BSI Forum
Organ des Bundesamtes
für Sicherheit in der Informationstechnik

Inhalt

Web Application Security

Sicher auf allen Ebenen

Ein Klassifizierungsschema zur Organisation von Sicherheit in Webanwendungen

Die Sicherheit einer Webanwendung sollte vor der Inbetriebnahme ebenso einer Prüfung unterzogen werden, wie dies für Laststabilität und funktionale Korrektheit bereits vielfach der Fall ist. Als geeignet für den Konzeptions- und Prüfprozess erweist sich eine dezentrale Organisationsstruktur, welche die Fachstellen in die Verantwortung mit einbezieht. Das vorgestellte Klassifizierungsschema hilft, die unterschiedlichen Aspekte der Websicherheit den Zuständigkeitsbereichen im Unternehmen zuzuordnen.

Von Thomas Schreiber, SecureNet GmbH, und Thomas Veit, BSI

Browser und Web sind heute allgegenwärtig. Nicht nur im Consumer-Bereich ist das Web unverzichtbares Medium für eine Vielzahl von Anwendungszwecken geworden. Auch Geschäftsprozesse zwischen Geschäftspartnern (B2B) sowie zwischen Bürger und Behörde (E-Government) werden immer stärker im Web abgewickelt. Die Spannweite reicht von einfachen Anwendungen wie der Prospektbestellung, über Auktionen und Shopping-Plattformen, bis hin zu sensitiven und schützenswerten Anwendungen wie der Abwicklung von Transaktionen, der Durchführung von Ausschreibungen oder dem Zugang ins unternehmenseigene Intranet.

Wird eine Webanwendung in den Produktivbetrieb übernommen, so hat sie in der Regel ausgiebige Last- und Funktionstests durchlaufen. Prozesse für derartige qualitätssichernde Maßnahmen sind in E-Business-Unternehmen heutzutage meist gut organisiert und fest verankert. Dem IT-Betrieb zugeordnete Instanzen führen diese Tests standardmäßig aus und sorgen für ein definiertes Qualitätsniveau. Anders ist die Situation, wenn es um die *Sicherheitsaspekte* der Webanwendung geht. Diese werden häufig alleine in der Verantwortung der beauftragenden Fachstelle belassen. Das Bestehen einer letzten Kontrollinstanz, welche zum Beispiel durch Penetrati-

Impressum

Redaktion:
Michael Dickopf (verantwortlich)
Pressesprecher
E-Mail: Michael.Dickopf@bsi.bund.de

Anja Hartmann
Referatsleiterin Öffentlichkeitsarbeit
E-Mail: Anja.Hartmann@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Postfach 20 03 63
53133 Bonn

Hausanschrift:
Godesberger Allee 185–189
53175 Bonn

Telefon: +49 1888 9582-0
Telefax: +49 1888 9582-455

Web: www.bsi.bund.de
www.bsi-fuer-buerger.de

Das BSI-Forum, Organ des Bundesamtes für Sicherheit in der Informationstechnik in Bonn, ist Bestandteil der <kes> – Die Zeitschrift für Informations-Sicherheit
13. Jahrgang 2005

onstests sicherstellt, dass die Anwendung nach aktuellem Kenntnisstand frei von typischen Schwachstellen ist, ist vielfach nicht vorgesehen. Dabei kann eine unsichere Webanwendung nicht nur selbst zum Missbrauchsziel werden, sondern die Sicherheit weiterer Anwendungen oder gar des Netzwerkes kompromittieren.

Setzt man sich mit der Planung eines organisatorischen Prozesses zur Sicherheit von Webanwendungen auseinander, so stellt sich recht schnell die Frage, wo Netzwerksicherheit aufhört, wo die Sicherheit in Webanwendungen beginnt, und wie weit diese reicht. Zur Beantwortung dieser Fragen hat sich ein Klassifizierungsschema bewährt, das wir im Folgenden vorstellen. Dieses setzt auf der Ebene von System und Netzwerk auf und reicht bis zu inhaltsbezogenen Fragen. Mithilfe dieser Klassifizierung lassen sich dann Zuständigkeiten den einzelnen Ebenen zuordnen und Anforderungen an Fähigkeiten und Kenntnisse für die jeweiligen Aspekte formulieren. Insgesamt ergibt sich ein Schema, welches als Modell für die Herstellung sicherer Webanwendungen im Unternehmen Verwendung finden kann.

Das Ebenenmodell

Die Sicherheit von Webanwendungen lässt sich in sechs Ebenen gliedern (vgl. Tab. 1).

