cash

«Der Mensch ist die grösste Schwachstelle beim E-Banking»

Hacker-Angriffe nehmen zu, während die Digitalisierung der Finanzindustrie voranschreitet. Was bedeutet das für Bankkunden? Und wie können sie sich schützen? E-Banking-Experte Daniel Walker gibt Tipps.

09.09.2016 13:30
Interview: Ivo Ruch

Daniel Walker ist wissenschaftlicher Mitarbeiter an der Hochschule Luzern.
Bild: ZVG

"Wichtiges Sicherheitsupdate empfohlen": Mit dieser Meldung sahen sich iPhone-Benutzer vor kurzem konfrontiert. Grund war eine ausgeklügelte Attacke, mit der sich ein Spionage-Programm Zugang zu den Apple-Telefonen verschafft hatte.

Das ist bei weitem kein Einzelfall: Bereits in diesem Frühling waren mehrere Schweizer Onlineshops jeweils für einige Stunden nicht mehr verfügbar, weil sie durch Hacker lahmgelegt wurden. Ebenfalls in diesem Jahr veröffentlichten die Sicherheitsexperten des Bundes ein anonymes Erpresserschreiben, das bei rund einem Dutzend Schweizer Finanzinstituten eingegangen sei. Die Tendenz ist klar: Cyber-Attacken nehmen zu und betreffen Konsumenten wie auch Unternehmen.

Daniel Walker ist Informatiker an der Hochschule Luzern und dort mitverantwortlich für das Kompetenzzentrum E-Banking-Sicherheit, das sich mit praktischen Tipps an Endkunden und Mitarbeitende der Finanzindustrie richtet. Im Interview mit cash schätzt er die Sicherheit von Schweizer E-Banking-Portalen ein und sagt, wie man sich vor unliebsamen Angriffen schützen kann.

cash: **Kartenleser, USB-Stick, SMS-Code: Es gibt verschiedene E-Banking-Systeme. Hat es darunter solche, die aus Informatikersicht besonders sicher sind?**

Daniel Walker: Alle in der Schweiz eingesetzten Systeme haben ihre Vor- und Nachteile, bieten durchwegs aber einen sehr hohen Sicherheitsstandard.

Gibt es unsichere Verfahren, die immer noch angewendet werden?

Wesentlich für die Sicherheit eines Verfahrens ist der korrekte Einsatz durch den Benutzer. Eine Transaktionssignatur bringt zum Beispiel nichts, wenn der User die angezeigten Daten nicht überprüft. Der Mensch bildet also die grösste Schwachstelle beim E-Banking. Beispiele von solchen Angriffen sind Phishing-Mails oder Aufforderungen zur Installation von Apps, hinter denen sich ein E-Banking-Trojaner verbirgt.

Aber bei den Finanzinstituten wäre doch viel mehr zu holen.

Ein Angriff auf ein Finanzinstitut oder eine Versicherung ist mit grossem kriminellem Aufwand verbunden. Bei einem erfolgreichen Angriff kann sehr schnell sehr viel Geld erbeutet werden. Dies zeigt etwa der Angriff auf die Zentralbank von Bangladesch Anfang des Jahres, bei dem rund 80 Millionen Dollar entwendet wurden. Es wären übrigens beinahe 850 Millionen geworden. Aufgrund der hohen Sicherheitsstandards bei Schweizer Finanzinstituten erachten wir die Wahrscheinlichkeit für einen erfolgreichen Angriff allerdings als gering. Demgegenüber ist das Schadenausmass bei den Kunden geringer, dafür die Wahrscheinlichkeit eines erfolgreichen Angriffs höher.

Banken müssen immer eine Balance finden zwischen Bedienungskomfort und Sicherheit. Besteht die Gefahr, dass sie zu stark auf die Bedürfnisse der Kunden eingehen?

Die Finanzinstitute in der Schweiz sind sich der Wichtigkeit der Sicherheit ihrer Systeme absolut bewusst. Sie investieren deshalb sehr viel, um die bestmögliche Sicherheit zu gewährleisten und entwickeln ihre Systeme laufend weiter. Gerade die neuen Lösungen für Mobile Banking und Mobile Payment zeigen aber, dass ein für Kunden und Finanzinstitut akzeptierbarer Kompromiss sehr wohl möglich ist.

Internet Banking wird immer häufiger auf Smartphones und Tablets genutzt. Sind diese mobilen Geräte besonders angreifbar?

Insbesondere Android-Smartphones zählen inzwischen zu den beliebtesten Angriffszielen. Dies aber nicht unbedingt deshalb, weil die Geräte per se unsicherer sind, sondern weil diese Geräte von den Benutzern in punkto Sicherheit gerne vernachlässigt werden. Dabei sollte man auf dem Smartphone dieselben Sicherheitsmassnahmen und Verhaltensregeln wie am Computer zu Hause treffen und befolgen.

Welche konkreten Massnahmen empfehlen Sie?

