WARNUNG VOR EINER AKTUELLEN PHISHING-ATTACKE GEGEN KUNDEN DER SPARKASSEN

Seit den Morgenstunden des 08.06.2006 werden massenhaft Emails versandt, die den Empfänger unter dem Vorwand der Verschärfung von Sicherheitsmaßnahmen bei Sparkassen auffordern, auf in der Email enthaltene Links zu klicken.

Hierbei wird zwischen Kunden unterschieden, die eine normale, unnummerierte Liste von "TANs" (5-stellige Transaktionsnummer) und solchen, die das neue "iTAN"-Verfahren (jeder "TAN" ist eine Nummer zugeordnet, die bei Durchführung einer Transaktion von der Bank vorgegeben wird) verwenden.

Bei Betätigung dieser Links werden die Kunden zu verschiedenen, insbesondere im asiatischen Raum befindlichen Internetservern geführt, auf denen die Täter gefälschte Seiten des Sparkassen-Online-Bankings abgelegt haben.

Auf diesen Seiten wird der Anwender aufgefordert, neben seiner Kontonummer und der Online-Banking-"PIN" auch seine Postleitzahl oder den Wohnort sowie nicht verwendete "TANs" bzw. nummerierte "iTANs" einzugeben. Diese Daten können sodann zu illegalen Geldüberweisungen von den Kundenkonten genutzt werden.

Das Bundeskriminalamt (BKA) rät dringend, bei Empfang einer solchen Email keinesfalls auf den enthaltenen Link zu klicken und die Email ungelesen zu löschen.

Neu an dieser Phishing-Welle ist, dass durch diese Email gleichermaßen Nutzer des "PIN/TAN"-Verfahrens als auch Nutzer des "iTAN"-Verfahrens betroffen sind.

Darüber hinaus wird durch die Betätigung der Links die Email-Adresse der Anwender übermittelt, was die Täter in die Lage versetzen könnte, eine Liste von möglichen Sparkassen-Kunden anzufertigen und zukünftig Phishing-Emails gezielter zu versenden.

Das BKA bemüht sich aktuell in Zusammenarbeit mit seinen internationalen Partnern um das Abschalten dieser sogenannten Phishing-Seiten.

Zur Erklärung:

Phishing, d.h. die illegale Erlangung von Kundendaten, um damit Gelder von den Kundenkonten abzuzweigen, ist durch die ständige Zunahme des Online-Verkehrs mit Banken ein wesentliches Kriminalitätsphänomen geworden. Es stellt eine lukrative Einnahmequelle für Straftäter dar, die über immer ausgereiftere technische Methoden verfügen.

Das Bundeskriminalamt empfiehlt:

- Ihre Bank wird von Ihnen keine vertraulichen Daten (Kontonummer, "PIN", "TAN" oder Telefonbanking-"PIN") per E-Mail abfragen oder Ihnen E-Mails zusenden, die einen Link zu ihrem Online-Banking-Login enthalten. Reagieren Sie deshalb nicht auf entsprechende E-Mails.
- Folgen Sie keinem "Link" zu ihrem Online-Banking-Login, sondern geben Sie die entsprechende Internetadresse immer direkt über die Tastatur ein.
- Verwenden Sie ein Virenschutzprogramm sowie eine Firewall und aktualisieren Sie diese Programme täglich.
- Halten Sie das von Ihnen verwendete Betriebssystem und die Internetzugangssoftware (z.B. Internet Explorer, Opera, etc.) stets auf aktuellem Stand, indem Sie immer die vom Hersteller empfohlenen aktuellen Sicherheitsupdates aufspielen.
- Überprüfen Sie ihren PC mittels entsprechender Programme (Virenscanner) regelmäßig auf Schadsoftware.
- Führen Sie keine Online-Transaktionen aus, wenn Sie vermuten, dass Ihr PC mit Schadsoftware infiziert ist.
- Seien sie misstrauisch. Bei Unregelmäßigkeiten während des Online-Banking-Vorgangs, brechen sie diesen ab und informieren sie ihre Bank, um möglicherweise unberechtigt durchgeführte Transaktionen zu stoppen. Dort können auch "TAN"-Listen gesperrt werden, sollten diese in einer gefälschten Anmeldemaske eingegeben worden sein.

Weitere Informationen zum Thema Phishing finden Sie auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (http://www.bsi-fuer-buerger.de) unter Abzocker und Spione / Passwort-Fischer sowie unter www.polizei-beratung.de .