Wer fällt noch auf Phishing rein?

Die Gefahr bleibt – sichtbare Sicherheitsmerkmale schaffen Vertrauen

Jeder halbwegs informierte Internetnutzer wird heute sicher nicht mehr auf simple Phishing-Mails hereinfallen und seine PINs und TANs an gefälschte Webseiten übergeben. Doch die Internetbetrüger sind trickreicher geworden. Es gibt für nahezu jede Opferzielgruppe einen passenden Angriff. Die neuen Angriffsmethoden tragen Namen wie Pharming, Spear-Phishing oder Whaling. Die Taktiken haben sich verändert, das Ziel ist jedoch das gleiche: das Geld der Opfer. ↘ *Christian Heutger*

Aktuelle Zahlen belegen, dass keinesfalls Entwarnung angesagt ist. Das Verisign-Fraud-Barometer vom März 2010 [1] zeigt, dass in den letzten zwölf Monaten 15 Prozent der deutschen Internetnutzer Opfer eines Onlinebetrugs waren. Das Ergebnis der Umfrage gibt auch Hinweise darauf, dass Betrüger in Deutschland immer mehr auf den Online-Diebstahl von Daten abzielen, mit denen sie sich auch finanziell bereichern können.

So stieg die durchschnittliche Schadenssumme der Opfer von Online-Identitätsbetrug in den letzten zwölf Monaten von 179 auf 183 Euro pro Person. Dieses Ergebnis passt dazu, dass Käufer in Deutschland unvorsichtiger geworden sind, wenn sie vertrauliche Informationen im Internet übermitteln. 77 Prozent der Befragten gaben an, dass sie bei Transaktionen oder der Weitergabe persönlicher Informationen auf sichere Authentifizierung und erkennbare Sicherheitsprüfmerkmale wie beispielsweise Sicherheitssiegel achten. Gegenüber der letzten Umfrage in 2009 ist dies ein Rückgang um vier Prozent.

Schöne neue Namen für Angriffsmethoden

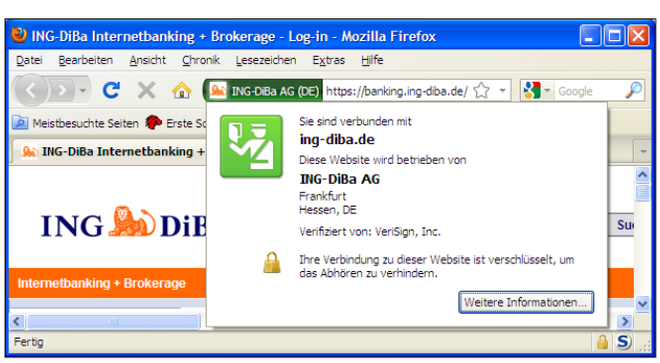
Doch was für Angriffen können Internetnutzer zum Opfer fallen? Die folgende Auflistung nennt Namen und klärt über das allgemeine Vorgehen auf:

- Phishing: Diebstahl von Zugangsdaten (Kreditkartennummer, Bankverbindung, Benutzername / Passwort), wurde ursprünglich als Begriff für Social-Engineering-Techniken verwendet, mittlerweile aber weiter gefasst
- Pharming: ein Phishing-Angriff, in dem der Domainname kompromittiert wird, also der Nutzer auf eine gefälschte Webseite umgeleitet wird
- Spear Phishing: eine Phishing-Attacke, die gegen ein eng gewähltes Ziel, wie beispielsweise eine bestimmte Person oder Gruppe, gerichtet ist
- Whaling: eine Phishing-Attacke gegen ein Ziel mit besonders hohem Wert, zum Beispiel ein CEO eines großen Unternehmens

Der kriminelle Untergrund wächst

Ein Großteil der Angriffe richtet sich auch heute noch gegen Bankkunden. Zwar konnte die Einführung von iTANs die Schadensfälle, die durch einfache Phishing-Mails verursacht werden, begrenzen, aber dafür rücken jetzt neue Gefahren wie Malware in den Mittelpunkt, die sich die Internetnutzer als Drive-by-Download einfangen können.

Auch der kriminelle Untergrund gewinnt an Bedeutung. Ein florierender Markt bietet Kartennummern, Zero-Day-Exploits und eine wachsende Zahl von Dienstleistungen für einfache Angriffe. Wer in dieser kriminellen Branche aktiv sein will, braucht selbst kaum noch technisches Wissen. Die Online-Betrüger mieten sich Dienste von Spam-Versendern und maßgeschneiderte Hacking-Tools von Botnet-Betreibern. Auch vermeintlich unwichtige Zugangsdaten zu sozialen Netzwerken sind für die Hacker Gold wert, wenn die arglosen User die gleichen Zugangsdaten auch für ihre Online-Shopping-Konten verwenden.



