BODFORSS

Granskning av säkerheten och skyddet mot bedrägerier för privatkunders bankkonton

Analytiker: Rikard Bodforss
Thomas Lilja
Erik Orrsjö
Christopher Rawlings

Datum: 2021-04-12
Version: 1.0
Uppdragsgivare: Ulf Stenberg, Villaägarna Produktgranskning

Innehåll

1 SAMMANFATTNING

Bodforss Consulting AB har på uppdrag av Villaägarna Produktgranskning genomfört en granskning av ett antal bankers skydd mot bedrägerier riktade mot privatkunders bankkonton. Vi har jämfört de olika bankernas metoder för att autentisera användare och vilka ytterligare steg som krävs för att genomföra olika transaktioner i internetbanken. Vi har också bedömt vilka autentiseringsmetoder som bäst står emot olika försök till bedrägerier.

Vi konstaterar i vår granskning av bankerna att alla banker vi har tittat på har haft en god säkerhetsnivå över lag. Det skiljer lite mellan bankerna på hur man betraktar tillförlitligheten i olika autentiseringsmetoder och bankerna har valt lite olika nivå på när man måste identifiera sig eller signera en transaktion.

Enligt vår bedömning är Mobilt BankID i kombination med en QR-kod den metod som är svårast för en bedragare att kringgå, eftersom den kräver att enheten som innehåller det Mobila BankIDt måste vara nära enheten som ska logga in, samt att Mobilt BankID skriver ut var man identifierar sig eller vad det är man signerar. Enklast för en bedragare är bankdosor eller kortläsare som inte är kopplade till en dator.

Som användare kan man påverka sin säkerhetsnivå genom att undvika att använda riskfyllda autentiseringsmetoder, samt att aldrig lämna ut engångskoder eller annan autentiseringsinformation till någon annan.

Om någon ringer upp dig, utger sig för att vara din bank och ber dig identifiera dig, lägg på luren.

2 INLEDNING

2.1 BAKGRUND

Villaägarnas Riksförbund har sedan starten 1952 arbetat för att driva de frågor som är viktiga för småhusägare och arbetat för att göra deras vardag enklare. Som ett led i detta arbete låter man inom ramen för sin verksamhet Villaägarna Produktgranskning granska sådant som funkar mindre väl, inte alls eller har bristande hållbarhet och säkerhet.

De flesta privatpersoner hanterar idag majoriteten av sina bankärenden elektroniskt. I takt med att tillgängligheten ökat och att fler och fler har börjat utföra sina bankärenden på Internet har också bankbedrägerier riktade mot användarna av internetbankerna ökat kraftigt i omfattning.

Villaägarna Produktgranskning har sedan tidigare låtit granska de utmaningar som är förknippade med elektronisk legitimering ur säkerhetssynpunkt och utifrån ett konsumentperspektiv. Detta resulterade i rapporten ”Säkerhet vid elektronisk legitimering och underskrift”[1] skriven av Fredrik Ljunggren på Kirei. I sin rapport konstaterar Fredrik att två av de vanligaste sätten att begå bedrägerier med e-legitimation är:

> ”1. Bedragaren tar kontakt med offret via telefon och övertalar offret att genomföra vissa åtgärder på sin internetbank. Bedragarna utger sig ofta att vara från banken, och kontakten sker under förevändning att några obehöriga transaktioner sker på kontot, och att innehavaren måste legitimera sig för att de ska kunna stoppa transaktionerna.
>
> 2. Bedragaren tillskansar sig en e-legitimation i någons namn på obehörig väg, t.ex. genom användande av förfalskade fysiska legitimationshandlingar, för att denna väg öppna ett bankkonto och sedan i nästa steg hämta hem ett BankID som kan nyttjas för att ta nya lån eller överföra pengar från konton i annan bank.”

Bodforss Consulting har på uppdrag av Villaägarna Produktgranskning gjort en djupdykning i det första scenariot ovan i en ansats för att kartlägga och jämföra de säkerhetskontroller som finns på plats för att förhindra liknande brott. Det vill säga de fall där kunderna utsätts för bedrägeriförsök bestående av att bedragarna kontaktar dem och utger sig för att vara banken eller någon annan betrodd part för att få olovlig tillgång till deras internetbank.

En frågeställning som Villaägarna ville ha svar på var om Mobilt BankID kan anses lika säkert som andra autentiseringsmetoder som BankID på kort och personlig bankdosa (Digipass). Förändras exempelvis säkerhetsmodellen av att banken använder sig av en QR-kod vid inloggningen?

I tillägg till detta har vi även granskat vilka kontroller som finns på plats för att försvåra för någon som redan är autentiserad mot en annan persons internetbank att agera i syfte att föra över tillgångar till ett konto som står under bedragarens kontroll.

2.2 OMFATTNING

Vi har granskat några av de bland privatkunderna vanligast förekommande bankerna i Sverige:

- Nordea (Nordea Bank AB)

[1] https://www.villaagarna.se/globalassets/dokument/press-bilagor/elektronisk-legitimering-och-underskrift-2019-01-23-slutversion.pdf

- Swedbank (Swedbank AB)
- SEB (Skandinaviska Enskilda Banken AB)
- Handelsbanken (Svenska Handelsbanken AB)
- ICA Banken (ICA Banken AB)
- Länsförsäkringar bank (Länsförsäkringar Bank AB)

Vi har även tittat på säkerhetslösningarna hos två nischbanker i något begränsad omfattning:

- Forex (FOREX Bank AB)
- Avanza (Avanza Bank Holding AB)

Valet av banker som vi har granskat har gjorts genom att välja de banker där våra anställda med familj hade bankengagemang. Principerna kan dock appliceras på alla banker så läsaren kan använda våra kriterier för att göra en egen bedömning av sin banks säkerhetslösning.

