

Presseinfo zu Phishing

- Mitschrift: Radiobeitrag und O-Töne
- Berlin, 29. August 2007
- O-Töne von Heinz Paul Bonn, Vizepräsident BITKOM

1. Sendefertiger Radiobeitrag

+++ Anmoderation +++

Online-Banking ist eine bequeme Sache: Überweisungen erledigt man von zu Hause, den Kontostand fragt man mal schnell vom Büro aus ab – kein Wunder, dass mittlerweile rund 20 Millionen Deutsche die Internetdienste ihrer Bank nutzen. Mit der Zahl der Online-Kunden steigt aber auch die Zahl der Betrugsfälle. Dabei ist Online-Banking eine sichere Angelegenheit, wenn man sich ein paar Tipps zu Herzen nimmt, wie Johannes Boos berichtet.

+++ Beitrag mit O-Tönen +++

Vorsorge gegen Betrug gegen Online-Banking wird immer wichtiger: Die Zahl der abgezockten Bankkunden ist im vergangenen Jahr bundesweit um 23 Prozent nach oben geschneit – besonders dramatisch ist die Entwicklung in Sachsen. Noch aber melden Baden-Württemberg, Bayern, Berlin und Nordrhein-Westfalen die meisten Fälle. Und die Tricks der Betrüger werden immer raffinierter. Nur noch jedes zehnte Opfer wird durch E-Mails auf gefälschte Bankseiten gelockt, weiß Heinz-Paul Bonn vom Branchenverband BITKOM:

In sehr vielen Fällen schicken die Betrüger jetzt per Mail ein sogenanntes Trojanisches Pferd – ein Schadprogramm, das die Daten heimlich ausspäht und weitergibt.

Aus Sicherheitsgründen sollten Nutzer beim Online-Banking die Adresse der Bank immer direkt im Web-Programm eingeben oder alternativ über selbst gespeicherte Lesezeichen aufrufen. Auch sollte die Verbindung verschlüsselt sein, außerdem sind ein aktuelles Anti-Viren-Programm und eine Firewall ein Muss. Aber auch ein wenig gesunder Menschenverstand kann Betrügereien einen Riegel vorschieben.

Die erste Grundregel ist, nie Geheimzahlen im Netz einzugeben, wenn eine E-Mail dazu auffordert. Solche Mails sind immer gefälscht – am besten sofort löschen. In den Papierkorb gehören auch Mails von Unbekannten, die eine Datei angehängt haben. Niemals öffnen, denn

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin
+49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Christian Spahr
Pressesprecher
Telekommunikation & Recht
+49. 30. 27576-112
Fax +49. 30. 27576-400
c.spahr@bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

dahinter könnte sich ein schädliches Programm verbergen, zum Beispiel ein Phishing-Trojaner.

Liegt eine betrügerische Überweisung erst kurz zurück, gelingt es immer wieder, den Transfer rückgängig zu machen. Viele Banken erstatten einen Schaden, der durch sogenanntes „Phishing“ entstanden ist. Einen Rechtsanspruch darauf gibt es aber nicht. Wer sich mit wenigen Kniffen vor Betrügern zu schützen weiß, für den ist Online-Banking aber eine äußerst sichere Angelegenheit.

2. Einzelne O-Töne

Ist Phishing weiter eine Gefahr für Nutzer von Online-Banking?

In manchen Bundesländern haben sich die Opferzahlen im vergangenen Jahr mehr als verdoppelt. Das trifft zum Beispiel auf Berlin und Sachsen zu. Und auch im bundesweiten Durchschnitt steigt die Zahl der Internet-Nutzer weiter an, deren Konten mit geklauten Passwörtern leer geräumt wurden. BITKOM hat dazu gerade eine Erhebung gemacht. Sie zeigt, dass diese Entwicklung im ersten Halbjahr dieses Jahres weitergeht. Es gibt also keine Entwarnung, im Gegenteil.

Wo gibt es die meisten Opfer, und wie viel Geld holen die Betrüger vom Konto?

Die meisten Phishing-Opfer gibt es in Bayern, in Baden-Württemberg, Berlin und Nordrhein-Westfalen – also in großen oder bevölkerungsreichen Bundesländern. Im Schnitt leiten die Betrüger – Pi mal Daumen – im Schnitt 4.000 bis 5.000 Euro von den Konten ihrer Opfer ab.

Woran liegt es, dass die Opferzahlen steigen?

Eine Ursache für steigende Opferzahlen sind raffiniertere Betrugsmethoden. Nur noch rund zehn Prozent der Schäden entstehen durch E-Mail-Links zu gefälschten Bank-Seiten, auf denen die Opfer selbst ihre Kontodaten eingeben. In sehr vielen Fällen schicken die Betrüger jetzt per Mail ein sogenanntes Trojanisches Pferd – ein Schadprogramm, das die Daten heimlich ausspäht und weitergibt. Deshalb ist es wichtig, die jeweils neuesten Schutzmethoden zu nutzen.

Wie können sich Internet-Nutzer gegen Phishing absichern?

Die erste Grundregel ist, nie – ich wiederhole: nie – Geheimzahlen im Netz einzugeben, wenn eine E-Mail dazu auffordert. Solche Mails sind immer gefälscht – am besten sofort löschen. In den Papierkorb gehören auch Mails von Unbekannten, die eine Datei angehängt haben. Niemals öffnen – wiederhole: niemals öffnen –, denn dahinter könnte sich ein schädliches Programm verbergen, zum Beispiel ein Phishing-Trojaner. Außerdem ist die Sicherheitsausstattung des PCs wichtig. Ein modernes Anti-Viren-Programm und eine sogenannte Firewall dürfen nicht fehlen.

Worauf müssen Kunden sonst achten, die sich online bei ihrer Bank einloggen?

Die Adresse der Bank immer direkt im Web-Programm eingeben oder alternativ selbst über gespeicherte Lesezeichen aufrufen. Die Online-Verbindung zum Bankcomputer muss verschlüsselt sein. Das ist erkennbar an den Buchstaben „https“ in der Internet-Adresse. Im Web-Programm muss ein Schloss- oder ein Schlüssel-Symbol zu sehen sein. Auch wichtig: Die meisten Banken bieten heute modernere Transaktions-Verfahren zum Verschlüsseln von Überweisungen an, etwa iTAN – wobei TAN für Transaktionsnummer steht – oder mTAN. Nutzer sollten diese aktuellen Überweisungsverfahren unbedingt nutzen.

Bleiben Bankkunden auf dem Schaden sitzen, falls es schon zu spät ist?

Viele Banken erstatten einen Phishing-Schaden, wenn der Nutzer nicht grob fahrlässig gehandelt hat. Einen Rechtsanspruch gibt es in aller Regel aber nicht. Phishing-Opfer sollten zuerst die Bank alarmieren: Wenn eine betrügerische Überweisung nicht lange zurückliegt, kann sie manchmal sogar noch gestoppt oder rückgängig gemacht werden. Falls ein finanzieller Schaden bleibt, empfehle ich unbedingt Anzeige bei der Polizei zu erstatten. Das ist die Voraussetzung generell für eine eventuelle Erstattung.

Ist Online-Banking dennoch eine gute Sache?

Mit ein paar Grundregeln lässt sich das Risiko leicht minimieren, sogar signifikant in seinem Risiko reduzieren. Dann ist Online-Banking eine sehr sichere Dienstleistung, die zu Recht hohe Akzeptanz genießt. Insgesamt nutzen rund 20 Millionen Deutsche die Internet-Kontodienste ihrer Bank.