6. oktober 2014

Se&Hør-sagen

Nets har overfor Finanstilsynet skriftligt redegjort for hændelsesforløbet omkring Se&Hør-sagen. Redegørelsen indeholder oplysninger, som er strengt fortrolige af hensyn til politiets efterforskning, og forretningshemmeligheder for Nets.

Den tværministerielle arbejdsgruppe vedrørende "elektroniske betalinger mv", som ledes af Justitsministeriet, har derfor bedt Nets om at udarbejde en beskrivelse af hændelsesforløbet, der ikke indeholder disse oplysninger.

Sammenfatning

Dagbladet BT bragte mandag den 28. april 2014 og i tiden derefter historier om, at fortrolige oplysninger om forskellige kendte danskeres brug af betalingskort er blevet videregivet til en eller flere ansatte på ugebladet Se & Hør i en periode fra 2008 og frem til 2012. Ifølge oplysningerne fra BT var der tale om, at en tidligere medarbejder i IBM, der er underleverandør af forskellige ydelser til Nets, skulle have videregivet de pågældende oplysninger.

Nets igangsætte straks en undersøgelse af faktiske forhold og har løbende været i tæt dialog med politiet. Blandt andet på baggrund af Nets' undersøgelse har politiet rejst sigtelse mod en tidligere medarbejder hos IBM.

Nets finder sagen dybt foruroligende og beklager dybt de gener, som en række danskere har oplevet ved at Nets' systemer (jf. politiets sigtelse) er blevet misbrugt til en kriminel adfærd. Nets vil gerne understrege, at denne type adfærd strider mod hele det fundament, virksomheden bygger på. Nets vil samtidig understrege, at datasikkerhed og dataintegritet har absolut topprioritet for virksomheden i den daglige drift, og det er kernefokus for den nye ejerkreds, som overtog virksomheden den 9. juli 2014.

Det er i sagens natur umuligt at forhindre, at personer, der har adgang til personhenførbare data, forsøger at udføre kriminelle handlinger. Derimod er det afgørende, at kriminelle handlinger hurtigt bliver opdaget, standset og straffet. Som følge af det nye rammeværk for informationssikkerhed, som Nets' bestyrelse vedtog i efteråret 2013, og hvis implementering er blevet fremskyndet som følge af Se&Hør-sagen, er det ikke sandsynligt, at et identisk misbrug vil kunne forekomme igen uden at blive opdaget, standset og straffet.

Det faktiske forløb

Indledningsvist skal det bemærkes, at Nets' interne undersøgelser har været vanskeliggjort af, at forholdene ligger mellem to og seks år tilbage i tid.

I henhold til sikkerhedsbekendtgørelsen med hjemmel i persondataloven skal logs slettes efter 6 måneder med mindre særlige forhold kræver yderligere opbevaring. I henhold til de gældende industrikrav (PCI DSS-kravene) er Nets forpligtiget til at opbevare detaljerede logdata i 12 måneder. Nets opbevarer dermed ikke detaljerede logs i længere tid end tilladt.

Nets' undersøgelser har derfor været baseret på tekniske logs, som ikke indeholder detaljeret information om opslag på specifikke kortnumre. Informationsmængden er endvidere ekstremt omfangsrig og vanskeligt tilgængelig. Nets arbejder således fortsat på at dokumentere og underbygge sagen til brug for politiets efterforskning.

Den mistænkte tidligere IBM-medarbejder (Kilden) var operatør hos IBM. Generelt er operatørrollen ansvarlig for at overvåge, kontrollere og udføre kommandoer i mainframe, netværk og applikationer i et multileverandørmiljø, herunder at håndtere hændelser i overensstemmelse med den aftalte Service Level Agreement. Kilden var berettiget til at foretage forespørgsler om transaktioner på et givet betalingskort, da Kilden som led i sit arbejde havde brug for denne adgang.