Grundlegend schützen kann man sich mit den folgenden fünf Schritten: Regelmässig ein Backup machen, ein aktuelles Virenschutzprogramm verwenden, die Firewall aktivieren und die Software

auf dem neusten Stand halten. Und, das wird immer wichtiger, den gesunden Menschenverstand walten lassen: Man darf nicht alles glauben, was man im Internet und Mails liest oder am Telefon hört.

Wir erleben eine Zeit der rasch fortschreitenden Digitalisierung in der Finanzbranche. Macht Ihnen das aus Sicht des Sicherheitsexperten Sorge?

Nein, Sorgen macht mir das nicht. Ich sehe aber spannende Herausforderungen auf uns zukommen.

Können Sie konkrete Beispiele nennen?

Wenn Finanzinstitute beispielsweise einen nahtlosen Übergang zwischen allen möglichen Kanälen schaffen möchten, müssen alle Informationen zu einem Kunden kanalübergreifend verfügbar sein – in der Filiale genauso wie auf dem Smartphone des Kundenberaters. Dieser Anspruch generiert neue Anforderungen hinsichtlich Datenschutz und Datensicherheit. Auch bin ich gespannt, welche Veränderungen die Blockchain-Technologie mit sich bringen wird.

Es gibt Experimente mit offenen Wi-Fi-Hotspots, die zeigen, dass sich die Leute sehr sorglos einwählen. Welche Gefahren bringt das mit sich?

Bei offenen unverschlüsselten WLAN werden grundsätzlich alle Daten unverschlüsselt übertragen. Das heisst, ein anderer Teilnehmer im selben Netzwerk kann diese Daten unter Umständen problemlos mitlesen und so an vertrauliche Daten wie Passwörter gelangen. Auch wäre etwa denkbar, dass ein Angreifer den Netzwerkverkehr manipuliert. Für solche Angriffe ist nicht mal spezielle Hardware oder Fachwissen erforderlich. Es gibt mittlerweile sogar einfach zu bedienende Apps fürs Smartphone mit denen automatisiert Angriffe durchgeführt werden können.

Wie kann man sich gegen WLAN-Köder schützen?

Benutzer sollten immer ein 'gesundes' Misstrauen gegenüber unbekannten Netzwerken an den Tag legen. Insbesondere sollte über unverschlüsselte Netzwerke kein E-Banking betrieben oder vertrauliche Daten versendet werden. Wenn immer möglich, sollte man sich nur mit WPA2-verschlüsselten Netzwerken verbinden.

Diverse Online-Shops wurden in den letzten Monaten attackiert, zuletzt wurde der Klau von Millionen Dropbox-Passwörtern bekannt. Nehmen Hacker-Angriffe ganz grundsätzlich zu?

Diesen Eindruck können wir grundsätzlich bestätigen. So hat sich seit Anfang Jahr etwa die Bedrohungslage durch Ransomware, ein sogenannter Erpressungs-Trojaner, deutlich verschärft. Immer häufiger geraten KMU ins Visier von Angreifern. Auch ist in letzter Zeit vermehrt von Datendiebstählen wie jenem bei Dropbox zu lesen. Umso wichtiger ist es, dass Benutzer für verschiedene Dienste, insbesondere etwa fürs E-Banking oder E-Mail-Konten verschiedene Passwörter wählen.

Investieren Schweizer KMU zu wenig in ihre Sicherheit?

Ich kann mir gut vorstellen, dass das Sicherheitsbewusstsein in kleineren Unternehmen weniger ausgeprägt ist als bei grösseren. Und vielfach dürften wohl auch die Ressourcen fehlen, um sich ausführlicher mit dem Thema Informationssicherheit auseinanderzusetzen.

Werden viele Schweizer E-Banking-Kunden Opfer von Hacker-Angriffen oder versuchen die Banken, das unter dem Deckel zu halten, damit die Öffentlichkeit wenig mitbekommt?

Dazu liegen uns keine genauen Zahlen vor. Die Zahl der Schweizer Opfer dürfte im internationalen Vergleich aber niedrig sein.

Gibt es einfache Sicherheits-Tipps, die man E-Banking-Nutzern mit auf den Weg geben kann?

Wie bereits erwähnt, sollte man ganz allgemein die fünf Schritte befolgen. Bezogen aufs E-Banking sollte man zudem nachfolgende Punkte beim Ein- und Ausloggen beachten. Beim Einloggen die Adresse zum Finanzinstitut immer von Hand in der Adresszeile eingeben. Bevor man sich anmeldet, sollte man die sichere Verbindung prüfen: Es darf keine Fehlermeldung angezeigt werden, in der Adresszeile muss https und ein Schloss-Symbol erscheinen und der Name ihres Finanzinstituts muss im Browser ersichtlich sein. Nach dem E-Banking sollte man sich über entsprechende Schaltflächen abmelden oder ausloggen. Zudem ist es empfehlenswert, den Browser-Speicher zu leeren.