RAPPORT DEN 18 JUNI 2007

DNR 07-7950-399

2007 : 10

Brottsliga angrepp mot internetbanker

INNEHÅLL

Så skyddar du dig som internetkund

Som kund hos ett företag som erbjuder finansiella tjänster via internet kan du själv bidra till att öka säkerheten och minska risken för brottsliga angrepp.

1. Uppdatera ditt virusskydd och din brandvägg regelbundet.

2. Installera inte program på din dator som du inte vet var de kommer ifrån.

3. Öppna aldrig bilagor i mejl om du inte vet vad de innehåller. Att känna igen avsändaren är inte säkert nog.

4. Var försiktig när du använder andra datorer än din egen, då dessa kanske inte går att lita på.

5. Logga alltid ut från webbplatsen när du inte använder den.

6. Uppge aldrig finansiell information, kontaktuppgifter och liknade på webbsidor som är okända.

7. Kontrollera webbadressen (URL-adressen) för alla webbplatser där du uppmanas att skriva in ID-information. Se till att du är på rätt webbplatsadress och att inte extra tecken lagts till i adressen.

8. Gå aldrig in på en webbplats för finansiella tjänster genom att klicka direkt på en länk i ett mejl eller på en annan webbsida än företagets egna.

9. Använd en pålitlig internetleverantör. Omfattande säkerhetsåtgärder på internetleverantörsnivå är ditt främsta försvar mot så kallad pharming (när du flyttas till en webbplats utan att vara medveten om det).

10. Kontrollera dina saldon och transaktioner regelbundet och gör en anmälan till din leverantör av finansiella tjänster om du ser något som du inte känner igen.

Sist men inte minst:

- Avslöja aldrig ditt lösenord för andra.
- Använd aldrig personlig information i lösenord som enkelt kan listas ut.
- Använd inte samma lösenord till flera olika tjänster.

Sammanfattning

Finansinspektionens kartläggning visar på en ökning av angreppen mot bankernas internetkontor, men relaterat till antalet internettransaktioner är omfattningen av problemet begränsat.

Storbankerna genomför 20 miljoner internettransaktioner varje månad. 2005 utfördes tio lyckade internetangrepp mot kunders konton i Sverige, 2006 hade antalet ökat till knappt 300 lyckade angrepp och förövarna kom över åtta miljoner kronor.

Bankerna bedömer att hoten ökar och att de brottsliga aktiviteterna blir mer avancerade. Fortsatta angrepp kan påverka förtroendet för bankernas tjänster, vilket kan påverka effektiviteten i det finansiella systemet genom att kunderna återgår till manuella tjänster. Det är en utveckling som inte kan anses gynna någon part.

FI gör bedömningen att angreppen mot internetkontoren för närvarande inte hotar stabiliteten i det finansiella systemet. De större aktörerna är väl finansiellt rustade för de risker som verksamheten medför. En ökning av antalet angrepp kan dock skada förtroendet för marknaden som helhet. Det ligger därför både i allmänhetens och företagens intresse att begränsa de bedrägliga attackerna. FI avser inte att detaljregelera vilken säkerhetslösning bankerna ska ha, men kommer noga att följa utvecklingen och analysera riskerna.

Företag som erbjuder finansiella tjänster via Internet bör tydligt informera kunderna om

- Riskerna med Internet
- Vilka säkerhetslösningar som har valts och varför
- Kundens behov av skydd
- Vem som har ansvaret när det uppstår en skada

Även om bankerna i stor omfattning hittills har ersatt kunder som har utsatts för bedrägerier är det ett stort frågetecken hur länge en sådan kundvänlig attityd kommer att bibehållas. Det finns inte särskilt lagreglerat vem som bär det ekonomiska ansvaret för brottsliga angrepp via internet och det förekommer långtgående friskrivningsklausuler i avtal mellan kund och företag. FI anser att företagen bör ha huvudansvaret och kommer att verka för att så blir fallet.

Finansiella tjänster via internet

SAMMANFATTNING
De flesta banker har en avancerad identifiering av kunden. Det är endast några få banker som inte har det och FI ifrågasätter om de har en tillräcklig grad av säkerhet.

De kunder som blivit utsatta har bankerna ersatt. FI har dock uppmärksammat att det förekommer omfattande friskrivningsklausuler i avtal mellan kund och företag. Informationen om dessa samt riskerna med internetanvändningen och säkerhetsnivåer bör bankerna tydligt informera om. Även kundens behov av skydd bör uppmärksammas tydligare.