Verwechselung ausgeschlossen: Kaum eine deutsche Bank leistet sich noch ein Internetbanking-Login ohne EV-SSL.

Fehlendes Vertrauen ist schädlich für das Geschäft

Angesichts der aktuellen Bedrohungen ist eine wirksame Strategie zur Erhöhung der Online-Sicherheit für jedes Unternehmen unerlässlich. Das gilt für die Großen genauso wie für die Kleinen. Mittelständische Unternehmen haben vielleicht nicht die gleichen Möglichkeiten wie große Unternehmen, aber die Herausforderungen sind ähnlich. Sie müssen ihr geistiges Eigentum und persönliche Daten schützen, die Kunden ihnen anvertrauen.

Auch wenn ein kleinerer Onlinehändler sicherlich nicht so bekannt ist wie eine große Marke, so ist dennoch der Ruf am Markt überaus wichtig. Mittelständische Unternehmen verlassen sich stark auf Stammkunden. Um weiter zu wachsen, ist es wichtig, sich einen treuen Kundenstamm aufzubauen. Kleine und mittelständische Unternehmen müssen sich das Vertrauen der Kunden verdienen, um erfolgreich zu sein. Das gilt besonders in schwierigen wirtschaftlichen Zeiten, in denen Verbraucher nervös und die Konkurrenten nur einen Klick entfernt sind.

Was also sollte ein mittelständisches Unternehmen tun? Ein beliebter Einwand ist, dass es in der unsicheren wirtschaftlichen Situation keine Budgets für mehr Sicherheit gibt. Das ist allerdings nicht die Realität, denn die Budgets werden zwar stärker überprüft, aber die Sicherheitsprojekte laufen weiter. Wenn Kunden sich beim

Online-Einkauf sicher fühlen, sind sie eher bereit, mehr zu bezahlen und ihre persönlichen Informationen preiszugeben – die Investition in mehr Sicherheit zahlt sich also auch wirtschaftlich aus.

Sichtbare Sicherheitsmerkmale lohnen sich

Eine Umfrage von YouGov [2] zeigt, dass Unternehmen, die Online-Sicherheitsmerkmale einsetzen, eher weiterempfohlen werden. Mit Sicherheitsmaßnahmen können kleine und mittelständische Unternehmen folglich von Empfehlungen profitieren und mehr Geschäft an sich ziehen. Eine Möglichkeit, dies zu erreichen, ist zum Beispiel die Einführung von Extended-Validation-Zertifikaten. Diese Zertifikate erlauben es dem Internetnutzer, auf einfache und zuverlässige Weise zu überprüfen, ob eine Website echt ist und ein sicheres Umfeld für einen Onlinekauf bietet.

Die „grüne Adressleiste" zeigt, dass das Unternehmen, dem die Website gehört, als juristische Person überprüft wurde. Extended Validation (EV) verpflichtet die Zertifizierungsstelle dazu, eine Reihe von Angaben vom Antragsteller anzufordern und zu überprüfen. Überprüft werden zum Beispiel der Eintrag ins Handelsregister und die Adresse des registrierten Bevollmächtigten des Unternehmens. Existiert das Unternehmen schon länger als drei Jahre, wird die Existenz überprüft, zum Beispiel per Gutachten eines Rechtsanwalts oder durch Prüfung, ob die Organisation ein ordnungsgemäßes, aktives Konto besitzt.

Validierungsverfahren	
Domain Validation (DV)	Antragsteller wird nur anhand einer E-Mail-Adresse überprüft; zeigt lediglich an, dass die Website gesichert ist.
Organization Validation (OV)	Überprüfung der Identität des Antragstellers über ein rechtsgültiges Dokument, Identität wird im Zertifikat angegeben.
Extended Validation (EV)	Überprüfung der Identität des Antragstellers durch die Zertifizierungsstelle, Identität und Zertifizierungsstelle werden in „grüner Adressleiste" angezeigt.

Extended-Validation-Zertifikate wurden eingeführt, damit Online-Kunden eine Website eindeutig identifizieren können. Entgegen einer ab und zu vorgebrachten Behauptung garantieren diese Zertifikate nicht, dass ein Onlineshop eine sichere Website hat oder dass der Kauf reibungslos abgewickelt wird. Aber Extended-Validation-Zertifikate bieten die Gewähr dafür, dass die Identität des Händlers in Übereinstimmung mit einer Reihe von Kriterien überprüft wurde, die das CA/Browser-Forum entwickelt hat. Diese Kriterien wurden entwickelt, um die Rechenschaftspflicht zu gewährleisten – in zivilrechtlicher oder gegebenenfalls auch in strafrechtlicher Hinsicht.

