

Applikationssicherheit

Sicherheitsrisiko Web-Applikationen

22.01.2010 | Autor: Von Cyrill Osterwalder

Web-Applikationen eignen sich als Einfallstor für Cyber-Kriminelle. Angriffe lassen sich aber mit Web Application Firewalls verhindern.

Web-Applikationen sind derzeit das beliebteste Einfallstor für Hacker. Sie sind einfach zu knacken und erlauben gewieften Angreifern den Zugriff auf sensible Unternehmensdaten. Dennoch halten sich auch unter erfahrenen Administratoren hartnäckig klassische Denkfehler.

«Über unsere Web-Applikationen erhält man keinen Zugang zu unseren Systemen.»

Zielgerichtete oder professionelle Datenzugriffe laufen oftmals im Verborgenen und über verdeckte Pfade ab — gerade Web-Applikationen bieten Hackern vielfältige Ansatzpunkte zum Datendiebstahl und gehören daher heute zu den bevorzugten Angriffszielen. Sie bieten direkte Zugriffe bis hin zu den wichtigsten Informationen eines Unternehmens. Anders als früher sind deshalb zielgerichtete Informationsdiebstähle heute an der Tagesordnung. Es werden keine Exploits mehr geschrieben, die Sicherheitslücken beliebiger Ziele ansteuern. Vielmehr wird ein interessantes Ziel mit technischen Manipulationen gezielt aus dem Tritt gebracht. Schon die klassischen Manipulationsmethoden wie Forceful Browsing, Cross-Site-Scripting oder SQL/Command Injections führen bei drei Viertel aller Web-Applikationen zum Erfolg. Diese zielgerichteten Datenzugriffe sind nicht über die Signatur erkennbar und kein reaktiver Sicherheitsschutz wie ein Intrusion-Detection- oder Intrusion-Prevention-System kann sie verhindern.

Einer der grössten Irrtümer hierbei ist, dass bei einem erfolgreichen Angriff nur die Daten in Gefahr seien, welche die Web-Applikation selbst verwendet. Allerdings ist es nicht unüblich, dass über eine vermeintlich harmlose Web-Applikation die gesamten internen Unternehmensdaten gestohlen werden.

Wirksamen Schutz gegen unerlaubte Datenzugriffe und Angriffe von Hackern bieten Web Application Firewalls (WAF) zwischen Anwender und Webanwendung, die nur gültige URLs zulassen und somit Backend-Systeme vor illegalem Zugriff schützen.

«Die Sicherheit von Web-Applikationen muss schon bei der Entwicklung sichergestellt werden.»

Natürlich lassen Applikationsentwickler Sicherheitsaspekte wie Logik, Fein-Autorisierung oder Datenverarbeitung in die Entwicklung einfließen. Im späteren Einsatz ist die Lösung allerdings immer Bestandteil einer komplexeren IT-Landschaft. Auf diese hat der Entwickler keinen Einfluss mehr. Der Applikation angeschlossene Komponenten wie Betriebssystem, Bibliotheken, Middleware

Web Server oder Datenbank stellen jeweils eigene Sicherheitsrisiken dar.

Erschwerend hinzu kommt, dass Entwickler nur die Risiken berücksichtigen können, die zum Zeitpunkt der Applikations-Entwicklung bekannt sind. Beim Projektstart können also Attacken auf die Web-Applikation treffen, die zum Entwicklungszeitpunkt unbekannt waren. Um schnell auf unvermittelte Bedrohungen reagieren zu können, sollten daher vorinstallierte Sicherheitsmassnahmen der Web-Applikationen mit einer vorgelagerten WAF kombiniert werden.

«Wir verschlüsseln den gesamten Datenverkehr mit SSL (HTTP/S) und das reicht.»

Das SSL-Netzwerkprotokoll gewährleistet den sicheren Datenverkehr zwischen dem Anwender beziehungsweise Web-Browser und dem Server, nicht aber die Absicherung des Servers selbst. Hacker nutzen das Protokoll, damit ihre Angriffe über diesen Weg auch «sicher» und verschlüsselt bis zum Firmen-Web-Server gelangen. Um diese Attacken früh genug zu erkennen, müssen SSL-verschlüsselte Verbindungen spätestens an den Unternehmensgrenzen enden – leistungsfähige WAFs verschaffen an diesem Punkt die nötige Kontrolle. Als Wächterinstanz zwischen Anwender und Applikation stoppt die WAF zunächst den einströmenden Datenverkehr, um ihn danach mehrstufig gefiltert weiterzuleiten. Über diesen Zwischenschritt erreichen nur autorisierte und mehrfach geprüfte Benutzeranfragen den Web-Server. Nach einmal erfolgter Autorisierung kann die WAF die Daten wieder SSL-verschlüsselt weiterschicken, sollte der Backend-Server SSL-Anfragen erwarten. Übernimmt eine WAF diese Sicherheitsfunktionen, wird der Server entlastet und die Performance der Anwendungen auf dem Server erhöht.

«Unsere Systeme sind immer aktuell gepatcht und wir lassen regelmässig einen automatischen Scanner laufen, da ist alles auf Grün.»