Ebene 0 – Netzwerk und Host

Die Ebene von Netzwerk und Host (mit Host bezeichnen wir Serverhardware und das darauf laufende Betriebssystem) ist nicht der Sicherheit der Webanwendung zugeordnet; sie schließt sich ihr vielmehr nach unten an. Ein sicheres Netzwerk und ein sicherer Host sind gleichwohl eine wichtige Voraussetzung für eine sichere Webanwendung. Trotzdem ist diese Ebene von Ebene 1 zu trennen: Die Fähigkeiten, die benötigt werden, um Netzwerk und Host abzusichern, sind anderer Natur als diejenigen für die Sicherheitsaspekte von Webanwendungen. Letztere erfordern die Erfahrungen von Softwareentwicklern. Nicht ausreichend sind Betriebssystem- und Netzwerkkenntnisse.

Auch die organisatorische Einbindung unterscheidet sich voneinander: Die Zuständigkeit für die Netzwerksicherheit ist im Unternehmen häufig an zentraler Stelle verankert. Die Zuständigkeit für die Sicherheit der Webanwendung ist jedoch wegen der Verzahnung der Software mit den von ihr abgebildeten Geschäftsprozessen dezentral zu organisieren. Der Bereich der Netzwerk- und Hostsicherheit ist heutzutage gut verstanden und in den Sicherheitsprozessen der Unternehmen in der Regel verankert.

Ebene 1 – Systemebene

Ebene 1 umfasst all jene Software, die eine Webanwendung benötigt, um überhaupt ablaufen zu können. Dazu gehören der Webserver und der Applikationsserver, aber auch die Datenbank und beteiligte Backend-Systeme. Alle diese Komponenten müssen bei der Betrachtung der Sicherheit einer Webanwendung mit einbezogen werden. Eine Webanwendung, die frei von Sicherheitsmängeln programmiert ist, muss trotzdem im Endeffekt als unsicher bewertet werden, wenn zum Beispiel die von ihr verwendete Datenbank über einen Seitenkanal manipulierbar ist.

Ebene 2 – Technologie

Dieser Bereich betrifft die Verwendung der für den jeweiligen Zweck und Schutzbedarf richtigen Technologie und technischen Verfahren – sowie ihren richtigen Einsatz. So setzt eine Webanwendung, die zum Beispiel sensitive Daten un-

Abbildung 1: Das Ebenenmodell

	Ebene	Inhalt (Beispiele)
6	**Vorschriften und Bestimmungen**	**Einhaltung gesetzlicher Regelungen und unternehmensspezifischer Vorgaben** - Fehlende Angaben zum Datenschutz - Nichteinhalten von Bestimmungen, z.B. des KontraG - Preisgabe vertraulicher Informationen
5	**Semantik**	**Schutz vor Täuschung und Betrug** - Informationen ermöglichen Social Engineering-Angriffe - Gebrauch von Popups u.ä. erleichtern Phishing-Angriffe - Keine Absicherung für den Fall der Fälschung der Website
4	**Logik**	**Absicherung von Prozessen und Workflows als Ganzes** - Verwendung unsicherer Email in einem ansonsten gesicherten Workflow - Angreifbarkeit des Passworts durch nachlässig gestaltete „Passwort vergessen"-Funktion - Die Verwendung sicherer Passworte wird nicht erzwungen
3	**Implementierung**	**Vermeiden von Programmierfehlern, die zu Schwachstellen führen** - Cross-Site Scripting - SQL-Injection - Session Riding - Information Disclosure
2	**Technologie**	**Richtige Wahl und sicherer Einsatz technischer Verfahren** - unverschlüsselte Übertragung sensitiver Daten - Authentisierungsverfahren, die nicht dem Schutzbedarf angemessen sind - Ungenügende Randomness von Token
1	**System**	**Absicherung der auf der Systemplattform eingesetzten Software** - Fehler in der Konfiguration des Webservers - „Known Vulnerabilities" in den eingesetzten Softwareprodukten - Mangelnder Zugriffsschutz in der Datenbank
0	**Netzwerk & Host**	Absicherung von Host und Netzwerk

verschlüsselt über das Internet transferiert, nicht die richtige Technologie ein. Eine Webanwendung, die Passwörter zwar verschlüsselt, dafür aber einen nicht ausreichend langen Schlüssel verwendet, setzt die richtige Technologie falsch ein. Das erste Anwendungsbeispiel ist gegen Ausspähen auf dem Übertragungswege nicht geschützt, das zweite nicht ausreichend gegen Passwort-Cracking. Beide Beispiele werden den typischen Sicherheitsanforderungen nicht gerecht, auch wenn sie im Programmcode keine Sicherheitslücken enthalten.

Ebene 3 – Implementierung

Die Implementierungsebene ist die offensichtliche Ebene der Sicherheit in Webanwendungen. Hiermit bezeichnen wir den Bereich, in dem unbeabsichtigte Programmierfehler (Bugs) auftreten und zu Sicherheitsproblemen führen, oder aber fehlerhafte Programmierung, wie nicht vorhandene oder ungenügende „Data Validation". Diese Ebene umfasst auch ungenügende Tests, sowie Tests mit einseitigem Fokus und die Vernachlässigung der Qualitätssicherung zugunsten des Inbetriebnahmetermins oder aus Kostengründen.

