Datum 2020-09-10
Vår referens 20-6207
Aktbilaga

Avdelningen för säker kommunikation

Stiftelsen för Internetinfrastruktur

Beslut – avskrivning av tillsyn över systematiskt och riskbaserat informationssäkerhetsarbete

Saken

Tillsyn över informationssäkerhetsarbete enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8).

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avskriver ärendet från vidare handläggning.

Bakgrund

Nätverk och informationssystem spelar en allt viktigare roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och den inre marknadens funktion. I synnerhet gäller detta inom ramen för tillhandahållandet av internettjänster som DNS[1]-tjänster och TLD-[2] tjänster, vilka spelar en viktig roll genom att bl.a. underlätta den gränsöverskridande rörligheten för varor, tjänster och personer.

NIS-lagen trädde i kraft den 1 augusti 2018 och syftar bl.a. till att uppnå en hög nivå på säkerheten i nätverk och informationssystem hos leverantörer av samhällsviktiga tjänster.

[1] Domain Name System
[2] Top Level Domain

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

Enligt NIS-lagen är leverantörer av samhällsviktiga tjänster skyldiga att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende de nätverk och informationssystem som de använder för att tillhandahålla den samhällsviktiga tjänsten. Myndigheten för samhällsskydd och beredskap (MSB) har meddelat närmare bestämmelser om detta arbete genom MSB:s informationssäkerhetsföreskrifter.

PTS är tillsynsmyndighet över leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur. PTS roll som tillsynsmyndighet är att granska och kontrollera att NIS-lagen och tillhörande föreskrifter följs.

PTS beslutade att inleda tillsyn den 28 maj 2020 för att inhämta information om Stiftelsen för Internetinfrastrukturs (Internetstiftelsen) systematiska och riskbaserade informationssäkerhetsarbete avseende de nätverk och informationssystem som används för att tillhandahålla den samhällsviktiga tjänsten.

Det huvudsakliga syftet med tillsynen har varit att få en övergripande bild av Internetstiftelsens systematiska och riskbaserade informationssäkerhetsarbete.

Skäl

Tillämpliga bestämmelser

Enligt 11 § NIS-lagen är leverantörer av samhällsviktiga tjänster skyldiga att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende de nätverk och informationssystem som de använder för att tillhandahålla den samhällsviktiga tjänsten.

Enligt 21 § NIS-lagen ska tillsynsmyndigheten utöva tillsyn över att NIS-lagen och föreskrifter som har meddelats i anslutning till NIS-lagen följs.

Enligt 24 § NIS-lagen ska den som står under tillsyn på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen.

MSB:s informationssäkerhetsföreskrifter innehåller närmare bestämmelser om det systematiska och riskbaserade informationssäkerhetsarbete som leverantörer av samhällsviktiga tjänster är skyldiga att bedriva enligt 11 § NIS-lagen.

Enligt 2 § MSB:s informationssäkerhetsföreskrifter ska leverantören bl.a. säkerställa att systematiskt och riskbaserat informationssäkerhetsarbete även bedrivs hos eventuella externa aktörer till vilka hantering av nätverk och informationssystem utkontrakterats.

Enligt 5 § första stycket MSB:s informationssäkerhetsföreskrifter ska leverantören bl.a. bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.

Enligt 6 § MSB:s informationssäkerhetsföreskrifter ska bl.a. en tydlig ansvars-, roll- och resursfördelning fastställas av leverantören, utifrån identifierade risker och behov.

Enligt 7 § MSB:s informationssäkerhetsföreskrifter ska leverantören upprätta en informationssäkerhetspolicy där ledningens målsättning med och inriktning för organisationens informationssäkerhetsarbete framgår. Leverantören ska också upprätta de interna regler och det stöd som i övrigt krävs för organisationens informationssäkerhetsarbete.

Enligt 8 § MSB:s informationssäkerhetsföreskrifter ska leverantören ha ett dokumenterat arbetssätt för att bl.a. kunna klassa och riskanalysera information.

Enligt 9 § MSB:s informationssäkerhetsföreskrifter ska leverantören säkerställa att medarbetare har relevant kunskap om säker informationshantering, bl.a. genom utbildning, informationsinsatser och övning.

Enligt 11 § MSB:s informationssäkerhetsföreskrifter ska leverantören bl.a. ha interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser relaterade till den samhällsviktiga tjänsten.

PTS är enligt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster tillsynsmyndighet över sektorn digital infrastruktur.

PTS bedömning

PTS har i sin tillsyn ställt ett antal frågor avseende Internetstiftelsens systematiska och riskbaserade säkerhetsarbete, som Internetstiftelsen har redogjort för i skriftligt svar till PTS.

Syftet med denna tillsyn har varit informationsinhämtning samt att få en övergripande bild av Internetstiftelsens säkerhetsarbete. Tillsynen har inte omfattat granskning eller bedömning av svaren i sig eller huruvida företaget efterlever aktuella krav. PTS anser att Internetstiftelsens svar är fullständiga och att de gett en övergripande bild av företagets systematiska och riskbaserade säkerhetsarbete.

Syftet med tillsynen är därmed uppfyllt och det saknas skäl att fortsätta tillsynen mot Internetstiftelsen. Ärendet avskrivs därför från vidare handläggning.

Beslutet har fattats av t.f. enhetschef Karin Lodin. I ärendets slutliga handläggning har även Anders Franzén deltagit.