Der Mann im Browser

SECURITY-RATGEBER

Man-in-The-Browser-Angriffe verstehen und abwehren

Inhalt

Einführung 2

Gefahren durch MiTB-Attacken 2

Den Cyber-Kriminellen einen Schritt voraus 3

Lösungen von SafeNet zur Abwehr von Man-in-The-Browser-Angriffen 4

MobilePASS SMS-Authentisierungslösungen 4

eToken NG-FLASH mit integriertem sicheren Browser 5

Über SafeNet 5

Der riesige Boom bei der Nutzung von Social-Media-Diensten ist für die Cyber-Kriminellen beim Verteilen von Schadprogrammen ein Segen. Immerhin wurden mehr als ein Drittel aller Malware-Angriffe im zweiten Halbjahr 2009 über Social-Media-Plattformen durchgeführt.

Einführung

Die Verluste durch Finanzbetrügereien sind alarmierend. Die Finanzbranche ist weltweit das bevorzugte Ziel von Cyber-Angriffen geworden und hat alleine im Jahr 2009 Verluste in Höhe von 54 Milliarden Dollar erlitten – gegenüber 48 Milliarden im Vorjahr. Und ebenso gravierend ist für die Finanzinstitute der Schaden, den die Cyber-Kriminalität dem guten Ruf zufügen kann. Zusammen mit einer möglichen Kundenabwanderung kann dieses einen ernsthaften, wenn nicht gar verheerenden Einfluss auf den Umsatz haben.

Während alle Arten von Cyber-Kriminalität zunehmen, steigt der Finanzbetrug durch Malware-infizierte Computer rasant an. Typischer Weise zielt Malware auf Desktop-PCs ab. Die Benutzer werden mittels Social Engineering dazu gebracht, bösartigen Code herunterzuladen und auf ihren Computern zu installieren.

Einer der gefährlichsten Malware-Typen für Online-Banking und andere Finanzdienstleistungen ist die so genannte „Man in The Browser“ -Attacke (MiTB). Bei einem Man-in-The-Browser-Angriff wird der Internet-Browser durch Schadcode infiziert. Dieser Code manipuliert Aktionen des Benutzers und kann in manchen Fällen sogar selbstständig Vorgänge einleiten. Meldet sich ein Benutzer an seinem Bankkonto ein, reicht ein infizierter Browser aus, um unerlaubte Transaktionen anzustoßen. Das Ergebnis: Online-Diebstahl.

Gefahren durch MiTB-Attacken

Man-in-The-Browser-Angriffe sind besonders schwer zu erkennen. In vielen Fällen wird der Schaden in aller Heimlichkeit angerichtet. Einige Arten, auf die Man-in-The-Browser-Attacken durchgeführt werden und warum sie so ein hohes Risiko bedeuten:

- **Computer werden leicht infiziert:** Der häufigste Weg, auf dem Internet-Browser mit Malware infiziert werden, ist Social Engineering. Beim Surfen oder beim Download von Medien werden die Benutzer oft dazu aufgefordert, aktualisierte Programmversionen zu installieren. Diese Anfragen sind so häufig, dass sie von vielen Benutzer automatisch akzeptiert werden. Genau dieses instinkthafte Verhalten machen sich Cyber-Kriminelle zunutze. Sie erstellen Download-Aufforderungen, die denen echter Software-Anbieter recht ähnlich sehen. Die meisten Benutzer bemerken die feinen Unterschiede nicht, stimmen dem Download zu – und infizieren ihren Browser so unwissentlich mit Malware.

  Der riesige Boom bei der Nutzung von Social-Media-Diensten ist für die Cyber-Kriminellen beim Verteilen von Schadprogrammen ein Segen. Immerhin wurden mehr als ein Drittel aller Malware-Angriffe im zweiten Halbjahr 2009 über Social-Media-Plattformen durchgeführt.

- **Schwer zu entdecken:** Schadprogramme lassen sich nur schwer aufspüren. Die Malware-Entwickler nutzen Werkzeuge, um die Schädlinge zu verschleiern und um sie für ein bestimmtes Ziel anzupassen. Durch diesen hohen Customizing-Aufwand – manchmal für ein spezifisches Land oder eine einzige Bank – sind Viren-Scanner machtlos. Sie wurden eher dafür entwickelt, generische Virentypen zu erkennen.