Automatische Scanner geben einen grundlegenden Überblick über Schwachstellen in einer Unternehmens-IT – die meisten der heutigen Angriffe auf Web-Applikationen erkennen sie jedoch nicht. Ein guter Hacker untersucht die Applikation gezielt und sucht basierend darauf einen Angriffspunkt. Er wendet nicht einfach bekannte Angriffsmuster an. Aber genau diese prüfen die automatischen Scanner, die sinnvolle Basisinformationen bieten, aber kein umfassendes Security Assessment. Ein automatischer Scanner sollte daher ein Element eines guten Penetrations-Tests sein, aber nicht mehr. Trotz unauffälligem Scan-Ergebnis können Hacker also unbemerkt in die Web-Applikation eingedrungen sein. Um gezielten Datendiebstahl aufzudecken, empfiehlt es sich daher, einen professionellen Penetration-Test einzusetzen. Er misst den Sicherheitslevel der Applikationsumgebung, sollte aber immer auch die Prüfung manueller Angriffe umfassen. Diese Prüfung basiert auf Reverse Engineering und sollte ein bis zwei Mal pro Jahr durchgeführt werden. Automatische Security-Scanner und Penetration-Tests prüfen den aktuellen Zustand einer Systemarchitektur, sind also immer nur eine Momentaufnahme. Sie bieten keinen proaktiven Schutz der Systeme. Mit einer WAF kann ein Unternehmen im Sinne von «virtuellem Patching» unmittelbar auf ein erkanntes Leck reagieren und unerlaubte Server-Anfragen verhindern. Das gibt der Firma die Zeit, im Hintergrund geordnet eine Aktualisierung zu implementieren.

«Unsere Web-Applikationen sind sicher, bei uns ist noch nie etwas passiert.»

Diese Annahme ist riskant, weil sich der Anwender und die Unternehmen oftmals in falscher Sicherheit wähnen: Denn laut Gartner sind drei von vier Web-Applikationen angreifbar, des weiteren richten sich heutzutage bereits drei Viertel aller Angriffe auf Web-Applikationen.

Dabei hinterlassen Hackerzugriffe auf Web-Anwendungen oft keine Spuren und werden deshalb nicht entdeckt, weil die Daten nicht verschwinden oder verändert werden. Alle Anwendungen funktionieren normal weiter, und es werden auch keine Systemzugriffe verzeichnet. Die heutige Wahrnehmung scheint immer noch geprägt zu sein von den Viren und Trojanern aus früheren Jahren, als ein Angriff stets auffällige Folgen hatte. Das Ziel jetziger Attacken besteht darin, möglichst unbemerkt Daten zu stehlen. Für solche zielgerichteten Angriffe existieren keine vorher bekannten Signaturen.

«Bei uns gab es Angriffe, aber es sind keine Daten gestohlen worden.»

Solche Aussagen tauchen dann auf, wenn eine Schwachstelle publik wird. Das Problem ist, dass elektronischer Datendiebstahl meist nicht von normalen Zugriffen zu unterscheiden ist. Somit kann man nicht wissen, ob schon lange jemand Daten elektronisch kopiert hat. Anders als bei Viren oder Trojanern werden die Systeme auch bei gezielten Angriffen nicht beeinträchtigt und laufen wie gewohnt weiter. Am wirksamsten ist daher der proaktive Schutz der Systeme mit Security-Lösungen mit mehreren Sicherheitsstufen. Der wichtigste Filter ist die Authentisierungsabfrage an den Benutzer, die den Anwendungen vorgelagert ist. So erhalten nur Befugte Zugang und dürfen überhaupt mit dem Applikationsserver interagieren. An zweiter Stelle kommt die dynamische Filterung, welche nur gültige Server-Anfragen zulässt, ohne sich auf Signaturen zu stützen. Zudem lassen sich über ein Reporting die Zugriffe und abgefragten Daten der angemeldeten ID-Nummern genau zurückverfolgen. Voraussetzung ist hierbei, dass vor den Web-Applikations-Servern ein Reverse Proxy Server installiert ist, der Netzwerkverbindungen und -protokolle wie SSL abfängt.

«Wir nutzen bereits einen Reverse Proxy Server und setzen die besten und teuersten Firewalls ein, sogar zwei verschiedene hintereinander.»

Netzwerk-Firewalls prüfen möglichst in Echtzeit den Datenverkehr zum Web-Server beziehungsweise die Signaturen und Protokolle der Anfragen an den Server. Die Firewall erkennt einfache Angriffe mittels vordefinierter Signaturen. Um die meist getarnten Hackerangriffe zu identifizieren, muss aber eine Firewall wenigstens auch auf den verschlüsselten Datenverkehr zugreifen können. Ein wirksamer Schutz von Web-Applikationen, der über die reine Filterung von URL-Signaturen hinausgeht, muss sich insbesondere auch mit applikatorischen Themen wie zum Beispiel der vorgelagerten Authentisierung, der Cookie Protection, dem Schutz von URL-Adressen und HTML-Formularen auseinandersetzen. Auch muss der Zugangsweg über manipulierte URLs gesperrt werden. Nur Web-Application-Security-Lösungen, die mehrstufig – sowohl statisch und dynamisch – alle Abfragen und Daten beim Zugriff auf die Web-Anwendungen filtern, bieten auch vor noch unbekanntem Angriffen proaktiven Schutz.

Redakteur:

Die Beiträge auf dieser Website sind urheberrechtlich geschützt. Bei Fragen zu den Nutzungsrechten wenden Sie sich bitte an manuela.maurer@vogel.de oder Tel.: 0931-418-2888.

Dieses PDF wurde Ihnen bereitgestellt von <http://www.swissitmagazine.ch>