

Der neue Gefahrenherd: Der PC des Kunden

Die jüngsten Attacken auf E-Business-Systeme sind gezielt, raffiniert, organisiert und komplex. Sie nutzen vermehrt den Kunden-PC und mobile Geräte als Sprungbrett. Daneben sehen Phishing-Angriffe wie harmlose Bubenstreiche aus.



Stefan Wengi

dipl. Informatik-Ing. ETH, ist CTO
der AdNovum Informatik AG

Bei Attacken auf Sicherheitssysteme vor allem im E-Banking-Umfeld stehen heute primär finanzielle Absichten im Vordergrund. Sie unterscheiden sich dadurch zunehmend von früheren Attacken von Script-Kiddies oder Hobby-Hackern, die einen aufklärerischen Anspruch verfolgten, durch rein technische Neugier motiviert oder einfach auf Publizität ausgerichtet waren.

Im Gegensatz zu High-Noise-Attacken wie Phishing wird darauf geachtet, wenig Aufsehen zu erregen und so lange wie möglich unbemerkt zu bleiben. Zusätzlich zeichnen sie sich durch einen weit höheren Professionalisierungs- und Individualisierungsgrad aus und

verfolgen kompliziertere, weltweit vernetzte Vorgehensweisen.

Massgeschneiderte Angriffsstrategien

Im Fokus steht die kriminelle Aneignung von Geldbeträgen oder – speziell in der Industrie- und Wirtschaftsspionage – Daten, Informationen und Know-how. Die Angreifer versuchen, die aufgrund der Phishing-Aufklärungskampagnen gestiegene Security Awareness bei den Benutzern und Unternehmen mit massgeschneiderter Angriffsstrategien zu unterwandern, die Social Engineering und technologiegestützte Bedrohungscluster geschickt miteinander kombinieren.

Aus nahe liegenden Gründen werden kaum Zahlen oder Einzelheiten von Angriffen publik. Die bekannt gewordenen Fälle verdeutlichen aber die Tragweite möglicher Schäden. So machte Ende Oktober 2006 ein gross angelegter Identitätsbetrug die Runde. Organisierte Hacker hätten sich, so mehrere Nachrichtendienste, illegal Zugang zu Kundendepots von US-Onlinebrokern verschafft. In einem konkreten Fall, den die US-Wertpapieraufsicht SEC aufdeckte, haben

Betrüger mit Anlegergeld die Kurse von wenig gehandelten Aktien hochgetrieben. Anschliessend verkauften sie die Papiere, die sie vorher günstig gekauft hatten, mit Gewinn. Allein bei E-Trade in New York soll der Schaden rund 18 Milliarden Dollar betragen haben. Insgesamt sollen sich die Schäden durch Trickbetrüger laut einer Schätzung des Analyseunternehmens Javelin Strategy & Research im Jahr 2006 auf 56,6 Milliarden Dollar belaufen haben. Anfang Januar sorgte der Angriff auf eine Skandinavische Bank für Schlagzeilen.

Mittels einer modifizierten Version des Trojaners «haxdoor» sollen Hacker über eine Million Dollar gestohlen haben. Die IT-forensischen Untersuchungen der Polizei ergaben, dass der Trojaner so modifiziert worden war, dass er nur spezifisch die Kunden der Bank angriff und die gestohlenen Informationen über US-Server nach Russland routete.

«Heute kann zudem massgeschneiderter Code für Fernsteuerungsprogramme (Bots) einfach und billig im Internet erworben werden.»

Kunde ist auf sich allein gestellt

Diese Fälle zeigen zum einen, dass Betrüger ausserhalb des Zugriffs von nationalen Strafverfolgungsbehörden verstärkt Internetbroker für ihre kriminellen Machenschaften ins Visier nehmen. Zum anderen zeigt insbesondere der zweite Fall, dass die Hacker gezielt Institute mit dedizierter respektive massgeschneiderter Malware attackieren und ihr Augenmerk verstärkt auf den Kunden-PC richten.