- **Herkömmliche starke Authentisierung reicht nicht:** Bei der starken Authentisierung wird sichergestellt, dass die Person, die sich an einer Online-Anwendung anmeldet, auch wirklich die ist, die sie vorgibt zu sein. Bei einem Man-in-The-Browser-Angriff kann der Benutzer erfolgreich authentisiert werden, obwohl in seinem Browser Schadcode aktiv ist. Führt der Benutzer eine Online-Transaktion durch, greift der infizierte Browser heimlich in den Vorgang ein – weder Bank noch Kunde können erkennen, dass etwas Unzulässiges geschieht.

- **Übliche Methoden zur Betrugsabwehr und risikobasierende Werkzeuge sind nicht effizient:** Risikobasierende Werkzeuge zur Betrugsbekämpfung fokussieren auf Benutzerauthentisierung und Validität der Transaktion. Dazu benötigen sie die Antwort des Kunden auf eine Reihe vordefinierter Sicherheitsfragen. Zudem analysieren sie das Benutzerverhalten und Banking-Muster. Sie können jedoch nicht erkennen, ob eine Transaktion durch eine Malware ausgelöst wurde oder nicht.

Den Cyber-Kriminellen einen Schritt voraus

Kundenvertrauen sicherstellen, die Integrität der Online-Banking-Services gewährleisten - neben dem Eindämmen der finanziellen Verluste durch Online-Betrug sind diese Aspekte für Finanzdienstleister äußerst wichtig. Obwohl die Bedrohungen durch Malware stetig zunehmen, gibt es gute Nachrichten: Banken können konkrete Schritte einleiten, um das Risiko von Man-in-The-Browser-Attacken zu senken. Einige Sicherheitsmaßnahmen, die Banken bereits heute zum Schutz ihrer Kunden, ihres Renommees und ihrer Finanzen implementieren können:

- **Out-of-Band (OOB)** -Authentisierung und Transfer-Verifizierung: Bei der OOB-Authentisierung und Transfer-Verifizierung werden die Informationen wie Transaktionsbestätigung oder Sicherheitscodes nicht über PC und Browser des Benutzers übertragen. Ein gängiger Kanal ist die Übertragung des Sicherheitscodes und der Transaktionsdetails per SMS auf das Handy des Anwenders. Dieser kann so erkennen, ob alle Details der Transaktion korrekt sind.

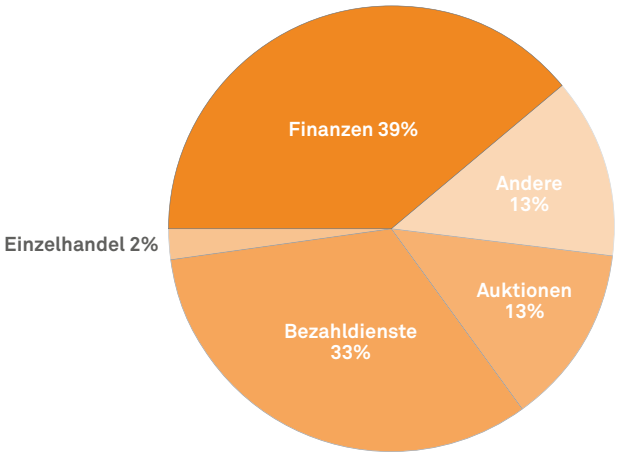
Wird über das Konto eines Kunden eine Transaktion angestoßen, sendet die Bank eine SMS mit einem Sicherheitscode und den Transaktionsdetails auf das Handy des Kunden. Erst wenn der Kunde die Transaktion durch Eingabe eines Einmal-Passworts im Banking-Portal bestätigt, wird die Transaktion ausgeführt.

Auch wenn die SMS-Authentisierung Malware nicht davon abhält, einen Browser zu infizieren: Sie nutzt einen sicheren Kommunikationskanal, um den Kunden auf Kontoaktivitäten hinzuweisen. Bekommt ein Bankkunde eine SMS-Benachrichtigung, dass eine Online-Transaktion initiiert wurde, kann er diese entweder bestätigen oder die Bank verständigen, wenn die Transaktion nicht beabsichtigt war.

