Gehärteter Browser: Airbag für das Online-Banking

Von Frank Bock und Detlev Mergemeier

Beim Online-Banking befindet sich die Kreditwirtschaft permanent im Wettlauf mit den Cyber-Kriminellen. Weil die neuen Authentifizierungsverfahren ein hohes Maß an Sicherheit bieten, verlagern sich Angriffe mehr und mehr auf die Manipulation der Bildschirmdarstellung, um die Nutzer zu falschem Verhalten zu bewegen. Technische Schwachstelle Nummer eins ist hier der Browser. Für die Genossenschaftsorganisation hat die GAD deshalb einen „gehärteten" Browser im Angebot, den die Autoren als zusätzlichen Sicherheitsring, ähnlich dem Airbag als Ergänzung zum Sicherheitsgurt beschreiben. Weil er für jede Bank einzeln erstellt wird, ist auch ein „Knacken" des ganzen Systems nicht möglich. Red.

In den letzten Jahren hat die Zahl der Computer in Deutschland mit über 50 Millionen registrierten Geräten die Zahl der zugelassenen Pkw überstiegen. Das Internet ist vom Tummelplatz für Computerfreaks und Wissenschaftler zum Online-Medium für alle Deutschen geworden. Eine Bestellung bei Amazon, eine Überweisung im Online-Banking und das Ummelden der Wohnung via Internet sind heute genauso einfach wie Autofahren.

Leider hat der große Erfolg der Online-Geschäftsprozesse auch seine Schattenseiten: Mit jedem umgesetzten Euro und mit jedem online bestellten Artikel wird der private PC mehr und mehr zum Lieblingsziel von Computerkriminellen und Trickbetrügern.

Fragt man die Hersteller von Sicherheitssoftware, so gibt es natürlich für jeden Computerschädling ein geeignetes Sicherheitspaket, für jeden Virus einen Antivirus und für jede Sicherheitslücke die passende Firewall. Trotzdem nimmt die Zahl der Computerviren und der ausspionierten PCs weiter zu. Hierbei liegen Banken nach wie vor im Fokus der Internetkriminellen, denn sie allein verfügen über einen massentauglichen Geschäftsprozess, aus dem man direkt Bargeld entwenden kann: das Online-Banking.

Banken sind schon seit zehn Jahren mit aggressiver Schadsoftware, Spionage-Programmen und den kriminellen Methoden der Internetmafia konfrontiert. Im Rahmen ihres Abwehrkampfes wurden Software und Verfahren mehrfach ausgetauscht. Die Authentifizierung des Nutzers wurde verbessert, Zertifikate eingeführt und teilweise auf externe Hardware ausgelagert. Am Ende wurden hochsichere Zwei-Schritt-Transaktionssysteme wie Sm@rt-TAN-plus/optic (VR-Banken) oder chip-TAN-comfort (Sparkassen) eingeführt, um dem Treiben der Banking-Trojaner ein Ende zu setzen.

Zu den Autoren

Dr. Frank Bock ist Geschäftsführender Gesellschafter der CORONIC GmbH, Kiel. **Detlev Mergemeier** ist Produktmanager Elektronische Vertriebswege bei der GAD eG, Münster.

Der Nutzer im Fokus der Angriffe

Weil diese neueren Verfahren bei korrekter Verwendung extrem sicher sind, haben die Internet-Kriminellen ihr Angriffsziel verlagert. Im Fokus steht nicht mehr das Verfahren selbst, sondern der Nutzer des Verfahrens, der Mensch. Kann die Aufmerksamkeit des Nutzers überlistet werden, sodass er die angezeigten Überweisungsdaten nicht mehr korrektauf Gültigkeit überprüft, so ist auch hier ein Zugriff auf das Online-Konto möglich.

Die Voraussetzung dafür ist meist nur die Manipulation der Bildschirmdarstellung, um den Nutzer zu falschem Verhalten zu animieren. Da sich Trojaner heute mit Rootkit-Technologie vor der Entdeckung verbergen und erst dann aktiv werden, wenn es darum geht, die Manipulation tatsächlich durchzuführen, ist diesem Vorgehen häufig Tür und Tor geöffnet.

Der Trick ist immer der gleiche, solange der Trojaner die Bildschirmanzeige mani-

pulieren kann, kann er den Nutzer zu jedem beliebigen Fehlverhalten verleiten. Auch Europas oberste Sicherheitsbehörde, die ENISA, empfiehlt vor diesem Hintergrund, „jeden PC als infiziert zu betrachten".

Schwachstelle Browser und Schwachstelle Mensch

Ein Beispiel für die gelungene Manipulation des Nutzers: Herr Müller meldet sich beim Online-Banking an und sieht, dass der Kontostand 5 000 Euro zu hoch ist. Diesen Umstand erklärt ein vorgetäuschtes elektronisches Schreiben seines Bankberaters. „Ihm sei versehentlich ein Betrag der Firma Mustermann gutgeschrieben worden, ob Herr Müller wohl so nett wäre, das Geld noch heute zurück zu überweisen." Kein Problem sagt sich Herr Müller und überweist die 5 000 Euro zurück. Erst beim nächsten Gang zum Kontoauszugsdrucker in den Geschäftsräumen der Bank erfährt er, dass es die Überweisung und das Schreiben des vermeintlichen Bankberaters in Wahrheit nie gegeben hat.