2.3 AVGRÄNSNINGAR

Vi har i vår analys inte genomfört några faktiska transaktioner av tillgångar mellan konton vilket innebär att eventuella rimlighetskontroller baserade på beteendeanalys eller riskklassificering av transaktioner som används av bankerna inte har utvärderats.

Vi har även under hela denna granskning hållit oss inom ramarna för normalt användande, det vill säga vi har inte på något sätt försökt att kringgå bankernas säkerhetskontroller genom att utnyttja eventuella sårbarheter i kod eller i implementationen av säkerhetskontrollerna.

Bankerna utvecklar kontinuerligt sina riskmodeller och justerar därför ibland vilka säkerhetskontroller som implementeras. Bedömningen är därför en ögonblicksbild av bankernas lösningar vid tiden då rapporten skrevs.

2.4 BEGREPP OCH FÖRKORTNINGAR

Autentiseringsenhet – Den dosa, telefon, eller kort som innehåller användarens hemliga nycklar och används för att identifiera användaren vid inloggning och signering.

Autentisering och elektronisk legitimering – Att identifiera sig som person med hjälp av en e-legitimation eller andra autentiseringsmetoder som bankdosa, lösenord och engångskoder. Elektronisk legitimering och autentisering är egentligen inte synonyma, men i denna granskning utgör legitimeringen oftast autentiseringen mot internetbanken och vi använder därför här begreppen synonymt.

Signering – I denna rapport handlar det uteslutande om elektronisk signering. Det kan likställas med att skriva under med sin namnteckning. Elektronisk signering använder sig av matematiska funktioner (kryptografiska algoritmer) som kombinerar indata som ska signeras med användarens hemlighet som finns lagrad i bankdosan eller BankIDt och räknar ut en svarskod som kan verifieras av banken.

BankID - Ett e-legitimeringssystem som är framtaget och förvaltas av Finansiell ID-Teknik BID AB. Används av över 80% av Sveriges befolkning (16+ år)[2]. BankID finns i tre varianter: BankID på kort,

[2] https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2019/banktjanster-och-handel/

BankID på fil och Mobilt BankID. BankID kan användas för att skapa engångskoder för legitimering (autentisering) och signaturer.

Kortläsare – En enhet som kan läsa smarta kort. Den kan vara utformad med eller utan knappsats och display och vara antingen fristående eller kopplas med sladd till dator. Kortet som stoppas i läsaren är det som innehåller användarens unika hemlighet som används för att skapa engångskoder och signaturer.

Bankdosa – En dosa som innehåller en unik personlig kryptografisk hemlighet som används för att skapa engångskoder och signaturer.

PIN-kod – Personal Identification Number, en personlig hemlig kod som oftast består av siffror för att exempelvis låsa upp en bankdosa eller auktorisera en transaktion med ett kreditkort.

QR-kod – Quick Response kod, en slags tredimensionell streckkod som kan innehålla olika information som en webbadress, eller ett transaktionsID.

Kontrollkod – En slumpmässig sifferkod som ska användas av autentiseringsenheten för att skapa en svarskod med hjälp av hemligheten och en kryptografisk algoritm.

TOTP - Time-based One-time Password, en algoritm som genererar en engångskod baserat på tidpunkten för när inloggningen påbörjades.

3 SÄKERHETSANALYS AV AUTENTISERINGSMETODER

Flera banker i Sverige införde tidigt flerfaktorsautentisering för sina internetbanker. Flerfaktorsautentisering innebär två eller fler faktorer av *någonting man vet* (till exempel lösenord och användarnamn), *någonting man har* (exempelvis digitalt certifikat eller en telefon), eller *någonting man är* (biometri som fingeravtryck eller ansiktsigenkänning). Genom att använda sig av flera faktorer ökas säkerheten i autentiseringen och risken för stulna autentiseringsuppgifter minskar.

Vid ett fysiskt besök på ett bankkontor så får man legitimera sig med fotolegitimation när man ska utföra transaktioner. Även här kan man se det som att det blir en tvåfaktorautentisering eftersom du visar upp din legitimation (*någonting du har*) och banktjänstepersonen verifierar att det är du på bilden (*någonting du är*).

En bankdosa eller BankID kombinerar två faktorer eftersom det är *någonting man har* (dosan eller BankIDt) och PIN-koden som är *någonting man vet*. För ett mobilt BankID kan man välja att använda sig av biometri i stället för PIN-kod och då blir den andra faktorn *någonting man är* (fingeravtrycket eller ansiktet).

Varje faktor som används skapar ett visst mått av omak för den som ska autentisera sig och valet av faktorer måste därför vägas mot värdet av en starkare autentisering. När det gäller bankernas bedömning av vilken nivå av autentisering som krävs för internetbanken så har man historiskt gjort olika riskbedömningar. På senare år har det skett en konvergens kring användandet av BankID och kanske främst Mobilt BankID för autentisering, även om de flesta bankerna stödjer flera olika autentiseringsmetoder. Flera banker har fortfarande kvar olika varianter av bankdosor och det skiljer sig fortfarande lite mellan bankerna vilken autentiseringsmetod som man litar mest på.