Användningen av internet mellan bank och kund

Bankerna började med internet år 1996 och numera är det en etablerad väg att nå sin bank. Privatpersoner och företag har stadigt ökat sitt användande av internetbaserade banktjänster.

Från 1997 till 2006 har antalet kunder som utnyttjar internet för finansiella tjänster i de fyra storbankerna ökat från 180 000 till 5,9 miljoner[1] kunder och andelen privatpersoner uppgick till nästan 90 procent.

Uppskattningsvis genererar storbankernas internetkunder 20 miljoner transaktioner varje månad. Den absolut största delen av antalet transaktioner sker utanför internet. Mellan 10-15 procent av storbankernas transaktioner går via internet.

Banker utsätts för olika former av brott. I och med internet har brottslingarna fått ytterligare en kanal in till banken. Bankerna har varit utsatta för internetangrepp alltsedan användningen startade. Det som hänt under de senaste åren är att bankernas kunder också blivit lurade och angripna på olika sätt. Gränsdragningen mellan när det är bankens respektive kunden som angrips är inte klar och behöver ur ansvarshänseende analyseras ytterligare.

På grund av angreppen har FI genomfört en kartläggning av hur bankerna och kunderna blivit angripna och lurade i användningen av internet.

FI har riktat undersökningen mot internet-användningen hos banker, värdepappersbolag och kreditmarknadsföretag. Dessa företag har internettjänster som innebär att kunder kan flytta sina tillgångar och kan därför antas bli intressanta mål för brottsliga aktiviteter.

1 Viss dubbelräkning kan förekomma då man kan vara internetbankkund i flera banker.

Vilka angrips och hur ser angreppen ut?

Mer än 80 procent av bankerna erbjuder finansiella tjänster via internet, samtliga storbanker och några till. Det är vanligare att kunder hos banker använder internet än kunder hos värdepappersbolag och kreditmarknadsbolag. De tjänster som erbjuds är naturligtvis beroende av vilken typ av verksamhet som bedrivs. Den avgjort största tjänsten är betalningsförmedling, dvs möjligheten att betala och ta emot pengar elektroniskt.

Syftet med de angrepp som identifierats och som riktat sig direkt mot banker har varit att utmatta bankernas brandväggar för att på det sättet ta sig in. Banker har temporärt tvingats stänga sina internet-tjänster för att attackerna blockerat alla andra försök att logga in.

Bankernas säkerhetslösningar med brandväggar och andra skyddsåtgärder har hittills varit tillräckliga för att undvika direkta intrång. Angriparna söker därför ytterligare vägar och kan därför inleda angreppet med att först lura bankkunderna.

Under 2005 rapporteras tio kunder ha förlorat pengar. År 2006 skedde en stark ökning av antalet till 294. Sammantaget är den ekonomiska förlust som uppstått för kunderna ungefär åtta miljoner kronor. Den metod som huvudsakligen har använts är att kunden blivit lurad att lämna ifrån sig sina identifikationsuppgifter, s k Phishing. På det sättet har banken kunnat missledas att tro att det har varit en annan person som identifierat sig.

Några kreditmarknadsbolag har uppgett att de varit utsatta för angrepp. Däremot uppgav inget värdepappersbolag att de hade noterat några angrepp genom sina kunder.

Phishing
Phishing innebär att man ”fiskar” efter någon att lura. Den lurade lämnar ut uppgifter som bedragarna vill åt. Vid bedrägerier mot företag som tillhandahåller finansiella tjänster är det t ex kontonummer, personnummer och olika former av lösenord som ”fiskaren” vill åt för att kunna disponera kundens medel.

Massmejl, så kallad spamming, är idag en vanlig metod för att lura kunderna att lämna ifrån sig uppgifter som bedragarna vill åt.

Kunden får ett mejl som ser ut att komma från det finansiella företaget. Ofta uppges supportavdelningen eller någon säkerhetsavdelning vara avsändare. Mejlet kan vara välgjort och svårt att skilja från ett autentiskt meddelande. I mejlet hävdas att någon slags incident inträffat och att kunden måste verifiera vissa data som företaget redan har.

Antingen ska kunden fylla i uppgifter i mejlet och returnera det, eller klicka på en länk som leder kunden till en (falsk) webbsida. De uppgifter som begärs förefaller ofta harmlösa, men genom att även kontonummer, PIN-koder med mera begärs öppnas vägen för bedragaren till kundens engagemang hos det finansiella företaget.

