Wie Phishing gemacht wird und wie man sich dagegen schützt

Illegal Dateien ge-„phisht“

Mit Fischen hat der Begriff Phishing (sprich: Fisching) nur indirekt zu tun: Denn „gefischt“ werden beim Phishing lediglich Dateien – und zwar illegal. Wenn dadurch Bankkonten geplündert werden, ist das ein Problem. Dem sollte man vorbeugen.

Phishing nutzt unsere Dummheit. Der Phisher überrascht wie ein Trickbetrüger mit abenteuerlichen Geschichten: Als käme ein fremder Schlosser ins Haus, erklärt er, er müsse sicherheitshalber alle Türschlösser austauschen, das habe der Hausbesitzer angeordnet – genauso bekommt der PC-Benutzer eine E-Mail, die angeblich von seiner Bank stammt und ihn auffordert, sicherheitshalber die Passwörter noch einmal einzugeben. Konkret werden dann außer der Pin-Nummer (der persönlichen Identifikationsnummer) gleich noch ein paar Tans erbeten, das sind Einmal-Transaktionsnummern. Die E-Mail stammt natürlich nicht von der Bank, und das Eingabeformular erst recht nicht, obwohl es danach aussieht. Beim simplen, kundenfreundlichen Pin-Tan-Verfahren kann der Phisher mit Pin und Tans vom Konto des Betrogenen online Geld überweisen.

Banken haben reagiert

Auf diese Betrügereien haben die Banken mittlerweile reagiert. Das einfache Pin-Tan-Verfahren ist inzwischen abgeschafft. Für eine gültige Überweisung muss beim „indizierten“ Tan-Verfahren jetzt eine ganz bestimmte der hundert Tans genutzt werden, die man von der Bank im Brief bekommen hatte – zufallsgesteuert. Da ist es unwahrscheinlich, dass man gerade diese Tan dem Phisher in Russland verraten hat.

Der Nachteil: Der Bankkunde trägt im Urlaub jetzt die ganze originale Tan-Liste bei sich und nicht nur ein paar Tans für den Notfall. Viele Banken, so die Südtiroler Raiffeisenkassen, lassen sich gar nicht auf ein Pin-Tan-Verfahren ein: Zum Online-Banking braucht da der Kunde eine Chipkarte mit fünfstelliger Geheimnummer, und die muss in einen kleinen Kartenleser in der Größe eines Schlüsselanhängers gesteckt werden. Für Überweisungen generiert der Leser dann einen achtstelligen Einmalkode.

Andere arbeiten mit „Challenge-Respose“: Die Challenge, Herausforderung, ist eine Zufallszahl, die von der Bank kommt. Man gibt sie mit Hand (oder optisch über einen Bildschirmleser) in den separaten Schlüsselrechner ein und erhält eine „Antwort“ – wieder eine Zahl. Nur mit dieser klappt dann die Überweisung, und auch das nur, wenn man nicht zu lange wartet. „Challenge-Response“ nutzt ein Extra-Kästchen und die Chipkarte, um zu prüfen, ob der oder die Rechtmäßige am Draht ist. Ein Betrüger hat weder Karte noch Kartenleser. Für den Bankkunden ist das zwar unbequem, aber sicher.

Wieder andere Verfahren (z. B. HBCI) arbeiten mit einer Chipkarte oder sonst etwas Körperlichem, die „gephisht“ werden kann.

Gefälschte Webseiten gibt es nicht nur bei Banken, auch bei anderen Sites, wo es um Geld geht. Man tut gut daran, die Web-Adresse selbst anzuwählen und nicht klickend einem Link aus einer E-Mail zu folgen (in HTML-Mails können Links falsch aussehen). Die Verbindung muss hernach verschlüsselt sein, erkennbar am Vorhangschloss vor der Web-Adresse und dem „s“ von „https“. Cookies, wichtig für wiedererkennbare und dann ununterbrochene Verbindungen, halte ich für harmlos. Warum, schreibe ich ein andermal.

Theoretisch lässt sich Phishing auch mit so genannten Keyloggern machen, das sind „Tasten-Mitschreiber“: Ein heimlich im PC laufendes Programm schreibt jeden Tastentipp mit und schickt das dann möglichst unauffällig als Datenpaket zum Phisher. Der sucht sich Passwörter heraus. Allerdings muss der Tasten-Mitschreiber erst installiert werden. Das erledigen sogenannte Trojaner, eine Abart von Viren und Würmern. Wer sich blauäugig fremde Programme aus dem Netz holt, ist selber schuld. Eine Prüfung eines Programms – vor Installation! – durch den Virenscanner hilft.

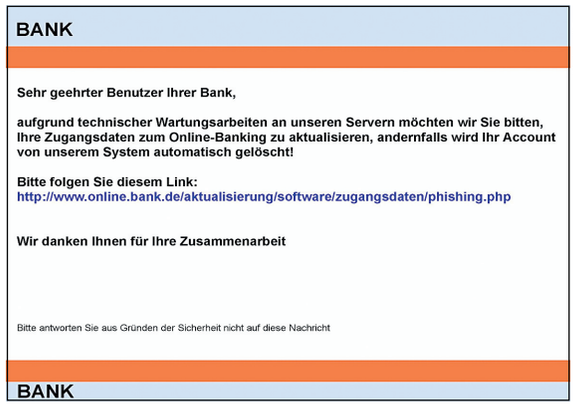

Foto: Jörn

Derlei Aufforderungen sollte man nie nachkommen. Dahinter steckt mit ziemlicher Sicherheit ein „Phisher“.

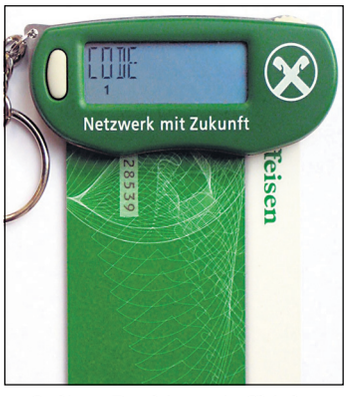

Foto: Schierenbeck/gms

Online- Banking mit Chipkarte und Leser: Dieses System schützt vor Phishing.

Denken, googeln, tippen

Ärgerlich sind auch wohlgemeinte Kettenbriefe mit Viren-Falschmeldungen („Hoaxe“), die zum Löschen irgendeiner harmlosen Standarddatei auffordern oder – schlimmer – gleich ein angebliches Löschprogramm mitbringen.

Auf vertrauliche Geschäftsanbahnungen, meist aus Nigeria, zum Transfer von Millionenbeträgen eines leider tragisch verunglückten Pseudo-Verwandten wird ja wohl niemand mehr hereinfallen: Da werden dann Vorschüsse veruntreut. Auch Lotteriegewinne, die nur auf einen warten, sind Betrug. Also: Nicht auf jede Aufforderung aus dem Netz eingehen, schon gar nicht hastig und übereilt. Erst denken, googeln, dann tippen.

FRITZ JÖRN