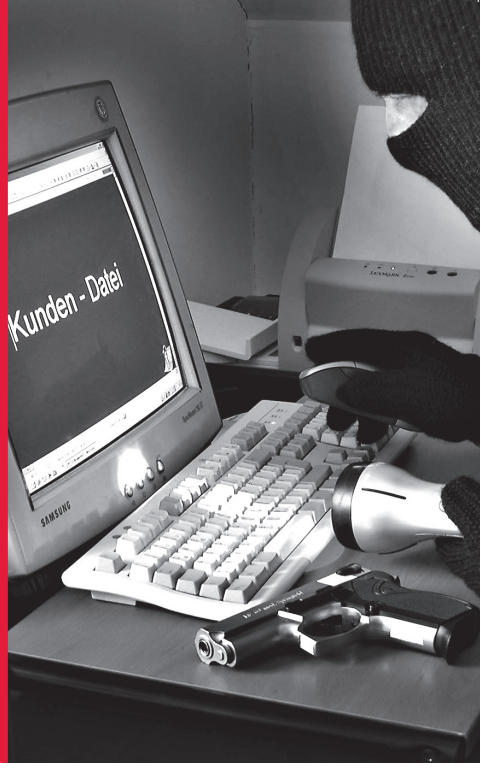
Cyber Crime – virtuell und sehr real

Von Stefan Klaeser



Absolute Sicherheit im Internet-Zahlungsverkehr ist eine Illusion, so Stefan Klaeser. Methoden, die Sicherheit zu erhöhen, müssen stets die Balance finden zwischen hinreichender Komplexität und dem, was der Kunde noch akzeptiert. Im Wettlauf mit den Kriminellen werden nach Einschätzung des Autors aber nicht neue Technologien entscheidend sein, sondern eine intelligente Nutzung vorhandener Methoden. Voraussetzung für den Erfolg: Alle Beteiligten müssen eng verzahnt agieren. Red.

Der Missbrauch von Zahlungskarten war in den vergangenen zehn Jahren einem starken Wandel unterzogen. Der „klassische" Diebstahl der Karte direkt vom Besitzer oder auf dem Postweg findet kaum noch statt. Viel zu aufwendig ist es für den Kriminellen, physisch in den Besitz des Zahlungsmittels zu gelangen.

Die zunehmende Virtualisierung unseres Lebensraumes hat uns viele Erleichterungen im Alltag gebracht und völlig neue Möglichkeiten eröffnet. So wird das Netz künftig auch mehr und mehr Schauplatz betrügerischer Aktivitäten. Der Missbrauch von Zahlungskarten kann nun überall dort stattfinden, wo online Transaktionen getätigt werden. Die im Englischen so treffend bezeichnete „face-to-face"-Situation entfällt und damit eine sehr bedeutende Hemmschwelle.

Ähnlich sieht die Situation beim Onlinebanking aus, welches für die Virtualisierung von Bankvorgängen eine zwingende Voraussetzung ist und einen maßgeblichen Anteil am schnellen Wachstum des Internet ausmacht. Erst durch den Verzicht auf den persönlichen Kontakt, der mit einem Komfortgewinn des Onlinebanking einhergeht, ist der Missbrauch in einer neuen Dimension möglich geworden. Ein wichtiger Aspekt hierbei ist, dass durch die Virtualisierung aller Zahlungssysteme diese auch alle denselben Gefahren ausgesetzt sind. Es spielt kaum mehr eine Rolle, welcher Zahlungsstrom angegriffen wird – die Angriffsmittel sind in jedem Fall gleich oder zumindest ähnlich.

