

05.09.2006 | 16:20:42

ZÜRICH – Zwar ermuntern die Banken ihre Kunden, ihre Bankgeschäfte auf ihrem eigenen Computer zu erledigen. Doch die Sache ist technisch noch nicht sicher genug. Betrüger haben leichtes Spiel.

Es geht ums so genannte Phishing: Das sind Betrugsfälle durch Ausspähen von persönlichen Kontoinformationen durch E-Mails mit gefälschten Absendern und durch präparierte Webseiten.

Phishing-Attacken laufen häufig nach einem erkennbaren Muster ab: Der Bankkunde erhält eine vermeintlich von seiner Bank stammende E-Mail mit der Aufforderung, sensible Daten wie seine Kontodaten oder PIN- und TAN-Nummern einzugeben (TAN: Transaktions-Nummer).

Erst kürzlich musste die Migros-Bank nach einer Phishing-Attacke ihren Online-Zahlungsverkehr vorübergehend stoppen. Aber das ist kein Einzelfall. Schweizer Banken und Finanzdienstleister werden immer häufiger Ziel von so genannten Phishing-Attacken.

Was ist zu tun?

Hundertprozentige Sicherheit wirds im Internet nicht geben, also auch nicht im Online-Banking. Aber das Risiko muss deutlich reduziert werden. Ausgereifte Methoden gibts aber noch nicht, berichtete die Software-Firma Symantec heute. Sie gibt diese Tipps:

Kurzfristige Abhilfe:

- Kunden müssen aufgeklärt und Mitarbeiter müssen speziell geschult werden. Banken sollten ihren Kunden klarmachen, dass sie grundsätzlich keine Mails mit Fragen nach vertraulichen Daten beantworten sollten.

Mittelfristig:

- Für die Identifizierung der Online-Banking-Kunden könnte die Abfrage von biometrischen Daten wie Iris oder Fingerabdruck eingeführt werden.

Das Problem ist dringend. Bereits entwickeln Online-Betrüger neue, noch raffiniertere Methoden. Das ist das so genannte Pharming, erklärt Candid Wüest, Schweizer Experte der Sicherheits-Software-Firma Symantec. Dabei manipulieren Hacker den DNS-Server, über den die IP-Adresse der Bank umgewandelt wird. Selbst wenn ein Kunde eine richtige Web-Adresse eingibt, lotst ihn dann das infizierte System auf eine falsche Seite der betreffenden Bank. Tätigt der Online-Banking-Kunde dann eine Überweisung, indem er das Passwort samt PIN und TAN eintippt, gibt er diese Informationen direkt an den Hacker weiter.

Wem also derzeit das Online-Banking schlicht zu unsicher ist, könnte vorerst vollständig darauf verzichten. Es gibt ja auch den Bancomaten. Hier ist die Bank allein verantwortlich.

Beglaubigte Auflage WEMF : 727 000 Deutschschweizer Leser

STIMMEN SIE AB!

Benutzen Sie Online-Banking?

- Ja
- Nein
- Ich warte noch ab

Abstimmen



Noch nicht sicher genug:
Online-Banking.

Bildzoom

RDB

ENORMER SCHADEN

Gemäss dem «Internet Security Threat Report» des Anti-Virus-Spezialisten Symantec wurden im zweiten Halbjahr 2005 täglich 7,92 Millionen Phishing-Versuche ermittelt, verglichen mit täglich 5,7 Millionen im ersten Halbjahr 2005. Der finanzielle Schaden ist enorm: Alleine in den USA wurden mit dem Ausspähen von sensiblen Kontodaten und PINs in Verbindung mit Kredit- und Bankkarten letztes Jahr Schäden von etwa 2,75 Milliarden Dollar (3,4 Milliarden Franken) verursacht.

Mittwoch, 6. September 2006

Phishing breitet sich rasant aus

Banken im Kampf gegen das kriminelle Ausspionieren sensibler Kundendaten

Zürich. Im Kampf gegen kriminelle Phishing-Attacken auf Banken und deren Kunden wird die Abfrage bio-metrischer Daten ein Thema.

