ERHVERVSSTYRELSEN

Fibia P/S
eeo@fibia.dk
sni@fibia.dk

13. december 2019
Sag nr.: 2019 - 1771

ERHVERVSSTYRELSEN
Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø

Tlf. 35 29 10 00
Fax 35 29 10 01
CVR-nr 10 15 08 17
E-post erst@erst.dk
www.erst.dk

ERHVERVSMINISTERIET

Påbud om gennemførelse af risikovurdering mv. på domænenavnsområdet

Indledning
Erhvervsstyrelsen har i forbindelse med styrelsens tilsyn med Fibia P/S' (herefter Fibia) overholdelse af reglerne om net- og informationssikkerhed for domænenavnssystemer fundet anledning til at påbyde selskabet at gennemføre en risikovurdering mv. på domænenavnsområdet.

Afgørelse
Erhvervsstyrelsen påbyder i medfør af § 14, stk. 4, i lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester følgende:

Fibia skal gennemføre og fremsende en risikovurdering, der tager stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i selskabets væsentlige DNS-tjenester, og som for hver enkel potentiel risiko vurderer på baggrund af objektive skalaer sandsynligheden for og konsekvenser af, at en sådan hændelse indtræder. Fibia skal endvidere for hver enkel potentiel risiko tage begrundet stilling til behovet for at implementere passende foranstaltninger til sikring af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester. Endvidere skal Fibia udarbejde og gennemføre en ledelsesgodkendt net- og informationspolitik med udgangspunkt i en anerkendt international standard samt ligeledes foretage risikostyring i forbindelse med de væsentlige tjenester med udgangspunkt i en anerkendt international standard. Endelig skal Fibia opdatere besvarelsen af spørgeskemaet og indsende dette til Erhvervsstyrelsen.

Påbuddet skal være efterkommet senest 1. april 2020.

Sagens faktiske omstændigheder
Erhvervsstyrelsen orienterede Fibia med brev af 18. maj 2018 om nye regler om net- og informationssikkerhed på domænenavnsområdet.

Samtidig blev Fibia bedt om at tage stilling til, hvorvidt selskabet er en operatør af væsentlige tjenester på domænenavnsområdet på baggrund af de kriterier, som fremgår af § 1 i bekendtgørelsen om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domænenavnsområdet (herefter NIS-bekendtgørelsen) og oplyse Erhvervsstyrelsen herom senest 1. september 2018.

Fibia har med e-mail af 13. september 2018 oplyst, at selskabet er en operatør af væsentlige tjenester på domænenavnsområdet.

Som led i Erhvervsstyrelsens tilsyn med Fibias overholdelse af sikkerhedsreglerne på domænenavnsområdet blev Fibia med brev af 27. maj 2019 bedt om at besvare og returnere et spørgeskema samt fremsende den af selskabet gennemførte risikovurdering på domænenavnsområdet senest den 23. august 2019.

Fibia returnerede spørgeskemaet den 23. august 2019 og eftersendte den 26. august 2019 dokumentet "Risiko- og sårbarhedsvurdering 4.2 - Net systemer".

I lyset af at Erhvervsstyrelsen havde en række spørgsmål til det fremsendte materiale inviterede Erhvervsstyrelsen den 12. september 2019 Fibia til et møde, der blev afholdt den 23. september 2019.

På baggrund af opfølgningsmødet blev Fibia med brev af 3. oktober 2019 bedt om at fremsende et revideret udfyldt spørgeskema og heri bl.a. korrekt angive, hvilke(n) tjeneste(r) selskabet er væsentlig operatør for, samt tillige angive detaljerede referencer til, hvor de forskellige sikkerhedskrav i NIS-bekendtgørelsen er dokumenteret med henvisning til f.eks. dokumentnavn, version eller dato samt afsnit eller sidetal.

Fibia blev ligeledes bedt om at redegøre for, hvorvidt der er udarbejdet en specifik politik for net- og informationssikkerhed, ligesom selskabet blev bedt om at redegøre for, efter hvilke standarder eller retningslinjer en sådan politik er udarbejdet. Videre blev Fibia bedt om at oplyse, hvilken anerkendt international standard Fibias risikostyring tager udgangspunkt i.

Endelig bad Erhvervsstyrelsen om, at den af Fibia gennemførte risikovurdering forholder sig til spørgsmålet om tab af tilgængelighed, integritet, autenticitet og fortrolighed i de væsentlige tjenester, som Fibia er væsentlig operatør for. I den forbindelse blev Fibia også bedt om at beskrive den anvendte metodik for risikovurderingen, herunder oplyse referencer til metodikken, eller hvor metodikken ellers anvendes, idet Erhvervsstyrelsen havde konstateret, at den anvendte metode ikke nødvendigvis giver et fokuseret resultat for, hvor der måtte være behov for at indføre sikkerhedstiltag.

Med e-mail af 7. november 2019 meddelte Fibia Erhvervsstyrelsen, at selskabet havde taget styrelsens argumenter på mødet den 23. september 2019 til efterretning og havde indkøbt et ISMS system til bl.a. understøttelse af net- og informationssikkerhed på domænenavnsområdet. Samtidig oplyste Fibia, at det er selskabets målsætning at kunne præsentere resultatet på et nyt opfølgningsmøde i første halvdel af 2020. Fibia har yderligere telefonisk oplyst, at selskabet for indeværende ikke reviderer besvarelsen af spørgeskemaet eller indsender yderligere materiale på baggrund af Erhvervsstyrelsens brev af 3. oktober 2019.

Vurdering
På baggrund af sagsforløbet og det modtagne materiale har Fibia ikke over for Erhvervsstyrelsen dokumenteret, at der er gennemført en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester, som Fibia er operatør for, jf. § 2, stk. 1, i NIS-bekendtgørelsen.