Kostnaden för en bedragare att göra ett massutskick av mejl är försumbar, och denne torde gå med vinst redan om någon enstaka kund luras att lämna ut infor-

mationen. Informationen kan bedragaren antingen använda för ett angrepp eller sälja till någon annan.

Det finns även andra former av möjliga angrepp, mer eller mindre sofistikerade. En bank har uppgett att en kund blivit utsatt för s k Pharming, vilket innebär att kunden ”kidnappas” och sänds till en hemsida som ser ut att vara bankens men som inte är det. Syftet med detta är att få kunden att tro att denne är inne hos banken. Det finns olika sätt att göra detta. En metod är med s k trojaner som innebär att man överför ett program till kundens dator för att på så sätt styra användaren.

Det som har hänt på bankområdet är inget unikt, utan det finns numera en omfattande flora av olika brott och angrepp som kan utföras vid internetanvändning. De vanligaste handelssajterna har t ex varit måltavlor för olika angrepp och försök att komma åt inloggningsuppgifter för att kunna beställa varor i andra personers namn. I USA har det också förekommit att börskurser manipulerats på så sätt att felaktiga uppgifter om en stor order till ett företag skickats som ett spammejl efter det att man med hjälp av stulna lösenord köpt upp billiga aktier i det specifika företaget. FI har efter undersökningens genomförande fått information om att ett angrepp genomförts mot en svensk internetbank, där förövaren tycks ha handlat från kundernas konto i syfte att påverka priset på värdepapper.

Pharming

Vid den enklaste formen av pharming manipuleras den ”vägvisning” som en dator frågar efter för att hitta önskad webbplats. Det gör att datorn leds till en falsk webbplats när kunden knappar in det finansiella företagets webbadress. Den webbsida kundens dator styrs till är ofta en kopia av den riktiga webbplatsen och den webbadress som syns i webbläsaren är den som kunden är van vid hos sitt företag. Kunden luras därför att tro att han har kommit rätt. Manipuleringen kan antingen ske i kundens dator eller internetleverantörernas servrar. När manipuleringen görs i kundens dator används s k trojaner.

En angripare kan också lägga in skadliga skript på seriösa webbplatser. Skripten har utformats för att utnyttja svagheter i kundernas webbläsare och på så sätt infektera deras datorer när de besöker en webbplats. Möjligheten att fånga in ett stort antal ovetande bankkunder med hjälp av ett enda angrepp av det här slaget gör metoden taktiskt lockande. Men svårigheten att tränga igenom välbevakade webbplatser har gjort att det inte inträffat så ofta.

Manipulering av internetleverantörernas s k DNS-servrar är den i nuläget mest avancerade formen av pharming och också den minst vanliga. En manipulering av en DNS-server bedöms ge angriparen den bästa möjligheten att samla in stora mängder identiteter i ett enda angrepp. Därför är det också ett hot som internetleverantörerna och nätverkssäkerhetsbranschen fokuserar på.

Från en bank har vi fått information om att kunder försetts med trojaner. Sammantaget kan FI konstatera att angreppen hittills inte har varit alltför avancerade. Bankerna gör dock bedömningen att det finns ett uppenbart hot att kunderna inom en snar framtid kan komma att föra med sig trojaner. Därmed kan vi räkna med att utnyttjandet av kunder för angrepp kommer att bli mer avancerade än i dag. Angreppen kan innebära att kunderna eller banken märker angreppen först när det är för sent.

Trojaner
Trojaner är datorprogram som döljs i t ex bilagor till mejl eller i webblänkar. Det vanligaste sättet är att bädda in dem i gratismaterial som skärmsläckare, spel och andra program med innehåll som hämtas av datoranvändarna själva. Effektiva och uppdaterade virusskydd förhindrar trojaner att tränga in i datorn. Om en trojan kommer in i en oskyddad dator märker användaren det förmodligen inte.

Det finns trojaner som kan kopiera innehållet i öppna fönster i kundens webbläsare. En del av de mer avancerade trojanerna kan också stjäla innehållet i vad som kallas ”autocomplete forms” (formulär som fylls i automatiskt tack vare instruktioner som finns i webbläsaren). De kan också stjäla information från webbläsarens internet-cache (mindre mängd snabbt åtkomliga data), kopiera olika cookies (data, som t ex sparade användarnamn, lösenord till inloggning av tjänster och besökta webbsidor), eller till och med användas för att fjärrstyra kundens dator.

