eCommerce
Sicherheit

Ist Internet-Banking (noch) sicher?
Phishing und Trojaner – eine permanente Bedrohung

Autor: **Dr. Harald Ritter**
Version: **1.1 vom 11.01.2008**

Zusammenfassung:

In jüngster Zeit mehren sich Angriffe auf das Internet-Banking mittels Phishing und Trojanern. In den Medien werden diese Angriffe oft damit gleichgesetzt, dass das PIN/TAN-Verfahren als solches unsicher sei und abgelöst werden müsse. Derartige Pauschalaussagen führen zu verminderter Akzeptanz des Internet-Banking, wodurch auch ein erheblicher Kostennachteil für die Banken entsteht. Der vorliegende Artikel stellt dem eine neutrale und objektive Betrachtung der Angriffsmöglichkeiten und möglicher Gegenmaßnahmen entgegen.

NOVOSEC Aktiengesellschaft

Berliner Straße 44
60311 Frankfurt am Main, Deutschland
Telefon +49 (0) 69 /130 1468-0
Telefax +49 (0) 69 /130 1468-11
contact@novosec.com, www.novosec.com

NOVOSEC Aktiengesellschaft

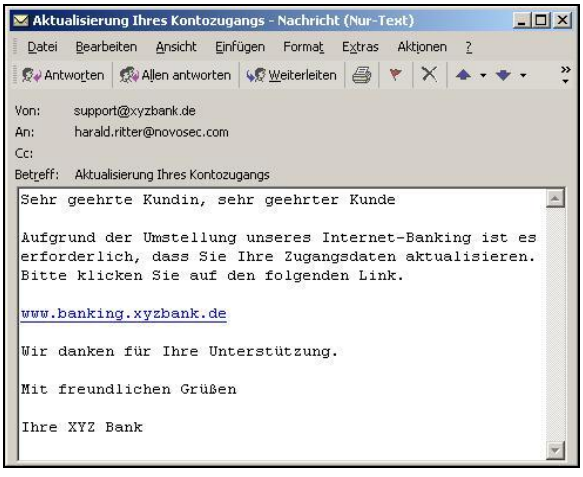
Berliner Straße 44, 60311 Frankfurt am Main, Deutschland
Telefon +49 (0) 69 /130 1468-0, Telefax +49 (0) 69 /130 1468-11
contact@novosec.com, www.novosec.com

Hintergrund

In Deutschland nutzen derzeit mehr als zehn Millionen Kunden die komfortable Möglichkeit, ihre Bankgeschäfte online abzuwickeln. Meist kommt hierbei das PIN/TAN Verfahren zum Einsatz. Gerade in jüngster Zeit sorgen Angriffe mittels Phishing und Trojanern immer wieder für Schlagzeilen. Was versteht man eigentlich unter diesen Begriffen? Sind die Meldungen Panikmache oder berechtigte Warnungen vor Risiken? Was sind geeignete Gegenmaßnahmen?

Phishing

"Phishing" ist ein Kunstwort und steht für "Passwort fischen". Der Versuch, die Kontenzugangsdaten von Bankkunden auszuspähen, beginnt meist mit einer eMail, die den Anschein erweckt, von der für den aktuellen Angriff ausgewählten Bank zu stammen. Da der Angreifer meist nicht über Kundendaten der Bank verfügt, erhalten auch zahlreiche Nicht-Kunden diese eMail. Der Empfänger wird aufgefordert, sich bei seiner Bank einzuloggen und seine Daten zu aktualisieren.



Klickt er auf den in der eMail enthaltenen Link, so landet er auf einer Webseite des Angreifers, die der seiner Bank ähnelt. Auf gut gemachten Seiten fehlen lediglich die Zeile mit der URL und das Schloss als Zeichen der verschlüsselten Verbindung.

