Web Application Security

Best Practices für sichere Webanwendungen mit dem neuen BSI-Handbuch

Das Web ist zu einem wesentlichen Teil der wirtschaftlichen Infrastruktur geworden und es rückt immer stärker in den Fokus von Angreifern. Doch nach wie vor ist die Sicherheit vieler Webanwendungen auf einem sehr niedrigen Niveau. So ist es für viele Unternehmen höchste Zeit, die Web Application Security zum Thema zu machen. Um E-Business-treibende Unternehmen bei der Herstellung von Sicherheit auf der Anwendungsebene zu unterstützen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Maßnahmenkatalog mit Best Practices herausgegeben.

Das 105-seitige Dokument, das auf der BSI-Homepage zum Download bereitsteht [1], wendet sich in erster Linie an Projektleiter und Softwareentwickler. Es stellt Schutzmaßnahmen und Best Practices zur Vorbeugung gegen typische Schwachstellen in Webanwendungen bereit. Ein vorangestellter Leitfaden gibt Hinweise für ein systematisches Vorgehen. Dabei werden sowohl bereits bestehende, als auch neu zu entwickelnde Anwendungen betrachtet.

Was ist anders im Web?

Vielen Sicherheitsverantwortlichen scheint nicht bewusst zu sein, dass Anwendungsicherheit nicht über eine gut konfigurierte Netzwerkfirewall oder gehärtete Server hergestellt werden kann. Sie ist ein eigener Aufgabenbereich, mit eigenen Lösungsansätzen, Herangehensweisen und Verantwortlichkeiten. Schon die Bedrohungslage ist eine andere als auf der Netzwerkebene: Angriffe im Web erfordern oftmals nur geringe Vorkenntnisse. Und reicht der Browser als Angriffswerkzeug nicht aus, so steht im Internet eine Reihe leicht zu bedienender Tools zur Verfügung. Die Hemmschwelle wird zusätzlich dadurch gesenkt, dass man mit einfachen Mitteln absolute Anonymität herstellen kann, eine Entdeckung also nicht zu fürchten braucht. Insbesondere bei kleineren Unternehmen ist das Web in vielen Fällen direkter Umsatzträger und hat dann einen großen Einfluss auf den Geschäftserfolg; eine nicht entdeckte Schwachstelle kann schnell zur Existenzbedrohung werden. Hinzu kommt, dass das Web auch von Anwendern genutzt wird, die nicht die erforderlichen Kenntnisse besitzen, um sich angemessen zu schützen.

Bei alledem ist nun festzustellen, dass die klassische Firewall nicht in der Lage ist zu erkennen, ob Eingaben des Benutzers legitim sind oder potentiell gefährlich. So lässt sie in der Regel einfach alles durch, was über die Ports 80 oder 443 hereinkommt. Die Verantwortung für die Sicherheit liegt damit weitestgehend bei der Anwendung selbst, also letztendlich bei jedem einzelnen Entwickler. Was bedeutet, dass die Anwendung nicht nur den eigenen Server und die eigenen Daten vor Schaden bewahren muss, sondern auch für die Sicherheit des Anwenders Verantwortung zu tragen hat.

Vorgehen bei alten und neuen Webanwendungen

Das BSI-Handbuch gibt in einem Leitfaden im ersten Kapitel Hinweise für ein systematisches Vorgehen zur Erstellung sicherer Webanwendungen. Dabei wird unterschieden zwischen alten und neuen Anwendungen. Allgemein gilt die Faustformel: je älter eine Webanwendung ist, desto anfälliger ist sie in der Regel auch. Als erste Maßnahme für mehr Sicherheit sind alte Webanwendungen einer Sicherheitsanalyse zu unterziehen und die kritischen Schwachstellen zu beseitigen. Ist eine Behebung zu teuer, so kann in manchen Fällen eine Application Firewall das Problem lösen. Sie wird so konfiguriert, dass sie die Angriffsmuster für die betreffende Schwachstelle herausfiltert.