Logik und Semantik

Die Bedeutung der beiden folgenden Ebenen für die Sicherheit von Webanwendungen wird gegenwärtig häufig noch unzureichend wahrgenommen. Dabei sind sie von hoher Relevanz, wenn man die Sicherheit von Webanwendungen nicht allein als den Schutz des Servers versteht, sondern eine umfassende Perspektive zugrunde legt: Der Anbieter einer Webanwendung trägt nicht nur Verantwortung für eigene Systeme, sondern auch für alle an der Nutzung der Webanwendung Beteiligten. Auf den Ebenen der Logik und der Semantik kommt dieser Aspekt ganz besonders zum Tragen.

Ebene 4 – Logik

Diese Ebene betrifft sowohl die Logik der Abläufe innerhalb einer Anwendung (Anwendungs- und Business-Logik) als auch die Interaktion mit dem Benutzer. Ist diese zu „zweckorientiert" implementiert, liegt gegebenenfalls eine Missbrauchsmöglichkeit vor. Wird etwa, um eine vielfach wiederholte missbräuchliche Mehrfacheingabe eines Passwortes (Enumeration) zu verhindern, ein Benutzer nach dem fünften fehlerhaften Login-Versuch gesperrt, so kann dieser Benutzer auch gezielt ausgesperrt werden (Denial of Service). Diese missbräuchliche Vorgehensweise wird weiter erleichtert, wenn die Benutzerkennung einfach zu erraten ist – zum Beispiel wenn hierzu die E-Mail-Adresse verwendet wird.

Ebene 5 – Semantik

Die semantische Ebene der Sicherheit in Webanwendungen umfasst inhalts- und kommunikationsbezogene Aspekte. Sie stellt den Vertrauenskontext für die Interaktion mit dem Benutzer her. Wird in diesem Bereich nicht ein hohes Maß an Sorgfalt aufgewandt, so kann eine Webanwendung von Dritten missbraucht werden, um den Benutzer zu täuschen. Dieser Bereich kann selten auf eine einzelne Anwendung beschränkt bleiben. Er ist in der Regel vielmehr website- oder unternehmensübergreifend zu betrachten. Missbrauchsmöglichkeiten, die sich Fehler auf der semantischen Ebene zunutze machen, sind Social Engineering, Phishing, Identitätsdiebstahl, Täuschung und andere.

Ebene 6 – Vorschriften und Bestimmungen

In diesen Bereich fallen Regelungen der eigenen Organisation, sowie Regelungen Dritter, gegebenenfalls auch gesetzliche Anforderungen. Auch wenn es sich hier nicht mehr um IT-Sicherheit im eigentlichen Sinne handelt, kann durch eine ungenügende Beachtung der diesbezüglichen Bestimmungen Schaden entstehen. Darunter fallen etwa Haftungs- und Datenschutzfragen oder auch Aspekte des Teledienstegesetzes, zum Beispiel ein Impressum mit bestimmten Pflichtangaben (Anbieterkennung) auf einer Website vorzuhalten.

Die Abfolge der Ebenen von unten nach oben spiegelt eine Einschätzung der wahrgenommenen Bedeutung wider, mit der Sicherheit in Webanwendungen gegenwärtig realisiert wird. Die größte Aufmerksamkeit kommt häufig der Systemebene zu. Die wahrgenommene Bedeutung schwächt sich dann nach „oben" hin deutlich ab, bis hin zur semantischen Ebene, die vielfach

	Ebene	Verantwortliche Organisationseinheit	Funktion	Fachkenntnisse	Toolunterstützung
6	**Vorschriften und Bestimmungen**	Zentrale	Plan	Juristischer Background	■. . . . .
5	**Semantik**			Corporate Identity und Unternehmens-kommunikation	. . . . .
4	**Logik**	Fachstelle (Anforderer)		Kenntnisse der Geschäftsprozesse	■. . . . .
3	**Implementierung**	Entwickler (Umsetzer)	Build	Softwareentwicklungs-skills	■■■■. . . . .
2	**Technologie**	Fachstelle, Entwickler, Betrieb		Allg. IT-Security	■■. . . . .
1	**System**	Betrieb	Run	Netzwerk- und Systemadministration	■■■■■■■■. .
0	**Netzwerk & Host**				

Abbildung 2: Organisation von Sicherheit in Webanwendungen

noch nicht als Bestandteil der Sicherheit in Webanwendungen erkannt worden ist. Die Ebene der Vorschriften und Bestimmungen wird bisher in der Regel nicht als Thema der IT-Sicherheit angesehen und beispielsweise im Rahmen einer redaktionellen Bearbeitung mit abgehandelt.

