

SICHERHEIT IM E-BANKING

Die LLB geht eigene Wege

Die Attacken auf Banken über den Web-Browser häufen sich. Die Liechtensteinische Landesbank verfolgt **im E-Banking einen neuen Ansatz** – und entledigt sich so der mit dem konventionellen Browser-Ansatz verbundenen Probleme. **MATTHIAS NIKLOWITZ**



Der moderne Banküberfall erfolgt auf dem elektronischen Kanal.

Wer als Informatikverantwortlicher einer Bank die Berichte der Melde- und Analysestelle Informationssicherung (Melani) des Bundes liest, findet da reichlich schlafraubende Meldungen. Die aktuellen Meldungen haben meistens mit dem E-Banking zu tun. «In der Schweiz nehmen die gezielten Hacker-Attacken auf Konti von Privaten und Institutionen zu, die ihren Zahlungsverkehr online über den PC abwickeln», heisst es etwa in einem Newsletter vom Mai, «die Schadfunktionen umfassen unter anderem auch den ungewollten Zugriff auf das E-Banking-Konto. Dem Surf-

verhalten kommt deshalb vermehrt grosse Bedeutung zu.»

Phishing, Hijacking und Spyware

Das kritische Element dabei ist der Web-Browser. Mit diesem können Benutzer zwar alle möglichen Internetseiten abrufen, aber der Browser bietet auch ein problematisches Einfallstor für Attacken unterschiedlicher Provenienz. Vor allem das «Phishing», das gezielte Umleiten des Nutzers auf eine täuschend echt nachgebaute Internetseite einer «Bank» sowie das «Hijacking», das unbemerkte «Entführen»

von laufenden Online-Vorgängen sind beliebt. Die Aufforderung zu Dateneingaben kommt meistens als unschuldiges Massen-E-Mail («Spam»), das den Empfänger auffordert, auf einer bestimmten Seite seine Passworte und Zugangsdaten – «aus Sicherheitsgründen» – einzugeben.

Allein der Besuch von bestimmten Seiten kann dazu führen, dass spezielle Software auf PC oder Notebook des Benutzers installiert wird, die seine Tastatureingaben weitermeldet oder Inhalte ausspäht. Auch solche «Spyware» gelangt teilweise über E-Mails auf die Festplatten der Opfer.

IT-Branche hinkt immer nach

In der Praxis behilft sich die IT-Branche mit einem gestaffelten Vorgehen: Browser-Hersteller wie Microsoft oder Firefox liefern regelmässig «Patches» («Flicken») aus, die erkannte Schwachstellen des Browsers beheben. Und die nicht erkannten?

Darauf kann die Industrie nur mit Warnungen, E-Mails unbekannter Absender nicht zu öffnen, reagieren. Sicherheits-Softwarefirmen wie Symantec, McAfee, Trend Micro und weitere beliefern ihre Kunden mit Firewall- und Antiviren-Programmen, aber gerade die Antiviren-Software erfordert regelmässige Update. Zwischen Attacken und der Reaktion von Firmen liegen immer einige Stunden, während denen Angriffe ungestört erfolgen können. Die meisten Banken erhöhen zudem die Zutrittschürden für unerlaubte Eindringlinge, indem sie die rechtmässigen Benutzer des E-Bankings mit Streichlisten usw. ausstatten. Der Zugriff erfolgt dann aber immer noch über den Browser.

Alternative: Java Rich Clients

Dabei stand gleich zu Beginn des E-Bankings eine sichere Alternative zur Verfügung – die «Java Rich Clients». Dieser Weg wurde indes von den Banken nicht weiterverfolgt – aus Kostengründen, wie es heisst. Als eines der wenigen Institute setzt die Liechtensteinische Landesbank LLB auf eine solche Java-Rich-Client-Lösung.

Die Verwendung der Programmiersprache Java hat den grossen Vorteil, dass die Software überall läuft, unabhängig vom Betriebssystem des PCs oder Notebooks. «Rich Client» bedeutet in der Informatikwelt, dass auf dem

Endgerät ein Programm installiert wird – im Gegensatz zum «Thin Client», bei dem das Programm auf einem zentralen Server läuft und auf dem Endgerät lediglich ein Browser als «Fenster» läuft.

Welches sind die Erfahrungen, welche die LLB mit ihrer Lösung der Zürcher Ergon Informatik gemacht hat?

«Das iBanking wurde im September 1999 in Produktion genommen», sagt Werner Schaedler, Leiter der Entwicklungsabteilung Electronic Banking bei der LLB, «damals basierte die Lösung noch auf der Browsertechnologie mit Java-Applets.» Und weiter: «Eine grosse Herausforderung an unsere Support-Abteilung waren die verschiedenen technischen Voraussetzungen bei den Kunden. Einzelne Browser entsprachen nicht unseren Sicherheitsanforderungen und mussten mit Produkten von Drittherstellern aufgerüstet werden. Sowohl durch unsere Sicherheitsanforderungen als auch die Inkompatibilität der verschiedenen Browser und deren Versionen waren unsere Supportleistungen sehr hoch und damit die Voraussetzungen für einen problemlosen Masseneinsatz nicht gegeben», erläutert Schaedler.