Rätt använda så är alla autentiseringsmetoder säkra, men mycket av säkerheten ligger i att utbilda användarna i att skydda sina inloggningsuppgifter på ett bra sätt. Det breda utbudet av olika autentiseringslösningar har också gjort att det är svårt för användarna att förstå vad som är skyddsvärt. Detta har gett upphov till bedrägerimetoder där offer luras att ”låna ut” engångskoder till bedragare som kapat kompisens Facebookprofil.

Anledningen att det råder förvirring kring vad som är skyddsvärt är troligen att för en användare är det svårt att förstå skillnaden på en personlig bankdosa och en kortläsare där kortet innehåller hemligheten. Detta har drivit på bankernas säkerhetsarbete och man arbetar mycket med att utbilda användarna, samtidigt som man går mer mot att försöka knyta autentiseringsenheten till den enhet där man loggas in.

De äldre varianterna på bankdosor bygger antingen på att de genererar en tidsbaserad engångskod, skapar en engångskod av en kontrollkod, eller en kombination av båda. Svagheten kring dessa ligger i att de är helt frånkopplade från autentiserings- eller signeringsförloppet och det är dessa som historiskt varit utsatta för olika bedrägeriscenarion.

Även Mobilt BankID har tidigare varit skiljt från den enhet som användaren autentiserar sig på, men den har däremot fördelen av att skriva ut i klartext var man identifierar sig eller vad man signerar. På senare tid har QR-koder börjat användas av fler och fler banker för att fysiskt knyta det mobila BankIDt till enheten som autentiseras. BankIDs QR-koder innehåller en textsträng som påminner om en webblänk men som är menad för BankID och inte för webbläsaren (exempel: bankid://autostarttoken=f5adeda0-3e37-4558-92a9-f79124355058). QR-kodens sessionsidentifierare (token) identifierar autentiseringssessionen unikt. För att försvåra för en bedragare att starta en

autentiseringssession och vidarebefordra QR-koden till offret är koderna bara giltiga några sekunder. Tiden varierar mellan olika implementationer men varierar mellan 1-30 sekunder.

Vid användning av Mobilt bankID i kombination med en banks mobilapplikation eller mobilens webbläsare så skickas sessionsidentifieraren (token) mellan bankens mobilapplikation och Mobiilt BankID, så QR koden visas aldrig för användaren.

Förutom flerfaktorautentisering så är de faktorer som påverkar hur säker en autentisering är mot olika bedrägeriscenarior:

1. Om det är tydligt för användaren var man identifierar sig eller vad man signerar, *synlighetsprincipen*.
2. Om det finns en koppling mellan autentiseringsenheten och enheten som loggas in, *närhetsprincipen*.
3. Att kontrollkod och svarskod har begränsad giltighet och inte kan återanvändas, *tidsaspekten*.

3.1 Rangordning av autentiseringsmetoders skydd mot bedrägeriförsök

Med bakgrund av ovanstående kan man rangordna olika autentiseringsmetoder som används i olika banksammanhang. Vi har rangordnat dem i fallande ordning från de med sämst skydd mot bedrägliga metoder till de som är svårast att kringgå för en bedragare. Autentiseringsmetoderna med minst skydd är inte mindre säkra ur teknisk synvinkel, men de kräver att användaren tar ett större ansvar för att skydda dem mot obehöriga och därmed ökar risken för fullbordat bedrägeri.

3.1.1 Minst skydd

- Lösenord eller lösenfraser
- Utskrivna engångskoder (kodkort, återställningskoder)

Lösenord eller lösenfraser ger det sämsta skyddet mot bedragare eftersom användare ofta själva synkroniserar lösenord mellan olika tjänster. Det är också relativt lätt att lura en användare till att avslöja sitt lösenord genom bedrägliga epostmeddelanden och falska internetsajter och ett lösenord har ofta väldigt lång giltighetstid. Lösenord ska endast användas i kombination med en andra faktor för skydd av känsliga konton och man ska aldrig återanvända lösenord mellan olika tjänster. En lösenordshanterare som skapar slumpmässiga och svårgissade lösenord är bra att använda där lösenord är enda metoden för autentisering.

Utskrivna engångskoder kan vara ett bra komplement till andra metoder för autentisering, eller som reservmetod om man har tappat bort sin mobiltelefon, men användaren måste skydda dem väl från obehöriga. Den största bristen med utskrivna engångskoder eller skrapkort med koder är att koderna är giltiga tills de har använts eller tills en senare kod i listan används. Detta gör att om en bedragare kommer över engångskoderna så är det ingen tidspress att använda dem.

Tidsaspekten, dvs bedragarna saknar tidspress om de kommer över lösenord eller utskrivna engångskoder, gör att dessa metoder måste anses ha lägst skydd mot bedrägeri.

3.1.2 Medelbra skydd

- Tidsbaserade engångskoder (TOTP, Microsoft Authenticator, Google Authenticator, osv.)
- Bankdosa
- Kortläsare utan sladd
- Mobilt BankID utan QR-kod

Tidsbaserade engångskoder, antingen genererade av en applikation eller en koddosa, är en relativt säker metod för att skapa en andra faktor. Även bankdosor, kortläsare och Mobilt BankID är säkra om hanteringen av dem sker på ett säkert sätt. De saknar dock *närhetsprincipen* eftersom autentiseringsenheten är helt frikopplad från den enhet som användaren loggar in på.