Die Underground-Economy ist ein mächtiger Wirtschaftszweig

Weitgehend unbemerkt, zumindest aber fast ungehindert von der Finanzwirtschaft, hat sich ein kriminelles System entwickelt, welches das Potenzial hat, künftig desaströse Schäden zu verursachen. Dieses System besteht in der Hauptsache aus drei kriminellen Gruppen: die Zulieferer, die Abnehmer und die Auftraggeber. Der Zulieferer entwickelt und vertreibt „Malware" (zu Deutsch: Schadsoftware). Mit dieser Malware greifen die Abnehmer Computer über das Internet an, um fremde Daten entweder massenhaft oder gezielt abzugreifen. Anschließend werden die Daten an die profitorientierten Auftraggeber übermittelt. Diese Marktsituation ist die Grundlage für das Wirtschaftssystem von Personen, die sich darauf spezialisiert haben, über das Internet Geld von Personen und Firmen zu stehlen: die Underground Economy.

Die größte Gefahr dieses Wirtschaftszweiges ist, dass es sich bei den Schlüsselpersonen um hervorragend ausgebildete Experten auf dem Gebiet der Informationstechnologie handelt. Sie setzen ihr Wissen ein, um die von ihren ehrlichen Kollegen mit besten Absichten vermeintlich sicher gestalteten Systeme auszuhebeln. Die jüngste Erfahrung mit 3-D-Secure zeigt uns, dass im Wettlauf um sicheres Bezahlen die kriminelle Welt selbst bei einer flächendeckenden Einführung neuer Sicherheitsmechanismen immer einen Schritt voraus ist.

Der Missbrauch von Daten ist nur ein Aspekt des Cyber Crime

Neben dem Diebstahl von virtuellem Geld gibt es weitere Bedrohungen, die täglich tausendfach stattfinden. Kürzlich wurden

Zum Autor

Stefan Klaeser ist Vorstand der PAYMINT AG, Frankfurt am Main.

die Auswirkungen auch für die breite Öffentlichkeit sichtbar. Die Webseiten von führenden Zahlungssystemen waren im Zusammenhang mit Wikileaks über viele Stunden nicht erreichbar. Dieses „Lahmlegen" war nichts anderes als die Überschüttung der Server dieser Unternehmen mit Website-Anfragen von vielen tausend Computern gleichzeitig (sogenannte d-DoS-Attacke – distributed Denial of Service). Dabei werden mittels Malware Rechner unfreiwillig zum Teil eines Bot-Netzes gemacht.

Bot-Netze bestehen aus ganz normalen Computern ganz normaler User, die mit Malware (konkret: Trojaner) infiziert wurden. Ein solches Bot-Netz schließt oft viele Tausende oder gar Millionen mit dem Internet verbundene Computer zu einer riesigen Einheit zusammen, die auf ein Ziel hin operiert. Man braucht nicht sehr viel Vorstellungskraft um sich auszumalen, dass auch die Onlinebanking-Systeme von solchen d-Dos-Attacken getroffen werden können. Einige Experten halten illegale Bot-Netze für die größte Bedrohung in der virtuellen Welt.

Der Konsument – Statist beim Cyber Crime

Den Virenscanner immer auf dem aktuellen Stand, die Firewall aktiv – der Beitrag des Internetnutzers reduziert sich hauptsächlich auf diese beiden Punkte. Und trotz dieser Maßnahmen können seine Bankzugangs- oder Kreditkartendaten entwendet und missbräuchlich genutzt werden. Die unrechtmäßigen Belastungen werden fast immer von seiner Bank zurückerstattet – entgegen Fernsehberichten, die etwas anderes suggerieren. Jedoch sinkt mit jedem solcher Fälle das Vertrauen des Konsumenten in das Online-Zahlungssystem.

Es ist jedoch anzunehmen, dass diese Haltung mit generell zunehmender Internetnutzung künftig weiter an Bedeutung verlieren wird. Die stark wachsenden sozialen Netzwerke verdeutlichen dies auf beeindruckende Weise. Und die freiwillig hinterlassenen Datenspuren in den sozialen Netzwerken werden zu mächtigen Werkzeugen für Kriminelle.

