Marts 2016

Opfølgning på notat til tværministeriel arbejdsgruppe

Nets udarbejdede i oktober 2014 en ikke-fortrolig skriftlig redegørelse til den tværministerielle arbejdsgruppe vedrørende "elektroniske betalinger mv". Redegørelsen beskrev hændelsesforløbet omkring den såkaldte Se&Hør-sag, hvor en IBM-ansat i perioden 2008-2012 på uretmæssig vis misbrugte sine adgangsrettigheder, uretmæssigt overtog andre medarbejderes identitet og uretmæssigt skaffede sig adgang til informationer, som den IBM-ansatte ellers var afskåret fra, med henblik på videregivelse og salg af informationer til ugebladet Se&Hør.

Nets' redegørelse til den tværministerielle arbejdsgruppe vedrørende "elektroniske betalinger mv" beskrev samtidig nogle af de øjeblikkelige tiltag, Nets havde gjort i umiddelbar forlængelse af Se&Hør-sagen. Redegørelsen beskrev desuden, hvordan Nets i efteråret 2013 vedtog et nyt rammeværk for informationssikkerhed, og at implementeringen af rammeværket blev fremskyndet som følge af Se&Hør-sagen. Det var – og er fortsat – ambitionen, at Nets efter gennemførelsen af de planlagte indsatser vil have implementeret det højst mulige niveau for risikostyring og informationssikkerhed, som man kan forvente af en virksomhed, der bl.a. arbejder med digitale betalinger. Dette billede blev bekræftet af konsulentfirmaet Deloitte, der i sommeren 2014 foretog en uvildig gennemgang af de forelagte planer.

IT-inspektion i Nets

I november 2014 foretog Finanstilsynet en ordinær og planlagt inspektion i Nets Denmark A/S (Nets), hvor Finanstilsynet blev grundigt introduceret for Nets' aktiviteter og processer omkring håndtering af IT-sikkerhed og IT-risikostyring.

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. På det grundlag fremlagde Finanstilsynet i maj 2015 en redegørelse om IT-inspektionen, som blev gennemført i november 2014.

Det fremgår af redegørelsen, at Nets blev pålagt en række påbud med henblik på bl.a. at sikre, at it-sikkerhedspolitikken i højere grad er baseret på en dokumenteret it-risikovurdering. Nets var ikke overrasket over kritikken og påbuddene, idet IT-inspektionen fandt sted på et tidspunkt, hvor der endnu var et stykke vej at tilbagelægge, inden Nets ville være på plads med opbygningen af sin nye IT-sikkerhedsorganisation. På tidspunktet for offentliggørelse af Finanstilsynets redegørelse var Nets allerede i fuld gang med at efterleve påbuddene i redegørelsen.

I lyset af Se&Hør-sagen er det er vigtigt at bemærke, at Finanstilsynet ikke konkluderede, at konkrete data på noget tidspunkt har været kompromitteret, eller at der har været svigt i Nets' syste-

mer. Finanstilsynets påbud orienterede sig primært mod, at Nets i højere grad skulle sikre, at de rette processer er på plads, at der er dokumentation for, at risikovurderinger er anvendt, og at der sker tilstrækkelig ledelsesopfølgning i forbindelse med outsourcing.

Finanstilsynet konstaterede samtidig, at "Nets har igangsat flere væsentlige forbedringstiltag, der fremadrettet skal styrke Nets' generelle it-sikkerhedsstyring". Finanstilsynet vurderede desuden, "at de planlagte forbedringstiltag, hvis tilstrækkeligt implementeret, herunder med fastholdt ledelsesmæssigt fokus og prioritering, vil imødekomme Finanstilsynets påbud".

Arbejdet med IT-sikkerhed og IT-risikostyring i Nets siden IT-inspektionen

Nets har efter offentliggørelsen af IT-inspektionens redegørelse i maj 2015 haft løbende dialog med Finanstilsynet med henblik på opfølgning på de konkrete påbud. Allerede i juli 2015 afleverede Nets 3 redegørelser om information, som Finanstilsynet havde efterspurgt i sin redegørelse, og der blev i august 2015 afholdt et informationsmøde, hvor Nets fremlagde status for hver enkelt forbedringspunkt.

Umiddelbart efter IT-inspektionen nedsatte Nets en intern task force med fuld støtte og bevågenhed hos koncernledelsen, der skal sikre, at Nets imødegår påbuddene. Alene i 2015 og 2016 investerer Nets et trecifret millionbeløb i udbygning af sikkerhedsorganisationen med henblik på at styrke sikkerheden på en måde, der ikke blot imødegår påbuddene men også sikrer, at Nets fremadrettet vil have en IT-sikkerhedsorganisation, der afspejler det højst mulige niveau for risikostyring og informationssikkerhed. Hvor Nets' afdeling for IT-sikkerhed i 2014 bestod af 10 personer, består den i dag af 40 interne og 15 eksterne konsulenter, der udelukkende beskæftiger sig med opgave som logning og monitorering af transaktioner, løbende trusselsopsamling, statistiske beregninger af trusselsscenarier, gennemførelse af prøvecases og screeninger af kommende medarbejdere.

Nets' interne systemrevision monitorerer løbende arbejdet med at imødegå påbuddene og implementere Nets' nye og forbedrede IT-sikkerhedsorganisation. Nets vil inden årets udgang have imødekommet samtlige påbud og anmodninger fra Finanstilsynet, samtidig med Nets implementerer det højst mulige niveau for risikostyring og informationssikkerhed, som man kan forvente af en virksomhed, der bl.a. arbejder med digitale betalinger.

Samlet set befinder Nets sig således på et langt højere niveau ift. IT-sikkerhed og IT-risikostyring, end det var tilfældet i perioden 2008-2012, hvor en IBM-ansat på uretmæssig vis skaffede sig adgang til informationer i Nets' systemer, og tillige på et markant forbedret niveau ift. 2014, hvor Se&Hør-sagen rullede i medierne, og hvor Finanstilsynet foretog en ordinær og planlagt IT-inspektion hos Nets.