Trojanska hästar som riktar sig mot finansiell information och mot finansiella system fortsätter att dyka upp i en allt raskare takt.

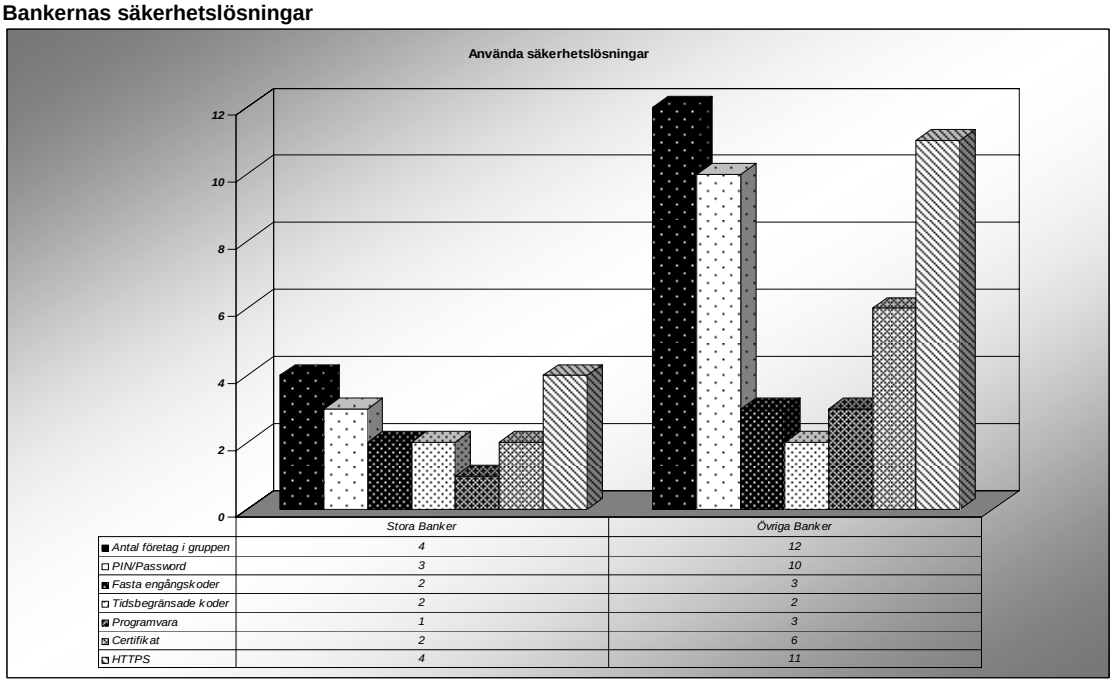
I ett antal fall har angriparna använt sig av andra kunders konton för att samla upp de medel de tillskansat sig. Kunderna har övertalats att medverka genom att ”låna” ut sitt konto mot ersättning. Därefter har medlen tagits ut eller skickats vidare.

Identifiering

Samtliga företag har någon form av säkerhetslösning för att identifiera kunderna. Processen för att identifiera en kund kan bestå av en eller två delar. Den första delen består i att kunden ska uppge något som denne vet, PIN/Password. Om det finns en andra del består den i att kunden ska uppge en kod som denne har, skrapa fram en engångskod eller skapa en ny kod genom en personlig säkerhetsdosa eller motsvarande. Hanteringen innebär att kunden verifieras och får tillgång till de tjänster som företaget erbjuder.

Den vanligaste identifieringsmetoden är PIN/Password tillsammans med något annat. Det är få företag som endast använder PIN/Password. Av de 35 företag som ingick i undersökningen använder sex företag fasta engångskoder och fem företag koder som produceras med någon form av säkerhetsdosa. Sex företag använder någon form av hårdvara som är installerad på kundens utrustning och som producerar koder med hjälp av t.ex. certifikat. De koder som tillverkas vid varje användningstillfälle har en giltighet som är begränsad i tiden till skillnad mot de engångskoder som producerats i förväg. Det är en kombination av flera olika metoder som innebär en förhöjd säkerhet. De få banker som inte använder en avancerad identifiering bör genast överväga förändringar beroende av vilka tjänster som deras kunder använder. FI för en dialog med dessa banker.