Authentifizierung – der Schlüssel zu mehr Sicherheit

Die virtuelle Authentifizierung funktioniert heute oft noch durch Benutzername-Passwort-Kombination, sogar im Banking-bereich. Finanzielle Transaktionen hingegen sind in der Regel nur über eine „2-factor-authentication" möglich. Hierzu bedarf es zweier Merkmale zur Durchführung einer Transaktion – etwas, das man weiß (zum Beispiel eine PIN oder Passwort) und etwas, das man hat (zum Beispiel eine TAN-Liste oder eine HBCI-Karte). Selten kommen auch bereits „Tokens" zum Einsatz, die einen Zahlencode generieren. Aus Konsumentensicht sind schon die heute bestehenden Authentifizierungssysteme kompliziert und benutzerunfreundlich. Doch wissen wir auch, dass viele der heutigen Verfahren und flankierende Sicherheitsmaßnahmen von Kriminellen ausgehebelt werden können.

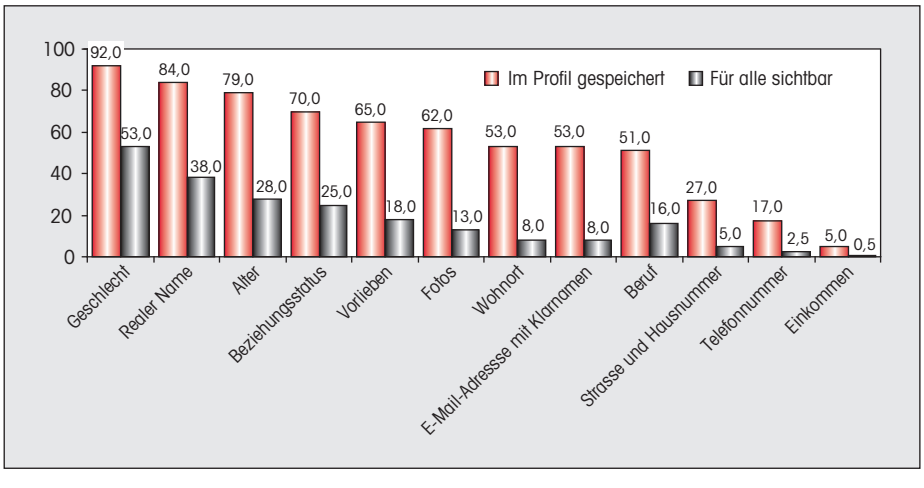
Neue Technologien wurden in der Vergangenheit oft zu spät eingeführt und nicht zuletzt dadurch ist ihre Halbwertszeit erheblich gesunken. Dabei gilt: Je höher die Sicherheit, desto komplizierter ist es für denjenigen, der seine Identität nachweisen muss. Das Mobiltelefon tragen vermutlich viele immer mit sich, und ein kombinierter Einsatz von Computer und Mobiltelefon wäre für internetaffine Konsumenten vermutlich akzeptabel, um Finanztransaktionen durchzuführen. Doch auch Mobiltelefone sind eigenständige Computer, und es war nur eine Frage der Zeit, bis auch diese mit Malware infiziert werden. Ende 2010 ist es Kriminellen gelungen, gewisse m-TAN-Verfahren zu „hacken".

Ein zusätzliches Gerät, um Zahlungstransaktionen abzusichern wird bei einem Großteil der Kunden jedoch kaum auf Gegenliebe stoßen. Auch würde es eine Einschränkung der Freiheit bedeuten, jederzeit überall einkaufen oder Finanztransaktionen durchführen zu können, sollte der Nutzer das zusätzliche Gerät an einem festen Ort aufbewahren.

Biometrie für den Zahlungsverkehr noch nicht geeignet

Zusätzlich zu diversen Authentifizierungsmerkmalen kann ein biometrisches Merkmal des Konsumenten hinzugezogen werden. Die technologischen Möglichkeiten im Bereich der Biometrie sind weit fortgeschritten. Jeder USA-Reisende muss bei der Einreise in das Land seinen Fingerabdruck scannen lassen und auch auf dem neuen Personalausweis kann er gespeichert werden.