Neue Webanwendungen benötigen ein ganzes Bündel an Maßnahmen. Auch hier liefert eine Faustformel ein Handlungsmuster: Je früher im Entwicklungszyklus einer Software angesetzt wird, desto nachhaltiger ist die Wirkung und desto leichter lassen sich entdeckte Probleme beheben. Bild 1 zeigt die wichtigsten Ansatzpunkte für ein systematisches Vorgehen zur Herstellung von Web Application Security. Ganz oben auf der Liste stehen diese Maßnahmen: Richtlinien für sicheres Programmieren, sogenannte Secure Coding Guidelines, sind zu entwickeln und verbindlich vorzuschreiben; als Grundlage bietet sich das BSI-Handbuch an. Werkverträge mit den Lieferanten von Individualsoftware sind so zu gestalten, dass sie Sicherheit einfordern und zum Gegenstand der Gewährleistung machen. Eine Application Firewall ist als Maßnahme zur Errichtung einer zweiten Sicherungslinie in Erwägung zu ziehen. Wer nicht gleich Geld für eine kommerzielle Lösung ausgeben will, der findet im Apache-Modul mod_security [2] eine leistungsfähige und in der Anschaffung kostenfreie Möglichkeit. Schließlich sind auch alle neuen Anwendungen vor der Lifeschaltung einer ausgiebigen Sicherheitsanalyse zu unterziehen. Große Unternehmen, die ihre eigenen Softwareabteilungen haben, werden möglicherweise ein eigenes Kompetenzteam dafür aufstellen. In der Regel ist dies jedoch eine typische Aufgabe, welche externe, auf die Web Application Security spezialisierte Dienstleister kostengünstiger und besser ausführen können.

Web Application Security auf 5 Ebenen

Dem BSI-Guide zugrunde liegt ein Modell, das die Web Application Security in 5 Ebenen strukturiert: Die Systemebene (Ebene 1) befasst sich mit der Sicherheit der zur Realiserung der Webanwendung benötigten Systemsoftware, die Technologieebene (2) behandelt Fragen wie die Wahl des richtigen Authentisierungsverfahrens und der Softwarearchitektur, Ebene 3, die Implementierungsebene, ist der Bereich der Codierung und damit so namhafter Schwachstellen wie Cross-Site Scripting und SQL-Injection. Auf der Logikebene (4) geht es um die Art, wie die Fachprozesse in der Anwendung abgebildet sind, und auf der

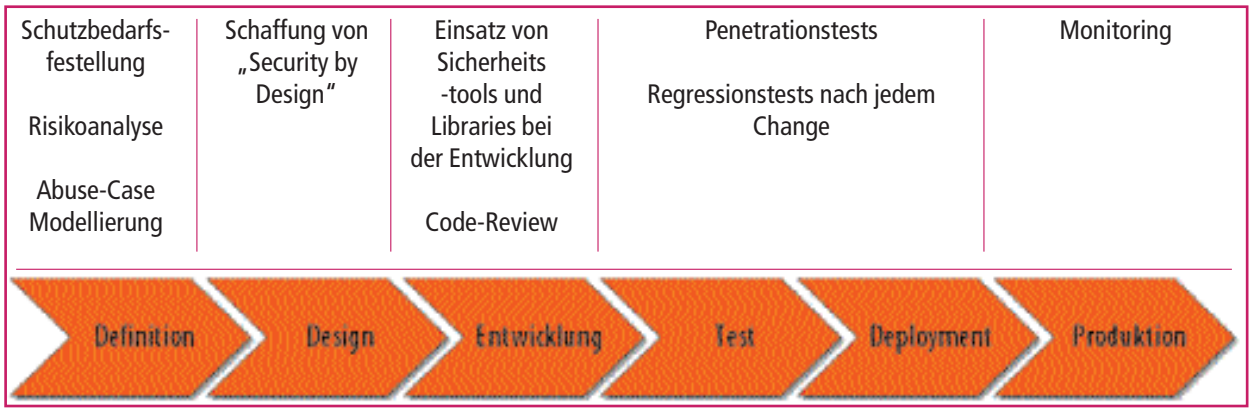
semantischen Ebene (5) schließlich um den Schutz vor Täuschung und Betrug. Zwei Beispiele für Best Practices bei der Entwicklung von Webanwendungen: Auf der Implementierungsebene spielt sich eine einfache Maßnahme ab, mit der sich Session-Fixation, eine weit verbreitete Schwachstelle, die das Eindringen in fremde Benutzerkonten ermöglicht, wirksam unterbinden lässt. Sie besagt, dass die bereits bestehende SessionID eines Benutzers direkt nach dem Login durch eine neue zu ersetzen ist. Auf der logischen Ebene empfiehlt eine Maßnahme, fehlerhafte Einlogversuche nicht mit Sperren des Benutzerkontos zu beantworten, all zu leicht hat es sonst ein Dritter, einen oder gleich massenweise Benutzer auszusperren. Vielmehr sollte das Passwortcracking durch Einsatz eines sog. Captchas unterbunden werden. Dieses lässt sich von einer Maschine nicht knacken und macht auf diese Weise die Interaktion mit einem menschlichen Nutzer erforderlich.