- **Zertifikat-basierende Authentisierung in Verbindung mit einer sicheren Browser-Umgebung:** Ein anderer Weg, sich gegen Man-in-The-Browser-Angriffe zu schützen, ist der Einsatz einer starken Authentisierung mit Zertifikaten und die Nutzung einer sicheren Browser-Umgebung. Hierbei werden zusätzliche Maßnahmen ergriffen, um den Browser gegen Malware zu schützen. So kann die Gefahr einer Infektion zum Beispiel dadurch reduziert werden, dass ein portabler Browser eingesetzt wird, der auf einem USB-Authentisierungs-Token gespeichert ist. In diesem Fall authentisiert sich der Benutzer zunächst und startet dann den sauberen Browser direkt vom Token. Dieser vertrauenswürdige Browser kann so konfiguriert werden, dass er eine bestimmte Internet-Seite öffnet und alle Versuche blockiert, auf nicht zugelassene Sites zuzugreifen.

Der vertrauenswürdige Browser ist eine Präventivmaßnahme gegen Schadprogramme. Da der Browser auf einem externen Flash-Medium gespeichert und durch eine Sicherheits-Shell geschützt ist, bleibt er vollständig von den normalen Online-Aktionen getrennt. Somit ist er auch keinen Malware-Angriffen ausgesetzt.

Durch Cyber-Kriminalität meist angegriffene Branchen, 3. Quartal 2009



Quelle: Anti Phishing Working Group

Lösungen von SafeNet zur Abwehr von Man-in-The-Browser-Angriffen

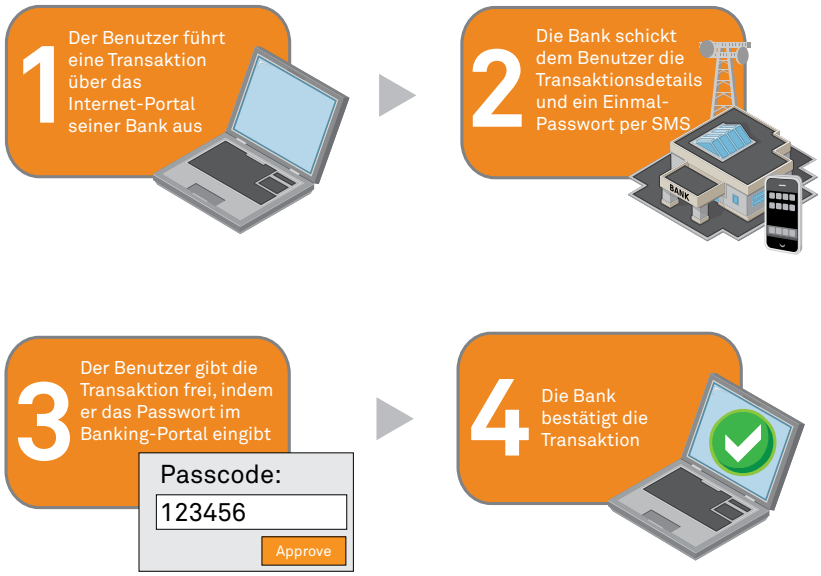
Die breite Palette an Lösungen für starke Authentisierung von SafeNet bietet alles Notwendige, um Finanzbetrug durch Man-in-The-Browser-Angriffe zu verhindern - sowohl OOB-Authentisierung über SMS als auch sichere Browser-Lösungen.

MobilePASS SMS-Authentisierungslösungen

Die MobilePASS-Familie von SafeNet mit Lösungen für Einmal-Passwörter (OTP, One-Time Password) und SMS-Software-Authentisierungslösungen verbindet die Sicherheit einer Zwei-Faktorenauthentisierung mit der Einfachheit mobiler Geräte und SMS. Die innovative Technologie von MobilePASS übermittelt Einmal-Passwörter via SMS an Mobiltelefone. Sie ermöglicht es so, Transaktionen zu verifizieren und gibt den Bankkunden die Möglichkeit, Online-Transaktionen zu validieren.

Vorteile von MobilePASS

- Zero Footprint (es muss keine Software installiert werden)
- Niedrige TCO und Einführungskosten – Hardware-Beschaffung oder Verteilung entfallen. Das Handy, das die Benutzer immer bei sich tragen, wird quasi zum Hardware-Token.
- Einfache Einführung und Konfiguration für Finanzinstitute
- Unterstützt jedes Gerät
- Einfach und bequem für die Endkunden
- Flexibler Umzug von einem Gerät zum anderen, wenn ein Kunde ein neues Handy hat
- Perfekt für Backup und Notfälle
- Ideal als vorübergehende Alternative zu verlorenen Token



eToken NG-FLASH mit integriertem sicheren Browser

eToken NG-FLASH mit einem portablen Browser ist ein sicheres Zero-Footprint-USB-Token mit starker, zertifikatbasierender Authentisierung und eingebautem Flash-Speicher. Mit dabei ist ein portabler Internet-Browser, der im verschlüsselten Flash-Speicher des eToken NG-FLASH ausgeführt wird und so den sicheren Zugriff auf Web-Anwendungen ermöglicht.

