fiskeri
Slotsholmsgade 12
DK-1216 København K
Tel +45 33 92 33 01
Fax +45 33 14 50 42
fvm@fvm.dk
www.fvm.dk

Fødevareministeriets institutioner; NaturErhvervstyrelsen, Fødevarestyrelsen samt Fødevareministeriets departement har fokus på de enkelte skridt i vejledningen, og Fødevareministeriets institutioner arbejder aktivt med at implementere de fire konkrete sikringstiltag.

Fødevareministeriets institutioner har generelt fokus på risikovurdering og risikostyring af konsekvenser af sikkerhedshændelser. Institutionerne modtager løbende information fra blandt andet Center for Cybersikkerhed om cybertrusler, som potentielt kan udgøre en sikkerhedsrisiko, og har fokus på, at der bliver etableret modforanstaltninger, som på passende vis imødekommer risiciene.

Der er desuden udarbejdet informationssikkerhedspolitikker i de enkelte institutioner, som danner den overordnede ramme for varetagelsen af informationssikkerheden. Politikkerne beskriver de processer, som institutionen gennemfører for at håndtere informationssikkerheden, samt hvorledes disse bliver forankret i organisationen. Der er udformet retningslinjer til medarbejdere om brug af it-udstyr og systemer mv., som er kommunikeret til alle medarbejdere, og der gennemføres løbende opmærksomhedsskabende aktiviteter (awareness) herom. Der foreligger desuden it-beredskabsplaner til anvendelse i it-beredskabssituationer i institutionerne. Endeligt er der informationssikkerhedsudvalg/datasikkerhedsudvalg, som behandler it-sikkerhedsmæssige spørgsmål og modtager årlige rapporteringer på informationssikkerhedsområdet i institutionerne.

Derudover kan nævnes, at overgangen til den nye sikkerhedsstandard ISO 27001 påbegyndes i 2014 i Fødevareministeriet. Overgangen til denne standard betyder, at der skal fokuseres yderligere på risikostyring, ledelsesforankring, og informationssikkerhedsstyring.

Dan Jørgensen

/Signe Nørgaard Haagensen