FINANSTILSYNET

N O T A T

Finanstilsynet

11. maj 2015

J.nr. 6941-0009

Redegørelse om it-inspektion i Nets Danmark A/S

1. Indledning

Finanstilsynet var med start i efteråret 2014 og henover årsskiftet på funktionsundersøgelse på it-området hos Nets Danmark A/S (efterfølgende Nets).

Finanstilsynet gennemgik udvalgte dele af it-området, herunder den generelle it-sikkerhedsstyring, strategi, organisation, beredskabsplaner, sikkerhedspolitikker og retningslinjer. Endvidere gennemgik Finanstilsynet Nets procedurer for styring af adgange til systemer og data, ændringshåndtering, kontrol med outsourcede it-funktioner samt krav og procedurer til kontrol og rapportering.

2. Sammenfatning og risikovurdering

Det er Finanstilsynets vurdering, at Nets på tidspunktet for inspektionens gennemførsel ikke i tilstrækkelig grad har implementeret en dokumenteret it-risiko- og sikkerhedsstyring på tværs af virksomheden. Det er vurderingen, at Nets har betydeligt fokus på efterlevelse af krav og kontrolstandarder, herunder bl.a. PCI krav, og mindre fokus på at sikre, at it-risici er tilstrækkelig synliggjorte og imødegået på tværs af Nets samt outsourcing leverandører. Finanstilsynet har i forbindelse med inspektionen konstateret flere svagheder, hvor ledelsen i Nets fremadrettet skal sikre, at væsentlige risici er tilstrækkeligt synliggjorte og imødegået.

Finanstilsynet har påbudt Nets i højere grad at sikre, at it-sikkerhedspolitikken tager afsæt i en dokumenteret it-risikovurdering, samt at ansvar og forventninger mellem direktion og bestyrelse, i relation til it-sikkerhedsstyringen, rapportering og ledelsesopfølgning, præciseres og implementeres. Herunder at der etableres øget dokumenteret kontrol med, at it-sikkerhedspolitikken er tilstrækkeligt implementeret og uddybet i procedurer, forretningsgange og kontroller, samt at Nets styrker it-

sikkerhedsorganisation med klart definerede roller og ansvar for organisering af it-arbejdet.

Endvidere skal Nets i højere grad sikre, at der etableres tilstrækkelige forretningsgange for it-risikostyring, herunder øget dokumentation af risici samt imødegående kontrol og sikringsforanstaltninger på tværs af Nets og dennes leverandører. Finanstilsynet har ligeledes påbudt Nets at sikre, at der er tilstrækkeligt fokus på at risikovurdere og udbedre svagheder konstateret af systemrevisionen, samt at disse bliver tilstrækkeligt inddraget i den etablerede it-risikostyring og ligeledes håndteres tilsvarende.

I relation til outsourcing af it-funktioner skal Nets i højere grad sikre, at it-sikkerhedsrelaterede krav, kontrol- og sikringsforanstaltninger i kontrakterne modsvarer ledelsens forventninger og beslutninger, samt at disse er baseret på tilstrækkeligt dokumenteret it-risikogrundlag. Endvidere skal Nets sikre, at outsourcing-bekendtgørelsens krav om udarbejdelse af interne retningslinjer i relation til ledelsesopfølgning og bestyrelsesrapportering ved outsourcing af it-opgaver bliver tilstrækkeligt dokumenteret og efterlevet.

Finanstilsynet har ligeledes påbudt Nets at styrke eksisterende procedurer for administration af adgange og rettigheder til systemer og data. Bl.a. at der etableres et tilstrækkeligt overblik over kritiske rettigheder, roller samt kombinationer heraf i og på tværs af systemer, databaser og kritisk infrastruktur, samt at disse i højere grad overvåges og kontrolleres tilsvarende. Endvidere er Nets blevet påbudt at styrke procedurer og krav til it-sikkerhedslogning.

Finanstilsynet har konstateret, at Nets har igangsat flere væsentlige forbedringstiltag, der fremadrettet skal styrke Nets` generelle it-sikkerhedsstyring, og i forlængelse heraf er det Finanstilsynets vurdering, at de planlagte forbedringstiltag, hvis tilstrækkeligt implementeret, herunder med fastholdt ledelsesmæssigt fokus og prioritering, vil imødekomme Finanstilsynets påbud.