Bankernas säkerhetslösningar



	Stora Banker	Övriga Banker
Antal företag i gruppen	4	12
PIN/Password	3	10
Fasta engångskoder	2	3
Tidsbegränsade koder	2	2
Programvara	1	3
Certifikat	2	6
HTTPS	4	11

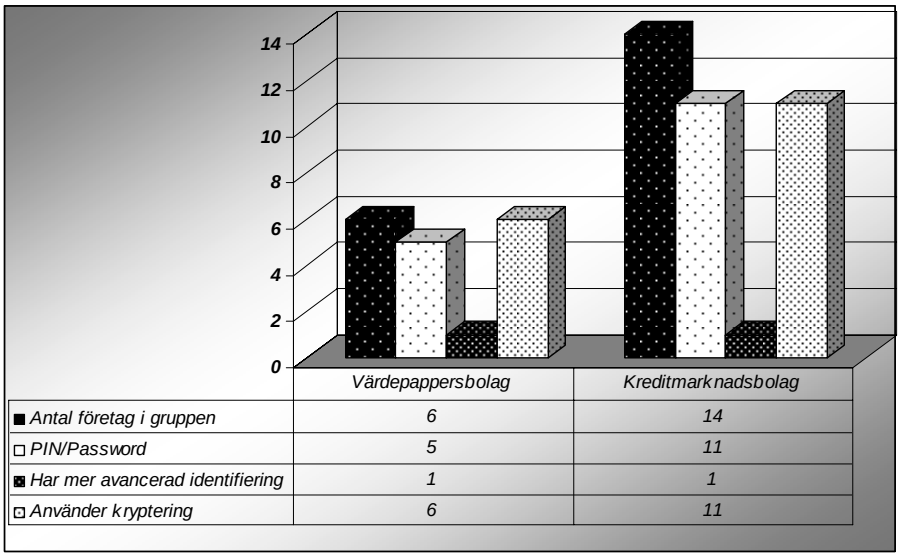
11 företag av 35 säger sig har ändrat sina säkerhetslösningar under de senaste två åren. En bank har som en följd av angreppen ändrat säkerhetslösning under 2006 och på så sätt försvårat för nya angrepp. En annan bank har aviserat att den under 2007 avser att erbjuda kunderna en annan säkerhetslösning som alternativ till den nuvarande.

Fyra företag av 35 ställer krav på kunderna att ha egna säkerhetsskydd.

De kunder som drabbades under hösten 2006 saknade virusskydd eller hade inte uppdaterat sitt skydd. Funktionaliteten av ett antivirusprogram (och brandvägg) är beroende av hur aktuell information programmet har om virus och annat som det ska skydda emot. Tre av storbankerna erbjuder kunderna sådana skydd. Det är banker som tidigare har utsatts för angrepp som erbjuder denna extra service till sina kunder. FI:s bedömning är att bankerna har ett ansvar för att de gentemot kund ställer relevanta krav på säkerhetsnivån även hos kunden.

Det är kunder till bankerna som använt fasta engångskoder som en del av säkerhetslösningen där angreppen lyckats.

Säkerhetslösningar hos kreditmarknadsbolag och värdepappersbolag



	Värdepappersbolag	Kreditmarknadsbolag
Antal företag i gruppen	6	14
PIN/Password	5	11
Har mer avancerad identifiering	1	1
Använder kryptering	6	11

Bankbesöket

Som beskrivits ovan krävs att kunden identifieras innan denne ges möjlighet att använda företagets tjänster. Företagen använder olika tekniska lösningar för att genomföra identifieringen av sina kunder. Gemensamt för dessa är att först då kunden identifierats som kunden så att säga har kommit in i banken och kan genomföra sina affärer. Banken har i detta avseende ersatts av ett virtuellt kontor som också gör det möjligt för kunden att i stort sett när och var som helst nå banken.

Bankens kontakter med kunderna sker sedan när de är uppkopplade, inne på det virtuella kontoret. En bank använder i dag därför inte mejl för att kontakta sina kunder. Så länge kunden är inne på det virtuella kontoret skyddas dennes transaktioner av bankens säkerhetslösning. Därför finns krav från banken för vissa tjänster, vanligtvis betalningsförmedling, att kunden verifierar genom att signera sin transaktion med något som kunden har, t ex en engångskod som är framskrapad eller producerad med en säkerhetsdosa. När kunden inte längre vill vara kvar på det virtuella kontoret och loggar ut, eller inte verifierar sig när så krävs, stängs banken eftersom kunden då lämnat kontoret.