Auf der gefälschten Seite wird der Bankkunde aufgefordert, seine Kontodaten einzugeben (z.B. Kundennummer, PIN und TAN). Folgt der Bankkunde diesen Anweisungen, verfügt der Angreifer über alle Informationen, um das echte Internet-Banking aufzurufen und eine Überweisung zu seinen Gunsten zu veranlassen.

Der Erfolg von Phishing-Attacken liegt darin begründet, dass ein Bankkunde, der nicht über das technische Hintergrundwissen verfügt, einer eMail, die scheinbar von seiner Bank stammt, Vertrauen entgegenbringt und seine Zugangsdaten preisgibt. Phishing-Attacken nutzen die Unkenntnis und Gutgläubigkeit der Bankkunden.

Berliner Straße 44, 60311 Frankfurt am Main, Deutschland
Telefon +49 (0) 69 /130 1468-0, Telefax +49 (0) 69 /130 1468-11
contact@novosec.com, www.novosec.com

Trojaner

Anders als bei Phishing ist bei Trojanern kein Zutun des Nutzers nötig und der Angriff richtet sich nicht spezifisch gegen Kunden einer vorher ausgewählten Bank. Trojaner oder Trojanische Pferde sind Programme, die sich (meist über das Internet) weitgehend unbemerkt vom Nutzer in den Computer einschleusen und von dort aus Daten bzw. Tastatur-Eingaben ausspähen und an den Angreifer weiterleiten. Speziell programmierte Trojaner sind auf diese Weise in der Lage, die Eingabe des Kunden beim LogIn in das Internet-Banking mitzulesen und eine gültige TAN auszuspähen. Direkt danach unterbricht der Trojaner die Verbindung zur Bank, so dass die vom Kunden eingegebene TAN nicht zur Bank gelangt und ergo weiterhin gültig bleibt. Der Angreifer ist nun in der Lage, sich selbst in das Internet-Banking einzuloggen und vom Konto des Opfers unter Benutzung der ausgespähten, noch gültigen TAN eine Überweisung zu tätigen.

Schäden durch Angriffe

Den unmittelbaren finanziellen Schaden bei einem erfolgreichen Angriff hat der Kunde. Doch dies ist bei weitem nicht der einzige Schaden, der durch derartige Angriffe entsteht. Transaktionen, die noch rechtzeitig entdeckt und von der Bank zurückgebucht werden können, verursachen Kosten für die manuelle Abwicklung. Die steigende Zahl von Anrufen besorgter Kunden belastet die Hotline. Filialmitarbeiter sind ebenfalls mit Anfragen besorgter Kunden beschäftigt, anstatt Beratungsleistungen zu Produktabschlüssen erbringen zu können.
Der bei weitem größte Schaden entsteht jedoch durch den Vertrauensverlust bei den Kunden. Das Vertrauen des Kunden in die Sicherheit und Zuverlässigkeit der von der Bank angebotenen Systeme wird durch die Häufung von Angriffen, unabhängig von deren Erfolg, und die teilweise sehr unsachliche Berichterstattung darüber stark beeinträchtigt. Dies kann dazu führen, dass Kunden in vermindertem Maße das Internet-Banking nutzen und stattdessen in erhöhter Zahl papiergebundene Überweisungen tätigen. Durch die daraus resultierenden höheren Kosten entsteht der Bank ein erheblicher Schaden!

Reaktionen

Jeder neue Angriff führt zu einer Reihe von mehr oder minder verständlichen Reaktionen:

- Banken veröffentlichen Sicherheitshinweise auf ihren Internet-Banking Seiten. Internet-Recherchen nach Banken-Logos sollen gefälschte Internetseiten ausfindig machen.
- Hersteller von Tokens preisen ihre Produkte als einzig sicheres System.
- Browser-Hersteller und Kritiker von Microsoft verweisen auf alternative, „absolut sichere“ Browser.
- Anbieter von Banking-Software weisen darauf hin, dass ihre Programme die Authentizität von Banking-Seiten prüfen und damit immun gegen Phishing-Angriffe seien.

