Peter Höpfl

»Sichere Wege im Onlineshop

Keine Frage: E-Commerce hilft, Geschäftsprozesse zu vereinfachen, die Produktivität zu erhöhen und verschafft nicht zuletzt Wettbewerbsvorteile. Doch die Konkurrenz ist groß. Wer die Potenziale im Onlinehandel optimal ausschöpfen will, muss dem Faktor Sicherheit eine bedeutende Rolle zukommen lassen, denn die Professionalisierung der Cyber-Kriminalität schreitet rasant voran und nicht zuletzt das Beispiel Sony zeigt, welche dramatischen Folgen eine unzureichende Absicherung der eigenen Internetplattform haben kann. Nur wer seinen Kunden höchste Sicherheit bietet und dabei immer neue und zahlreichere Ansatzpunkte einbezieht, profitiert langfristig vom Onlinehandel.

Webshop-Bedrohungen dauerhaft vorbeugen

Um Bedrohungen von Webshops effektiv zu begegnen und im entscheidenden Moment schnell reagieren zu können, betrachten komplexe Konzepte Sicherheit als einen an¬dauernden Prozess und fließen – nicht nur zum optimalen Schutz, sondern auch aus Kostengründen – bereits in die Planungsphase von E-Commerce-Projekten ein. Sie basieren vereinfacht dargestellt auf drei Säulen (siehe Abb. 1). Deren wesentliche Bestandteile sind die Sicherheit innerhalb der Serverplattform, die Absicherung der Weban¬wendungen selbst sowie der Umgang mit Daten innerhalb der Firma und bei Miet-Lösungen.

Weiterhin sollte im Hinblick auf eine umfassende Sicherheit im System prinzipiell allen fremden Daten misstraut werden, denn es ist nie auszuschließen, dass sie manipuliert sein könnten. Neben der Implementierung gängiger Sicherheitsstandards und einem gesunden Misstrauen spielt letztendlich eine erhöhte Wachsamkeit – also die fortwährende Überwachung – eine tragende Rolle.

Absicherung der Serverplattform

Server und Netzwerk bilden das Sicherheitsfundament einer Webanwendung. Grundsätzlich muss die Serverplattform in mehrere Zonen aufgeteilt sein und selbst¬verständlich eine Firewall einsetzen. Eine zeitgemäße Firewall bietet mindestens eine „Stateful Inspection“ und sollte idealerweise bis auf http-Ebene (Application Firewall) Angriffe im Vorfeld unterbinden.

Zudem empfiehlt es sich, nur Webapplikationsserver direkt mit dem Internet zu verknüpfen; alle weiteren Systeme, die nicht unmittelbar vom User angesprochen werden – beispielsweise der Datenbankserver – sollten dagegen eine Webverbindung vermeiden. Nur so kann das Risiko von Angriffen minimiert werden. Gelangt ein Angreifer beispiels-weise an Log-in-Daten eines Datenbankservers, sind diese für ihn wertlos, solange er gemäß der Devise der geringsten Privilegien keinen Zugriff auf den Server erlangt.

Außerdem gelten regelmäßige Software-Updates als unabdingbarer Standard, um vor Angriffen von außen geschützt zu sein. Ebenso sollten auf den eingesetzten Systemen nur Dienste laufen, die für den Betrieb zwingend notwendig sind. Je weniger „Default“-Anwendungen aktiviert sind, desto geringer ist die potenzielle Angriffsfläche.

Was aber, wenn Onlinehändler den Webshop nicht inhouse betreiben? Wie wird gewährleistet, dass der Dienstleister seine Hosting-Umgebung sicher aufgebaut hat?

Hier gilt für Unternehmen zunächst, im Vorfeld detaillierte Informationen über den Anbieter ihrer Wahl einzuholen. Erster Anhaltspunkt und zugleich sehr gutes Qualitätskriterium ist dabei die sogenannte PCI-DSS-Zertifizierung (Payment Card Industry Data Security Standard). Die von führenden Kreditkartenanbietern aufgesetzte Zertifizierung umfasst ein Regelwerk für den sicheren Online-Zahlungsverkehr und die ebenso sichere Abwicklung von Kreditkartentransaktionen. Sie garantiert allen Anwendern sowie deren Kun-

DER AUTOR

Peter Höpfl betreute seit 1999 zunächst die Weiterentwicklung verschiedener E-Commerce-Plattformen, bevor er 2001 die IT-Leitung innerhalb der Atrada AG übernahm.