In Zusammenarbeit mit anderen Banken habe man sich dann unter Herstellern und Anbietern wie der AGI, NCR, Hewlett-Packard, Ergon oder Brokat nach anderen Lösungen umgesehen. Eine Kooperation unter diesen Banken sei zwar nicht zustande gekommen, aber das Lösungskonzept und die Erfahrung von Ergon seien für die Landesbank so interessant gewesen, dass eine Zusammenarbeit ins Auge gefasst worden sei.

Nach einer kurzen, aber intensiven Konzeptphase konnten gemäss Schaedler bereits erste Funktions- und Kompatibilitätstests anhand eines Prototypen gemacht werden. «Das iBanking der Liechtensteinischen Landesbank AG basierte fortan auf einem Rich Client, welcher mit einem einfachen Installationsprozedere auf jedem PC oder Notebook unter den Betriebssystemen WinXP, Vista, Linux, Mac zum Einsatz kommen konnte», erklärt er.

Erfahrungen mit Java-Anwendungen hatte die LLB zuvor keine gesammelt. «Wir entwickeln unsere zentralen Bankenanwendungen selber», sagt Schaedler, «hier jedoch haben wir uns

entschieden, mit einem Partner zusammenzuarbeiten, der das ganze Frontend entwickelt, während wir die Integration in das Banken-Backend vornehmen.» Massgeblich für den Entscheid war auch die effiziente Zusammenarbeit in diesem Vorprojekt mit Ergon. «Der Prototyp war in einem Monat fertiggestellt», schildert Schaedler, «das hat uns darin bestärkt, uns für diese Lösung und diesen Partner zu entscheiden.»

Die LLB setzte schon bei der Browser-Lösung auf x.509-Zertifikate. Durch den Wegfall des Browsers und den kombinierten Einsatz einer eigenen und somit speziellen iBanking-Software mit digitalen Zertifikaten erreichte die LLB-iBanking-Lösung das höchste Sicherheitsniveau. Auch die gängigen Angriffswege auf das iBanking wie das Phishing sind damit laut Schaedler unmöglich.

Höchstmass an Sicherheit statt Kosten/Nutzen

Kosten-Nutzen-Überlegungen bezüglich der Sicherheitslösung wurden dabei nicht angestellt, ein Höchstmass an Sicherheit war das Ziel. Kunden haben auf einem USB-Token, den sie an ihrem Schlüsselbund tragen können, den elektronischen Schlüssel zu ihren Online-Transaktionen.

Welchen konkreten Nutzen haben die Kunden? «Der Zugang ist gleichermaßen einfach und sehr sicher», erklärt Schaedler, «iBanking-Kunden benötigen neben einem Passwort lediglich den USB-Token. Die Verwendung einer Streichliste oder Geräte zur Ge-

nerierung von Transaktionsnummern entfallen.» Er hat nie ernsthafte Attacken auf das System erlebt. «Dies ist auch darauf zurückzuführen, dass wir unser iBanking regelmässig durch ständig wechselnde spezielle Sicherheitsfirmen überprüfen lassen und auch laufend Investitionen zur Aktualisierung unserer Sicherheitslösungen tätigen», sagt Schaedler, «und von den grossen Phishing-Wellen, welche vorwiegend die browserbasierenden iBanking-Lösungen betroffen haben, waren wir nie tangiert.»

Und wenn ein Notebook gestohlen würde? «Das alleine stellt kein Problem dar, denn den Zugang auf seine Konten erlangt der Kunde ausschliesslich mittels seines persönlichen Zertifikates, welches sich geschützt durch ein Kennwort auf dem USB-Token befindet. Somit stellt auch der Verlust oder Diebstahl des USB-Token keine unmittelbare Gefahr dar, sofern mit dem Token nicht auch das Kennwort und Passwort in falsche Hände gerät. Bei Verlust, Diebstahl oder sonstigem Verdacht auf Missbrauch kann unsere Hotline kontaktiert und der Zugang jederzeit gesperrt werden.»

Eine Erweiterung des iBanking in Richtung weitere Typen von Endgeräten – beispielsweise Handys, Smartphones usw. – ist laut Schaedler derzeit nicht geplant. «Wir haben sowohl mit der Lösung als auch dem Partner sehr gute Erfahrungen gemacht», resümiert er, «und ich rechne damit, dass zukünftig vor allem Zertifikatslösungen vermehrt im iBanking-Umfeld zum Einsatz kommen werden.»

Anzeige

:: Frontend-Tools
:: Fondsadministration
:: Kundendokumente


 Wirkung erzielen.
www.kwsoft.ch