Bristen i banksammanhang ligger i att tidsbaserade engångslösenord och genererade engångslösenord från kontrollkoder brister i *synlighetsprincipen* då de saknar koppling till vad det är man identifierar sig mot eller signerar. Detta kan utnyttjas av en bedragare som utger sig för att komma från banken och användaren kan luras att lämna ifrån sig koder som kan användas för inloggning och signering. Bankerna informerar tydligt att när man exempelvis signerar en transaktion med belopp så ska man kontrollera att beloppet är korrekt, men i ett telefonsamtal kan en bedragare lura användaren att signeringen bara är en identifiering. Att exempelvis signera koden 2152 2391 kan i själva vara en auktorisation för en transaktion på 215 223 kr och 91 öre.

Mobilt BankID är något bättre än de andra alternativen i listan eftersom det även använder sig av *synlighetsprincipen* där det oftast tydligt framgår av texten var man identifierar sig eller vad det är man signerar. Det finns dock ändå en risk att användaren kan luras att signera transaktioner genom att bedragaren skapar en stressituation i signeringsögonblicket.

3.1.3 Bäst skydd

- Kortläsare med sladd (BankID på kort)
- Mobilt BankID med QR-kod
- Kortläsare med QR-kod

Dessa har det starkaste skyddet mot bedragare, eftersom de kombinerar styrkorna från gruppen innan med *närhetsprincipen* genom en koppling till den enhet där användaren försöker logga in. QR-koden säkerställer förvisso inte fysisk kontakt, men ger ändå en ytterligare försäkran om att användaren som försöker logga in har autentiseringsenheten (telefonen eller bankdosan) i närheten.

QR koderna har en kort livslängd som varierar mellan 1-30 sekunder. Vi testade att skicka QR-koden med epost till en annan person för att försöka dela på autentiseringsenhet och inloggningen. Det var möjligt i de fall QR koden var giltig i 30 sekunder, men då måste den som ska ta emot koden vara beredd och snabb. Det är osannolikt att det skulle fungera i ett bedrägeriscenario, men vi vill ändå rekommendera de banker som använder metoden att byta ut QR koden oftare.

Återigen vill vi framhålla en stor fördel med Mobilt BankID som även använder sig av *synlighetsprincipen* och visar var man legitimerar sig eller vad man signerar. Hur utförlig beskrivningen av transaktionen är i texten är upp till banken som har implementerat lösningen.

4 TESTFÖRFARANDE

Vi har jämfört nivån på de säkerhetskontroller som finns på plats för att skydda kunderna från bedrägeriförsök genom att simulera olika testfall. För att kunna åstadkomma detta har vi använt ett flertal mobiltelefoner och datorer i kombination med kortläsare utfärdade från de olika bankerna. Utgångspunkten har varit att en tänkt bedragare inte har fysisk närhet till enheten som används för att legitimera offret.

4.1 TESTFALL 1 – ÅTKOMST TILL INTERNETBANK

I det första testfallet har vi utvärderat hur svårt det är för en bedragare att få tillgång till offrets internetbank genom att försöka ansluta till internetbanken från en annan dator eller mobil enhet som inte innehåller eller är kopplat till autentiseringsenheten.

Utvärderingskriterier:
Vilka autentiseringsmetoder tillåts?
Finns det några sätt att runda säkerhetskontrollerna som skall förhindra att fel person legitimeras?

4.2 TESTFALL 2 – ÖVERFÖRING AV TILLGÅNGAR

I det andra testfallet har vi undersökt vilka, om några, tekniska kontroller som finns på plats för att begränsa bedragarens förmåga att föra över tillgångar från offret efter att ha lyckats logga in på internetbanken.

Utvärderingskriterier:
Hur många identifikationer/signeringar krävs för att föra över pengar till ny mottagare?
Finns det några begränsningar i vad som tillåts baserat på olika identifieringsmetoder?
Har man ytterligare skyddsåtgärder?

4.3 TESTFALL 3 – SKAPA NYTT BANKID

Det tredje testfallet är ett skräckscenario där en bedragare lyckas utfärda ett nytt Mobilt BankID till sin egen telefon. Detta kan sedan användas för att agera som offret utan att behöva lura av offret fler koder.

Utvärderingskriterier:
Vad krävs för att skapa ett nytt BankID?
Finns det några ytterligare skyddsmekanismer för att stoppa bedrägerier?

Resultaten av de olika testfallen har sedan vägts samman med eventuella kompenserande kontroller för att göra en helhetsbedömning. För att underlätta för läsaren och skapa en översiktlighet, har vi även utifrån helhetsbedömningen betygsatt säkerheten för respektive bank. Där har vi använt en traditionell 1-5 skala, där

1 = underkänd säkerhet
2 = godkänd säkerhet
3 = hög säkerhet
4 = mycket hög säkerhet
5 = extremt hög säkerhet

5 ANALYS

5.1 SEB

5.1.1 Testfall 1 Inloggning

SEB kräver QR-kod vid inloggning med Mobilt BankID, men har fortfarande kvar möjligheten att använda sig av bankdosa som saknar närhetsprincipen. Det är ett minus att bankdosa fortfarande anses som lika stark autentisering som Mobilt BankID med QR-kod, då bankdosan saknar både *närhetsprincipen* och *synlighetsprincipen*.