Die hohen Sicherheitsstandards zum Beispiel der Schweizer Banken sind weltweit ein Begriff. So verwenden heute alle Finanzinstitute eine Zwei-Faktor-Authentisierung, und die Ablösung noch vorhandener Rasterkarten respektive Streichlisten ist mehrheitlich angekündigt. Die Schweizer Banken sind damit gegen Angreifer gut gewappnet und zählen in der Regel auch zu den First Movern, setzen also neue Abwehrtechniken früher als andere Serviceanbieter ein.

Auf Seiten des Kunden hingegen wird die Authentizität eines Servers selten mit modernsten Sicherheitsvorkehrungen überprüft. Der Kunde ist diesbezüglich auf sich allein gestellt, was Nichttechniker erfahrungsgemäss überfordert. Der bevorzugte Angriffspunkt hat sich deshalb vom Anbieter auf den Kunden und seinen PC oder die mobilen Pendants verlagert. Die Hauptproblematik liegt in unsicheren respektive zu wenig geschützten Betriebssystemen, bei der Usability und bei Malware.

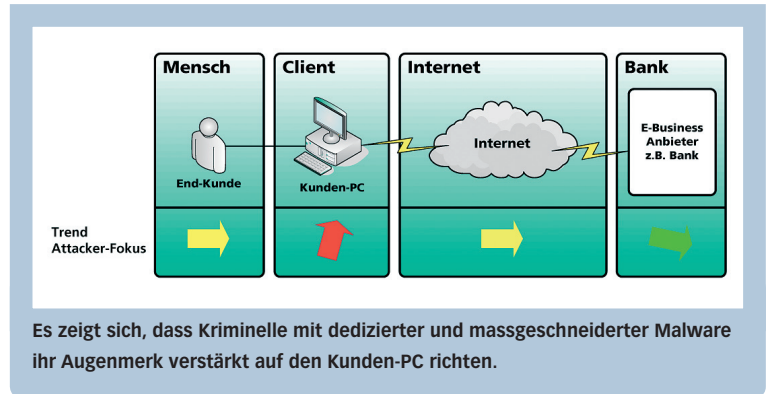
Sicherheitsfeatures als lästiges Übel

Bei Malware-Attacken führt ein vom Benutzer unbemerkt geladenes Programm wie etwa ein Virus, ein Wurm oder ein Trojanisches Pferd zwecks Informationsgewinnung oder -veränderung ferngesteuert auf dem Rechner des Anwenders beliebige Funktionen aus. Beim Browser Poisoning handelt es sich um Malware, die die Verbindung zwischen der E-Banking-Applikation und dem Kunden innerhalb des Webbrowsers manipuliert und dadurch sauber eingesetzte Authentisierungsmechanismen umgehen kann. Heute kann zudem massgeschneiderter Code für Fernsteuerungsprogramme (Bots) einfach und billig im Internet erworben werden. Bei der Verbreitung von Malware hilft den Angreifern einerseits die heute etablierte flächige Vernetzung von Firmen und Privaten, andererseits nutzen sie Schwächen in diversen Softwarepaketen, um sich auf den PCs ihrer Opfer einzunisten.

Die Usability, also die einfache, intuitive Benutzung der Sicherheitsmechanismen, spielt bei mobilen Geräten wie Smartphones und PDAs eine noch grössere Rolle als auf Desktop- oder Serversystemen. Denn nicht nur durch den einfacheren Gerätediebstahl oder die zunehmende Vernetzung und den erhöhten Funktionsumfang dieser Geräte steigt das Risiko des Daten- und Informationsklau, sondern zum Beispiel auch durch anspruchsvolle Verschlüsselungstechniken, die dem Benutzer aufgrund der langsameren Prozessoren, des geringeren Speicherplatzes oder knappen Akkulaufzeiten längere Wartezeiten abverlangen, was ihn eventuell dazu veranlasst, die Sicherheitsfeatures als lästiges Übel auszuschalten.

