FOKUS: BANKEN

Bankraub im Web: Geld weg, was tun?

Jeder Fünfte wird im Laufe seines Lebens Opfer von Internetkriminellen. Die illegal abgebuchten Franken sind meist auf Nimmerwiedersehen verschwunden. Wie kann man sich schützen und was tun eigentlich die Banken gegen Onlinebetrügereien?

→ **VON MICHAEL KURZIDIM**

Die Internetkriminalität ist zu einem einträglichen Geschäft geworden, das weltweit höhere Profite abwirft als der Drogenhandel. Der Schattenhandel, also der Verkauf von Kreditkartendaten und Hacking-Tools, blüht, gedeiht und hat sich längst internationalisiert. Visa- und Mastercards gibt es in einschlägigen Onlineforen schon für einen US-Dollar, American Express kostet etwas mehr.

Mit immer neuen Tricks spionieren cyberkriminelle Banden die Passwörter und geheimen Zugangscodes von Bankkunden aus, um sie danach selbst zu benutzen oder auf dem Schwarzmarkt zu verscherbeln. Der Schweiz entstehe durch Spionage-Software, sogenannte Malware, ein jährlicher Schaden von etwa 200 Millionen Franken, schätzt Walter Sprenger, CEO von Compass Security. Es sei jedoch von einer wesentlich höheren Dunkelziffer auszugehen. Denn Banken kehren Verluste durch E-Fraud gerne unter den Teppich.

Natürlich trommeln Anbieter von Sicherheitslösungen auch im eigenen Interesse, indem sie das aktuelle Bedrohungsszenario in möglichst grellen Farben schildern. Meist verbunden mit dem diskreten Hinweis, Virenscanner und Firewalls durch regelmässige Updates auf dem aktuellsten Stand zu halten. Das bestgehütete Geheimnisse dabei: Virenscanner schützen zwar, das ist unbestritten, aber hundertprozentige Sicherheit können auch die Software-Polizisten heute nicht mehr bieten.

NEUSTER TRICK: DRIVE-BY-INFEKTION

Die aktuelle Masche der Cyberkriminellen sei die Drive-by-Infektion, erklärt Candid Wüest, Senior Threat Researcher bei Symantec. Eine besonders hinterlistige Methode: Bereits durch das Surfen auf eine infizierte Webseite können sich Internetnutzer Schadcode einfangen. Gefährliche Codezeilen verstecken sich in Plug-ins oder im DHTML-Code und werden daher vom Browser nicht bemerkt. Diese Code-Schnipsel leiten den Kommunikationskanal auf einen zweiten Server um, der dann den verhängnisvollen Schadcode auf den PC des Surfers schmuggelt. Betrüger präparieren so inzwischen auch seriöse Seiten, denen Surfer grosses Vertrauen entgegenbringen.

Hat sich erst einmal Malware auf dem Privat-PC eingenistet, dann geraten mit extrem hoher Wahrscheinlichkeit bei der nächsten Onlinetransaktion geheime Passwörter und Transaktionsnummern in kriminelle Hände. Der Schadcode manipuliert die gesamte Kommunikation in beiden Richtungen und versucht, so lange wie möglich unerkannt zu bleiben. Er gaukelt beispielsweise eine korrekte Überweisung von 150 Franken an den lokalen Energieversorger vor, während 15 000 Franken bereits ihren Weg auf ein ausländisches Konto gefunden haben.

BILD: FOTOLIA

Das Perfide daran: Trojaner der neusten Generation manipulieren auch die Kontoübersicht, spielen dem Kunden eine heile Welt vor. Die getürkte Überweisung ins Ausland taucht also in der Übersicht gar nicht auf. Der geprellte Bankkunde schöpft keinen Verdacht, während im Hintergrund sein Bankkonto leer geräumt wird – möglicherweise wochenlang. Gerne manipulieren Kriminelle etwa weihnachtliche Überweisungen an Wohltätigkeitsorganisationen, erzählt Christof Dornbierer, CTO bei AdNovum. Treffe das Geld nicht ein, falle dies niemandem auf, denn es bestehe ja keine Zahlungsverpflichtung.

TYPISCHE VERHALTENSMUSTER

Um herbe Verluste zu vermeiden, klopfen grosse Schweizer Bankhäuser die Verhaltensmuster ihrer Kunden auf Anormalitäten ab und schlagen bei abweichendem Verhalten Alarm. Sie vertrauen dabei meist auf Eigenentwicklungen ihrer IT-Abteilungen. Das klassische Beispiel: Hat ein Kunde der Credit Suisse in Zürich eine Transaktion getätigt und weist am nächsten Tag eine höhere Geldsumme aus Usbekistan an, dann ist die Abfolge beider Ereignisse zwar nicht unmöglich, aber verdächtig. Die Bank würde den dadurch ausgelösten Alarm ins Back Office

«In der Schweiz gab es offiziell nur vier Fälle manipulierter Bankomaten, in Deutschland Hunderte»

Candid Wüest, Symantec

delegieren und sich die Transaktion telefonisch vom Kunden bestätigen lassen.

