

# SCHLUPFLÖCHER IM ONLINE-SHOP

**NICHT NUR BETREIBER VON ONLINE-SHOPS UND BANKING-PORTALEN BANGEN UM DIE SICHERHEIT IHRER WEBANWENDUNGEN. AUCH WEBSITES VON KMUS SIND ZIEL VON ANGREIFERN. WER GÄNGIGE SICHERHEITSLÜCKEN KENNT, KANN BÖSEWICHTEN DIE STIRN BIETEN.**

VON PETER HÖPFL

**Die möglichen Angriffsszenarien** in mittelständischen Unternehmen lassen sich im Grunde auf ein paar wenige „Modelle“ reduzieren. Das dabei am weitesten verbreitete ist Phishing. Abgefischt werden nicht nur Zugangs- und Transaktionsdaten, sondern auch Informationen zur Identität wie etwa Geburtsdatum, Anschrift und Führerscheinnummern sowie Konten- und Kreditkartennummern.

Auch das so genannte Cross Site Scripting (XSS) ist eine verbreitete Angriffsform. Dabei versucht ein Angreifer, die Webanwendung so zu manipulieren,

zur Datensicherung und erschwert somit das Wiederherstellen von Daten. Sicherheitsrisiken bergen auch die Abwicklung von Zahlverfahren via Internet. Doch das Ausfallrisiko lässt sich reduzieren, etwa durch Kreditkartenzahlungen. Auch das für den Kunden Bequemlichkeit bietende Lastschriftverfahren stellt eine Option dar. Jedoch sollte es zunächst nur Kunden angeboten werden, die bereits im Shop gekauft haben. Zusätzlich sollte man einen Höchstbetrag für die Bezahlung per elektronischem Lastschriftverfahren definieren. In bestimm-



**Peter Höpfl**, Leiter IT Atrada: „Wer schnell reagieren können will, sollte bereits während der Planung ein Sicherheitskonzept entwickeln.“

halb der Serverplattform, die Absicherung der Webanwendungen selbst sowie der Umgang mit Daten innerhalb der Firma und bei Miet-Lösungen.



Gute Sicherheitskonzepte basieren auf drei Säulen: Sicherheit innerhalb der Server, Absicherung der Webanwendungen sowie dem Umgang mit Daten innerhalb der Firma. (Quelle: Atrada 2008)

## SERVERPLATTFORM – PRINZIP DER GERINGSTEN PRIVILEGIEN

Die Sicherheit des Servers und des Netzwerks bilden das Fundament der Sicherheit einer Webanwendung. Grundsätzlich muss die Serverplattform in mehrere Zonen aufgeteilt sein und eine Firewall einsetzen. Es empfiehlt sich, nur Webapplikationsserver direkt mit dem Internet zu verknüpfen; alle weiteren Systeme, die nicht unmittelbar vom User angesprochen werden, sollten eine Webverbindung vermeiden. 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. Ein Großteil denkbarer Angriffsszenarien kann durch die richtige Konfiguration abgewehrt werden. Nicht vergessen: Auch was die Webapplikation angeht, hat der Leitsatz der geringsten Privilegien Be-

dass sie schädlichen Skriptcode in die beim Besucher angezeigte Seite einbettet. Der Browser verarbeitet den eingeschmuggelten Code, als wäre es ein legitimer Inhalt der Webseite – mit allen entsprechenden Sicherheitsfreigaben. Darüber hinaus droht Unternehmen im Falle eines Serverabsturzes und dem damit verbundenen Datenverlust erheblicher Schaden. Denn oftmals fehlt ein im Vorfeld ausgearbeiteter Krisenplan im Blick auf ein verlässliches Ersatzsystem

ten Fällen besteht die Möglichkeit, im Hintergrund einen Bonitätscheck durchzuführen und dem Kunden aufgrund des Ergebnisses bestimmte Zahlarten anzuzeigen beziehungsweise vorzuenthalten. Um den skizzierten Problemen effektiv zu begegnen, betrachten komplexe Konzepte Sicherheit als einen andauernden Prozess und fließen bereits in die Planungsphase von E-Commerce-Projekten ein. Sie basieren auf drei Säulen. Deren Bestandteile sind die Sicherheit inner-

stand. Je weniger Rechte und Funktionen eine Applikation voraussetzt und erhält, desto weniger kann schiefgehen.

#### WEBAPPLIKATIONEN – AN DER WURZEL PACKEN

Durch Setzen von einer Handvoll Optionen und Parameter lassen sich gefährliche Funktionen abstellen oder der mögliche Schaden im Ernstfall begrenzen. So schützt zum Beispiel das Arbeiten mit Doppel-Opt-Ins bei der Online-Registrierung über eine E-Mail-Adresse vor Missbrauch. Der User erhält hier nach der Anmeldung per E-Mail die Aufforderung, die angegebenen Daten nochmals zu bestätigen. Erst dann wird sein Account akzeptiert. Weiterhin sollten Sicherheitsvorkehrungen wie das Filtern von Java Script Codes beziehungsweise Cross Site Scripting (XSS), der Gebrauch von Globally Unique Identifiers (GUIDs) und Schutzmaßnahmen vor SQL-Injection getroffen und in alle Webanwendungen integriert werden.