Rein technisch betrachtet hat Herr Müller alles richtig gemacht. Er hat sich korrekt angemeldet und sich richtig authentifiziert. Er hat das vorgesehene Verschlüsselungsverfahren der Bank eingesetzt und sich sogar von der Echtheit der SSL-Zertifikate überzeugt – aber all das hilft nicht, das Geld ist trotzdem weg.

Bankindividueller Browser als zusätzliche Sicherheit

Die technische Schwachstelle ist hierbei Prinzip-bedingt immer der Internet-Browser. Seine Aufgabe ist es, jede Internetseite anzuzeigen und jedes Video abzuspielen. Der Browser erlaubt erst einmal alles – und ist damit alles andere als sicher. So zielen auch die Angriffe der Banking-Trojaner stets auf die Manipulation von Browserfunktionen ab. Sie verändern die Seitendarstellung der Bank im Browser und täuschen den Nutzer mit gefälschten Einblendungen.

Genau hier setzt die Lösung VR-Protect an. VR-Protect sieht aus wie ein normaler Browser, funktioniert wie ein normaler Browser und bietet doch optisch-individuelle Unterscheidungsmerkmale, die für den Kunden klarmachen: Jetzt arbeite ich mit dem sicheren Browser.

Das Programm wird als ausführbare Datei mit nur sechzehn MB Dateigröße (inklusive eines Plugin zur Verarbeitung von Chipkarten) an den Kunden ausgeliefert. Es läuft ohne Installation, ohne Konfiguration, ohne Administratorrechte und kann per Doppelklick direkt vom Desktop aus gestartet werden. Der Browser schreibt nichts auf den PC, trägt keine Werte in die Windows-Datenbank ein und verhält sich so gegenüber dem Kunden-PC nicht intrusiv.

Der Bank-Browser wird für jede Bank einzeln erstellt und unterschiedlich mit Funktionen angereichert. Jede Bank erhält so ihren eigenen individuellen Browser. Selbst wenn also eine Browserversion geknackt würde, sind doch alle anderen Bank-Versionen davon nicht betrof-

fen und der Angriff wird ökonomisch unsinnig.

Im Pilotbetrieb getestet

20 Banken haben VR-Protect fast ein Jahr lang im Pilotbetrieb getestet. Eingesetzt wird die Lösung sowohl bei Privat- als auch Firmenkunden. Die Erfahrungen sind durch die Bank weg positiv.

Bei den Privatkunden der Banken werden insbesondere die einfache Handhabung und die hohe Mobilität der Lösung gelobt. Aufgrund der geringen Dateigröße kann der Browser immer mitgenommen werden und so können an jedem Computer – auch einem bereits infizierten – sichere Online-Transaktionen durchgeführt werden.

Bei den Geschäftskunden besteht der größte Erfolg in der mobilen und absolut sicheren Kombination von voll signaturfähiger Hardware zusammen mit dem gehärteten Browser, der so auch an Arbeitsplätzen mit eingeschränkten Nutzungsrechten (zum Beispiel Hotel oder Internetcafé) immer funktionsfähig ist.

Bei beiden Kundengruppen gibt es außerdem ein sehr positives Feedback in Bezug auf die verbesserte „gefühlte Sicherheit". Dies stärkt beim Kunden das Vertrauen in das Online-Banking. Selbst neue Kunden, die bislang andere Vertriebswege nutzen oder noch beleghafte Zahlungsaufträge einreichen, lassen sich so für das Online-Banking gewinnen.

Leicht veränderliche Sicherheitsmaßnahmen

Bei dem Bank-Browser handelt es sich um ein dynamisches System von leicht veränderlichen Sicherheitsmaßnahmen. Bei einem Angriff kann binnen weniger Stunden durch Veränderung der Sicherheitsfunktionen und ein schnelles Update reagiert werden. Dadurch steht den Banken endlich ein Mittel zur Verfügung, das schnell und zielgerichtet auf Trojaner-Angriffe reagieren kann.

Der Bank-Browser versteht sich dabei nicht als alleiniges Sicherheitsmerkmal, sondern als zusätzlicher Sicherheitsring, der die bestehenden Verfahren umschließt und zusätzlich härtet. So kann der Browser der allgemein schlechten gefühlten Sicherheit entgegenwirken und dem Online-Banking neue Impulse verleihen. Mittelfristig kann er als Vorlage dienen, um weitere Geschäftsprozesse im Internet zu härten.

Seit Februar 2013 ist VR-Protect für alle Volks- und Raiffeisenbanken im Geschäftsgebiet der GAD freigegeben. Die VR-Banken sind die erste Bankengruppe, die diesen zusätzlichen Schutz für ihre Kunden nutzt. Andere Banken setzen nur auf Verbesserungen bei den bestehenden Sicherheitsverfahren oder die zusätzliche Sensibilisierung der Kunden. VR-Protect hingegen schützt den Kunden vorbeugend und setzt dort an, wo die meisten Angriffe passieren – am PC des Kunden. In Kombination mit dem sicheren Online-Banking bietet VR-Protect damit einen zusätzlichen Schutzring für den Kunden. Er ist wie der Airbag zum Sicherheitsgurt, die perfekte Ergänzung, um das Online-Banking auf allen Seiten noch sicherer zu machen.