Es riecht nach Phish

22.02.2010

Fachartikel VKÖ - Tam Hanna

Banker lieben kassenlose Filialen. Nicht klassenlos, sondern kassenlos – im Finanzjargon steht dieser Begriff für Bankstandorte, an denen keine Überweisungen etc. getätigt werden können.

„Kleingeschäfte“ im persönlichen Kontakt mit einem Berater zu erledigen, ist für den Kunden zweifelsohne angenehm, verursacht dem Institut jedoch enorme Kosten. Als Lösung bot sich – wie in so vielen anderen Bereichen – das Internet an. Doch bald zeigte sich, dass die virtuellen Geldgeschäfte – so praktisch sie auch für alle Beteiligten sein mochten – nicht wenige Gefahren bergen.

Passwörter herbei

Die ersten Versuche mit Onlinebanking orientierten sich an der seit langem bekannten und beliebten Methode der Authentifizierung durch Passwörter. Der Benutzer besitzt hierbei einen nur ihm und der Bank bekannten Code – wenn er diesen auf der Website der Bank eingibt, gilt er als identifiziert.

Cyberkriminelle reagierten schnell: Sie versandten massenhaft E-Mails, in denen die Benutzer aufgefordert wurden, ihr Passwort auf einer dem Original mehr oder minder geschickt nachempfundenen – allerdings natürlich von den Angreifern kontrollierten - Website

einzugeben. Diese leitete das Passwort an ihren „Meister“ weiter und der räumte dann seelenruhig die Konten seiner Opfer leer.

Um eine Nachverfolgung der Überweisungen zu erschweren, wurden Mittelsmänner im Quellland akquiriert. Diese wurden per „Jobangebot“ geködert und gaben den Betrügern arglos ihre Kontonummer. Die Kriminellen überwiesen das Geld ihrer Opfer nun auf die Konten dieser Mittelsmänner. Diese wiederum ließen ihren Auftraggebern das Geld - abzüglich ihrer Provision - per Western Union zukommen. In vielen Fällen waren diese auch „Mules“ (also Maulwürfe) genannten Personen völlig überrascht, als sie plötzlich Besuch vom Staatsanwalt erhielten - sie waren nämlich fest davon überzeugt, einer ganz legalen Arbeit für ein seriöses Unternehmen nachzugehen…

Tan, Tan, Tan

Die Einführung der TANs (Transaction Authentication Numbers) war der erste Schritt zu mehr Sicherheit im digitalen Bankwesen. Der Online-Banking-Kunde erhält dabei eine Liste von Nummern, die er auf der Bankwebseite zur Bestätigung einer Überweisung eingeben muss. Da der Server die anzugebende Nummer zufällig auswählt, genügt es nicht mehr, einfach das Passwort einzugeben – soll heißen: Ohne die richtige TAN gibt’s kein Moos...

Mann in der Mitte

Dies brachte der Welt die so genannte Man-in-the-Middle-Attacke. Dabei wird das Opfer auf eine Webseite geleitet, die der Bankwebseite täuschend ähnlich sieht. Diese ist mit einem Server verbunden, der gleichzeitig eine Verbindung mit dem Computersystem der Bank aufbaut und sich diesem gegenüber als legitimer Bankkunde ausgibt. Dann werden die Anfragen der Bank an das Opfer weitergeleitet, das

diese nichtsahnend beantwortet. Der Server der Gangster leitet diese Angaben dann an das Banksystem weiter...

Sebstschutz…

Bitte verstehen Sie den Autor dieser Zeilen nicht falsch: Es wäre – nicht zuletzt ob der sinkenden Temperaturen – natürlich unsinnig, jetzt wieder den zeitraubenden Weg zum Bankhaus auf sich zu nehmen und dabei auch noch seine Bankgeschäfte nur zu Banköffnungszeiten erledigen zu können. Wenn man auf seinem Rechner ein aktuelles Antivirenprogramm installiert, eingehende E-Mails von Banken (egal, wie echt sie auch aussehen) konsequent ignoriert und URLs immer von Hand in die Adresszeile eingibt, ist man fast 100% geschützt.

…und Fremdschutz

Mittlerweile bieten immer mehr Banken einen noch sichereren - SMS-TAN genannten - Service an. Dabei wird eine SMS mit dem Überweisungsempfänger sowie einem Zahlencode ans Handy des Benutzers gesendet, ohne den die Transaktion nicht freigegeben wird. Da der Benutzer den Empfänger am Display angezeigt bekommt, wird er keine Transaktionen an Unbekannte freigeben – womit auch Man-in-the-Middle-Attacken der Vergangenheit angehören sollten. Abgesehen davon, dass womöglich gerade dann der Akku des Handys leer ist, wenn man eine dringende Überweisung tätigen muss, bietet dieses Verfahren absolute Sicherheit - zumindest so lange, bis der GSM-Verschlüsselungsalgorithmus geknackt wird...

Tam Hanna

Weiterführende Links

http://www.free-av.de - (für Privatanwender kostenlose Antivirensoftware)

http://windowsupdate.microsoft.com - (Sicherheitsupdates für Microsoft-Betriebssysteme)