Kann durch derartige Reaktionen die Verunsicherung von Kunden beseitigt werden? Welche Möglichkeiten gibt es, die beschriebenen Angriffe abzuwehren?

Maßnahmen gegen Angriffe

Die Mehrzahl der derzeit installierten Sicherheitsmaßnahmen dient der Authentisierung des Kunden gegenüber der Bank. Die Authentisierung der Bank gegenüber dem Kunden hingegen beschränkt sich oft ausschließlich auf das Vertrauen in die automatische Prüfung, dass das Zertifikat des Servers von einer im Browser registrierten Zertifizierungsstelle stammt. Die Prüfung, ob das Zertifikat tatsächlich der Bank gehört, wird dem Kunden überlassen. Und welcher

Berliner Straße 44, 60311 Frankfurt am Main, Deutschland
Telefon +49 (0) 69 /130 1468-0, Telefax +49 (0) 69 /130 1468-11
contact@novosec.com, www.novosec.com

Kunde prüft dies schon? Die Prüfung des Zertifikats schützt darüber hinaus nur gegen Phishing, aber keineswegs vor Trojanern!
Die grundsätzlich denkbaren Maßnahmen lassen sich in die Gruppen „Änderungen der Kunden-Authentisierung“ (ID-Tokens, TAN Generatoren, mobile TAN, Signaturen, Biometrie, etc.), „Änderungen der Bank-Authentisierung“ (SenderID, Personal Watermarking, etc.) und „Organisatorische Maßnahmen“ (Rückfrage bei ungewöhnlichen Transaktionen, Aufklärung der Kunden, aktive Recherche nach Angriffen, etc.) einteilen.

Auswahl geeigneter Maßnahmen

Geeignete Maßnahmen lassen sich in kurz- bis mittelfristigen Lösungen und eine langfristige Strategie unterteilen. Kurz- bis mittelfristige Lösungen reagieren auf Attacken und versuchen, Schäden und Schadenswahrscheinlichkeiten zu minimieren. Eine langfristige Strategie ermöglicht es, auch auf geänderte Angriffsszenarien schnell reagieren zu können.
Bei der Bewertung der Maßnahmen sind insbesondere die folgenden Aspekte und Kriterien zu berücksichtigen:

- Bankspezifische Rahmenbedingungen (z.B. vorhandene Banking-Infrastruktur)
- Subjektiv und objektiv erreichbarer Sicherheitsgewinn
- Akzeptanz durch die Kunden
- Benutzerfreundlichkeit
- Erklärungsbedarf
- Wirkung der Maßnahme in der Öffentlichkeit
- Kosten für Umsetzung und Betrieb
- Supportkosten
- Kosten für die Kunden
- Für die Umsetzung erforderliche Zeit
- Technologische Entwicklungen

Fazit

Die Abwehr von Angriffen und damit die Erhöhung der Sicherheit ist eine Kombination von organisatorischen und technischen Maßnahmen. Hierfür ist eine langfristige bankenspezifische Strategie zu entwickeln. Voraussetzung für die Etablierung wirkungsvoller Maßnahmen gegen Phishing und Trojaner ist eine genaue Analyse der speziellen Gegebenheiten sowie eine sorgfältige Abwägung der Konsequenzen aus der Umsetzung der ermittelten Maßnahmen.
Wegen der Komplexität von Internet-Banking-Systemen und der fortschreitenden technologischen Entwicklung gibt es gegen Attacken kein Patentrezept. Sicherheit im Internet-Banking ist ein Wettlauf zwischen Bedrohungen und Gegenmaßnahmen, mithin ein permanenter Prozess!

Wünschen Sie nähere Informationen zu diesem Thema?

harald.ritter@novosec.com

Weitere Artikel finden Sie unter:
http://www.novosec.com/downloads