Angriffe innerhalb des gesicherten Kanals

Die technische Netzwerkverbindung vom Kunden-PC zum Serviceanbieter ist mit den etablierten Sicherheitsmitteln vor Attacken gut geschützt. Das Perfide an modernen Attacken wie Browser Poisoning oder «Man in the Middle» ist, dass



die Angriffe innerhalb des gesicherten Kanals stattfinden. Für den Benutzer sind die Angriffe dadurch nicht oder nur schwer erkennbar, da er aufgrund des sichtbaren Sicherheitsschlusses im Browser von einer sicheren Verbindung ausgeht. Der Benutzer gibt dabei etwa unwissend seine Sicherheitselemente einem Dritten bekannt, der anschliessend in der Lage ist, als dieser Benutzer aufzutreten und die Transaktionen nahezu beliebig zu manipulieren. Eine solche Attacke kann als Realtime Phishing bezeichnet werden. Sie funktioniert auch mit hardwarebasierter Zwei-Faktor-Authentisierung, sofern der «Man in the Middle» die Authentisierungscodes sofort verwendet, um sich im Namen des Opfers bei der Bank einzuloggen.

Eine noch weiter gehende Variante, die etwa mit Browser Poisoning möglich wird, ist die Manipulation von Transaktionsdaten innerhalb eines Kunden-Browsers, bevor diese an die Bank versendet werden. Professionelle Attacken gehen so weit, dass in der Resultatseite wieder die durch den Kunden eingegebenen Daten erscheinen und dass auch die Übersicht über offene Transaktionen so manipuliert wird, dass der Benutzer keinen Verdacht schöpfen kann. Das böse Erwachen erfolgt erst am Ende des Monats, sofern dann überhaupt ein Kontoauszug ins Haus flattert.

Prävention und Detektion

Es existieren heute sowohl für Serviceanbieter wie auch für Benutzer verschiedene Ansätze, dieser Problematik mit geeigneten Abwehrmechanismen die Stirn zu bieten. Auf Anbieterseite kann grundsätzlich zwischen Prävention und Detektion differenziert werden. Weiter sind verschiedene Kombinationen davon möglich. In der Prävention wird beispielsweise eine «Offline»-Transaktionssicherung über einen zweiten Kanal oder mittels Signaturen eingesetzt. Dies führt dazu, dass bei jeder sensitiven Transaktion die relevanten Daten vom Server signiert werden und der Benutzer die Transaktion explizit auf einem externen zweiten Gerät wie einer Smartcard oder einem Mobiltelefon quittiert respektive signiert.

Im Bereich der Detektion werden Profiling-Ansätze eingesetzt, wie sie bei Kreditkarteninstituten oder zur Bekämpfung von Geldwäscherei gang und gäbe sind. Anhand von detaillierten Benutzerprofilen können so schnell Anomalien gegenüber dem üblichen Geschäftsgebaren erkannt und verfolgt und Missbräuche unterbunden werden. In diese Richtung gehen auch Anbieter, bei denen die Kunden selbst bestimmen, welche Aktionen und Empfänger erlaubt sind. Am effizientesten ist auch hier eine Kombination der beiden Ansätze.

Benutzer können sich jedoch auch selbst vor ausgefeilten Angriffen schützen. Neben den allgemein zu empfehlenden Massnahmen wie Einsatz von Virenschutz, Firewalls, Browser-Toolbars und regelmässigen Software-Updates gibt es verschiedenste marktgängige Werkzeuge und Produktsuiten zur Abwehr unliebsamer Besucher. Je weniger Aktivitäten ausserhalb von sicherheitskritischen Transaktionen auf einem Rechner stattfinden, desto kleiner ist die Wahrscheinlichkeit, dass man schädliche Software einfängt. Besonders Vorsichtige sind unterdessen dazu übergegangen, ihr Betriebssystem für eine E-Banking Session jeweils auf einer CD-ROM zu starten, wie dies das Linux Derivat Knoppix einfach ermöglicht. Alternativ dazu kann ein dedizierter Rechner, zum Beispiel ein alter Laptop, für sensitive Transaktionen verwendet werden. Ebenfalls hilfreich ist es, für den Zugriff auf sicherheitskritische Daten statt Mainstream-Software mit ihrer hohen Exponierung ein weniger verbreitetes und vergleichsweise sicheres Betriebssystem wie Unix/Linux oder Mac OS X einzusetzen. Allerdings nimmt die Wahrscheinlichkeit von Attacken auch bei diesen Systemen mit steigendem Marktanteil zu. ■