Framtida hot

En stor del av de angrepp bankerna identifierat det senaste året har varit tekniskt enkla i sin utformning. Vi kan framöver förvänta oss att falska mejl och hemsidor kommer att vara betydligt bättre utformade och mer trovärdiga.

Det är heller inte osannolikt att angreppen kommer att ändra karaktär och t.ex. riktas mot kunder som har stora tillgångar och som utför många transaktioner. Företag hanterar ofta betydligt större summor än privatpersoner, samtidigt som säkerheten kan vara bristfällig. Det är svårare att skydda sig mot ett riktat angrepp än mot de massmejl mm som skickas ut på vinst och förlust.

Vad händer med utsatta kunder?

De kunder som utsatts för s k Phishing har samtliga blivit ersatta av bankerna. Även i det fall där en kund blivit utsatt för en trojan har kunden ersatts. Sammanlagt har bankerna totalt betalat ut ca åtta miljoner kronor i ersättning till drabbade kunder. FI har dock uppmärksammat att det förekommer omfattande friskrivningsklausuler.

Information till kunden

Av undersökningen framgår att det endast är bankerna som informerar om riskerna med användningen av internet. Den information som anges är dock begränsad till riskerna kring säkerheten. Någon tydlig information om vem som bär risken om det inträffar en skada förekommer inte.

Förtroendet för internet

SAMMANFATTNING
Förtroendet för att kunna utföra finansiella tjänster via internet är en avgörande fråga för att vi på sikt ska säkerställa en effektivitet i betalningssystemet och i andra finansiella tjänster.

Företag som erbjuder tjänster via internet har ansvar för den övergripande säkerhetslösningen och att den alltid är i nivå med de risker och hot som finns. Det är också viktigt att företagen har en god beredskap vid angrepp och rutiner för hur valda säkerhetslösningar ska omprövas. De kunder som saknar virusskydd eller inte har det uppdaterat och saknar brandvägg är den svagaste länken i kedjan.

FI kommer noga att följa utvecklingen av angreppen och företagens beredskap.

Hur stort är problemet?

Utifrån antalet finansiella transaktioner på internet har bankerna endast drabbats av mindre lyckade angrepp och få kunder är indragna. Det faktum att en stor del av befolkningen och många företag utnyttjar tjänster som erbjuds via internet, sett i relation till antalet inblandade kunder talar emot att angreppen har varit av betydelse för systemet som sådant.

Det som talar för att angreppen ändå är av betydelse är att det främst är de största aktörerna som har angripits och att det har skett en kraftig ökning av antalet drabbade kunder.

Bankerna bedömer att hoten ökar och att de brottsliga aktiviteterna blir mer avancerade. Fortsatta angrepp kan påverka förtroendet för bankernas tjänster, vilket påverkar effektiviteten i det finansiella systemet genom att kunderna återgår till manuella tjänster. Det är en utveckling som inte kan anses gynna någon part.

FI gör bedömningen att angreppen mot internetkontoren för närvarande inte hotar stabiliteten i det finansiella systemet. De större aktörerna är väl finansiellt rustade för de risker som verksamheten medför.

En ökning av antalet angrepp kan dock skada förtroendet för marknaden som helhet. Det ligger därför både i allmänhetens och företagens intresse att begränsa de bedrägliga attackerna.

Vid uppmärksammade händelser som några av internet-angreppen på senare tid, uppstår krav på att tjänsterna måste vara säkra. Problemet är att absolut säkra lösningar inte existerar vare sig det handlar om att skydda sig mot inbrott, bankrån eller internetangepp.

Vad som är en rimlig säkerhetsnivå är något som förändras över tiden. I fall risken för fullbordade angrepp ökar kan en förhöjd säkerhetsnivå vara nöd-

vändig för att behålla förtroendet hos kunderna. Acceptansen bland kunden för t ex en mer komplicerad inloggningsprocedur kan samtidigt öka.

Företagen måste därför göra relevanta riskkalkyler där inte bara hårda ekonomiska faktorer spelar in såsom systemkostnader och risk för ersättningskrav. Även frågor som kundernas förtroende för tekniken, teknikens användbarhet och kundernas förståelse av tekniken är aspekter som måste vägas in. I detta sammanhang måste också frågan om vem som ska skydda sig och vem som har bäst möjlighet att skydda sig ställas.