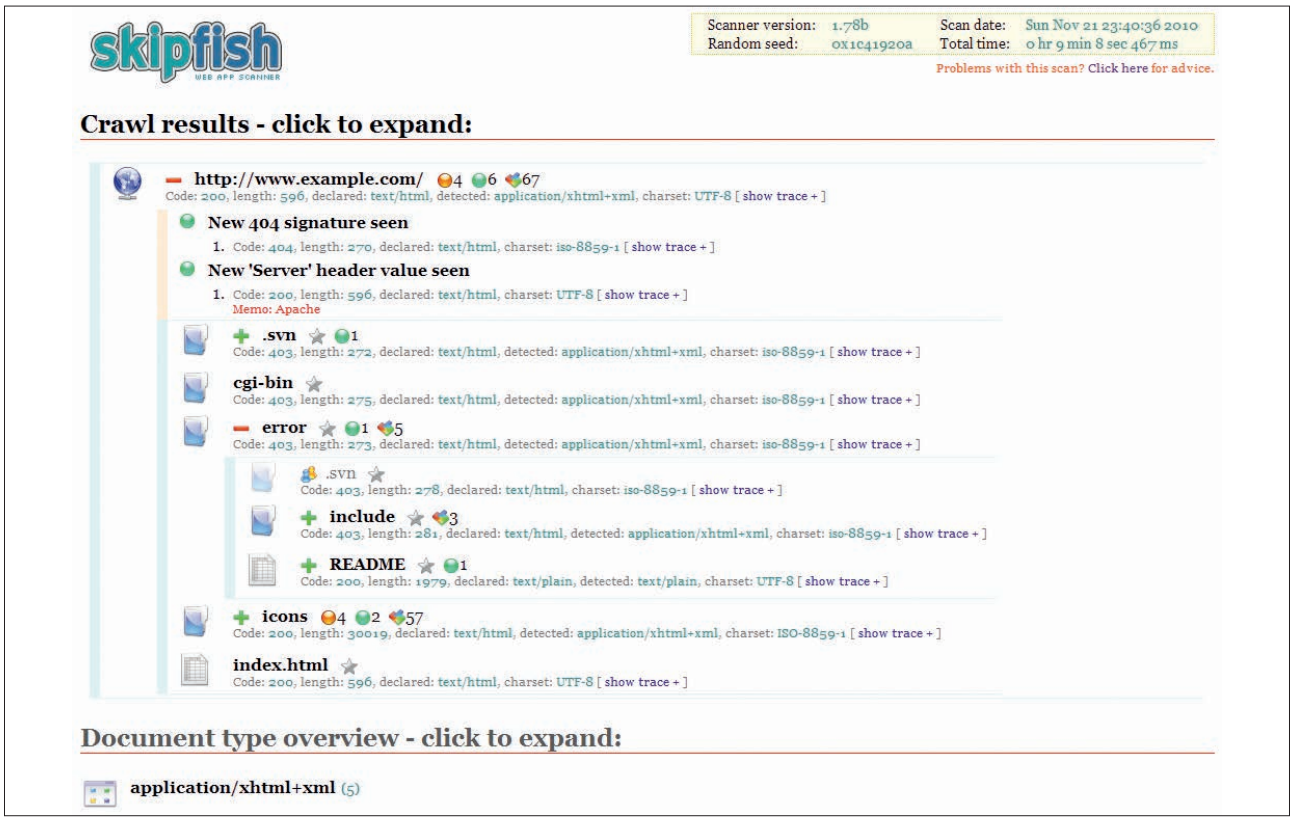

Abb. 1: Sample Screenshot von der SkipFish-Webseite

den ein Höchstmaß an Sicherheit und schützt somit Kundendaten vor Missbrauch (siehe Infokasten).

Überprüfung der Serverplattform

Unabhängig davon, ob der Onlineshop in Eigenregie oder von einem Dienstleister betrieben wird: Essenziell ist eine regelmäßige Prüfung – mindestens alle 3 Monate –, ob die Plattform gegenüber aktuellen Gefahren geschützt ist. Dafür gibt es inzwischen eine Vielzahl von Security-Lösungen im Netz. Zu meinen Favoriten unter den freien Tools gehören OpenVAS (*http://www.openvas.org*) und SkipFish (*http://code.google.com/p/skipfish/*). Während OpenVAS die komplette Infrastruktur der zu untersuchenden Plattform auf Schwachstellen überprüft, beschränkt sich SkipFish auf die reine Webapplikation. Damit eignet sich OpenVAS eher für in eigener Verantwortung betriebene größere E-Commerce-Systeme, während SkipFish auch einen gemieteten Webshop analysieren kann.

