Sicherheit für Ihre Website

Angreifer kommen aus unterschiedlichen Richtungen mit vielen verschiedenen Motiven – so wehren Sie sie ab und schützen Ihren Web-Auftritt.

Wenn kleinere Unternehmen keine eigene IT-Abteilung finanzieren können, stehen sie bei der Absicherung ihrer Website oft vor Problemen. Wartung, Pflege und Sicherheit der Online-Präsenz müssen vom Unternehmen selbst organisiert werden. Wird die Webseite aber richtig strukturiert, lassen sich die meisten Sicherheitslücken von Anfang an vermeiden.

Am besten können Verantwortliche Sicherheitslücken aufspüren, indem sie sich in die Angreifersituation versetzen. Welche Kenntnisse und Werkzeuge haben potenzielle Angreifer und welche Vorteile erhalten sie?

Angriffsvektoren definieren

Bei Online-Präsenzen können schnell zwei Angreifergruppen definiert werden. Zum einen Datendiebe, deren Ziel nur der materielle Gewinn durch Systemeinbruch ist. Beispielweise, um mit gestohlenen Kreditkartendaten auf fremde Rechnung einzukaufen. Im Fokus dieser Angreifergruppe liegt nur der Einbruch ins System und der Datenklau. Daneben gibt es aber auch noch die Gruppe der Konkurrenten. Diese Gruppe versucht die Online-Präsenz so weit zu sabotieren, dass die Webseite nicht mehr aufgerufen werden kann. Der Imageschaden ist hier dann das Ziel dieser Art von Angriff: Funktioniert der Webshop meines Konkurrenten nicht, wird meine Webseite öfter besucht und erscheint als performante Internet-Präsenz in einem besseren Licht.

Aus der Angreifermotivation können der Angriffsweg und die Angriffstechnik abgeleitet werden. Fachleute bezeichnen dies als "Angriffsvektor". Im Folgenden werden verschiedene Angriffsszenarien beschrieben – und wie man sich gegen sie schützt:

Foto: Moreinput@Pixelio

Sicher verschlossen ist eine Webseite nie; Security gleicht eher einem Wettlauf zwischen Hacker und Betreiber.

Foto: Fotolia/sk-design

Wer eine Webseite ins Netz stellt, muss sie gegen mögliche Angriffe, zum Beispiel SQL-Injection oder Pufferüberläufe, absichern.

Schutzschirm Pufferüberlauf

Bei einem Pufferüberlauf versucht der Angreifer, eine zu grosse Datenmenge an Systemteile zu senden, die dann aufgrund der nicht zu verarbeitenden Datenmenge zusammenbrechen, sprich: überlaufen. Gelingt es einem Angreifer, so die Zugangsbeschränkung überlaufen zu lassen, hat er für die Dauer dieses Zustands vollen Systemzugang. Das kann er nutzen, etwa um Administratorenkonten einzurichten oder die Rechte bestehender Konten zu ändern. In letzter Konsequenz hat der Angreifer dauerhaft einen Systemzugang.

Allerdings sind nur bestimmte Programmiersprachen für diese Pufferüberläufe anfällig; für Web-Anwendungen sind hier die Sprachen C und C++ für die Server-Software sowie PHP für die Web-Anwendungen zu nennen; sicher sind Java und Perl. Um Pufferüberläufe zu verhindern, sollten die Newsticker der einschlägigen Online-Magazine oder Seiten wie zum Beispiel www.osvdb.org (Open Source Vulnerability Database) täglich geprüft und verfügbare Patches sofort eingespielt werden.

Mit gefälschten Anfragen ins System

Angreifer können auch über schlecht geschützte Datenbankanbindungen ins System gelangen. Das wird als "SQL-Injection" (SQL-Einschleusung) bezeichnet. Dabei versuchen Angreifer, manipulierte Befehle an Datenbankanfragen zu hängen, um so den Zugriffsschutz zu knacken. Beachtet werden muss, dass die meisten Redaktionssysteme heute modular aufgebaut sind. Das heisst, dass der Betreiber für viele Anforderungen Zusatzmodule selbst installieren kann, die wiederum Datenbankanfragen an das System senden, beispielsweise eine bessere Bildergalerie, ein Umfrageformular oder ein leichter zu bedienendes Shop-System. So macht also jedes zusätzlich installierte Modul das System nicht nur langsamer, sondern auch anfälliger für SQL-Injections und Pufferüberläufe.