eToken NG-FLASH mit portablem Browser bietet eine All-in-One-Sicherheitslösung zum Internet-Zugriff und senkt die Risiken einer Infektion mit Schadprogrammen:

Sicherung der Browser-Integrität – Der Einsatz des Browsers vom eToken NG-FLASH stellt sicher, dass ein sauberes und nicht infiziertes Browser-Image genutzt wird. Da der Browser auf einem schreibgeschützten Speicherbereich des eToken NG-FLASH abgelegt ist, ist er sicher vor unbefugten Eingriffen und Malware.

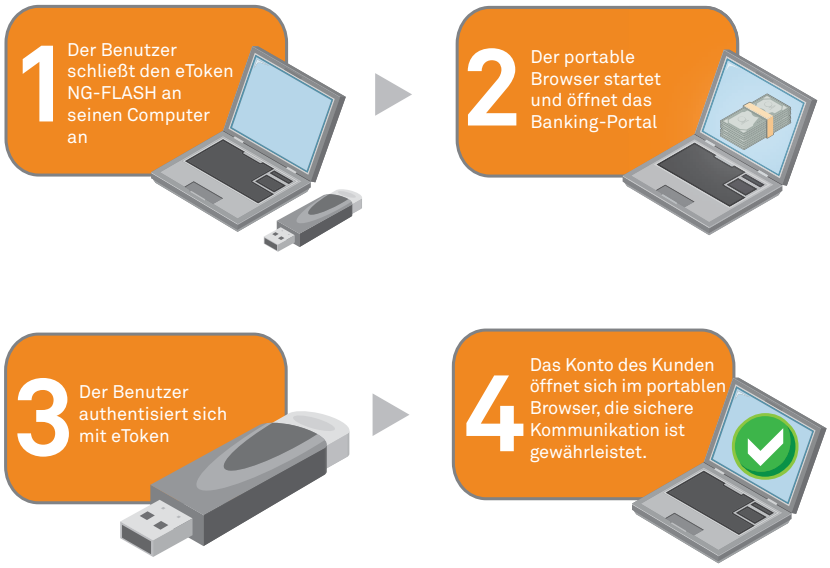
Schutz des Browser-Prozesses – Sicherheitsmaßnahmen für Speicher und Prozesse schützen im Zusammenspiel mit einem gehärteten Browser eines Drittanbieters davor, dass laufende Browser-Prozesse auf dem PC infiziert und sensible Daten zur Laufzeit manipuliert werden.

mehrstufige Authentisierung – Die Identität des Benutzers wird durch seine Anmeldedaten eindeutig ermittelt, die Kommunikation zwischen Browser und Internet-Anwendung mittels der Authentisierung per SSL-Client-Zertifikat von SafeNet abgesichert.

Vorteile des eToken NG-FLASH mit portablem Browser

Umfassende Lösung für den sicheren Zugang: Authentisiert den Benutzer und wehrt alle Arten von Cyber-Angriffen ab wie:

- phishing
- pharmimg
- Man-in-the-Middle
- Man-in-the-Browser
- Bequemer Plug-and-Play-Einsatz: Es werden weder Administratorrechte benötigt, noch muss eine Software installiert werden. Der portable Browser startet automatisch, sobald der Token am Computer angeschlossen wird.
- Flexibilität und Portabilität: eToken NG-FLASH kann an jedem Computer mit USB-Anschluss und Internet-Zugang eingesetzt werden.



Über SafeNet

SafeNet ist ein führender Anbieter von Lösungen für die Informationssicherheit und wurde 1983 gegründet. SafeNet schützt die wichtigsten Informationen seiner Kunden, einschließlich Identitäten, Transaktionen, Kommunikationsprozesse, Daten sowie Softwarelizenzen über den gesamten Lebenszyklus hinweg. Über 25,000 Unternehmen und Behörden in 100 Ländern vertrauen in Sicherheitsfragen auf SafeNet.

Weitere Informationen zu den SafeNet Authentisierungslösungen für Finanzdienstleister finden Sie unter www.safenet-inc.com/authetication

Kontakt: Die Kontaktdaten sämtlicher Niederlassungen finden Sie unter **www.safenet-inc.com**
Folgen Sie uns: www.safenet-inc.com/connected