SkipFish weist neben den gängigen Sicherheitslücken wie Cross-Site-Scripting oder SQL Injection auch auf eine Vielzahl weiterer möglicher Schwachstellen hin. Im Gegensatz zu vielen anderen Tools zeichnet sich der Sicherheitsscanner durch einen intelligenten, heuristischen Ansatz aus und deckt so die eine oder andere potenzielle Schwachstelle mehr auf. Hinweis: Bevor ein Security-Tool für den eigenen Webshop verwendet wird, sollten sich Anwender vergewissern, dass dieses auch wirklich nur die eigene Online¬plattform testet. Im ungünstigsten Fall könnten nämlich Drittsysteme wie etwa „benachbarte“ Webserver im gleichen IP-Netz durch den Testlauf Kollateralschäden erleiden!

Absicherung der Webplattform

Einen echten Schwachpunkt bei jeder Webplattform stellt die eingesetzte Webapplikation an sich dar – egal, ob es

PCI DSS (Payment Card Industry Data Security Standard)

Kreditkartenschutzvorschrift und Standard, der einen sinnvollen IT-Sicherheitslevel zwischen Geschäftspartnern definiert. Das Regelwerk für den Zahlungsverkehr wird von allen wichtigen Kreditkartenorganisationen unterstützt und umfasst folgende 12 Anforderungen an Anwendersicherheitsstandards:

1. Installation und Pflege einer Firewall zum Schutz der Daten
2. Ändern von Kennwörtern und anderen Sicherheitseinstellungen nach der Werksauslieferung
3. Schutz der gespeicherten Daten von Kreditkarteninhabern
4. Verschlüsselte Übertragung sensibler Daten von Kreditkarteninhabern in öffentlichen Rechnernetzen
5. Einsatz und regelmäßiges Update von Virenschutzprogrammen
6. Entwicklung und Pflege sicherer Systeme und Anwendungen
7. Einschränken von Datenzugriffen auf das Notwendige
8. Zuteilen einer eindeutigen Benutzerkennung für jede Person mit Rechnerzugang
9. Beschränkung des physikalischen Zugriffs auf Daten von Kreditkarteninhabern
10. Protokollieren und Prüfen aller Zugriffe auf Daten von Kreditkarteninhabern
11. Regelmäßige Prüfungen aller Sicherheitssysteme und -prozesse
12. Einführen und Einhalten von Richtlinien in Bezug auf Informationssicherheit

sich um eine Individual-, eine kommerzielle Standard- oder eine Open-Source-Lösung handelt. Hier gilt immer, den Hersteller mit Blick auf eine sichere Entwicklung zu hinterfragen, wobei gerade Open-Source-Lösungen meistens nicht allzu strengen Sicherheitsrichtlinien unterliegen. Beispiel: Angenommen, ein Webshop besteht aus einem populären CMS mit zwanzig Extensions, inklusive Shopmodule. Selbst bei einer guten Absicherung dieses CMS kann jedes noch so unbedeutend erscheinende Plug-in ein Einfallstor für Hacker sein. Da oftmals unterschätzt, werden im Folgenden die gängigsten durch Hacker ausgenutzten Angriffspunkte vorgestellt.

Manipulation via Cross-Site-Scripting

So genanntes Cross-Site-Scripting (XSS)* ist nach wie vor die gängigste Angriffsform. Dabei wird versucht, die Webanwendung so zu manipulieren, dass sie schädlichen Skriptcode in die beim Besucher angezeigte Seite einbettet. Der Browser verarbeitet dann den eingeschmuggelten Code, als wäre es ein legitimer Inhalt der Webseite – mit allen entsprechenden Sicherheitsfreigaben. Darüber hinaus droht Unternehmen im Falle eines Serverabsturzes und des damit verbundenen Datenverlustes erheblicher Schaden, denn oftmals fehlt ein im Vorfeld ausgearbeiteter Krisenplan hinsichtlich eines absolut verlässlichen Ersatzsystems zur Datensicherung, was das zeitnahe Wiederherstellen von Daten erschwert.