Viele Webapplikation arbeiten mit Sessions, um den User nach dem Ein-

Sicherheitskriterien müssen bereits in der Planungsphase einer Webapplikation bedacht werden. Nicht nur zum optimalen Schutz der Lösung, sondern auch aus Kostengründen.

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 (so genanntes Session Hijacking) praktisch unmöglich macht.

Ein Teil der Webanwendungen greift auf eine SQL-Datenbank zurück. Das Einschleusen oder Manipulieren von SQL-Kommandos bezeichnet man als SQL-Injektion; dies ist derzeit die von Hackern am häufigsten eingesetzte Angriffstechnik auf Anwendungsebene. Besonders anfällig sind fehlerhafte Webseiten, deren Datenbankschnittstellen unnötig Informationen preisgeben. Schwachstellen lassen sich vor allem in Anmeldeformularen oder Formularen zur Anforderung

vergessener Passwörter ausmachen. Um dies zu verhindern, sollten alle Zugriffe auf die Datenbank von der Webanwendung aus nur über so genannte Prepared Statements oder besser Stored Procedures erfolgen; der Einsatz von SQL-Befehlen ist wenn möglich zu vermeiden. Der richtige Umgang mit sicherheitsrelevanten Themen im Unternehmen selbst wird oft vernachlässigt, ist zum eigenen Schutz allerdings unabdingbar. Demzufolge muss die Zugriffsberechtigung auf Kundendaten für jeden Mitarbeiter klar geregelt sein –, und zwar nach dem Ansatz „weniger ist mehr“. Je weniger Mitarbeiter 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 Protokollieren von Zugriffen seitens der Supportmitarbeiter. Auf diesem Weg können bei Bedarf Änderungen in den Bestandsdaten jederzeit nachvollzogen werden.

Breibt man seine Webanwendung nicht selbst, so heißt es „Augen auf“ bei der Auswahl des richtigen Systems. Vor

allem bei Miet- und ASP-Systemen ist zu beachten, wo die Anwendungen laufen und die Daten gespeichert werden – unterschiedliche Standards in Rechenzentren sowie deren geografische Standorte haben hier maßgeblichen Einfluss.

#### SICHERHEIT UMFASSEND PLANEN

Sicherheitskriterien müssen bereits in der Planungsphase einer Webapplikation bedacht werden, nicht nur zum Schutz der Lösung, sondern auch aus Kostengründen. Neben der Implementierung gängiger Sicherheitsstandards und einem gesunden Misstrauen spielt letztendlich eine erhöhte Wachsamkeit eine tragende Rolle, was die Sicherheit im System betrifft. ■

› Kennziffer: ECM14257

## GLOSSAR

### CROSS SITE SCRIPTING

Manipulation von Parametern, so dass im Browser Skriptcode ausgeführt wird.

### DOPPEL-OPT-IN

Verfahren, bei dem der Eintrag in eine Abonnentenliste bestätigt wird. Meist wird hierzu eine E-Mail-Nachricht mit Bitte um Bestätigung an die eingetragene Kontaktadresse gesendet.

### GUID (GLOBALLY UNIQUE IDENTIFIERS)

global eindeutige Zahl, die in verteilten Computersystemen zum Einsatz kommt.

### OPT-IN

Verfahren, bei dem der Empfang regelmäßiger Nachrichten wie E-Mails oder auch SMS explizit bestätigt werden muss.

### PHISHING

Betrügerei, bei der versucht wird, Internetbenutzer mit E-Mails von angeblich vertrauenswürdigen Absendern auf gefälschte Websites zu locken.

### PREPARED STATEMENTS

vorbereitete Anweisung für ein Datenbanksystem, das anstelle von Parameterwerten Platzhalter enthält.

### SCANNER

allgemeine Bezeichnung für ein Programm, das Informationen durch systematische Tests sammelt; siehe auch Webscanner

### SESSION

logische Verbindung zwischen Client und Server; kann über mehrere Einzel-Zugriffe hinweg bestehen

### SESSION HIJACKING

Angriff auf eine verbindungsbehaftete Datenkommunikation zwischen zwei Computern.

### SESSION-ID

Identifikationsmerkmal, um mehrere zusammengehörige Anfragen eines Benutzers zu erkennen und einer Sitzung zuzuordnen.

### SKRIPT

Programm, das in einer Interpretersprache geschrieben ist.

### STORED PROCEDURES

eigenständiger Befehl, der eine Abfolge von gespeicherten Befehlen ausführt.

### SQL-INJECTION

spezielle Angriffsmethode auf Datenbanken.

### WEB SCANNER

Programm zum Testen von Verwundbarkeit, Angriffspunkten und Schwachstellen einer Webapplikation.