

Mythos: Sichere Web-Applikationen

Obwohl sich in letzter Zeit Web-Applikationen zum bevorzugten Ziel von Hacker-Angriffen entwickelt haben, unterschätzen viele Firmen noch immer die damit verbundenen Risiken. Statt teures eigenes Knowhow zum Schutz webbasierter Anwendungen aufzubauen, bieten hierfür Services eine echte Alternative.

Nach wie vor werden bei Investitionen in die IT-Security die Web-Applikationen zu wenig beachtet. So haben sie sich inzwischen zum veritablen Einfallstor in die Unternehmen entwickelt, über das Cyber-Kriminelle relativ einfach an qualifizierte Daten herankommen. Und weil der Einsatz Web-basierter Systeme für die eigenen Geschäftsprozesse, die Transaktionen mit Lieferanten und Kunden sowie für immer mehr Online-Services ständig wächst, nimmt auch die Abhängigkeit vieler Unternehmen von Webanwendungen zu. In diesem Dilemma stanno zwar viele Firmen ihre Websites mit Firewalls, Verschlüsselung (SSL) und Sicherheitsmechanismen für Netzwerke und Hosts aus, doch verringert sich damit nicht das Risiko, die komplexen Komponenten der eigentlichen Webanwendungen adäquat zu schützen.

Denn bei Angriffen auf Webseiten, mit denen in der Regel sensible Daten kompromittiert werden, heissen die Übeltäter oft Cross Site Scripting (XSS) und SQL Injection. Solche Schwachstellen fallen allerdings meist nicht in den traditionellen Kompetenzbereich von Netzwerk-Sicherheitsmanagern. Deshalb bleiben Sicherheitslücken in Webanwendungen häufig unbemerkt und werden immer öfter für Angriffe genutzt. Obwohl in diesem sensiblen Security-Bereich genaue Zahlen fehlen, ist heute klar, dass viele Unternehmen gegen diese Angriffe nicht mehr durch ihre herkömmlichen Abwehrmechanismen auf Netzwerkebene geschützt und neue Vorsichtsmassnahmen unumgänglich sind.

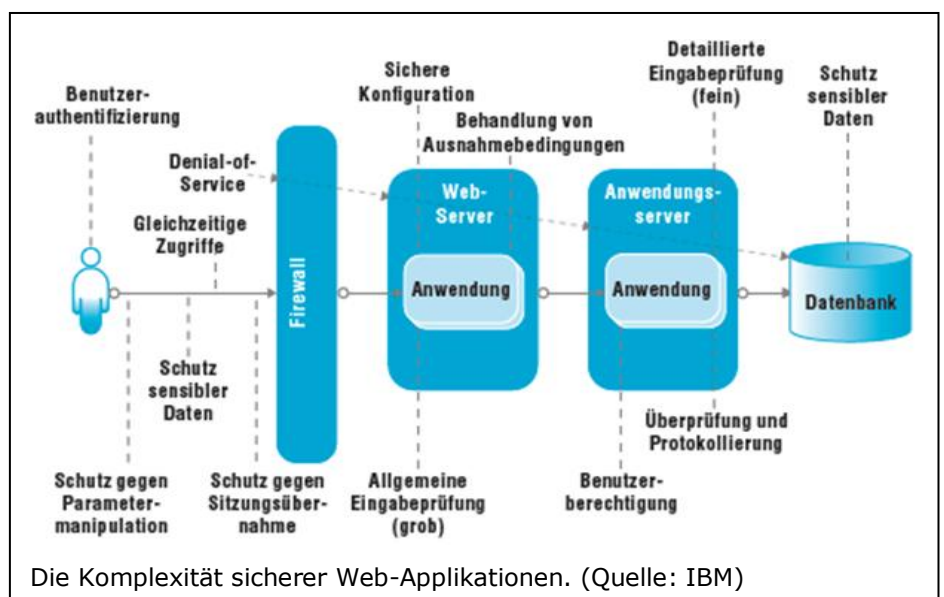
Laut Analysten von Gartner sind heute gegen 70 Prozent aller Web-Applikationen verwundbar und 75 Prozent aller Attacken laufen direkt über Webanwendungen. Die Motive der Hacker liegen in der besonderen Qualität und damit im grossen Wert der über Web-Applikationen erbeuteten Daten. Und die möglichen Folgen für die betroffenen Unternehmen sind entsprechend drastisch: Neben dem zu erwartenden Imageschaden, fallen Kosten für die Behebung der Fehler an und es kann zu Datenverlusten, Betriebsunterbrechungen sowie zu Strafzahlungen oder Verlust von Kunden kommen.