Alle Informationen, die per Formulareingabe oder URL-Parameter (Uniform Resource Locator) an den Server übermittelt werden, sind zuerst dahingehend zu prüfen, dass sie auch wirklich keine schädlichen Codes enthalten. Gibt ein User zur Registrierung auf einer Website etwa als Benutzernamen

```
<script type='text/javascript'>
alert('hallo'); </script>
```

ein, dürfte nach Senden der Formulareingabe in keinem Falle ein Dialogfenster ‚Hallo' statt des Benutzernamens erscheinen. Dies wäre ein eindeutiges Indiz für eine nicht geprüfte und deshalb für Cross-Site-Scripting und eventuell sogar SQL-Injections anfällige Webseite.

Gerade Schwachstellen im Eingabefeld wie dem Suchformular ermöglichen das Austauschen des Inhalts oder das Ausführen von schädlichem Programmcode, um den Benutzer zu täuschen und an dessen Zugangsdaten oder Kontoinformationen zu gelangen. Sicherheitslücken der Webseite für Angriffe per Cross-Site-Scripting lassen sich einfach mithilfe eines Web Vulnerability Scanners wie des oben erwähnten SkipFish feststellen.

Sicheres Einloggen

Viele Applikationen von Webshops arbeiten mit Sessions, um den User nach dem Ein¬loggen zu identifizieren. Hier hat sich der Gebrauch von GUIDs (Globally Unique Identifier) bewährt. Darunter ist eine 32-stellige alphanumerische Zeichenkette zu verstehen, die das Identifizieren der Session-ID durch Ausschnüffeln (sogenanntes Session-Hijacking) praktisch unmöglich macht. Zusätzlich sollten natürlich sensible Daten wie eben Username/Passwort, aber auch die Session-ID ausschließlich per SSL übertragen werden. Der Webshop hat erkennbar ein Problem, wenn etwa das Bookmarken bzw. Weiterschicken eines Links zu einem Artikel die Session-ID in der URL ablegt. In diesem Fall kann jeder Empfänger des Links den Account des Shopkunden übernehmen.

Basisschutz vor SQL Injections

Ein großer Teil der Webanwendungen greift auf eine SQL-Datenbank zurück. Das Einschleusen oder Manipulieren von SQL-Kommandos bezeichnet man als SQL-Injection. Es ist derzeit die von Hackern am häufigsten eingesetzte Angriffstechnik auf Anwendungsebene.