Med udgangspunkt i konkrete, tidsfæstede hændelser, som har været omtalt i Se og Hør, og hvor information om brug af betalingskort antages at have været anvendt til at spore kendte personer, har Nets kortlagt Kildens brug af Nets' systemer (adfærd) i disse perioder og sammenlignet dels med vedkommendes adfærd uden for disse perioder, dels med sammenlignelige medarbejderes adfærd i de samme perioder. På den baggrund kan det konstateres, at kildens adfærd i de pågældende perioder har været afvigende.

En årsag til, at Kildens adfærd ikke dengang fremstod som afvigende, var, at Kildens brug af Nets' systemer var begrænset til få opslag ud af et daværende dagligt antal opslag i Nets' systemer i størrelsesordenen 40.000-50.000 (herunder systemgenererede opslag). I dag er både bevidstheden om og fokus på informationssikkerhed et andet, og Nets' værktøjer til at styrke informationssikkerheden er mere omfattende og effektive, end de var i den periode, hvor Kildens misbrug foregik.

Adgang til information om en bestemt persons brug af betalingskort kræver kendskab til den pågældendes kortnummer. Kilden havde ikke adgang til at foretage søgning på navn og ad den vej få adgang til at forbinde en persons navn med den pågældende persons kortnummer.

Denne adgang anvendes blandt andet af medarbejdere i kundeservice – fx når kortholdere rapporterer deres kort som stjålet eller på anden måde bortkommet. I disse situationer kan kortholder sjældent huske kortnummeret, og det er derfor nødvendigt at kunne finde kortnummeret med udgangspunkt i informationer om kortholders identitet. Der bliver årligt spærret ca. 190.000 kort i Danmark.

Kilden havde som en del af sin jobfunktion adgang til at nulstille andre brugeres password, hvilket blandt andet kan være nødvendigt, hvis en bruger har glemt sit password eller har indtastet forkert password tre på hinanden følgende gange. En sådan nulstilling af passwords blev inden for normal kontortid foretaget af Helpdesk. Uden for dette tidsrum blev opgaven varetaget af driftspersonalet hos IBM, herunder operatørerne, da operatørfunktionen er døgnbemandet.

Nets og IBM har konstateret, at Kilden i perioder, der passer med de "vinduer", der har været omtalt i interne mails hos Se&Hør, har foretaget nulstilling af passwords på bruger-id'er tilhørende medarbejdere i kundeservice, selv om disse bruger-id'er ikke var spærret, og der således ikke forelå en "request for reset password". Dette kunne for eksempel ske under de pågældende medarbejderes ferie. Ved på denne måde midlertidigt at kunne overtage andre medarbejderes identitet har Kilden kunnet skaffe sig adgang til informationer, som Kilden ellers var afskåret fra.

Det er ikke længere muligt for IBM-operatører at foretage søgninger i transaktioner. Der er heller ikke adgang til at nulstille passwords. Samtidig har Nets iværksat en række umiddelbare tiltag i direkte forlængelse af Se&Hør-sagen for yderligere at styrke informationssikkerheden i Nets. Disse tiltag repræsenter en fremskyndelse af implementeringen af det nyt rammeværk for informationssikkerhed, som blev vedtaget af Nets' bestyrelse i efteråret 2013.

Arbejdet med datasikkerhed i Nets

Nets' er underlagt en række sikkerhedskrav og standarder i henhold til lovgivning og regulering fra de internationale kortselskaber, ligesom Nets i sin generelle ansættelsesprocedure stiller relevante krav til medarbejdere, der skal udføre meget betroede jobs med adgang til fortrolige persondata, herunder ren straffeattest.

Nets vurderer, at Nets' behandling af persondata er i overensstemmelse med de gældende fortrolighedskrav til en sådan behandling. Der har således i Nets' systemer været foretaget de logninger og kontroller, som vurderes at opfylde gældende krav for sådan et system. På baggrund af Se&Hør-sagen igangsatte Nets dog umiddelbart en række yderligere initiativer. Nets har således udvidet adfærdsmonitoreringen og omfanget af stikprøvekontroller, ligesom der er foretaget en ekstraordinær gennemgang og indsnævring af brugeradgange til et absolut minimum. Alle ansættelseskontrakter er desuden blevet opdateret med skærpning og tydeliggørelse af konsekvenser ved overtrædelser. Alle ansatte i Nets har derudover modtaget ekstraordinær sikkerhedsundervisning. Der er endvidere oprettet en ekstern whistleblower-hotline for ansatte, der måtte få mistanke om misbrug.