SEBs QR-kod byts varje sekund.

5.1.2 Testfall 2 Överföring

Vid överföring eller betalning till ny mottagare behöver man inte signera nya mottagare, däremot signeras alla transaktioner i klump när man skickar dem för betalning. Det är ingen skillnad mellan förtroendet för Mobilt BankID eller bankdosa, så den största risken för bedrägerier torde vara vid användningen av bankdosor.

5.1.3 Testfall 3 Utfärda BankID

Ett nytt Mobilt BankID går att skapa med både bankdosa och BankID. Som extra säkerhetskontroll vid beställning av BankID skickas även en engångskod till registrerad mobiltelefon. Detta utgör ett extra hinder för en bedragare, men det är inte omöjligt att lura en användare att även uppge en engångskod som skickas till mobilen.

SEB har en ytterligare säkerhetsåtgärd första gången ett nytt BankID används för att logga in på internetbanken. Användaren måste då verifiera det nya BankIDt med en annan autentiseringsmetod (befintligt BankID, SMS eller bankdosa). Detta ökar skyddet för om en bedragare skulle lyckas skaffa sig ett BankID på ett bedrägligt sätt. Verifieringen sker oavsett om det är SEB eller någon annan som har utfärdat det nya BankIDt.

5.1.4 Sammanfattning

SEB har en generellt hög säkerhet och har dessutom implementerat ytterligare verifiering av nya BankID, vilket är bra. Det är mindre bra att man fortfarande litar lika mycket på bankdosan som är lättare för en bedragare att utnyttja. Vi ger SEB:s säkerhet betyget 3.

5.2 NORDEA

5.2.1 Testfall 1 Inloggning

Nordea kräver QR-kod vid inloggning med Mobilt BankID, men har fortfarande kvar möjligheten att använda sig av kortläsare som saknar närhetsprincipen. Det är ett minus att en lös kortläsare anses som lika stark autentisering som Mobilt BankID med QR-kod, då den brister i fråga om *närhetsprincipen* och *synlighetsprincipen*. Nordea har tagit fram en ny kortläsare som även kan läsa av QR-koder vilket är mycket bra för användare som inte har tillgång till mobiltelefon. Troligen kommer banken på sikt att fasa ut stödet för de gamla kortläsarna, som inte bygger på *närhetsprincipen* och *synlighetsprincipen*, men vid tillfället för testen gick de fortfarande att använda.

Ett litet minus för att Nordeas QR-koder visas i 30 sekunder.

5.2.2 Testfall 2 Överföring

Vid överföring eller betalning till ny mottagare behöver man inte signera nya mottagare, däremot signeras alla transaktioner i klump när man skickar dem för betalning. Det är ingen skillnad mellan förtroendet för Mobilt BankID eller kortläsare, så den största risken för bedrägerier torde vara i användningen av kortläsare tills alla är utbytta mot modeller som stödjer QR-kod.

5.2.3 Testfall 3 Utfärda BankID

Ett nytt Mobilt BankID går att skapa med både kortläsare och BankID.

5.2.4 Sammanfattning

Nordea har en generellt hög säkerhet och håller på att rulla ut kortläsare med stöd för QR-koder. När dessa är på plats och de gamla kortläsarna har fasats ut kommer Nordea att ha mycket gott skydd mot bedrägerier. Tiden som QR-koden visas skulle också kunna kortas. Nordeas säkerhet får 4 i betyg.

5.3 SWEDBANK

5.3.1 Testfall 1 Inloggning

Swedbank kräver QR-kod vid inloggning med Mobilt BankID, men har fortfarande kvar möjligheten att använda sig av bankdosa som saknar närhetsprincipen. Det är ett minus att bankdosa fortfarande anses som lika stark autentisering som Mobilt BankID med QR-kod, då bankdosan saknar både *närhetsprincipen* och *synlighetsprincipen*.

Swedbanks QR-kod byts varje sekund.

5.3.2 Testfall 2 Överföring

Här skiljer sig Swedbank markant från de övriga storbankerna genom att nya betalnings- eller överföringsmottagare måste signeras innan man kan lägga upp ett betalningsuppdrag. Det som är anmärkningsvärt är att Swedbank inte tillåter att man lägger upp nya mottagare om man har loggat in med Mobilt BankID. För detta krävs att man aktiverar ”utökad användning” och autentiserar sig ytterligare med engångskoder. ”Utökad användning” krävs också om man ska förändra beloppsgränser för Swishbetalningar. Detta är självklart säkerhetshöjande åtgärder som minskar risken för bedrägerier radikalt, men den begränsningen finns inte om man använder bankdosan.

Enligt vår bedömning så motverkar säkerhetsåtgärderna med engångskoder övergången till en säkrare autentisering, då det är lättare att utföra sina bankärenden med bankdosan. Här bedömer vi att Swedbank har tänkt lite galet i sitt riskarbete genom att favorisera en osäkrare autentiseringsmetod.

5.3.3 Testfall 3 Utfärda BankID

Ett nytt mobilt BankID går att utfärda med bankdosa eller BankID efter ny scanning av QR-kod.