Den af selskabet indsendte risikovurdering tager desuden ikke stilling til - for hver af de potentielle risici - behovet for at implementere passende foranstaltninger til sikring af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester, jf. § 2, stk. 3, i NIS-bekendtgørelsen.

Fibia har desuden ikke anvendt operationelle skalaer for sandsynlig og konsekvens ved vurdering af de enkelte hændelser.

Fibia har endvidere ved besvarelse af spørgeskemaet angivet, at selskabets net- og sikkerhedspolitik ikke tager udgangspunkt i en anerkendt international standard, hvilket er et krav i henhold til NIS-bekendtgørelsens § 3, stk. 1.

Fibia har yderligere oplyst, at selskabets risikostyring ikke tager udgangspunkt i DS/ISO/IEC 27001 og har – på trods af opfordring fra Erhvervsstyrelsen – ikke redegjort for, hvilken anden anerkendt international standard selskabets risikostyring tager udgangspunkt i, jf. kravet i § 5, stk. 1 i NIS-bekendtgørelsen.

Begrundelse
Operatører af væsentlige tjenester på domænenavnsområdet skal gennemføre en risikovurdering, der tager stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester på domænenavnsområdet. Desuden skal operatører af væsentlige tjenester på domænenavnsområdet tage udgangspunkt i anerkendte internationale standarder ved udarbejdelse af net- og sikkerhedspolitik samt foretage risikostyring med udgangspunkt i anerkendte internationale standarder. Disse lovgivningsmæssige krav har været gældende siden 10. maj 2018.

Fibia er en operatør af væsentlige tjenester på domænenavnsområdet. Fibia har ikke gennemført en risikovurdering på området i overensstemmelse med kravene. Ydermere tager Fibias net- og sikkerhedspolitik samt risikostyring ikke udgangspunkt i en anerkendt international standard.

Gennemførelse af en risikovurdering er fundamentet for net- og informationssikkerhed på domænenavnsområdet. Ved ikke at tage udgangspunkt i anerkendte internationale standarder ved udarbejdelse af net- og sikkerhedspolitik samt ikke at foretage risikostyring med udgangspunkt i anerkendte internationale standarder, har Fibia ikke på en systematisk måde taget stilling til alle væsentlige aspekter af net- og informationssikkerhed på domænenavnsområdet, hvorved sikkerhedsniveauet for selskabets væsentlige tjenester på domænenavnsområdet forringes.

Det retlige grundlag
Det fremgår af § 14, stk. 1, i lov nr. 436 af 8. maj 2018 om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester, at:

"Erhvervsstyrelsen fører tilsyn med overholdelsen af denne lov og de regler, der er udstedt i medfør af loven."

I lovens § 4 fastsættes følgende regler for operatører af væsentlige tjenester:

"§ 4 Operatører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til deres aktiviteter. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står mål med risikoen.
[…]
Stk. 3. Erhvervsministeren kan fastsætte nærmere regler om foranstaltninger efter stk. 1 og 2."

I medfør af ovennævnte lov er bekendtgørelse nr. 453 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domænenavnsområdet udstedt.

Af bekendtgørelsens § 2, stk. 1, fremgår:

"Operatører af væsentlige tjenester skal gennemføre en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester, som fremgår af bilag 1."

Af bilag 1 til bekendtgørelsen fremgår bl.a. følgende væsentlig tjeneste på domænenavnsområdet:

"*DNS-tjeneste: Den tjeneste, som en DNS-tjenesteudbyder leverer på internettet, og som muliggør, at et internetdomænenavn konverteres til en IP-adresse, herunder rekursive og autoritative navneservere.*"

Videre fremgår det af bekendtgørelsens § 2, stk. 3:

"På baggrund af risikovurderingen efter stk. 1 og 2 skal operatørerne implementere passende foranstaltninger til sikring af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester […]."
.

Endvidere fremgår det af bekendtgørelsens § 3, stk. 1:

"*Operatører af væsentlige tjenester skal udarbejde og gennemføre en ledelsesgodkendt net- og sikkerhedspolitik med udgangspunkt i en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende. [….]"*

Endelig fremgår det af bekendtgørelsens § 5, stk. 1:

"*Operatører af væsentlige tjenester skal foretage risikostyring i forbindelse med de væsentlige tjenester, som fremgår af bilag 1, med udgangspunkt i en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende.*"

Af ovennævnte lovs § 14, stk. 4, kan Erhvervsstyrelsen *"som led i sit tilsyn udstede påbud til operatører af væsentlige tjenester om at afhjælpe mangler i opfyldelsen af de krav, der fremgår af henholdsvis af lovens §§ 4 og 5 og §§ 7-9 og regler, som fastsættes i medfør af § 4, stk. 3, § 5, stk. 4, § 8, stk. 3 eller § 9, stk. 4."*

Klagevejledning
Erhvervsstyrelsens afgørelse om at påbyde Fibia at gennemføre en risikovurdering mv. af selskabets væsentlige tjenester på domænenavnsområdet kan i henhold til § 16 i lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester ikke påklages til anden administrativ myndighed. Sagen vil herefter alene kunne indbringes for domstolene.

o - o - O - o – o

Denne afgørelse offentliggøres i medfør af § 15, stk. 1 i lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester på Erhvervsstyrelsens hjemmeside.

Opmærksomheden henledes på, at manglende efterlevelse af påbud efter § 14, stk. 4, i lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester, kan straffes med bøde, jf. ovennævnte lovs § 17, stk. 1, nr. 2 og stk. 2.

Med venlig hilsen

Finn Petersen