Datainspektionen

Datum	Diarienr
2013-09-11	1613-2011

Danske Bank A/S Filial Sverige
NN
Box 7523
103 92 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) – bankers användning av s.k. appar

Datainspektionens beslut

Danske Bank A/S, Sverige Filial uppfyller inte kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen när det gäller åtkomsten till integritetskänsliga personuppgifter via bankens appar.

Danske Bank A/S, Sverige Filial föreläggs, enligt 45 § första stycket personuppgiftslagen, att genomföra åtgärder som innebär att åtkomst till integritetskänsliga personuppgifter i Danske Bank A/S, Sverige Filials appar föregås av stark autentisering av användarna.

Redogörelse för tillsynsärendet

Datainspektionen har inspekterat Danske Bank A/S, Sverige Filials (Danske Bank) personuppgiftsbehandling i appen för smarta telefoner med operativsystemen iOS från Apple (iPhone) och Android från Google som banken tillhandahåller sina kunder.

Datainspektionen konstaterade i beslut den 12 september 2012 att Danske Bank inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att man via bankens appar kommer åt integritetskänsliga personuppgifter efter autentisering med enbart användarnamn och lösenord.

I samma beslut förelade Datainspektionen Danske Bank att komma in med en skriftlig åtgärdsplan. I åtgärdsplanen skulle banken redogöra för

a) vilka konkreta åtgärder banken avser att vidta för att leva upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen,

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

b) på vilka grunder banken bedömer att åtgärderna är verkningsfulla och tillräckliga samt
c) när åtgärderna kan vara vidtagna.

Danske Bank har därefter kommit in med ett konkret lösningsförslag, sin grund för bedömningen att åtgärden är verkningsfull och tillräcklig för att höja säkerheten samt en tidplan för när åtgärden kan genomföras. Av yttrandet framgår i huvudsak följande.

> Tanken är att man vid autentiseringen ska lägga till ytterligare en faktor utöver PIN-koden med hjälp av en teknik som kallas behavioral biometrics.
>
> Behavioral biometrics innebär att man identifierar en person genom att mäta olika parametrar i personens beteende. Man utgår ifrån att varje människa har unika beteendemönster när man utför samma handling vilket gör det möjligt att identifiera en person med hjälp av dessa beteendemönster.
>
> Danske Bank avser att mäta bland annat hastigheten och trycket på tangenten vid inmatningen av PIN-koden. Med hjälp av ett antal insamlade mätvärden skapar systemet en profil för en viss person. Profilen innehåller ett undre och ett övre gränsvärde som Danske Bank sätter för att kunna avgöra om det är den behöriga personen som försöker logga in.Autentiseringen sker genom att systemet jämför mätvärdena från varje ny inmatning av PIN-koden med gränsvärdena i den lagrade profilen.
>
> Mellan tre och fem mätningar vid inloggningen via appen krävs för att kunna uppnå en tillräckligt hög nivå av sannolikhet för att kunna skilja en behörig användare från en obehörig.
>
> Man behöver inte göra om insamlingen av mätvärdena när en användare byter till en annan smarttelefon.
>
> Danske Bank vet inte hur mätvärdena påverkas vid olika väderlekar och olika sinnestillstånd hos användaren.
>
> Baserat på lärdomar från implementeringen av behavioral biometrics på bärbara datorer räknar Danske Bank med att den mobila plattformen har en bra säkerhetsnivå vid första uppstarten. Danske Bank förnekar dock inte att man måste lära sig mer om den mobila plattformen.

Skäl för beslut

Av 31 § personuppgiftslagen följer att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder, för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av hur pass känsliga de behandlade personuppgifterna är, riskerna som finns med behandlingen av personuppgifterna, de tekniska möjligheter som finns tillgängliga på marknaden samt vad det kostar att genomföra åtgärderna.

Genom att logga in i appen med hjälp av sitt personnummer och en fyrsiffrig servicekod kan den som är kund i Danske Banks internetbank se följande över ett öppet nät.

- Konto-/depånamn
- Kontonummer
- Saldo
- Disponibelt belopp
- Transaktioner (innehållande namn, belopp och datum)
- Värde och värdeutveckling på depåinnehav
- Kurslista med värdepapper som användaren valt
- Lista med värdepapper som användaren valt att få ett meddelande om när kursen förändras
- Uppgifter om tagna lån

Enligt Datainspektionens allmänna råd är uppgifter om enskildas personliga och ekonomiska förhållanden inom bankväsendet normalt att anse som integritetskänsliga. Ett uttryck för att det är fråga om integritetskänsliga uppgifter är att uppgifterna omfattas av tystnadsplikt eller sekretess.

Särskilt med tanke på att appar ofta används på offentliga platser finns en ökad risk för att någon obehörig lyckas komma åt inloggningsuppgifterna. Denne skulle därefter, genom att enkelt ladda ner bankens app till sin egen smarta telefon, kunna logga in i appen och obehörigen ta del av en stor mängd uppgifter, utan att den behörige användaren märker det.

Datainspektionen anser att det kan medföra stora risker för den enskildes personliga integritet om någon obehörig får tillgång till t.ex. uppgifter om konton, transaktioner med namn på mottagaren eller avsändaren och skuldsättning. Uppgifterna skulle kunna användas till att kartlägga, inte bara stora delar av en persons ekonomiska förhållanden, utan även var denne har befunnit sig och dennes inköpsvanor. Uppgifterna om transaktioner kan dessutom innehålla känsliga uppgifter i personuppgiftslagens mening, t.ex. genom att avslöja den enskildes vårdgivare.