Die Zahl der Betrugsfälle durch Phishing, das Ausspähen persönlicher Kontoinformationen mittels E-Mails mit gefälschten Absendern und präparierter Webseiten, nimmt zu. Erst kürzlich musste die Migrosbank ihren Online-Zahlungsverkehr vorübergehend stoppen. Wiederholt im Visier von Phishing war auch Postfinance.

Laut dem «Internet Security Threat Report» des Anti-Virus-Spezialisten Symantec wurden im 2. Halbjahr 2005 täglich 7,9 Mio. Phishing-Versuche ermittelt, 2,2 Mio. mehr als im 1. Semester. Alleine in den USA wurden mit dem Ausspähen sensibler Kontodaten und PIN-Codes in Verbindung mit Kredit- und Bankkarten letztes Jahr Schäden von 2,75 Mrd. \$ angerichtet. Phishing-Attacken laufen häufig nach dem Muster ab, dass der Bankkunde ein vermeintlich von seiner Bank stammendes E-Mail erhält mit der Aufforderung, sensible Daten wie seine Kontodaten oder Codes einzugeben. Banken sollten daher ihren Kunden klarmachen, generell keine Mails mit Fragen nach vertraulichen Daten zu beantworten.

Die Online-Betrüger werden immer raffinierter. So hat sich laut Symantec-Experte Candid Wüest nebst Phishing die viel gefährlichere Variante Pharming herausgebildet. Dabei manipulieren Hacker den DNS-Server, über den die IP-Adresse der Bank umgewandelt wird. Selbst wenn ein Kunde eine richtige Web-Adresse eingibt, lotst ihn das infizierte System auf eine gefälschte Seite der Bank. Tätigt der Online-Banking-Kunde eine Überweisung, indem er das Passwort samt Codes eintippt, gibt er diese Informationen direkt an den Hacker weiter.

Viele Banken arbeiten an Sicherheitslösungen. Für die Identifizierung der Online-Kunden wird bereits die Abfrage biometrischer Daten wie Iris oder Fingerabdruck erörtert. Weil die kriminellen Strategien immer öfter auch auf ein Fehlverhalten von Bankangestellten abzielen, müssen laut Syman- tec auch die eigenen Mitarbeiter geschult und die eigenen IT-Systeme überprüft werden. (ap)

Copyright © St.Galler Tagblatt
Eine Publikation der [Tagblatt Medien](#)

http://www.tagblatt.ch/index.php?artikelxml=jsp&artikel_id=1232177&ressort=tagblattheute/wirtschaft#

Beglaubigte Auflage WEMF: 106'101 Leser



Immer mehr Phishing-Attacken auf Schweizer Banken

Schweizer Banken und Finanzdienstleister werden immer häufiger Ziel von so genannten Phishing-Attacken. Um die Internetkriminellen zu stoppen, wird die Identitätsabfrage mittels biometrischer Daten diskutiert.

Die Zahl der Betrugsfälle durch Phishing, dem Ausspähen von persönlichen Kontoinformationen mittels E-Mails mit gefälschten Absendern und präparierter Webseiten, hat sich in jüngster Zeit markant erhöht. Im Visier sind vor allem Banken und andere Finanzinstitute. So hatte erst kürzlich die Migros-Bank nach einer Phishing-Attacke ihren Online-Zahlungsverkehr vorübergehend stoppen müssen.

Gemäss dem «Internet Security Threat Report» des Anti-Virus-Spezialisten Symantec wurden im zweiten Halbjahr 2005 täglich 7,92 Millionen Phishing-Versuche ermittelt, verglichen mit täglich 5,7 Millionen im ersten Halbjahr 2005. Der finanzielle Schaden ist enorm: Alleine in den USA wurden mit dem Ausspähen von sensiblen Kontodaten und PINs in Verbindung mit Kredit- und Bankkarten letztes Jahr Schäden von etwa 2,75 Milliarden Dollar verursacht.