5.3.4 Sammanfattning

Swedbank har ett mycket gott skydd mot bedrägerier riktade mot Mobilt BankID och en generellt hög säkerhetsnivå i övrigt. Bankens riskbedömning känns dock inte riktigt genomtänkt när man föredrar bankdosan framför Mobilt BankID med QR-kod. Detta bedömer vi motverkar övergången till säkrare autentiseringsmetoder. Swedbank får betyget 3 för sin säkerhet.

5.4 HANDELSBANKEN

5.4.1 Testfall 1 Inloggning

Handelsbanken kräver QR-kod vid inloggning med Mobilt BankID, men har fortfarande kvar möjligheten att använda sig av en lös kortläsare som saknar närhetsprincipen. Det är ett minus att en lös kortläsare anses som lika stark autentisering som Mobilt BankID med QR-kod, då den saknar både *närhetsprincipen* och *synlighetsprincipen*. Bankens kortläsare går att ansluta med sladd, men det är inget krav vid inloggning.

QR-koden byts var tredje sekund.

5.4.2 Testfall 2 Överföring

Handelsbanken kräver att man signerar nya mottagare innan man kan lägga upp betalningsuppdrag. Det finns också olika beloppsgränser för nya respektive ”etablerade” mottagare vilket ytterligare skyddar mot bedrägliga transaktioner. En mottagare anses vara ”ny” i 21 dagar.

5.4.3 Testfall 3 Utfärda BankID

Vid utfärdande av nytt mobilt BankID krävs antingen Mobilt BankID med QR kod eller att kortläsaren ansluts med sladd, vilket är mycket bra. Detta försvårar för en bedragare att utfärda BankID.

5.4.4 Sammanfattning

Handelsbanken har en generellt hög säkerhetsnivå och känns som den bank som har den mest genomtänkta riskprofilen för identifiering av kunderna. Det finns förbättringsområden, som att begränsa möjligheten till inloggning utan närhetsprincipen, men det skulle innebära inskränkningar i kundernas valmöjligheter kring inloggningen. Handelsbanken får betyget 4 för sin säkerhet och är dessutom bästa bank i detta säkerhetstest.

5.5 ICA-BANKEN

5.5.1 Testfall 1 Inloggning

ICA Banken kräver QR-kod vid inloggning med Mobilt BankID, men har fortfarande kvar möjligheten att använda sig av bankdosa som saknar närhetsprincipen. Det är ett minus att bankdosa fortfarande anses som lika stark autentisering som Mobilt BankID med QR-kod, då bankdosan saknar både *närhetsprincipen* och *synlighetsprincipen*.

Ett litet minus för att ICA Bankens QR-koder visas i 30 sekunder.

5.5.2 Testfall 2 Överföring

Vid överföring eller betalning till ny mottagare behöver man inte signera nya mottagare, däremot signeras alla transaktioner i klump när man skickar dem för betalning. Det är ingen skillnad mellan förtroendet för Mobilt BankID eller bankdosa, så den största risken för bedrägerier torde vara i användningen av bankdosor.

5.5.3 Testfall 3 Utfärda BankID

Ett nytt Mobilt BankID går att skapa med både bankdosa och BankID.

5.5.4 Sammanfattning

ICA Banken har en generellt hög säkerhetsnivå, men med ett minus för att man litar lika mycket på bankdosan som på ett Mobilt BankID med QR-kod. Tiden som QR-koden visas skulle kunna kortas. ICA Banken får betyget 3 för sin säkerhet.

5.6 LÄNSFÖRSÄKRINGAR BANK

5.6.1 Testfall 1 Inloggning

Länsförsäkringar bank kräver QR-kod vid inloggning med Mobilt BankID, men har fortfarande kvar möjligheten att använda sig av bankdosa som saknar närhetsprincipen. Det är ett minus att bankdosa fortfarande anses som lika stark autentisering som Mobilt BankID med QR-kod, då bankdosan saknar både *närhetsprincipen* och *synlighetsprincipen*.

Ett litet minus för att Länsförsäkringars QR-koder visas i 30 sekunder

5.6.2 Testfall 2 Överföring

Vid överföring eller betalning till ny mottagare behöver man inte signera nya mottagare, däremot signeras alla transaktioner i klump när man skickar dem för betalning. Det är ingen skillnad mellan förtroendet för Mobilt BankID eller bankdosa, så den största risken för bedrägerier torde vara i användningen av bankdosor.

5.6.3 Testfall 3 Utfärda BankID

För att utfärda nytt Mobilt BankID krävs signering med bankdosa. (Uppgiften är hämtad från Länsförsäkringars hemsida, då vi inte hade möjlighet att testa att utfärda ett nytt BankID på Länsförsäkringar bank)

5.6.4 Sammanfattning

Länsförsäkringar har en generellt hög nivå av säkerhet. Ett minus för att man visar QR-koden i 30 sekunder och att bankdosan har samma förtroendenivå som Mobilt BankID med QR-kod. Länsförsäkringar Bank får betyget 3 i säkerhet.

5.7 FOREX BANK

Forex bank har avyttrat sin vanliga bankverksamhet till ICA banken. Befintliga bankkunder kommer att flyttas dit. Testerna har genomförts på ett inlåningskonto, varför några av testfallen inte var möjliga att genomföra.