Det er ikke muligt for en virksomhed som Nets alene ved interne procedurer at sikre sig fuldstændigt mod medarbejdere, der måtte forsøge at misbruge deres stilling med kriminelle formål for øje. Nets tilpasser dog løbende virksomhedens kontrol- og sikkerhedsforanstaltninger i takt med, at udviklingen i IT-kriminalitet m.v. giver anledning til at revurdere Nets´ trusselsbillede og afdække behov for at justere sikkerhedsindsatsen.

Over de seneste år har Nets set en øget risiko på informationssikkerhedsområdet. Som svar herpå har Nets intensiveret informationssikkerhedsarbejdet betydeligt og den operationelle informationssikkerhedsafdelings ressourcer er blevet øget væsentligt. På baggrund af ændringer i det generelle trusselsbillede har Nets taget en række strategiske initiativer, herunder vedtagelse af et nyt rammeværk for informationssikkerhed, som blev vedtaget af Nets' bestyrelse i efteråret 2013 og er i færd med at blive implementeret.

På baggrund af Se&Hør-sagen igangsatte Nets' bestyrelse et gennemgribende internt og eksternet review af datasikkerheden i Nets, herunder review af samtlige Nets' interne politikker, systemer og kontroller. Den eksterne gennemgang viser, at informationssikkerhed i Nets i dag er på et tilfredsstillende niveau. Efter gennemførelsen af de planlagte indsatser vil Nets have implementeret det højst mulige niveau for risikostyring og informationssikkerhed.

Øvrige forhold, der har været beskrevet i medierne

Som beskrevet i flere medier blev Nets i 2013 kontaktet af en fotograf, der har arbejdet som freelance for Se&Hør, med oplysninger om et formodet misbrug i 2008 og 2009. Det fremstår i mediernes beskrivelse som om, Nets ikke tog denne oplysning alvorligt. Det er ikke korrekt.

Nets foretog en undersøgelse af de påstående forhold på baggrund af de informationer, Nets havde adgang til angående transaktioner, der lå 4-5 år tilbage i tiden. På den baggrund kunne det ikke sandsynliggøres, at der havde fundet et misbrug sted. Den påståede brug af betalingskort kunne ikke konstateres på baggrund af de datoer, navne og steder, som freelance-fotografen havde oplyst. Nets opfordrede fotografen til at melde sagen til politiet.

Som beskrevet i flere medier har medarbejdere i Nets' kundeservice adgang til at foretage opslag på kortholderes transaktionsdata. Som serviceleverandør til kortudstedere servicerer Nets' kundeservice mange personer, der benytter danskudstedte betalingskort i ind- og udland. Nets opretholder således en døgnbemandet telefonservice 365 dage om året. Nets skal således stå til rådighed og uden unødigt ophold kunne hjælpe kortholdere, der ringer ind. Adgangen til de systemer, som Nets bruger til at yde denne service, er derfor begrundet i et arbejdsbetinget behov i forhold til de serviceydelser, som Nets yder på vegne af bankerne til kortholder. De omfattede serviceydelser dækker bl.a. kortspærring og kortaktivering. Nets kan dog slet ikke genkende det billede, nogle medier har forsøgt at tegne af, at kundeservicemedarbejdere foretager opslag, der ikke er arbejdsrelaterede.

Kundeservicemedarbejdernes adgang til data er undergivet en række forebyggende foranstaltninger, som skal sikre en høj integritet omkring brugen af data, samtidig med at der tages de nødvendige hensyn for at opretholde et effektivt og hensigtsmæssigt serviceniveau. Forebyggende foranstaltninger er blandt andet kontrol af logs, stikprøvekontroller, sikkerhedskurser, awarenesskurser vedrørende behandling af fortrolige kortdata, intern auditering, mv.