Die Transaktionsbestätigung per Telefon sei allerdings sehr aufwendig, SMS seien personalfreundlicher und würden daher bevorzugt, sagt Dornbierer. Die Zürcher Kantonalbank und die Raiffeisenbank bieten ihren Kunden diese Option bereits an. Threat Researcher Wüest berichtet jedoch von einem Fall aus Südafrika, bei dem auch diese Sicherheitshürde genommen wurde: Dort kontrollierten Cyberkriminelle sowohl den Online- als auch den SMS-Kommunikationskanal, und täuschten damit das Opfer. Die Wahrscheinlichkeit, dass ein solcher Mega-Angriff Erfolg hat, kann zwar heute noch als gering eingestuft werden. Aber Vorsicht: Handy-Viren sind auf dem Vormarsch.

GEGENMITTEL: GEHÄRTETE SYSTEME

Als sichere Alternative schlägt CTO Dornbierer sogenannte gehärtete Systeme auf DVD oder USB-Stick vor, wie sie die Migrosbank mit ihrer Kobil-Lösung oder Crealogix mit seinem CLX-Stick im Regal haben. Auch der SwissStick der Post soll in Zukunft E-Banking ermöglichen. Ein sauberes, abgeschottetes System, das in der Regel aus einer schlanken Linuxvariante wie Ubuntu oder Knoppix und einem handelsüblichen Browser besteht, wird dabei ausschliesslich fürs Onlinebanking eingesetzt. Dadurch ist die Lösung vor Viren- und Trojanerbefall sicher, solange die Bankenseiten selbst sauber bleiben.

Angreifer hätten allerdings damit begonnen, eigene Banking-DVDs zu brennen und sie an ahnungslose Bankkunden zu verschicken, warnt Candid Wüest. Auch hier gilt es also, die Augen offenzuhalten. Er persönlich sei kein Freund der gehärteten Systeme auf autonomen Datenträgern, weil diese Lösung zu umständlich sei, meint der Virenexperte. Trotz des – eher seltenen – Betrugsfalls aus Südafrika bevorzugt Wüest die Bestätigung per SMS, oder aber mobile Transaktionsnummern (mTAN), die bei Bedarf aktuell aufs Handy gesendet werden, nur für eine Transaktion gültig sind und danach verfallen.

ALARM BEI MEHRFACHEINGABEN

Um den Flaschenhals der Einmalgültigkeit zu umgehen, haben Trickbetrüger Trojaner programmiert, die mehrere TANs sammeln und an Fremdrechner weiterleiten. Generell verdächtig sei es daher, wenn am Bildschirm die Eingabe einer zweiten oder dritten TAN verlangt werde, weil die erste bereits benutzt worden oder aus irgendeinem fadenscheinigen Grund nicht mehr gültig sei, betont Wüest. Dann sollten beim Bankkunden die Alarmglocken klingeln.

AdNovum-CTO Dornbierer rät Onlinekunden, ihren Kontostand in regelmässigen Abständen am Bankomaten ihrer Hausbank abzufragen, weil diese Terminals wesentlich schwerer zu manipulieren und oft an exponierten Orten aufgestellt seien. Steht der PC zu Hause unter der Befehlsgewalt eines Trojaners, gibt zumindest das Terminal zuverlässig Auskunft über den Kontostand.

VIER FÄLLE IN DER SCHWEIZ

Candid Wüest nimmt aber auch dieser Sicherheitstechnik die Illusion der Unangreifbarkeit. In Russland sei es Banden gelungen, selbst Bankomaten mit Trojanern zu infizieren, erzählt er. Wesentlich häufiger aber arbeiten Betrüger mit einem aufgesetzten Kartenschlitz und einer doppelten Tastatur, um an die Zugangscodes heranzukommen. Sie legen dabei ein erstaunliches Geschick an den Tag: Zusatztastaturen sind heute nur zwei bis drei Millimeter dick, fallen so kaum auf und sind mit Sekundenkleber innerhalb kürzester Zeit angebracht. «In der Schweiz gab es offiziell nur vier Fälle, in Deutschland aber geht die Zahl manipulierte Bankomaten in die Hunderte», meint Wüest