5.7.1 Testfall 1 Inloggning

Forex kräver QR-kod eller anslutet BankID på fil eller kort, vilket är mycket bra. Det är enda banken vi testat som har krav på närhetsprincipen.

Ett litet minus för att Forex QR-koder visas i 30 sekunder

5.7.2 Testfall 2 Överföring

Vid överföring eller betalning till ny mottagare behöver man inte signera nya mottagare, däremot signeras alla transaktioner i klump när man skickar dem för betalning.

5.7.3 Testfall 3 Utfärda BankID

Ej testat. Kontotypen har ingen möjlighet att utfärda BankID.

5.7.4 Sammanfattning

Forex är den enda testade banken som ställer krav enligt närhetsprincipen fullt ut. Vid överföring till andra konton krävs ingen separat signering för att lägga till en ny mottagare, överföringen i sig måste dock signeras. Erbjuder över lag bra säkerhet. Forex bankkunder kommer att flyttas till ICA banken,

så testerna av ICA banken kommer att gälla för de som var helkunder i Forex bank tidigare. Forex Bank får betyget 4 för sin säkerhet.

5.8 AVANZA BANK

Avanza bank är en nischbank som fokuserar på sparande och placeringar i värdepapper. Flera av testfallen har därför inte gått att testa.

5.8.1 Testfall 1 Inloggning

För inloggning med Mobilt BankID krävs QR-kod, men Avanza tillåter fortfarande användarnamn och lösenord i kombination med tidsbaserad engångskod.

Ett litet minus för att Avanzas QR-koder visas i 30 sekunder

5.8.2 Testfall 2 Överföring

Ej testat. Man kan bara överföra pengar till egna konton i andra banker.

5.8.3 Testfall 3 Utfärda BankID

Ej testat. Funktionen finns inte hos Avanza bank.

5.8.4 Sammanfattning

Även om man inte kan direkt överföra pengar till konton i andra banker så finns det risker med att ha en låg nivå av säkerhet i inloggningen på banken. En bedragare skulle kunna använda köp och försäljning av värdepapper på ett sätt som skulle kunna gagna bedragarens intressen. Användarnamn och lösenord borde inte förekomma på en internetbank 2021, även om man använder tvåfaktorautentisering genom tidsbaserade engångskoder. Det är oklart varför Avanza har kvar möjligheten när det finns stöd för bättre alternativ. Avanza Bank får betyget 2 för sin säkerhet.

6 SLUTSATSER

Generellt så har svenska banker en hög nivå på säkerheten och vidtar kontinuerligt åtgärder för att försvåra bedrägerier mot sina kunder. Utöver det som vi har testat har bankerna även mekanismer för att identifiera misstänkta transaktioner, både för att motverka bedrägerier och för att uppfylla lagkrav på skydd mot pengatvätt. I vår granskning har vi sett en tydlig trend att bankerna går mot att mer och mer använda Mobilt BankID med QR-kod som främsta alternativ för autentisering och signering av transaktioner, men vi ser också att bankerna har gjort olika riskbedömningar kring hur man litar på olika autentiseringsmetoder. Bankerna gör hela tiden nya bedömningar baserat på hur tekniken går framåt, hur hotbilden ser ut och vad som kan accepteras av kunderna. Säkerhet i autentisering är alltid en avvägning mot bekvämlighet och här kan kunderna fort rösta med fötterna om en bank anses vara för krånglig eller upplevs ha för låg säkerhet.

Det finns tre viktiga principer i arbetet att försvåra för en bedragare som försöker lura en bankkund över telefonen, synlighet, närhet och tid. Med synlighetsprincipen menas att man genom att tydligt visualisera för kunderna vilken transaktion man godkänner så minimerar man risken för att de skall bli lurade. Med närhetsprincipen avses de funktioner som förhindrar möjligheten till inloggning på en enhet som inte finns på samma fysiska plats som den enhet som används för legitimeringen. Tidsaspekten handlar om att begränsa giltigheten för kontrollkoder, engångskoder och QR-koder som används i legitimering eller signering. Då försvårar man för en potentiell bedragare att lyckas komma åt internetbanken eller genomföra obehöriga transaktioner.

Vid legitimering via Mobilt BankID är synligheten god, i och med att det tydligt står vad det är man godkänner, medan man vid legitimering via en kortläsare inte har samma typ av återkoppling. Bra exempel på hur närhetsprincipen använts för att höja säkerheten är de QR-koder som introducerats i legitimeringsprocessen via BankID eller de fall där man behöver ansluta sin kortläsare med sladd till den enhet där transaktionen initierades. Detta saknas då man tillåter legitimering via bankdosa, kortläsare utan sladd eller Mobilt BankID utan QR-kod.

Ett flertal av bankerna kräver en separat signering vid tillägg av nya betalningsmottagare och samtliga banker i utvärderingen kräver signering vid skapande av en ny betalningsorder eller utförande av en direktbetalning. I de fall där signering krävs för att lägga till nya betalningsmottagare höjs ribban för bedragarna ytterligare då de i detta fall måste få offret att utföra minst tre olika åtgärder innan de kan komma över några tillgångar, något som förhoppningsvis väcker misstänksamhet hos offret. Ingen av bankerna i utvärderingen tillåter heller utfärdande av BankID eller koppling av ett nytt telefonnummer för Swish utan signering via BankID eller kortläsare.

