



Tipps für sicheres E-Banking

Immer neuere Bedrohungen machen das E-Banking unsicherer. Bis vor kurzem war das „Phishing“ eine der gängigsten Methoden. Dabei wurde der Bankkunde durch ein vermeintlich von der Bank kommendes E-Mail auf eine gefälschte Bankseite gelockt. Phishing-Angriffe haben im letzten halben Jahr aber stark abgenommen, da gefälschte E-Mails mittlerweile von aktueller Schutzsoftware erkannt werden.

Ein neues, schwer entdeckbares Angriffsszenario ist die „man-in-the-middle-Attacke“. Dabei genügt es auf einer infizierten Seite zu surfen, um sich den schädlichen Code einzufangen. Meist wird man durch eine E-Mail aufgefordert, auf eine bestimmte Webseite zu gehen, weil dort etwas vermeintlich Interessantes ist (gratis Musik, Filme, pornografische Inhalte etc.). Geht man nun auf die E-Bankingseite, so kann es sein, dass sich die „man-in-the-middle-Software“ zwischen Bank und Benutzer schaltet. So ist es möglich, dass man zwar tatsächlich auf der richtigen Bankenseite ist, die gemachten Eingaben (inkl. Strichlistencode) zum Angreifer gehen. Dieser sendet dem Benutzer möglicherweise eine Fehlermeldung oder sogar eine gefälschte Bestätigung der Bank. Dadurch schöpft der Benutzer keinen Verdacht und der Angreifer kann sich mit den gewonnenen Daten über das Bankkonto hermachen.

Natürlich versuchen die Banken ständig neue Bedrohungsszenarien abzuwenden. Es liegt aber in der Natur der Sache, dass die Angreifer immer einen Schritt voraus sind.

Einen neuen Weg geht dabei die Migros Bank, welche das Übel an den Wurzeln packt. Das Haupteinfallstor für Betrugssoftware ist der Internet Explorer. Deshalb liefert die Bank einen schreibgeschützten USB-Stick mit einem eigenen Internet-Browser für die Bankgeschäfte.

Um einen möglichst sicheren Umgang mit E-Banking zu erlangen, sind folgende Tipps zu befolgen:

- Achten Sie darauf, dass Ihr PC über aktuelle Antivirensoftware verfügt und alle Software-Updates regelmässig ausgeführt werden.
- Pflegen Sie einen wachsamem Umgang während der E-Banking-Sitzung. Melden Sie ungewöhnliche Vorgänge sofort Ihrer Bank. Dazu zählen ungewohnte Fehlermeldungen oder Pop-up-Fenster.
- Misstrauen Sie E-Mails von Absendern, die Sie nicht kennen. Lassen Sie sich nicht durch vermeintlich tolle Angebote auf eine Ihnen unbekannte Webseite locken.
- Verwenden Sie einen anderen Webbrowser anstelle des Microsoft Internet Explorers. Eine gute Alternative ist Mozilla Firefox. Download unter: <http://www.mozilla-europe.org/de/products/firefox/>
- Verwenden Sie ein sicheres Betriebssystem für E-Banking wie z.Bsp. Linux. Ein entsprechendes Angebot finden Sie auf unserer Startseite.

Diese Tipps stellen momentan den besten Schutz für sicheres E-Banking dar. Letztlich muss aber gesagt werden, dass es einen 100%igen Schutz, wie überall im Leben, nie geben wird und sich Angriffsszenarien schnell ändern können.

Neben technischen Massnahmen ist ein gesundes Misstrauen und ein wachsamem Umgang mit dem Medium Internet und E-Mail immer noch der beste Schutz!

Tomtronic GmbH, 3.08 / ts

COMPUTER – MULTIMEDIA – SERVICE

Tomtronic GmbH – Bösch 63 – 6331 Hünenberg – Telefon 041 781 15 19 – Fax 041 781 15 39

E-MAIL info@tomtronic.ch - INTERNET www.tomtronic.ch