

Neue Lösungen für neue Herausforderungen

Internetattacken werden immer ausgefeilter und gefährlicher. Deshalb werden laufend neue Lösungen zur Absicherung von Onlinetransaktionen entwickelt. Diese bieten dem weit verbreiteten Ansatz der «starken Authentisierung» eine zweite Chance. *Reto Fankhauser*



Reto Fankhauser
ist IT Architect und Security
Specialist bei ELCA

Online-Services liegen zwar im Trend, jedoch ist das Vertrauen in die Sicherheit, die notwendig ist, um die Internetbenutzer anzuziehen, gefährdet. Einerseits schätzen immer mehr Konsumenten die Möglichkeiten des Internets, um nach der Arbeit bequem einkaufen zu können oder Formalitäten nicht mehr ausser Haus erledigen zu müssen. Händler, Banken und Behörden sind zudem zunehmend in der Lage, ihre Dienste innerhalb kurzer Zeit online, einfach und kostensparend anzubieten. Andererseits stellt die zunehmende Cyberkriminalität sowohl aus finanzieller Sicht als auch aus Imagegründen ein ernst zu nehmendes Problem für die Dienst anbietenden Firmen dar. Die Anzahl schädigender Übergriffe im Netz nimmt stetig zu. Schon im Jahr 2004 gaben britische Banken zu, Internetdiebstähle mit Schadenssummen von mehr als 4,5 Millionen Pfund erlitten zu haben. Französische und brasilianische Banken gingen von Verlusten in der Höhe von 1 bis 4 Millionen US-Dollar aus, die durch Key-Logger (Spionageprogramme, mit denen User-Eingaben ausgespäht werden) verursacht wurden. Exakte Zahlen sind nicht bekannt; es ist jedoch von einer hohen Dunkelziffer auszugehen. Kriminelle Attacken, bei denen es darum geht, Geld zu erschleichen, wurden in den letzten Monaten immer ausgefeilter und somit gefährlicher! Zusammengefasst können drei Kategorien von Zielen definiert werden, auf die sich solche Angriffe richten:

1. Angriffe auf den Benutzer selbst: Beim so genannten Phishing versucht der Hacker dem Internetnutzer die Zugangsdaten zu einem bestimmten Account zu stehlen, indem er dem Benutzer eine falsche Identität vortäuscht. Phishing-Angriffe sind heute allgegenwärtig.
2. Attacken auf die Kommunikation zwischen Browser und Service: Bei so genannten «Man-in-the-Middle»-Angriffen klinkt sich der Hacker in die Kommunika-

tion zwischen dem Webbrowser des Benutzers und dem Service ein. Dabei kann der Hacker die Transaktionsdaten abfangen und für sich nutzen, beziehungsweise diese verändern. In letzter Zeit wird diese seit langem bekannte Art von Angriffen auch zunehmend von Erfolg gekrönt.

Bösartige Angriffe

Seit 2003 sehen sich Banken mit den Angriffen bössartiger Programme (so genannter Malware) konfrontiert, die in der Lage sind, im Webbrowser eingegebene oder angezeigte Daten abzufangen und zu verändern. Erst jüngst wurden 10000 australische PCs mit einer Malware infiziert, die in der Lage ist, alle vom Benutzer mit einer Anwendung ausgetauschten persönlichen Daten abzufangen und diese weiterzuleiten. Im Rahmen einer jüngst erstellten Untersuchung hat Microsoft mit Hilfe seiner Anti-Spyware-Lösung festgestellt, dass zirka 62 Prozent aller untersuchten PCs infiziert waren. Experten schätzen, dass allein in den USA etwa 9,9 Millionen Rechner mit Key-Loggern infiziert sind. Die Citibank in den USA war das erste Opfer eines dokumentierten «Man-in-the-Middle»-Angriffs. Dieser Angriff setzte die kostspieligen «Time-Token»-Generatoren (Programme zur Erzeugung zeitlich begrenzter, einmaliger Passwörter) ausser Kraft, die gerade erst eingeführt worden waren, um Phishing-Angriffe zu bekämpfen. Es ist möglich, massenhaft Transaktionen, die über einen Webbrowser abgesetzt werden, zu fälschen. Die Machbarkeit ist dabei gegeben, unabhängig davon, ob die angegriffene Website durch eine wechselseitige Authentisierung und durch eine Verschlüsselung der Kommunikation geschützt ist oder nicht.



Die zunehmende Cyberkriminalität stellt aus finanzieller Sicht und aus Imagegründen ein ernst zu nehmendes Problem für die Dienst anbietenden Firmen dar.

Quelle: www.aboutpixel.de/Uwe Dressler

3. Angriffe auf die Kommunikation zwischen Browser und Benutzer: Bei solchen Angriffen manipuliert eine Malware (von «Malicious Software» – «böswartige Software») auf dem Rechner des Benutzers die Kommunikation zwischen dem Browser und dem Benutzer im Auftrag des Hackers. Erst kürzlich bestätigten Schweizer Grossbanken gegenüber den Medien, dass auch sie respektive ihre Kunden Opfer solcher neuartigen Angriffe geworden sind.