Proaktiver Schutz der Webanwendungen

Die meisten Unternehmen versuchen sich vor solchen Angriffen heute durch eine Kombination von verschiedenen Lösungen zu schützen. Dazu zählen unter anderem Firewalls und Intrusion Detection Systeme. Damit soll der nichtautorisierte Zugriff vermieden beziehungsweise die Sicherheit der eigenen IT-Landschaft gewährleistet werden. Laut Ingo Hefti, Senior Consultant Software und Security beim Berner IT-Dienstleister Sedna Informatik AG, „leidet diese Vorgehensweise jedoch daran, nur zu reagieren und die Security nicht proaktiv zu gewährleisten“. Hinzu komme, dass sich nur wenige Un-

ternehmen Mitarbeiter leisten können, die sich ausschliesslich dieser Problematik widmen und bereits bei der Entwicklung ihrer Webapplikationen, spätestens aber vor dem Release Sicherheitslücken innerhalb des Software Lifecycle aufspüren.

Deshalb setzen die Berner Spezialisten an diesem Punkt an. Einerseits identifizieren, validieren und berichten ihre zertifizierten „Ethical Hacker“ den Unternehmen über die Schwachstellen in den vorhandenen Webanwendungen. Auf dem Prüfstand kommt dabei die gesamte IT-Infrastruktur einschliesslich der Systeme – also neben dem Internet auch das interne Netzwerk. Die Schwachstellen, Sicherheitsmängel und Verwundbarkeiten der jeweiligen Unternehmensumgebung werden dazu mit Methoden und Tools aufgespürt, wie sie auch professionelle Hacker anwenden. Neben den internen und externen Angriffen können die Tests auch als blinde Attacken, ohne Kenntnisse der jeweiligen Infrastruktur durchgeführt werden. „Da alle Angriffsszenarien mit dem Kunden abgesprochen sind, lässt sich von Anfang an bestimmen, welche installierten Systeme und Prozesse involviert sein sollen“, erklärt Hefti. Am Ende derartiger Tests stehen immer Reports und ein Abschlussbericht mit konkreten technischen und allenfalls organisatorischen Verbesserungsvorschlägen.



Häufige Angriffsverfahren auf Web-Applikationen

Cross-Site Scripting (XSS) sind Angriffsverfahren, die darauf zielen, dem Benutzer einer Webseite beispielsweise via Phishing Mail fremden Code unterzubeln. Dazu versucht der Angreifer den Benutzer mit einer manipulierten URL innerhalb seiner gewohnten Umgebung etwa beim E-Banking ein Skript ausführen zu lassen, das zum Beispiel alle Eingaben und Mausclicks des Benutzers aufzeichnet und an einen fremden Server schickt. Der Angreifer will Informationen wie Passworte und Logins, die ein Webseiten-Benutzer ihm freiwillig nie geben würde. Hier geht es also nicht darum, dass ein Cyber-Krimineller in einen Server einbrechen will, sondern gezielt um den Angriff auf eine Webseite.

Anders als beim XSS geht es bei der SQL Injection, dem Einschleusen von SQL-Code, nicht darum, den Anwender einer Webseite auszuschnüffeln. Vielmehr wird dieses Verfahren verwendet, um direkt die Datenbank hinter einem Webserver anzugreifen. Die Folgen sind gleichwohl fatal, weil ein Angreifer möglicherweise in den Besitz geschützter Daten gelangt. Trotzdem ist das Verfahren ähnlich gelagert wie beim XSS. Um Daten in den Webserver zu schmuggeln, werden bei der Attacke in vorhandene Formfelder auf einer Webseite zusätzliche Befehle zum Umbiegen der Datenbankabfragen eingegeben. Lassen sich beispielsweise über das Login-Feld einer Webanwendung Daten ungefiltert an die dahinterliegende Datenbank weitergeben, ist diese Datenbank mit SQL Injection angreifbar und es ist denkbar, dass so etwa Benutzerdaten des Unternehmens ausgelesen werden können.