En orsak till att kunder angripits kan vara att domännamnsadministratörer tillåter registrering av ordet bank i domännamn utan att säkerställa att det är bankrörelse som bedrivs. FI anser att detta är i strid med gällande regelverk och har kontaktat Stiftelsen för internetstruktur (NIC-SE) angående detta. Stiftelsen har ännu inte reagerat på skrivelserna. Det blir då enkelt för bedrägliga individer att sätta upp en falsk banksida på internet för att lura bankkunder att uppge koder. En annan orsak till angreppen kan vara att rörligheten och tillgången via internet inte har några nationella begränsningar.

Det är banker och främst deras kunder som är mest exponerade för kriminella attacker via internetbaserade tjänster. Kreditmarknadsbolag tillhandahåller inte tjänster som erbjuder motsvarande rörlighet för kunders medel. Detsamma gäller för värdepappersbolag. Detta kan förklara varför dessa bolags kunder inte utsatts för liknande angrepp som bankkunderna.

Eftersom problemet hittills inte kan anses som omfattande gör FI bedömningen att det inte finns skäl att ställa generella krav i form av föreskrifter eller liknande på bankernas säkerhetslösningar. Sådana krav bör också vägas mot dagens relativa enkelhet att använda bankernas tjänster. En detaljreglering skulle riskera att bli alltför styrande och dessutom inte tillräckligt aktuell.

Vem ansvarar för säkerheten?

Genom internet tillhandahåller bankerna och andra finansiella företag vissa tjänster. Det ligger därför nära till hands att dessa företag har ett stort ansvar för säkerheten, både den egna och kundens. Vilka krav på identifiering som ska ställas kan mycket väl vara beroende av den tjänst som tillhandahålls. Graden av säkerhet måste ställas i relation till hoten och företagen bör därför kontinuerligt se till att det görs analyser av risker och hot.

Eftersom dessa typer av attacker bedöms bli vanligare och det kan påverka förtroendet för distributionskanalen men även för den finansiella sektorn är det väsentligt att attackerna analyseras. FI kommer därför att följa och noga analysera utvecklingen av de attacker som bankerna direkt och indirekt utsätts för. Därutöver bör samtliga finansiella företag i sina beredskapsplaner behandla denna typ av attacker och ha rutiner för att ompröva beslut om etablerad säkerhetsnivå.

Man kan ifrågasätta om inte användningen av engångskoder som är giltiga till de förbrukas, har varit en väsentlig omständighet för de bedrägerier som ägt rum. Fördelen med engångskoder, till skillnad mot fasta koder, är att de

bara kan användas en gång. Men om någon obehörigen kommer över oanvända engångskoder finns en risk för angrepp.

Kundens hantering av identifieringsuppgifter är väsentlig i detta sammanhang, men också hanteringen av teknisk utrustning med antivirusprogram och brandvägg, samt kunskapen om hur seriösa finansiella aktörer beter sig (t ex vetskapen att banker inte mejlar sina kunder för att be om PIN-koden).

Ett IT-säkerhetsföretag gjorde år 2004 bedömningen att det är hos kunderna som det största hotet mot bankerna finns. En tredjedel av kunderna saknade då virusskydd. Ytterligare ett antal hade ett antivirusprogram som de aldrig hade installerat eller startat, eller uppdaterat efter det första årets prenumeration av virusdefinitioner.

Genom att skydda sina datorer på ett bättre sätt med antivirusprogram kan kunden begränsa risken att dennes dator fjärrstyrs eller att någon obehörigen kopierar och för ut information som digitala certifikat, användaridentiteter, lösenord, bankkontonummer, kreditkortsnummer etc.

Förutom antivirusskydd är det viktigt att kunderna också skyddar sina datorer med hjälp av personliga brandväggar. Utan detta kompletterande skydd kommer aldrig antivirusprogram att vara ett fullgott skydd mot annat än virus. Trojaner kommer i alltför stor utsträckning att kunna verka odetekterade på de datorer som ansluts till bankernas system.

De krav som allmänt kan ställas är att den som tillhandahåller tjänster via internet ska säkerställa att metoden för identifiering och vägen in till banken har sådan säkerhet att allmänhetens förtroende för denna distributionskanal upprätthålls. Den av banken valda säkerhetsnivån bör dock vid varje tillfälle stämmas av med säkerhetsexperter och FI förordar att banken tar in en s k second opinion för att säkerställa den för banken rätta nivån.

Om företagen informerade om riskerna skulle kunderna få en större förståelse för att begränsa riskerna vid användningen av internet. FI anser att det är en brist att inte alla företag informerar om riskerna och vad kunderna kan och bör göra för att minska dessa.

Även om antivirusprogram (och brandväggar) ger ett gott grundskydd innebär det inte att det skyddar mot alla former av angrepp. Angrepp som inleds genom att samla in information med hjälp av falska webbsidor, s k pharming, hindras inte av antivirusprogram.

Vem har ansvar när en skada uppstår?

Det finns inte särskilt lagreglerat vem som bär det ekonomiska ansvaret för ett lyckat angrepp mot en finansiell tjänst via internet. En statlig utredning konstaterade 2005[2] att banker i brist på reglering i sina standardvillkor anger att kunden är ansvarig för i stort sett samtliga transaktioner som skett med användning av personliga bankkoder. Det vill säga att kunden är ansvarig även om denne utsatts för brott. Detta fann utredningen anmärkningsvärt och konstaterade att skyddet för konsumenterna i Sverige är avsevärt svagare än i

[2] Sid 275, Slutbetänkande av Utredningen om obehörig användning av kontokort samt konsumentskydd vid s.k. modemkapning (SOU 2005:108)

bl a Danmark, Norge och Finland. FI anser att en lagreglering av ansvarsfördelningen vid obehörig användning av internet-banker och liknande självbetjäningstjänster bör införas i enlighet med utredningens förslag. På så sätt skulle en mer ändamålsenlig fördelning av riskerna åstadkommas. Det skulle dessutom kunna innebära att oskäliga avtalsvillkor sållas bort från marknaden. FI kommer i avvaktan på detta att arbeta för att Konsumentombudsmannen tar upp frågor om de långtgående friskrivningsklausulerna till rättslig prövning.

Även om bankerna i stor omfattning hittills har ersatt drabbade kunder är det ett stort frågetecken hur länge en sådan kundvänlig attityd kommer att bibehållas. Man kan också ifrågasätta skäligheten i alltför omfattande ansvarsfriskrivningar. Sådana villkor kan dessutom hämma utvecklingen mot säkrare och mer kostnadseffektiva kanaler till finansiella tjänster. Detta på grund av att incitamenten för företagen att ta fram säkrare metoder minskar när konsekvenserna av angrepp får bäras av någon annan, i detta fall kunderna. Dessutom kan kunderna bli tveksamma till nyttan av att välja t ex internet som kanal om de får bära hela risken.

Finansinspektionens rapporter

finns på www.fi.se

2007:9 Konsumentskyddet på finansmarknaden
2007:8 Pension under utbetalning
2007:7 Pensionsspara i försäkring
2007:6 Fondbolagens informationsgivning II
2007.5 Rådgivningen, kunden och lagen – en undersökning av finansiell rådgivning
2007:4 Kreditmarknadsbolagen och konsumentskyddet
2007:3 Ordning och reda ? II – en granskning av 678 försäkringsförmedlare
2007:2 Utvärdering av Stockholmsbörsen AB som central motpart, 2006
2007:1 Utvärdering av VPC:s clearingsystem, 2006
2006:18 Operativa risker – företagens hantering och FI:s rekommendationer
2006:17 Penningtvätt och terroristfinansiering
2006:16 Flytträtt för sparande i pensionsförsäkring – kartläggning och förslag
2006:15 Oreglerade erbjudanden på aktiemarknaden
2006:14 Finanssektorns stabilitet 2006
2006:13 Warrantmarknaden – en granskning av informationen till småsparare
2006:12 Blancokrediter till konsumenter II – uppföljning
2006:11 Skatte- och försäkringsrörelseregler för livförsäkring
2006:10 Pensionssparandet och värdebeskeden
2006:9 Utvecklingen på bolånemarknaden
2006:8 Ordning och reda – en granskning av 150 försäkringsförmedlare
2006:7 Livbolagens förlusttäckning – redovisning av olika metoder
2006:6 Bankernas kapitalkrav med Basel 2
2006:5 Avgift efter prestation – en granskning av avgifter i 37 fondbolag
2006:4 Marknadstillsyn 2006
2006:3 Handel med förfallna fordringar och inkasso
2006:2 Företagens tillämpning av internationella redovisningsregler
2006:1 Fondbolagens informationsgivning

Finansinspektionen
Box 7821, 103 97 Stockholm
Tel 08-787 80 00
Fax 08-24 13 35
finansinspektionen@fi.se