Anzahl der aktiven Nutzer von Facebook in Deutschland (Angaben in Prozent)



Jedoch ist fraglich, ob diese Technologie bereits massentauglich ist, um elektronische Zahlungen zu authentifizieren. Darüber hinaus stellt sich hier ebenso die Frage nach der notwendigen Hardware. Die Gesichtsfelderkennung hat aus Hardware-Gesichtspunkten den Vorteil, dass viele Computer bereits mit einer Kamera ausgestattet sind. Einige Computer-Hersteller nutzen die Gesichtsfelderkennung bereits für die Authentifizierung des Bedieners. Neuere Verfahren wie Hand-Venen-Erkennung sind noch wenig bekannt und zumindest derzeit noch keine Alternative.

Allen biometrischen Verfahren ist gemein, dass es eine sichere Erstregistrierung geben muss, die – um hier Missbrauch auszuschließen beziehungsweise einen vollkommenen Schutz gewährleisten zu können – in einer sicheren Umgebung zum Beispiel bei der Bank stattfinden muss. Es entsteht relativ schnell der Eindruck, dass solche Lösungen für das Massenprodukt elektronischer Zahlungsverkehr noch nicht geeignet sind. Die Angst vor möglichem Missbrauch der gespeicherten biometrischen Daten beziehungsweise möglicher Identitätsdiebstahl wird die Einführung solcher Verfahren in der Breite der Bevölkerung ebenso behindern.

Absolute Sicherheit ist eine Illusion

Die Angst vor dem Missbrauch persönlicher Daten steht augenscheinlich in einem extremen Widerspruch zu dem, was Menschen in sozialen Netzwerken über sich preisgeben. Argwohn entsteht offenbar erst, wenn persönliche Daten abgefragt werden, nicht aber wenn sie freiwillig zum „Networking" auf Facebook, Wer-kennt-wen?, Studi-VZ und dergleichen gepostet werden. Könnte hier der Schlüssel zur einfachen, aber sicheren Authentifizierung von Personen liegen?

In der Diskussion um mehr Sicherheit und neue Verfahren gerät eine wichtige Tatsache leicht in Vergessenheit: Der Kauf im Internet ist eine beabsichtigte Aktion, die die Bedürfnisse des Käufers befriedigt. Das Bezahlen selbst hingegen gehört nur zwangsläufig dazu und muss daher zwar sicher, aber auch so einfach wie möglich gestaltet werden. Die meisten heute genutzten Verfahren sind jedoch genau das nicht: Einfach. Angesichts der sinkenden Halbwertszeit von neuen Technologien und der hinsichtlich Ausbildung und technischer Ausstattung „auf Augenhöhe" agierenden kriminellen Szene werden nicht neue Technologien eine entscheidende Rolle spielen, sondern die intelligente Nutzung bereits vorhandener Mechanismen und Quellen.

All diese Themen und Punkte zeigen, dass die absolute Sicherheit – insbesondere im Internet – eine Illusion ist. Es wird immer Bestrebungen von Kriminellen geben, sich auf Kosten anderer zu bereichern.

Ein entscheidender Erfolgsfaktor beim Kampf gegen die Gefahren des Cyber Crime wird sein, wie gut die betroffenen Player kooperieren. Die Angriffsszenarien sind für alle virtuellen Aktivitäten – völlig ungeachtet des verwendeten Zahlungsmittels – identisch. Strategien und Aktivitäten zur Abwehr von Missbrauch dürfen daher nicht mehr auf ein Produkt oder auf einen Zahlungskanal beschränkt werden, sondern müssen übergreifend stattfinden.

Voraussetzung ist eine enge Vernetzung der Beteiligten – analog zum kriminellen Netzwerk. Es besteht sonst die Gefahr, dass die Kriminellen der Finanzbranche bald nicht mehr nur einen Schritt, sondern um Längen voraus sind. Der Kampf gegen die Internet-Kriminalität hat gerade erst begonnen.