Sichere Zahlungswege

In Bezug auf Module müssen auch nachträglich installierte Bezahlsysteme besonders berücksichtigt werden. Denn gelingt es einem Angreifer, mittels SQL-Injection oder Pufferüberlauf Zugriff auf das Bezahlsystem zu erhalten, hat der Shop-Betreiber schon verloren – der Zugriff reicht aus, um die Bezahldaten der Kunden zu stehlen. Als Mindeststandard müssen die Bezahlsysteme ein gesichertes Rechenzentrum und eine Payment-Card-Industry-Data-Security-Standard-Lizenzierung vorweisen können. Weitere Pluspunkte sind eine 128-Bit-SSL-Verschlüsselung und die Referenzen seriöser Banken.

Das Passwort aus dem Wörterbuch

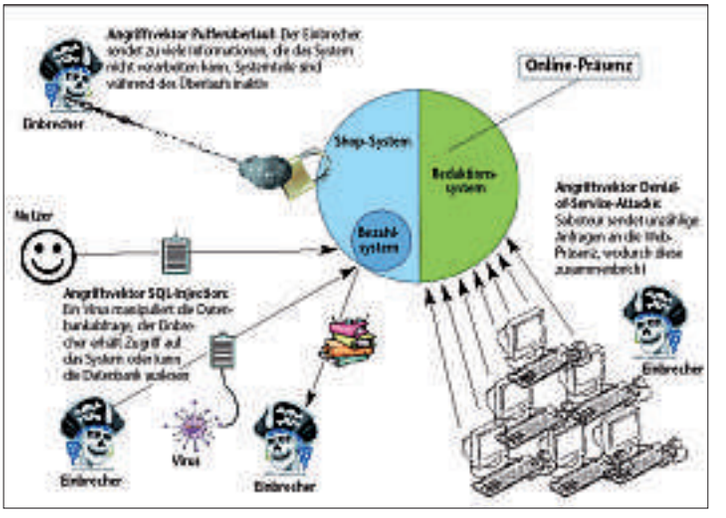
Weil es so banal ist und schon so häufig funktioniert hat, unterschätzen Sicherheitsverantwortliche oft die Gefahr zu simpler Passwörter. Angreifer probieren bei der Passwortabfrage einfach die häufigsten Passwörter so lange aus, bis sie per Zufall oder Wahrscheinlichkeitsbe-

rechnung das richtige Passwort gefunden haben. Teilweise finden sich im Internet auch speziell für diese Aufgabe entwickelte Programme. Diese Programme können anhand von Wörterbüchern mehrere Tausend Passwörter in kurzer Zeit an Passwortabfragen ausprobieren. Neben kryptischen Passwörtern ist hier die wirksamste Gegenmassnahme, nach mehrmaliger falscher Passwortabfrage die Passwortabfrage für kurze Zeit zu sperren.

Kryptische Passwörter sind manchmal schwerer zu erstellen als gedacht. Daher bieten einige Redaktionssysteme an, per Knopfdruck Zufallspasswörter zu erstellen. Zu beachten ist dabei aber, dass Computer Zufallspasswörter eben nicht per Zufall erstellen. Computer können nicht würfeln, sondern erstellen Zufallszahlen aus Datum und Uhrzeit, die mit einem Algorithmus verändert werden. Gelangen nun Angreifer an mehrere solcher Zufallspasswörter – beispielsweise, indem sie bei der Erstellung mehrerer Kundenkonten vom selben Algorithmus ein Zufallspasswort erhalten –, können sie diese Passwörter nutzen, um den Algorithmus zu berechnen. Das heisst, dass Passwörter möglichst ohne Zufallsgenerator erstellt werden sollten und lang sowie in sich unlogisch sein sollten.

Sabotage: Angriff der Konkurrenz

Auch in der Offline-Welt ist das Schema von Denial-of-Service-Attacken bekannt. Denial-of-Service heisst übersetzt "Dienstverweigerung". Konkurrenten können zum Beispiel die Verwaltung ihrer Mitbewerber ausschalten, indem sie viele gefälschte Anfragen und Bestellungen an sie senden. Der geschädigte Mitbewerber hat dann bei der Bearbeitung der ganzen Anfragen und Bestellungen zu viel Arbeit, die ihm ausser Schaden nichts bringt.



Die Angreifer: Sind die Angriffsvektoren definiert, lassen sich Sicherheitslücken schnell finden – und auch schliessen.

In der IT-Welt funktioniert dies nach demselben Prinzip, nur viel effizienter. Automatisiert wird über einen Rechner oder über ganze Rechnernetze eine Vielzahl an Anfragen an die Online-Präsenz gesandt. Das Ergebnis: Kunden können den Webshop nicht erreichen, die Performance der Webseite fällt in den Keller. Durch eine Firewall und durch Sperren der entsprechenden IP-Adressen können Shop-Betreiber diese Anfragen aber blocken und ihr System schützen. Dazu benötigt die IT ein Log-System, das die Angreifer-IP-Adressen aufspüren und ein Redaktionssystem, das bestimmte IP-Adressen blocken kann. ■

David Dangel/jb