* siehe Glossar Seite 112-113

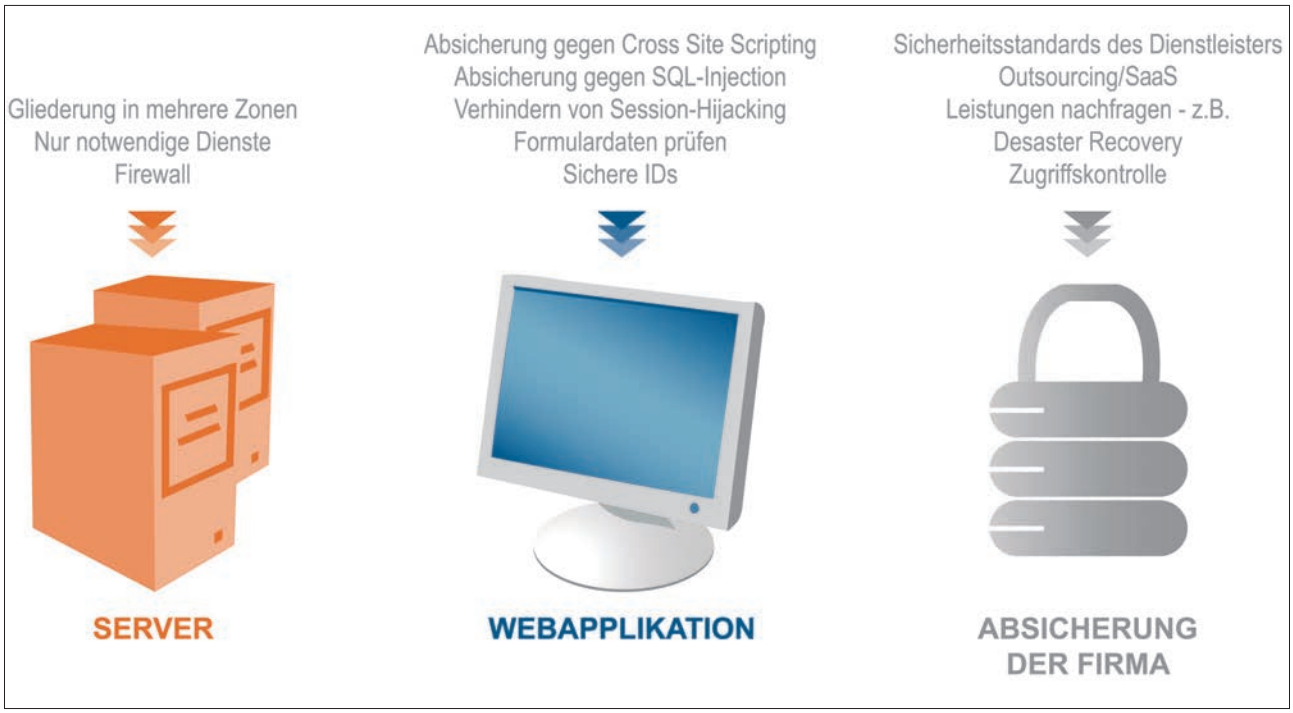

Abb. 2: Komplexe Konzepte betrachten Sicherheit als einen andauernden Prozess und basieren vereinfacht dargestellt auf drei Säulen. Deren wesentliche Bestandteile sind die Sicherheit innerhalb der Serverplattform, die Absicherung der Webanwendungen selbst sowie der Umgang mit Daten innerhalb der Firma und bei Miet-Lösungen.

Besonders anfällig für SQL-Injection sind fehlerhaft konzeptionierte Webseiten, deren Datenbankschnittstellen unnötig Informationen preisgeben. Schwachstellen können vor allem in Anmeldeformula¬ren oder Formularen zur Anforderung vergessener Passwörter ausgemacht werden. Um dies zu verhindern, sollten alle Zugriffe auf die Datenbank von der Webanwendung aus nur über sogenannte ‚Prepared Statements' oder besser ‚Stored Procedures' erfolgen; der direkte Einsatz von SQL-Befehlen ist – wenn möglich – zu vermeiden.

Schutz direkt an der Wurzel

Ein Großteil denkbarer Angriffsszenarien kann bereits durch die richtige Konfiguration der Scripting-Umgebung abgewehrt werden. Nicht vergessen: Auch bezüglich der Webapplikation hat der Leitsatz der geringsten Privilegien Bestand. Je weniger Rechte und Funktionen eine Applikation voraussetzt und erhält, desto weniger kann schiefgehen.

Generell sollte eine Webshop-Applikation idealerweise auf Basis der ‚Secure Coding Guidelines' entwickelt sein und regelmäßig daraufhin geprüft werden. Eine gute Quelle sind hier die online erhältlichen Guidelines des Open Web Application Security Project, kurz OWASP (*https://www.owasp.org*). Ebenso lassen sich (z. B. in der PHP Scripting Engine) durch Setzen einer Handvoll Optionen und Parameter gefährliche Funktionen abstellen oder der mögliche Schaden im Ernstfall begrenzen.

Zugriffsberechtigung: „Weniger ist mehr"

Der richtige Umgang mit sicherheitsrelevanten Themen im Unternehmen selbst wird oft vernachlässigt, ist allerdings zum eigenen Schutz unabdingbar. Demzufolge sollte die Zugriffsberechtigung auf Kundendaten für jeden Mitarbeiter klar geregelt sein – und zwar nach dem Ansatz: „Weniger ist mehr." Je weniger Mitarbeiter hier Einblick haben, desto geschützter sind die Daten vor unbefugtem Zugriff. Vor diesem Hintergrund empfiehlt sich zum einen die Installation eines Zugriffsschutzes von innen, zum anderen das Proto¬kollieren von Zugriffen seitens der Supportmitarbeiter mithilfe einer spezifischen Applikation. Auf diesem Weg können bei Bedarf Änderungen in den Bestandsdaten jederzeit nachvollzogen werden. Ebenfalls sollte das „Wer darf auf was zugreifen?" schriftlich festgehalten werden. Dies gibt im Falle eines Sicherheitsverstoßes beiden Seiten Klarheit, wer überhaupt die Möglichkeit hatte, eine „Tat" zu begehen. Und nicht zu vergessen: Passwörter sollten nie unbegrenzt lange gelten und immer personalisiert sein. Sonst hat der Ex-Kollege eventuell auch noch Jahre nach seinem Ausscheiden Zugriff auf vertrauliche Daten.

Fazit

Sicherheit fängt im Kopf an – nur wer alle Aspekte rund um das Thema Sicherheit für seinen Onlineshop beachtet und immer wieder aufs Neue überdenkt, wird im Kampf gegen Cyber-Kriminelle erfolgreich sein. ¶