Vi kan konstatera att ribban har höjts avsevärt den senaste tiden för bedrägeriförsök, åtminstone för de bankkunder som nyttjar Mobilt BankID för legitimering mot sin internetbank. Detta främst i och med införandet av QR-koder i legitimeringsprocessen för Mobilt BankID, vilket genom sitt krav på närhet minimerar risken att fel person legitimeras. QR-koden som förnyas löpande säkerställer att endast den person som har tillgång till QR-koden kan legitimeras. Giltighetstiden på QR-koden är i samtliga fall också så pass kort att det måste anses osannolikt att en bedragare hinner skicka över den till offret och lyckas övertala dem att godkänna inloggningen. De enda fall där QR-kod inte krävs för Mobilt BankID hos de utvärderade bankerna idag är de fall där det Mobila BankIDt finns på samma enhet som inloggningen initierades från. Synligheten hos Mobilt BankID också är god då kunden vid legitimering presenteras med en text som förtydligar vilken typ av transaktion det är som utförs.

Av de banker vi har testat inom ramen för denna granskning är det bara Forex bank som har strikt krav på autentisering med närhetsprincipen. Övriga banker har någon variant som skulle kunna användas för att logga in en enhet som inte kräver strikt närhet. I de fall en bankkund använder sig av en bankdosa eller kortläsare utan sladd för att autentisera sig går det fortfarande att lura till sig tillgång till offrets internetbank då närhetsprincipen satts ur spel. Vid användning av bankdosa eller kortläsare får användaren ingen visuell indikation om vilken typ av transaktion det är som godkänns, vilket också underlättar för en bedragare.

Endast SEB hade en ytterligare verifiering av ett nytt BankID. Det pekar på att utfärdande av BankID kan vara en svag punkt och om någon bank skulle slarva med säkerheten kring utfärdandeprocessen skulle det potentiellt kunna orsaka stor skada.

De svagaste punkterna som vi har identifierat är de autentiseringar och signeringar som görs med bankdosa eller kortläsare utan sladd. Här finns det en risk att en bedragare skulle kunna lura sitt offer att knappa in koder två gånger i sin dosa. Det kan i några fall räcka för att bedragaren ska kunna genomföra en transaktion eller utfärda ett nytt BankID, vilket sedan kan utnyttjas för vidare transaktioner.

Ett stort problem är att många äldre inte har anammat Mobilt BankID utan förlitar sig på bankdosor för att göra sina bankärenden. Det är också denna grupp som i många fall utgör målgruppen för bedragare. Detta gör att riskerna för att äldre blir lurade ökar.

Bankerna har mycket information på sina hemsidor som handlar om säkerhet och bedrägerier och det står varningar vid inloggning på nära nog alla internetbankerna. Problemet är att det inte blinkar några varningar när man knappar in sin PIN-kod i bankdosan. Det är där risken är som störst, inte när man själv loggar in på sin bank.

7 REKOMMENDATIONER

Det finns mycket vi skulle kunna skriva som rekommendationer till de olika bankerna, men många av deras val styrs av risk- och marknadsbeslut som vi inte har insyn i. Förändringar i säkerhetsfunktioner driver också kostnader som slutligen måste finansieras via kunderna och det är förståeligt att man inte vill göra sig helt beroende av en extern tjänst (BankID) för all autentisering och därför behåller gamla bankdosor. Vi väljer därför att främst rikta våra rekommendationer till kunderna.

Vi kan konstatera att alla bankerna vi har granskat fungerar i säkerhetshänseende. Vilken du väljer bör snarare styras av bankens övriga erbjudanden och dina preferenser, men det kan i vissa fall finnas skäl att göra en annan bedömning och ta större hänsyn till säkerhetsaspekten. Många bankbedragare väljer att inrikta sig mot personer som de upplever vara lättare att manipulera som de äldsta grupperna av pensionärer, personer med intellektuell funktionsnedsättning med flera. Som medveten konsument kan man först och främst använda vår genomgång för att välja en bank som passar ens behov av tillgänglighet och nivå av säkerhet. Sedan finns det ett antal säkerhetshöjande åtgärder man kan vidta för att undvika att falla offer för bedragare:

- Banken ringer aldrig upp en kund och ber dem legitimera sig. Om någon ringer och utger sig för att vara din bank och vill att du identifierar dig på något sätt, lägg på luren. Den enda gången banken ber dig identifiera dig över telefon är när du har ringt kundtjänst.
- Klicka inte på länkar i epost som ser ut att vara från banken. Om det verkar spännande eller viktigt, öppna en webbläsare, gå till din bank och logga in där i så fall.
- Förvara ”farliga” autentiseringsmetoder (t.ex. engångskoder) på ett säkert sätt så att ingen obehörig kommer åt dem.
- Använd säkra autentiseringsmetoder som Mobilt BankID med QR-kod när det går. Lägg undan bankdosor tills du måste använda dem.
- Lämna aldrig ut engångskoder eller annan autentiseringsinformation till någon annan.

Om du följer dessa enkla regler är det närmast omöjligt att du faller offer för ett bedrägeriförsök mot ditt bankkonto (vishing-bedrägeri). Det är betydligt vanligare att svenska bankkunder råkar ut för andra slags bedrägerier som kreditkortsbedrägerier i samband med internetköp, annonsbedrägerier där bedragaren förmår intresserade att betala i förskott för varor som sedan aldrig levereras eller investeringsbedrägerier