Andererseits setzt Sedna bei der Schwachstellensuche auf ein proaktives Vorgehen. Eingesetzt wird dafür die Software Rational AppScan von IBM, womit hoch entwickelte und intelligente Scanning-Technologien (White- und Blackbox Scanner) zur Verfügung stehen. Sie enthält - ständig aktualisiert - alle Pattern, also die schematischen und codespezifischen Strukturen bekannter Angriffsszenarien. Hefti: „Vom Erstellen einer Webanwendung bis hin zur Integration in die vorhandene Infrastruktur werden auf der Basis dieser Software stets auch die jüngsten Gefahrenquellen eruiert“.

Die Software kann im Lizenzmodell vom Kunden selbst gekauft oder einfach als Service (nur Blackbox-Scanning) bei Sedna bezogen werden. Hefti sieht den Vorteil des Service-Modells darin, dass kein teures eigenes Knowhow aufgebaut werden muss und dennoch über regelmässige Scans die höchste Sicherheit von Webapplikationen in einem Unternehmen garantiert ist.

Drei Schritte zur sicheren Webanwendung

Da die Software als automatisiertes Tool zum Einsatz kommt, entfällt die oft aufgrund von personellen und finanziellen Engpässen vernachlässigte Suche nach Schwachstellen in den Web-Applikationen. Rational AppScan lokalisiert in den Webanwendungen der Unternehmen bekannte Verwundbarkeiten wie XSS, SQL Injection und viele

weitere. In einem zweiten Schritt unterstützt ein umfangreiches Security Reporting die Risikoanalyse und vereinfacht damit die Einhaltung der gängigen Standards. Und schliesslich werden zuletzt Korrektorempfehlungen ausgegeben. Den



Entwicklern von Webanwendungen stehen auf diese Weise intelligente Korrektorempfehlungen zur Verfügung, die konkrete Listen mit Aufgabenstellungen und Erläuterungen umfassen, um erkannte Schwachstellen rasch beheben zu können.

Mit Rational AppScan liegt also nicht nur eine umfassende Scan-

Abdeckung vor, IBM spricht von der geringsten „False Positive“ Rate in der Industrie, sondern neben den erprobten Korrektorempfehlungen sind die Sicherheitsüberprüfungen direkt in den Entwicklungsprozess von Web-Applikationen integriert. Zudem erlaubt die Übersichtlichkeit der Software eine effektive Kommunikation innerhalb von Entwicklungsteams, was zur raschen Korrekturen nach der Entdeckung von Schwachstellen führt. Bei Sedna betont man ausserdem die Serviceorientierten Möglichkeiten dieses Angebotes. „Weil die Software auch von aussen eingesetzt werden kann“, führt Hefti aus, „halten sich die Kosten dieser Lösung in Grenzen, wenn ein Unternehmen nur von Zeit zu Zeit (etwa vor jedem neuen Release oder einmal pro Jahr) manuelle Sicherheitstests vornehmen will“.

Das Unternehmen

Die in Gümligen bei Bern 2004 gegründete Sedna Informatik AG versteht sich als IT-Dienstleister, der in verschiedenen Bereichen arbeitet:

- Als unabhängige Berater fokussieren sie die Evaluationen und Konzeptionen von Infrastrukturen.
- Sie liefern zudem als IBM Premier Partner alle Server- und Storage-Hard- und Software inklusive Installation und Implementation.
- Sedna übernimmt ausserdem als Outsourcer die Verantwortung für den Betrieb von Infrastrukturen.
- Zwei Mitarbeiter sind zertifizierte „Ethical Hacker“, deren Schwerpunkte die Analyse und Tests von bestehenden IT-Infrastrukturen sind, um mögliche Angriffe auf die Kundensysteme respektive Web-Applikationen der Kunden zu vermeiden.