Abgrenzung

Die Sicherheit in Webanwendungen befindet sich in teilweise enger Abhängigkeit und Wechselwirkung zu anderen Bereichen der IT-Sicherheit. Eine klare Abgrenzung ist jedoch wichtig, wenngleich nicht immer einfach, um die richtigen Maßnahmen an den richtigen Stellen ergreifen zu können. Mit dem Klassifizierungsschema lassen sich nun für die Sicherheit von Webanwendungen innerhalb einer Organisation Zuständigkeiten zuordnen und Verantwortlichkeiten definieren.

Als Ausgangspunkt hierfür kann das in Tabelle 2 dargestellte Gerüst herangezogen werden. Vorschriften und Bestimmungen (Ebene 6) werden unter anderem von der Unternehmensführung organisationsweit festgelegt. Die semantische Ebene (Ebene 5) ist in Zusammenarbeit der Unternehmensführung mit den Fachstellen zu behandeln. Die Ebene der Anwendungslogik (Ebene 4) ist Sache der anfordernden Fachstelle. Diese verlässt sich darauf, dass die Entwicklungseinheit die Anwendung sicher implementiert hat (Ebene 3) und dass der Betrieb die Anwendung sicher „hostet" (Ebene 1). Auf der Technologieebene (Ebene 2) ist zu unterscheiden zwischen der Verantwortung der Fachstelle, der Entwickler und des Betriebes.

Im Rahmen einer Plan/Build/Run-Organisation ergibt sich darüber hinaus grob die in der Spalte „Funktion" dargestellte Zuordnung zu den drei Funktionen. Die Spalte „Fachkenntnisse" zeigt für die einzelnen Bereiche, welche Kenntnisse jeweils erforderlich sind, um eine Webanwendung auf ihre Sicherheit hin zu überprüfen. In der letzten Spalte ist größenordnungsmäßig dargestellt, in welchem Umfang dabei auf Toolunterstützung gesetzt werden kann.

Neben dem hier geschilderten Anwendungszweck hat sich das Schema zudem als hilfreich für die Darstellung von Schwachstellen in Webanwendungen erwiesen – zum Beispiel im Rahmen von Schulungen. ■

Literatur

[1] Web Application Security Consortium (WASC), Web Security Threat Classification, www.webappsec.org/tc/WASC-TC-v1_0.pdf

[2] Open Web Application Security Consortium (OWASP), Web Application Penetration Checklist, http://prdownloads.sourceforge.net/owasp/OWASPWebAppPenTestList1.1.pdf

[3] Organization for the Advancement of Structured Information Standards (OASIS), Application Vulnerability Description Language (AVDL) Technical Committee, www.oasis-open.org/committees/tc_home.php?wg_abbrev=avdl

[4] OASIS Web Application Security (WAS) Technical Committee, www.oasis-open.org/committees/tc_home.php?wg_abbrev=was

[5] Thomas Schreiber, Die semantische Ebene der Sicherheit von Webanwendungen, Securenet GmbH, 2003, www.securenet.de/papers/WebApplicationSecurity_Semantik.pdf

kurz notiert

Technische Sicherheit beim ePass

Ab November 2005 sollen deutsche Reisepässe ein elektronisch lesbares Gesichtsbild – später auch Fingerabdruck – auf einem kontaktlosen Sicherheitschip im Pass enthalten. Die technische Sicherheit gewährleistet dabei das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Damit sich Daten des Ausweises nicht manipulieren oder unberechtigt auslesen lassen, wird ein zertifizierter Sicherheitschip mit kryptographischen Koprozessor eingesetzt. Die biometrischen Daten sind nach der Passproduktion durch eine digitale Signatur geschützt. Es ist zudem nicht möglich, die Kommunikation zwischen Pass und Lesegerät während der Kontrolle zu belauschen: Nur wer den Reisepass physisch lesen kann, ist in der Lage, Daten über die Funkschnittstelle zu erhalten (s. www.bsi.bund.de/fachthem/epass/Sicherheitsmerkmale.pdf)

Mit der Verwendung von RF-Chips (Radio Frequency) und der Speicherung des Gesichtbildes werden die Empfehlungen der Internationalen Zivil-Luftfahrtorganisation ICAO umgesetzt. Die ICAO stuft die kontaktlose Übertragung durch RF-Chips als die geeignetste Technik ein, weil diese Chips keine fehleranfälligen Kontaktflächen besitzen, die benötigte Speichergröße bereitstellen und die Beibehaltung des bisherigen Passformats ermöglichen. Zudem bleibt die zukünftige Implementierung aktiver Sicherheitsmechanismen möglich. Damit sind die Pässe weltweit einsetzbar und offen für technische Fortschritte. ■