Die starke Authentisierung allein reicht nicht mehr aus

In der Schweiz ist eine starke Authentisierung mittels Einmalpasswörter weit verbreitet. Auch im Ausland wird diese Methode vermehrt als Standard für die Abwicklung von Geldgeschäften vorgeschrieben. Lösungen, bei denen ein Gerät das Einmalpasswort bei Bedarf erzeugt, stellen ein wirksames Mittel gegen Phishing dar. Allerdings geraten sie aufgrund der unverhältnismässig hohen Kosten im Vergleich zum tatsächlichen Schutz vor den neuartigen Angriffen auch immer mehr in die Kritik. Per definitionem ist ein Einmalpasswort erst nach der tatsächlichen Verwendung sicher. Wird es vorher ausgespäht, beispielsweise durch einen «Man-in-the-Middle»-Angriff oder durch eine Malware, so bleibt die Gefahr des Missbrauchs durch Betrüger bestehen (siehe Kasten: Böswartige Angriffe).

Wie lässt sich also der Missbrauch von einmaligen Passwörtern und von Chiffrierschlüsseln durch Malware verhindern? Das Verteilen von Software zum gesicherten Zugriff auf die Passwörter und Schlüssel macht den Einsatz entsprechender Lösungen komplex, ohne jedoch die Bedrohung tatsächlich auszuschalten.

Aktuell werden deshalb neue Lösungen entwickelt, um der beschriebenen Problematik Herr zu werden. Dabei wird den Lösungen, die bereits zur starken Authentisierung eingesetzt werden, eine «zweite Chance» gegeben. Das Grundkonzept dieser Lösungen ist, dass die Benutzersitzung nach der initialen Authentisierung nicht als «für immer» gesichert angesehen wird. Im Laufe der Benutzersitzung wird jede getätigte Transaktion untrennbar mit einem Einmalpasswort – wie es auch für die starke Authentisierung verwendet wird – verbunden. Somit wird das beliebige Ausführen von Transaktionen auch in einer «entführten» Benutzersitzung unterbunden.

Lösungsansätze

Es werden zwei Arten von Lösungen vorgeschlagen, um die Sicherheit von Transaktionen zu verstärken und um deren Validierbarkeit zu erreichen. Der erste Typ von Lösungsansätzen basiert auf einer Art Taschenrechner. Der Internetnutzer gibt die Daten der Transaktion, die er tätigen will, zusätzlich (zur Angabe im Webbrowser) in dieses Gerät ein. Das Gerät erzeugt nun ein Einmalpasswort, das untrennbar mit den eingegebenen Transaktionsdaten zusammenhängt. Das generierte Einmalpasswort wird nun vom Benutzer zur Ausführung der Transaktion im Webbrowser eingegeben. Da dieses Verfahren für den Benutzer sehr aufwändig ist, könnte man zur Vereinfachung anstelle aller Transaktionsdaten lediglich eine Zusammenfassung zur Erzeugung des Einmalpasswortes verwenden. Dies wäre jedoch wieder mit einer Sicherheitseinbusse verbunden.

Bei der zweiten Ausprägung von Lösungsansätzen erhält der Internetnutzer einen Beleg der Transaktion über einen «zweiten Kanal», typischerweise in Form einer SMS. Ein

solcher Beleg enthält einerseits die Transaktionsdaten sowie ein untrennbar mit diesen Daten verbundenes Einmalpasswort. Die Verwendung von SMS als zweiter Kanal garantiert jedoch häufig nicht die von den Banken angestrebte Verfügbarkeit und Vertraulichkeit. Aus diesen Gründen bieten erste Anbieter eine interessante Alternative, die lediglich einen aktuellen Webbrowser voraussetzt und dabei eine starke Authentisierung zum Aufbau von Benutzersitzungen bietet und zudem erlaubt, jede ausgeführte Transaktion mit einer Signatur zu versehen (siehe Kasten: Eine praktische und sichere Lösung). Diese Lösung ist sowohl aus technischer Sicht, wie auch für den Benutzer weniger anspruchsvoll als die Variante mit «Taschenrechner», erreicht jedoch dasselbe Niveau an Sicherheit. Wie immer stellt die Auswahl der richtigen Lösung einen Kompromiss zwischen Sicherheit, Bedarfsdeckung, Erfordernissen einer Bank, Benutzerfreundlichkeit und Kosten dar. Eines scheint jedoch sicher: Transaktionen im Netz müssen geschützt werden. Die bereits vorhandenen Methoden zur starken Authentisierung, ergänzt um neue Konzepte zur Signierung von einzelnen Transaktionen, eröffnen dabei interessante Lösungsansätze. ■

Eine praktische und sichere Lösung

Bei dieser neu entwickelten Methode wird ein einfaches, aber höchst sicheres Vorgehen bei der Ausführung jeder einzelnen Transaktion angewendet. Wenn der Internetnutzer eine Transaktion in seinem Webbrowser startet, wird diese vom Service (z.B. Banksystem) registriert. Der Service präsentiert als Antwort einen gesicherten Transaktionsbeleg, der eine «Challenge» (Frage) enthält. Der Benutzer unterzieht diesen Beleg nun einer «visuellen Kontrolle» und antwortet, falls der Beleg korrekt ist, mit der «Response» (Antwort) auf die im Beleg enthaltene Challenge. Mit diesem Schritt wird die Transaktion bestätigt und ist gültig. Die Antwort auf die Challenge erlaubt der Bank den Zugriff auf einen Schlüssel, der verwendet wird, um die Transaktion gegenzuzeichnen. Die Bank bewahrt die von beiden Parteien digital signierte Quittung auf und der Internetnutzer kann seine Kopie ebenfalls aufbewahren. Die archivierte Quittung dient als unabstreibarere Transaktionsbeleg.