Applikationssicherheit: Protect7

13.09.2012, 14:37 | IT, New Media & Software

Pressemitteilung von: *Freier IT-Journalist*
Presseagentur: *Wolfgang Adis - Freier IT-Journalist*

Die Situation

In jeder Organisation gibt es sicherheitskritische Applikationen, die businessrelevante Daten verarbeiten. Dies können externe oder interne (Web-)Applikationen sein. Sie werden häufig als Individualsoftware erstellt oder auch als Standardsoftware eingekauft.
Lösungen, um die Risiken dieser Applikationen zu minimieren oder auszuschalten, gibt es schon länger, nur werden diese kaum angewendet. Heute wird das Security Budget meist in andere Bereiche als die Applikationssicherheit investiert, obwohl die häufigsten „erfolgreichen" Angriffe auf Applikationsebene erfolgen.
Die Gründe dafür liegen bei einer ungenügenden Sicherheitsbetrachtung während der Entwicklung. Bei der Softwareentwicklung werden Sicherheitsaspekte kaum oder in ungenügenden Maße berücksichtigt. Daher bestehen Sicherheitsrisiken wie Datendiebstahl und Server-Kompromittierenung bei einer Großzahl von Unternehmen. Dies zeigt sich auch häufig bei durchgeführten Application Penetration Tests. Hier werden sehr oft gravierende Schwachstellen gefunden.
Bei der Problematik steht eine Organisation einer veränderten „Angriffskultur" gegenüber. Während noch vor Jahren Angriffe ausschließlich über Netzwerke, Viren und Trojaner stattfanden und daher leicht entdeckt und über entsprechende Systeme abgewehrt werden konnten, nutzen Hacker heute zum Datendiebstahl Schwachstellen in (Web-)Applikationen aus. Ein Angriff wird somit häufig nicht einmal entdeckt. Web-Applikationen sind eine gefährliche Schnittstelle zu Daten und Transaktionen. Dabei erhält der Angreifer Zugang nicht nur zu den die Applikation betreffenden Informationen, sondern zu allen an sie angeschlossenen Systemen, Schnittstellen und deren Daten. So können über eine Web-Applikation schlimmstenfalls die gesamten Unternehmensdaten gestohlen werden. Durch das Web 2.0 und die damit einhergehenden hochdynamischen Web-Applikationen erhalten organisierte Cybercrime-Gruppen Zugang zu vertraulichen Informationen.

Der wirksamste Schutz vor solchen Applikationsrisiken ist die genügend sichere Entwicklung. Dabei dreht es sich oft um folgende Themen, um nur die wichtigsten aufzuzählen:
- Sicheres Session-Management
- Sauberes Error-Handling
- Validierung aller vom Client übermittelten Daten
- Escaping aller ausgegebenen Daten

Werden diese Aspekte bereits beim Design der Applikation berücksichtig und anschließend bei der Entwicklung entsprechend umgesetzt, so ist man schon einen großen Schritt weiter.
Möchte man diese Themen nachhaltig und institutionalisiert anwenden, so etabliert man einen entsprechenden Secure Development Lifecycle (SDL).
Möchte man jedoch noch einen zusätzlichen Schutz für die kritischen Web-Applikationen oder hat man eingekaufte Standardsoftware im Einsatz, wo eine Behebung nicht möglich ist, bietet sich der Einsatz einer sogenannten Web Application Firewall (WAF) an, die zwischen Anwender und Web-Applikation eingesetzt wird.

Heute existiert häufig die Meinung, dass eine Netzwerkfirewall, das patchen von Systemen oder der Einsatz von Verschlüsselung (SSL) die Sicherheit der Applikation und der Daten gewährleistet. Dies ist jedoch ein gefährlicher Trugschluss, dem sich kein Unternehmen aussetzen sollte. Hacker können trotzdem ins System eindringen.

Protect7: Dienstleistungen zur Applikationssicherheit

Die Firma Protect7 (http://www.protect7.com) bietet Applikationssicherheits-Dienstleistungen für alle Bereiche und

Phasen des Software-Lifecycles an. Dies beginnt bei der Spezifikation von Sicherheitsanforderungen, dem Erstellen von Sicherheitskonzepten in Software-Lösungen über die Unterstützung bei der Softwareentwicklung bis hin zur Durchführung von Software-Audits und Penetration Tests. Darüber hinaus gibt es Schulungen für Software-Entwickler.