Abschließend sei auf zwei Open Source-Projekte hingewiesen, die sich die Sicherheit von Webanwendungen auf die Fahnen geschrieben haben und eine Vielzahl von Hilfestellungen, Anleitungen und Tools bereitstellen: Das Open Web Application Security Project (OWASP), www.owasp.org und das Web Application Security Consortium (WASC), www.webappsec.org.

Thomas Schreiber ist Geschäftsführer der SecureNet GmbH in München und einer der Autoren des BSI-Handbuchs.

Quellen

[1] www.bsi.de/literat/studien/websec/WebSec.pdf
[2] www.modsecurity.org



Compliance

Tools zur Unterstützung **der Compliance**

Um feststellen zu können, ob ein Unternehmen konform zu bestehenden Regelungen arbeitet, ist es erforderlich, einige Aspekte zur IT-Sicherheit dokumentieren zu können. Hierfür existieren bereits einige Tools, die unterschiedliche Gesichtspunkte abdecken. Die gebräuchlichsten Tools werden kurz vorgestellt.

Anforderungen an Compliance-Tools

Neben etwaigen gesetzlichen Vorgaben definiert sich eine Behörde oder ein Unternehmen oft selbst gesteckte Sicherheitsanforderungen oder vereinbart solche mit Vertragspartnern, was sich i.d.R. in Policies und Richtlinien bzw. SLAs widerspiegelt. Anforderungen der Compliance wirken sich direkt auf das Berichtswesen aus, weshalb ein Tool zur Unterstützung der Compliance vor allem bei den Dokumentationsfunktionen hilfreich sein muss.

Auf dem Markt gibt es hierzu sehr viele, verschiedene Tools, die jeweils spezifische Anforderungen (z.B. Durchführung einer datenschutzrechtlichen Vorabkontrolle, Visualisierung berechneter IT-Risiken oder schematische Darstellung von Angriffsszenarien) erfüllen. Angesicht vielfältiger Fragestellungen decken Tools stets nur verschiedene Abstraktionsebenen ab. In diesem Aufsatz werden exemplarisch drei Tools kurz vorgestellt.

Dokumentation via Audits

In der Praxis wird das aktuelle Sicherheitsniveau einer Behörde oder eines Unternehmens im Wesentlichen auf der Grundlage von Audits beschrieben. Diese dokumentieren allerdings lediglich eine Momentaufnahme: Anhand vordefinierter Vorgaben (z.B. hinsichtlich zu erreichender Sicherheitsziele) wird jeweils der zum Zeitpunkt des Audits festgestellte Ist-Stand dem Soll-Stand gegenüber gestellt. Da ein Audit i.d.R. zeitaufwändig ist, ist eine unterstützende Software hilfreich. Hier steckt meist ein erheblicher Zeitaufwand in der Modellierung des Untersuchungsgegenstandes im verwendeten Tool.

Gerade für kleinere und mittelständische Unternehmen hat sich in Deutschland eine Orientierung an den IT-Grundschutz-Katalogen des BSI bewährt. Sobald die Abbildung des vorhandenen IT-Verbundes im betreffenden Tool erfolgt ist, können die Ergebnisse des Audits eingegeben und damit letztlich die Einhaltung von Vorgaben dokumentiert werden. Dabei werden sowohl technische, als auch organisatorische bzw. bauliche