Technische Sicherheit ist für Online-Shops eine Frage des Vertrauens

Tests und Analysen der amerikanischen Sicherheitsfirma WhiteHat Security (Registrierung erforderlich) haben ergeben, dass 80 % aller Webseiten bekannte Schwachstellen aufweisen. Laut Studie gelten Online-Shops als besonders gefährdet. Denn sie verwalten in der Regel eine Vielzahl sensibler Kundendaten und ermöglichen die Durchführung von Transaktionen mit monetärem Wert. Angriffe können somit sowohl dem Shopbetreiber, als auch dem Shopkunden auf direktem Wege Schaden zufügen.

Für einen Angriff sind heute grundsätzlich keine speziellen Werkzeuge, Skripte, Programme oder Expertenwissen mehr notwendig. Diese niedrigen Einstiegsbarrieren und die steigende Popularität von Web-Applikationen erregen erhöhte Aufmerksamkeit seitens potentieller Angreifer. Damit steigt auch die Gefahr, dass verdientes Vertrauen bei den Kunden schnell wieder verspielt wird, sollte der Online-Shop Opfer eines schädigenden Angriffs werden.

Angriffe auf E-Commerce Sites

Potentiell gefährdet sind dynamische Web-Applikation, die einem ständigen Änderungsprozess unterliegen. Dies gilt allerdings auch für Standard-Softwarelösungen. Die Häufigkeit von Meldungen über gehackte E-Commerce Sites nimmt weiterhin stetig zu, wobei folgende Angriffsauswirkungen zu verzeichnen sind, die zu einem Image- bzw. Kundenverlust der betroffenen Online-Shops führen können:

Angriffsauswirkung	Opfer	Beispielszenario für Online-Shops
Diebstahl oder Modifikation sensibler Kundendaten	Online-Shop/Benutzer	Diebstahl von Kontodaten, Kreditkartennummern, Telefonnummern, Email-Adressen oder Passwörtern.
Durchführung ungewünschter Transaktionen durch unerlaubten Systemzugang	Online-Shop/Benutzer	Über den Zugang eines Kunden werden ohne dessen Wissen Produkte gekauft.
Umleitung der Zugriffe auf die Webseiten des Online-Shops	Online-Shop	Auf die Webseiten des Online-Shops kann nicht zugegriffen werden. Somit sinkt die Konversationsrate auf 0.
Manipulation von Datenbanken	Online-Shop	Produktdaten, Transaktionsdaten, Zugangsdaten können geändert werden. Datenbanken können gelöscht werden.
Herausgabe falscher Informationen an Shopkunden	Benutzer	Es werden falsche Inhalte eingeblendet, um den Benutzer zu täuschen und bspw. an seine Zugangsdaten zu gelangen.

Übernahme und Manipulation des Webservers der Web-Applikation	Online-Shop	Zugriff auf die Dateiebene des Webservers ermöglicht die vollständige Veränderung von Inhalten oder die Löschung des Systems.
Übernahme des Computers eines Shopkunden	Benutzer	Bspw. können Cookies aus dem Internet Browser ausgelesen werden und somit einen Zugang zu weiteren Applikationen des Benutzers ermöglichen.

Um die genannten Schäden anzurichten, bedienen sich Angreifer so genannter „Low-Hanging-Fruits"-Schwachstellen (z.B. fehlende Validierung von Benutzereingaben), die 80 % der Angriffe auf Web-Applikationen zugrunde liegen. Sind diese Schwachstellen jedoch nicht vorhanden, so steigen die Einstiegsbarrieren für den Angreifer und der Online-Shop bleibt höchstwahrscheinlich von einem Angriff verschont.

Ein Selbst-Test für Shopbetreiber sowie ein Beitrag über potentielle Schwachstellen von Online-Shops folgen in Kürze.

UPDATE: Im neuen **Trusted Shops Security-Audit** wird in enger Zusammenarbeit mit dem Shopbetreiber eine sicherheitstechnische Untersuchung vorgenommen. Mittels aktueller Prüfungssoftware testen Sicherheitsexperten die Site auf bekannte grundlegende Sicherheitsrisiken. Die Durchführung des Audits gliedert sich in fünf Phasen und wird in enger Zusammenarbeit mit dem Shopbetreiber durchgeführt. Ein detaillierter Audit-Report gibt Auskunft über Verwundbarkeiten und beschreibt erforderliche Gegenmaßnahmen.