Security Audit

Der erste Schritt der Analyse des Sicherheitslevels einer Organisation ist ein Security Audit. In ihm werden die Organisation, Sicherheitsvorgaben und die Infrastruktur berücksichtigt.
Das Resultat des Security Audits ist ein umfassender Bericht über die Stärken und Schwächen der Vorgaben und deren Umsetzung sowie ein Maßnahmenkatalog zur Behebung der gefundenen Schwächen.

Penetration Testing

Angriffe auf die Applikationen oder Datenbestände werden über Schwachstellen in Applikationen, Systemen und Netzwerken ausgeführt. Um diese Schwachstellen ausfindig zu machen, verwendet Protect7 Penetrationstests, die entweder manuell oder halbautomatisiert durchgeführt werden. Damit wird ein Vorgehen wie das eines Hackers simuliert.

Code Analyse

Sichere Applikationen basieren auf sicherem Code. Dies ist beim Software-Design und der Implementierung zu berücksichtigen, denn spätere Änderungen am Code sind sehr aufwändig oder gar schlicht unmöglich. Protect7 bietet hier einen Code-Review an, mittels dessen Schwachstellen direkt im Code eruiert und behoben werden können.
Im Zusammenhang mit der Dienstleistung „Software Engineering“ bietet Protect7 die optimale Möglichkeit, den Code sicher zu gestalten.

Software Engineering

Protect7 bietet die komplette Umsetzung oder teilweise Unterstützung bei der sicheren Softwareentwicklung. Dies betrifft das Requirements Engineering, die Architektur und das Design und die Implementierung, aber auch die Bereiche Prototyping und Testing.
Ebenso gehört die Definition und gezielte Umsetzung eines Secure Software Development Lifecycle zu den Dienstleistungen der Firma.

Lösungen

Web Application Firewall (WAF)

Eine von Protect7 eingesetzte Lösung ist die Web Application Firewall (WAF). Sie schützt eine Applikation vor den gängigsten Angriffsszenarien auf Applikationsebene. Dies beinhaltet den Schutz des Web-Auftritts, Online-Bankings oder E-Commerce gegenüber dem Internet.
Protect7 leistet als herstellerneutraler Anbieter Unterstützung bei der Auswahl der geeignetsten Lösung und bietet im Einzelnen die Evaluation der optimalen Lösung für die gegebene Problemstellung, Unterstützung bei der Integration, der Mitarbeiterschulung zum Thema WAF sowie beim Betrieb der Lösung.

XML Security Gateways

Mit den XML Security Gateways bietet Protect7 Schutz für Webservices, die denselben Schutz wie Web-Applikationen benötigen. Die Lösung prüft Serviceanfragen auf korrekte Authentisierung und Autorisierung und lässt nur erlaubte Requests passieren. Zusammen mit einer WAF werden von der Firma dieselben Leistungen wie oben beschrieben angeboten.

Access & Identity Management

Diese Leistung gewährleistet den sicheren Zutritt zu Applikationen und System und den sicheren Zugriff auf Daten. Protect7 nimmt hier die Integration und Konfiguration sowie die Entwicklung von kundenspezifischen Erweiterungen vor.

Automatisiertes Schwachstellen-Scanning

Ein Schwachstellen-Scanning ist bei Web-Applikationen sowie Webservices sinnvoll. Lösungen, dies automatisiert vorzunehmen, können mit Hilfe von Protect7 ausgewählt werden. Protect7 bietet einen speziellen Web-Application Scan-Dienst an: ajbal (www.ajbal.net). Er scannt web-basiert Anwendungen auf Schwachstellen und liefert einen Report mit Behebungsempfehlungen.

Wolfgang Adis

Quelle:
Protect7 GmbH
Franklinstrasse 7
CH-8050 Zürich / Schweiz
Tel +41-44-515-6868
www.protect7.com

Portrait

Wolfgang Adis ist freier IT-Journalist mit den Schwerpunkten Software, Netzwerktechnik und Netzwerksicherheit.

News-ID: 663118 • Views: 1045 (Stand: 01.06.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/663118/Applikationssicherheit-Protect7.html