Risken för dataintrång är betydligt högre om man använder sig av enbart lösenord för autentisering, än om man utöver lösenord använder sig av ytterligare någon faktor vid autentiseringen. Den ökade risken beror naturligtvis på att det är lättare att komma åt enbart ett lösenord, än att skaffa sig åtkomst till exempelvis både någons bankkort eller smarta telefon och lösenordet. Dessutom är det lättare för en användare att upptäcka att man har blivit av med till exempel sitt bankkort eller sin smarta telefon, än att någon obehörig har lyckats avslöja lösenordet.

Datainspektionen gör bedömningen att flera av de uppgifter som man får åtkomst till via Danske Banks app har ett sådant högt skyddsvärde att åtkomsten till dessa uppgifter ska föregås av stark autentisering.

Stark autentisering, också kallat flerfaktorsautentisering, kan realiseras på olika sätt. Det kan ske exempelvis med e-legitimation, men även andra tekniska funktioner för asymmetrisk kryptering samt vissa lösningar för engångslösenord och liknande kan användas. Inom bankväsendet används redan idag den typen av lösningar, vilket talar för att kostnaden för att införa en starkare autentiseringslösning inte skulle behöva bli orimligt hög.

Frågan är då om den av Danske Bank föreslagna lösningen innebär stark autentisering.

Danske Banks lösning skulle visserligen kunna tillföra en andra faktor till autentiseringen, men det finns ett antal problem.

För det första är det inte möjligt att genom behavioral biometrics med säkerhet avgöra om det är en behörig person som vill ha åtkomst till uppgifterna.

I vedertagna lösningar för flerfaktorsautentisering finns bara två värden för resultatet av autentiseringen, behörig eller obehörig. Man kan direkt efter implementeringen av lösningen avgöra om en person är behörig eller inte. Lösningen med behavioral biometrics bygger däremot på sannolikhetsberäkningar.

När en person ska autentiseras genom behavioral biometrics samlar systemet in mätvärden för hastigheten och tangenttrycket från inmatningen av PIN-koden. Systemet kontrollerar om mätvärdena ligger innanför gränsvärdena för den tidigare framtagna profilen. Ju vidare gränsvärdena är desto lägre är sannolikheten för att det är den behöriga användaren som försöker få åtkomst och ju snävare gränsvärdena är desto högre är sannolikheten för det.

Om man sätter för vida gränsvärden finns risken att andra än den behörige användaren får åtkomst till uppgifterna och att autentiseringen i praktiken sker med endast en faktor, dvs. PIN-koden.

För det andra ställer Datainspektionen sig tveksam till påståendet att det räcker med tre till fem mätvärden för att upprätta en profil med så snäva gränsvärden att Danske Bank vid varje tillfälle med tillräckligt stor sannolikhet kan avgöra att det är just den behöriga användaren som vill ha åtkomst.

För det tredje sker autentiseringen med endast en faktor fram till dess att man efter den initiala implementeringen av lösningen har tillräckligt många mätvärden för att kunna skapa en profil.

För det fjärde är det rimligt att anta att tiden mellan knapptryckningarna förändras när en användare byter från en apparat med en viss skärm till en annan apparat med till exempel en större skärm och att det leder till att mätvärden i profilen blir oanvändbara och att Danske Bank måste börja om med insamlingen av mätvärden . Även under den perioden sker autentiseringen med endast en faktor.

För det femte har Danske Bank inte beskrivit hur banken avser att säkerställa att det är just den behöriga användaren som genomför de inmatningar som ligger till grund för profilen. Profilen skulle kunna bygga på någon obehörig persons beteendemönster, vilket ger denne åtkomst till de integritetskänsliga uppgifterna.

För det sjätte förändras normalt en människas beteende beroende på i vilket sinnestillstånd personen befinner sig. Beteendet kan även variera beroende på i vilken situation appen används. Detta borde leda till att gränsvärdena måste sättas ganska vida för att inte avvisa även den behöriga användaren. Detta riskerar att leda till att autentiseringen inte blir tillräckligt säker.

För det sjunde är lösningen med behavioral biometrics inte beprövad. Av materialet som Danske Bank har gett in framgår att lösningen till dags dato inte har använts i större skala och under verkliga förhållanden. Datainspektionen känner inte till att något försök med behavioral biometrics har blivit så framgångsrikt att man har ersatt traditionella starka autentiseringslösningar med en sådan lösning.

Vid en samlad bedömning finner Datainspektionen att den av Danske Bank föreslagna lösningen inte tillför autentiseringen en andra faktor och att den således inte innebär stark autentisering av användarna. Danske Bank kan därför inte anses uppfylla kraven på säkerhetsåtgärder enligt 31 § personuppgifts-

lagen när det gäller åtkomsten till integritetskänsliga personuppgifter via bankens appar. Det finns därför anledning att förelägga Danske Bank, enligt 45 § första stycket personuppgiftslagen, att genomföra åtgärder som innebär att åtkomst till integritetskänsliga personuppgifter i Danske Bank A/S, Sverige Filials appar föregås av stark autentisering av användarna.

Hur man överklagar

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Inspektionen måste ha fått ert överklagande inom tre veckor från den dag ni fick ta del av beslutet, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Kristina Svahn Starrsjö i närvaro av chefsjuristen Hans-Olof Lindblom, juristen Malin Fredholm och IT-säkerhetsspecialisten Adolf Slama, föredragande.

Kristina Svahn Starrsjö

Adolf Slama