Phishing-Attacken laufen häufig nach einem erkennbaren Muster ab, indem der Bankkunde eine vermeintlich von seiner Bank stammende E-Mail erhält mit der Aufforderung, sensible Daten wie seine Kontodaten oder PIN- und TAN-Nummern einzugeben. Banken sollten deshalb ihren Kunden klarmachen, dass sie grundsätzlich keine Mails mit Fragen nach vertraulichen Daten beantworten sollten.

Die Methoden der Onlinebetrüger immer ausgefeilter. So hat sich laut Candid Wüest, Schweizer Experte aus dem Symantec-Virenlabor in Dublin, nebst Phishing eine weitaus gefährlichere Variante herausgebildet, das so genannte Pharming. Dabei manipulieren Hacker den DNS-Server, über den die IP-Adresse der Bank umgewandelt wird. Selbst wenn ein Kunde eine richtige Web-Adresse eingibt, lotst ihn dann das infizierte System auf eine falsche Seite der betreffenden Bank. Tätigt der Online-Banking-Kunde dann eine Überweisung, indem er das Passwort samt PIN und TAN eintippt, gibt er diese Informationen direkt an den Hacker weiter.

Viele Banken arbeiten an Sicherheitslösungen, die ihren Kunden eine vertrauensvolle Nutzung der Online-Dienste ermöglichen sollen. Für die Identifizierung der Online-Banking-Kunden wird inzwischen bereits die Abfrage von biometrischen Daten wie Iris oder Fingerabdruck erörtert. Weil die kriminellen Strategien immer häufiger auch auf das Fehlverhalten von Bankmitarbeitern abzielen, müssen laut Symantec aber nicht nur die Kunden aufgeklärt, sondern auch die eigenen Mitarbeiter geschult und die eigenen IT-Systeme überprüft werden.

Pub: 05.09.06; 10:37/ mab

Akt: 05.09.06; 17:08

Quelle: AP

Beglaubigte Auflage WEMF: 1'039'000 Leser

Internetbanking

Onlinebetrüger setzen Banken zu

ap. Banken und Finanzdienstleister werden immer häufiger Ziel von so genannten Phishing-Attacken. So hatte erst kürzlich die Migros-Bank nach einer solchen Attacke ihren Online-Zahlungsverkehr vorübergehend stoppen müssen.

Bei Phishing-Attacken erhält der Kunde eine vermeintlich von seiner Bank stammende E-Mail mit der Aufforderung, sensible Daten wie seine Kontodaten oder PIN- und TAN-Nummern einzugeben.

Die Betrüger werden aber immer dreister. So hat sich eine weitaus gefährlichere Variante herausgebildet, das Pharming. Dabei manipulieren Hacker den Server. Selbst wenn ein Kunde eine richtige Adresse eingibt, wird er auf eine falsche Seite gelotst. Tätigt der Kunde dann eine Überweisung, indem er das Passwort samt PIN und TAN eintippt, gibt er diese Informationen direkt an den Hacker weiter.

Schäden in Milliardenhöhe

Gemäss dem «Internet Security Threat Report» des Anti-Virus-Spezialisten Symantec wurden im zweiten Halbjahr 2005 täglich 7,92 Millionen Phishing-Versuche ermittelt, sechs Monate zuvor waren es noch 5,7 Millionen. Der finanzielle Schaden ist enorm: Alleine in den USA kam es deswegen letztes Jahr zu Schäden von 2,75 Milliarden Dollar. Für die Identifizierung der Online-Banking-Kunden wird deshalb die Abfrage von biometrischen Daten wie Iris oder Fingerabdruck erörtert. Eine drastische Steigerung der Sicherheit versprechen sich Forscher von der Kombination mehrerer biometrischer Methoden in einem Verfahren. In diesem Bereich ist auch die in Root ansässige Software-Firma ID-Development AG tätig.

<http://www.zisch.ch>

Beglaubigte Auflage WEMF: 132'179 Leser