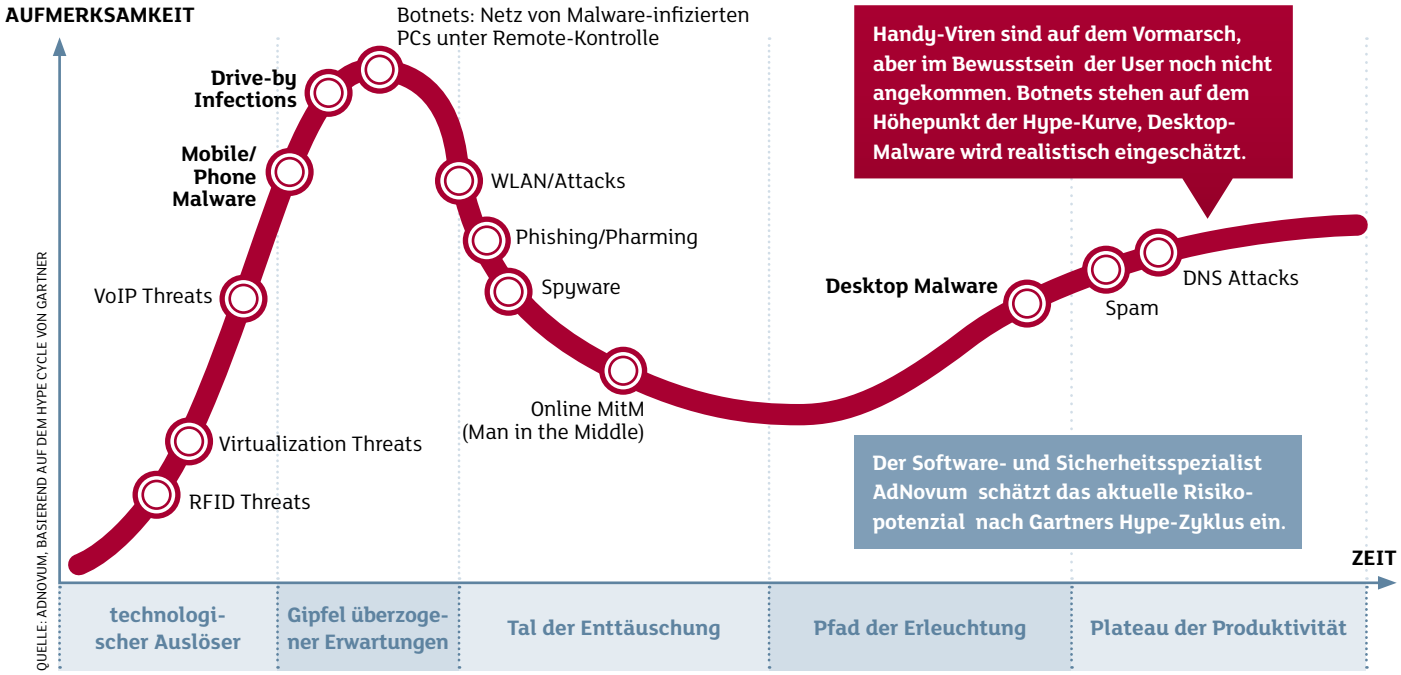
Prinzipiell sei es möglich, mithilfe eines Lasers die Höhe der Eingabetastatur zu überprüfen und damit einen nachträglich angebrachten Tastaturaufsatz zu erkennen, betont Christoph Baumgartner, CEO bei OneConsult. Allerdings seien viele Gegenmassnahmen zwar technisch machbar, aber den Banken in der Ausführung zu teuer. Sie setzen deshalb lieber auf nachträgliche Schadensbegrenzung und bieten geprellten Kunden etwa Hilfe bei der Schadensregulierung an. Kunden seien dabei jedoch auf die Kulanz der Bankhäuser angewiesen, betont er.

Eine relativ preisgünstige Möglichkeit, Kartenleser an Bankomaten fälschungssicher zu machen, sei ein individuelles Wellenmuster am Einsaugschlitz. Kriminelle müssten erst einmal einen Abdruck nehmen, um einen passgenauen Aufsatz zu fertigen – ein aufwendiges Verfahren. Ausserdem spucken viele Bankomaten eingezogene Karten aus und ziehen sie danach ein zweites Mal ein. Der doppelte Einzug hat einen guten Grund: Im Kartenleser kappt nach dem ersten Einzug eine Art Messer den Kontakt zur Aussenwelt. Dadurch soll verhindert werden, dass Kriminelle über ein mit der Karte verbundenes Kabel die Zugangscodes mitlesen.

BANKANGESTELLTE: SCHWARZE SCHAFE

«Es wird also schon einiges getan», resümiert Baumgartner. Die übelsten Täter aber, so Baumgartner zu Computerworld, seien →

Hype-Zyklus für Bedrohungen



unter den Bankangestellten selbst zu finden. Baumgartner berichtet zum Beispiel von IT-Leitern, die Rundungssummen im hohen Nachkommastellenbereich – auf den im Normalfall kaum jemand ein Auge wirft – manipulierten und den Differenzbetrag auf ihr eigenes Konto überführten. Im Einzelfall handelt es sich dabei um Minimalbeträge, bei zehntausend Transaktionen pro Tag kommt aber auf diese Weise trotzdem ein recht erkleckliches Sümmchen zustande.

