HELPDESK

Applikationen auf den Zahn gefühlt

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

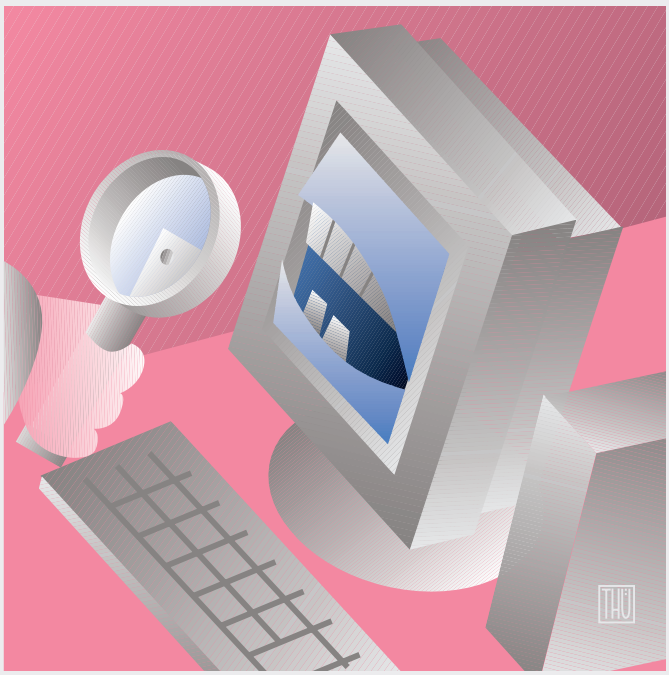

ILLUSTRATION: CW/THÜ

Frage: Für unsere Aussendienstmitarbeiter haben wir eine Web-Applikation implementiert. Diese bietet Zugriff auf Kundendaten, weshalb wir eine Sicherheitsüberprüfung vornehmen wollen. Wie ist hierbei vorzugehen und wie gross ist der Aufwand?

Definition

Eine Sicherheitsüberprüfung mit Fokus Applikation wird als «Application Security Audit» bezeichnet. Im Gegensatz zu einem Penetration-Test, dem unprivilegierten Einbruchsversuch, wird die Applikation beim Application-Security-Audit mittels Benutzer- und Admin-Rechten überprüft. Zudem beinhaltet diese Form von Tests auch organisatorische Aspekte, wie Backup oder Abläufe bei der Erstellung von Benutzerkonten. Der Application-Security-Audit beginnt in etwa dort, wo der Penetration-Test aufhört.

Bei dieser Thematik tauchen immer wieder die folgenden drei Irrtümer auf:

1. «Es ist ausschliesslich die Applikation zu untersuchen.»

Richtig ist: Es macht durchaus Sinn, den Application-Security-Audit mit einem Penetration-Test zu kombinieren: Denn eine Applikation kann nur so sicher sein, wie das Umfeld, in dem sie betrieben wird. Weisen das Betriebssystem oder der Webserver Sicherheitslücken auf, gefährden diese auch die Sicherheit der gesamten Anwendung. Generell sollten alle Datenwege, vom Benutzer über den Client, das Netzwerk, den Server bis hin zur zentralen Datenbank oder Backup-Tape im Audit berücksichtigt werden.

2. «Nur was angeklickt werden kann, kann auch ausgeführt werden.»

Richtig ist: Die Schnittstelle des Servers muss davon ausgehen, dass alle Eingaben grundsätzlich bösartig sind. Dieses Credo sollte vor allem den Entwicklern bei jeder Codezeile bewusst sein. Sämtliche sicherheitsrelevanten Entscheidungen müssen auf der Serverkomponente gefällt werden.

3. Funktionalität geht vor Sicherheit.

Richtig ist: Eine gute Projektplanung lässt den Entwicklern genügend Zeit, sich um die Sicherheitsaspekte zu kümmern. Übermüdete und gehetzte Programmierer erweisen der Sicherheit keine guten Dienste.

Aufwand

Der Aufwand für einen Application-Security-Audit variiert stark, da jede Applikation einzigartig ist. Die Komplexität und die Verwendung von Standardkomponenten erhöhen oder verkleinern den zeitlichen Aufwand, welcher typischerweise zwischen zehn und zwanzig Personentagen liegt. Um sich vor unliebsamen Überraschungen zu schützen, macht es manchmal Sinn, bereits während der Konzeptphase eine unbeteiligte Instanz beizuziehen und damit eine neue Perspektive zu gewinnen.

> «Eine Applikation kann nur so sicher sein, wie das Umfeld, in dem sie betrieben wird.»

Welche Module untersucht werden, hängt ebenfalls von der Applikation ab. Oft wird zur Schonung des Projektbudgets auf einen kompletten Review des Quellcodes verzichtet, und nur die sicherheitsrelevanten Klassen untersucht. Ein dokumentenbezogener Review bildet meist die Grundlage und gibt dem Auditor die Zeit, sich in die Applikation einzuarbeiten. Daraus resultieren eventuell Mängel in der Dokumentation oder weitere zu untersuchende Schnittstellen und Prozesse. Auf technischer Ebene wird der Soll/Ist-Zustand manuell oder mittels Tools überprüft und neben dem analytischen auch ein kreativer Ansatz verfolgt.

Für den Projektablauf kann auch ein iteratives Modell gewählt werden, welches aufgedeckte Sicherheitslücken schliessen und erneut kontrollieren lässt. Dies kann das Projekt um Wochen hinaus verzögern. Bei zahlreichen Veränderungen besteht eine andere Möglichkeit darin, die Nachkontrolle in einem kleinen Folgeprojekt durchzuführen. Diesen Review könnte gar ein neuer Security-Anbieter durchführen.

Das Projekt sollte in einem unabhängigen, fairen Bericht resultieren, der die konzeptionell-organisatorischen sowie die technischen Sicherheitsmängel der Anwendung ausweist und praktikable Verbesserungsvorschläge liefert. ■

Der Autor
Simon Wepfer ist Consultant bei der Sicherheitsberaterin Oneconsult, Thalwil, www.oneconsult.com.

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch