ERHVERVSMINISTERIET

Folketingets Erhvervs-, Vækst- og Eksportudvalg

ERHVERVSMINISTEREN

5. april 2018

ERHVERVSMINISTERIET

Slotsholmsgade 10-12
1216 København K

Tlf. 33 92 33 50
Fax. 33 12 37 78
CVR-nr. 10092485
EAN nr. 5798000026001
em@em.dk
www.em.dk

Besvarelse af spørgsmål 10 ad L 144 stillet af udvalget den 19. marts 2018 efter ønske fra Karin Gaardsted (S) og Lisbeth Bech Poulsen (SF)

Spørgsmål:
Vi ministeren uddybe - herunder med eksempler - hvad der forstås ved "passende sikkerhedsforanstaltninger", jf. at operatører og udbydere skal træffe "passende sikkerhedsforanstaltninger" på baggrund af en vurdering af de konkrete risici.

Svar:
Et centralt princip i forbindelse med it-sikkerhed generelt og i lovforslaget er, at virksomheder, der er omfattet af lovforslaget, skal gennemføre en risikoanalyse. Det betyder, at operatører og udbydere skal identificere og vurdere alle væsentlige risici for driften af den væsentlige tjeneste.

På baggrund af risikoanalysen skal operatører af væsentlige tjenester og udbydere af digitale tjenester i overensstemmelse med NIS-direktivet træffe passende sikkerhedsforanstaltninger for at forebygge og minimere konsekvensen af eventuelle hændelser, der berører sikkerheden i deres net- og informationssystemer.

En passende sikkerhedsforanstaltning til at håndtere risici kan derfor være indførelsen af et rapporteringskrav om risici til de relevante funktioner i virksomheden, herunder it-sikkerhedsfunktionen og det øverste ledelsesorgan.

Et konkret eksempel kan være en situation, hvor en risikoanalyse viser, at et serverrum i en kælder kan risikere at blive oversvømmet af opstigende kloakvand ved et skybrud. En passende foranstaltning kunne være at installere et højvandsluk. Såfremt der er risiko for indtrængning af vand andre steder fra, kunne en passende foranstaltning være at flytte serverrummet, fx til 1. sal.

Et andet eksempel kunne være risiko for overgravning af virksomhedens bredbåndsforbindelse på grund af omfattende anlægsaktivitet ved virk-

somheden. En passende foranstaltning kunne være etablering af en back-up bredbåndsforbindelse, fx en radiobaseret løsning.

Passende sikkerhedsforanstaltninger kan eksempelvis også være løbende test af virksomhedens systemer og et effektivt beredskab, der kan minimere konsekvensen af en eventuel hændelse. Både test af systemer og beredskabet skal tage højde for relevante trusler mod de relevante tjenester.

Et tredje eksempel på en passende sikkerhedsforanstaltning kan således være udarbejdelse af en IT-beredskabsplan, der indeholder målsætninger for genetablering af normal drift i tilfælde af nedbrud. En beredskabsplan skal afprøves regelmæssigt, således at virksomheden ved, at genetableringen er mulig.

Praksis omkring passende sikkerhedsforanstaltninger vil blive udviklet løbende.

For eksisterende praksis kan henvises til bekendtgørelse nr. 567 af 3. juni 2016 om informationssikkerhed og beredskab i net- og tjenester, som Center for Cybersikkerhed administrerer. I bekendtgørelsens § 2, stk. 3, fremgår, at "på baggrund af risikovurderingen efter stk. 1 og 2 skal udbyderne implementere passende foranstaltninger til sikring af tilgængelighed, integritet og fortrolighed i net og tjenester samt sikre, at tredjepart opretholder en tilsvarende sikkerhed i forhold til driftsleverancer til udbyderne efter stk. 2." Praksis på dette område kan anvendes i relevant omfang.

Herudover vil der muligvis blive udarbejdet retningslinjer i EU-regi, som vil indeholde fortolkningsbidrag til, hvad passende sikkerhedsforanstaltninger er.

Med venlig hilsen

Brian Mikkelsen