«Fliegt eine Manipulation auf, wird dem Täter ein Maulkorb verpasst»

Christoph Baumgartner, OneConsult

Die gesamte Finanzbranche basiere auf Verschwiegenheit, Diskretion und Vertrauen seien extrem wichtig. Fliege also eine solche Manipulation auf, werde eine interne Regelung gefunden und dem Täter ein Maulkorb verpasst, meint Baumgartner. Ans Licht der Öffentlichkeit geraten solche Betrügereien daher nur in sehr seltenen Fällen.

Da kann einem die Lust am Onlinebanking schon vergehen. Wie Robert Mueller, dem Chef der US-amerikanischen Bundespolizei FBI. Mueller hat Anfang Oktober dieses Jahres öffentlich verkündet, dass er in Zukunft auf Onlinebanking ganz verzichten will. Auf einer Veranstaltung in San Francisco gab er unumwunden zu, dass er beinahe auf eine Masche von Phishern hereingefallen sei. Phisher versuchen, Kunden zu täuschen und auf gefälschte Bankseiten zu locken. Dort sollen sie dann Passwort und Zugangscode eingeben – eine Technik, die inzwischen ein wenig aus dem Blickfeld geraten ist (siehe Grafik oben).

FBI-CHEF SAGT NEIN

«Ich war nur wenige Klicks davon entfernt, das Opfer einer klassischen Internetbetrügerei zu werden», berichtete Mueller. «Die Phisher hatten die E-Mails gefälscht, die meine Bank normalerweise an ihre Kunden verschickt, und sie hatten das äusserst professionell gemacht. Obwohl der FBI-Chef dann doch noch Verdacht schöpfte und keine Zugangscodes an die E-Bankräuber übermittelte, möchte er nach diesem Vorfall keine Onlinegeldgeschäfte mehr tätigen.

Selbst Spionage-Experten sind also vor Attacken nicht gefeit. Social-Engineering-Techniken, die geschickt mit den Ängsten, Wünschen und Hoffnungen ihrer Adressaten spielen, treffen häufig ins Schwarze. Tatort Facebook: Die beiden Schweizer DJs Phil Svanee und Christian P erhielten ein äusserst verlockendes Angebot. Ein DJ-Broker namens Ale Conti lockte die beiden mit einem Job in einem der angesagtesten Clubs in Miami. «Das war wie ein Sechser im Lotto und hätte für mich den Durchbruch als DJ bedeutet», sagt Svanee rückblickend.

BETRUG AUF FACEBOOK

Die Sache hatte jedoch einen Haken, die beiden sollten die Kosten für die Flugtickets vorstrecken. Er sei selbst schon öfter reingelegt worden und wolle dieses Risiko nicht mehr tragen, begründete Broker Conti diese Vorgehensweise. Um auf Nummer sicher zu gehen, stellten Phil Svanee und Cristian P eigene Recherchen an, mit dem Ergebnis: Der Flug bei Air France war gebucht, das Hotel in Miami reserviert. Also überwiesen sie das Geld. Danach war DJ-Broker Ale Conti wie vom Erdboden verschluckt, sein Facebook-Konto gelöscht und die Hotelreservierung storniert.

Freunde der beiden Schweizer eröffneten daraufhin die Facebook-Gruppe «Stopped de DJ-Betrüger vo de USA» und rasch wurde klar: Phil Svanee und Christian P waren nicht alleine, zahlreiche Kollegen aus mehreren Ländern waren bereits auf Ale Conti, der unter wechselnden Namen auftritt, hereingefallen.

Die Moral von der Geschichte: Vorkasse ist immer verdächtig, ganz gleich, wie logisch und einleuchtend sich die Begründung anhört. Gegen geschickt aufgegleistes Social Engineering helfen nur waches Misstrauen und ein gesunder Menschenverstand. Technischen Attacken aber könnte eine Kombination der in diesem Artikel diskutierten Abwehrstrategien einen wirksamen Riegel vorschieben.

VIER KERNMASSNAHMEN

AdNovum-CTO Dornbierer empfiehlt vier Kernmassnahmen: eine Transaktionssignatur über einen zweiten, vertrauenswürdigen Kommunikationskanal, ein gehärteter Browser auf einem unveränderbaren USB-Stick, den Einsatz eines lokalen Proxy-Servers mit verschlüsselter SSL-Verbindung und schliesslich ein Fraud-Detection-System, das Benutzerprofile erstellt und Verhaltensanomalien auch auf Serverseite bemerkt. Sicher erfordert das einiges an Aufwand, die Sicherheit beim Onlinebanking sollte uns diese Mühe jedoch wert sein. ←