EV SSL: mehr als nur Verschlüsselung

Extended-Validation-Zertifikate verwenden wie traditionelle digitale Zertifikate das seit Jahren bewährte SSL-Sicherheitsprotokoll. In einem Browser, der EV-SSL unterstützt, sieht der Internetnutzer deutlich an der „grünen Adressleiste", dass eine sichere Verbindung zur Webseite besteht. Als weiteres wesentliches Merkmal von EV-SSL wird die ausgebende Registrierungsstelle des Zertifikats prominent für den Benutzer angezeigt. Sollte ein Zertifikatsanbieter konsequent fahrlässig handeln, so wird die Marke beschädigt und die Verbraucher werden Websites, die diese Zertifikate nutzen, nicht mehr vertrauen und Unternehmen werden diese nicht mehr einsetzen.

Extended-Validation-Zertifikate haben eine große Wirkung auf das Nutzerverhalten. Es gibt eine Reihe von Beispielen, dass sich nach einem Wechsel auf EV-SSL-Zertifikate der Anteil der abgebrochenen Kaufvorgänge reduziert hat. Andere beobachteten eine Umsatzsteigerung im zweistelligen Prozentbereich. Unternehmen können anhand ihres Jahresumsatzes leicht abschätzen, ob sich der Aufpreis für ein EV-SSL-Zertifikat gegenüber niedrigeren Validierungsstandards wie Domain Validation (DV) und Organization Validation (OV) rechnet. Extended Validation ist teurer als das DV-Zertifikat, weil es genauere Prüfungen des beantragenden Unternehmens erfordert. Dafür zeigt es dem Internetnutzer aber unmissverständlich, dass der Webseitenbetreiber einen hohen Sicherheitsstandard als Maßstab hat.

Die Zertifikate werden durch eine Reihe von Certificate Authorities (CA) wie zum Beispiel Comodo, Entrust oder Verisign ausgestellt. Website-Besitzer können sie direkt bei diesen CAs erwerben. Das bietet sich an, wenn Unternehmen die Verwaltung und Installation der Zertifikate aus Sicherheitsgründen nicht außer Haus geben wollen und zudem das technische Know-how im Unternehmen haben. Für den Erwerb einzelner Zertifikate wenden sich Unternehmen besser an Anbieter von Sicherheitslösungen und Internetdienste wie zum Beispiel Domain-Registrare, Web-Hosting-Provider und Reseller von Sicherheitsprodukten. Diese berechnen in der Regel weniger pro Zertifikat und unterstützen das Unternehmen außerdem mit Beratung. Darüber hinaus bieten sie technische Service-Dienstleistungen wie Neuinstallation und Umzug von SSL-Zertifikaten auf Unternehmensserver. Auch bei Problemen helfen diese Anbieter weiter, zum Beispiel bei der SSL-Fehlerbeseitigung in HTML-Seiten, Skripten und Programmen.

Fazit

Bei der Einführung von SSL ging es darum, mit einer Verschlüsselung für eine sichere Verbindung zwischen Server und Browser zu sorgen. Heute wird mit den wachsenden Internetbedrohungen klarer denn je, dass die Verbindung nicht beim Browser endet. Das letztendliche Ziel einer Internet-Kommunikation ist der Mensch, keine Maschine. Und genau an der Schnittstelle zwischen Browser und Nutzer – den letzten Metern zwischen Auge und Bildschirm – liegen die Sicherheitsprobleme, die schon zu lange vernachlässigt wurden.

Links und Literatur

↗ Softlink auf t3n.de/magazin 2635

[1] Verisign-Fraud-Barometer: http://www.verisign.de/press/page_03232010.html

[2] YouGov-Umfrage: http://www.verisign.de/press/page_040567.html

Der Autor

Christian Heutger ist Geschäftsführer der PSW GROUP GmbH & Co. KG und verfügt über mehr als elf Jahre Erfahrung in der Branche für SSL-Zertifikate. Sein Wissen über IT-Sicherheit vermittelt er als Lehrbeauftragter für den DV-Bereich am Fachbereich Wirtschaft der Hochschule Fulda und im Rahmen seiner nebenberuflichen Tätigkeit als Informatiklehrer am Marianum Fulda.