Sicherheit für Webanwendungen der öffentlichen Verwaltung

Highlights

- ***Reduzierte Kosten für manuelle Sicherheitstests***
- ***Schließung von Sicherheitslücken und Vorbeugung gegen Datenmissbrauch***
- ***Erhöhte Sicherheit gegenüber Angriffen von außen***

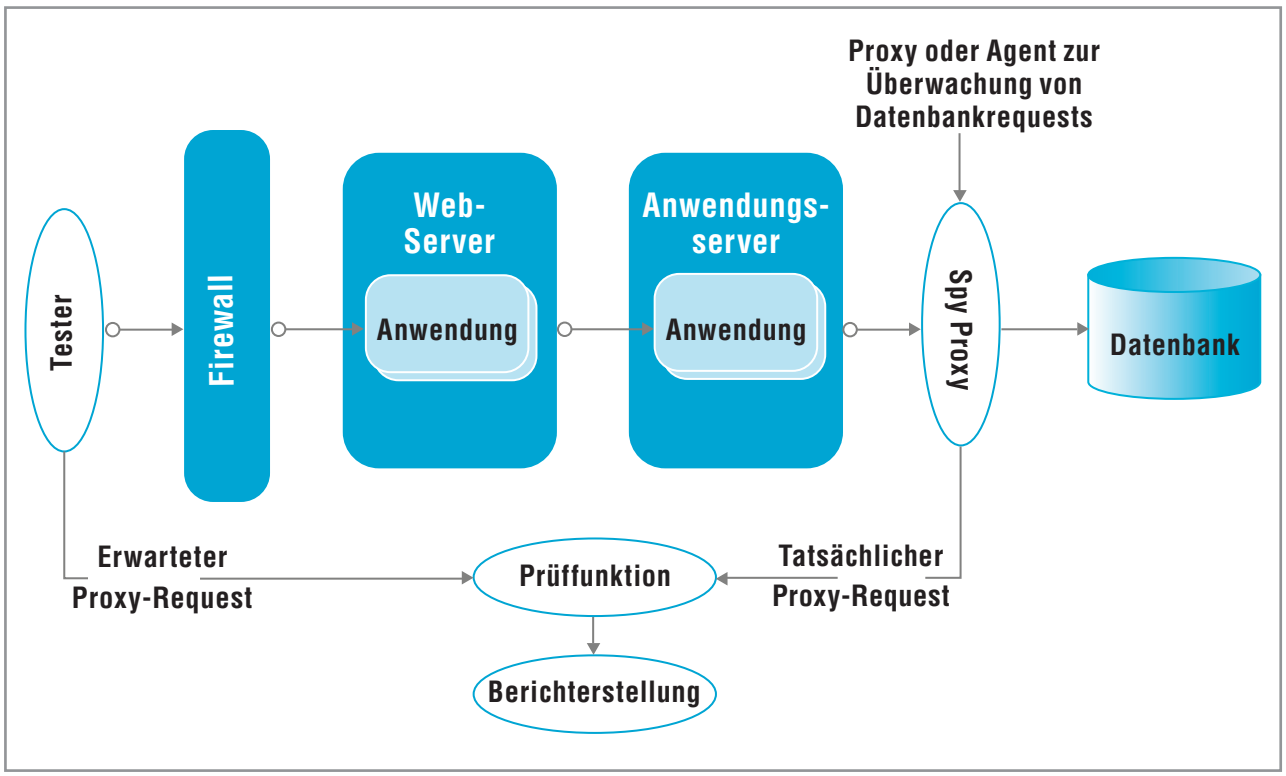
Herausforderungen auf dem Markt

„Untersuchungen zufolge wurden im Zeitraum von Januar bis März 2008 durchschnittlich 15.000 infizierte Webseiten pro Tag entdeckt. Davon gehörten 79 Prozent zu vermeintlich harmlosen Internetangeboten. Die meisten Angriffe erfolgen dabei über das Einschleusen von so genannten Inlineframes, was mit geringem Aufwand über automatisierte Vorgänge möglich ist, wenn die Webseite eine Schwachstelle enthält. Ein einziger Angreifer kann auf diese Weise mehrere tausend Webseiten innerhalb weniger Stunden infizieren. In den meisten Fällen müssen dazu aktive Inhalte auf dem Rechner des Webseitenbesuchers freigeschaltet sein, damit die Schadprogramme eingeschleust und ausgeführt werden können."

– BSI – https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

Verwaltungen sind heute gefordert, die Möglichkeiten des Internets für sich zu nutzen. Mit diesen neuen Möglichkeiten entstehen jedoch neue Risiken. Denn während immer weniger Daten auf den klassischen Arbeitsplatzrechnern zu finden sind, die durch stets aktuell gehaltene Virenscanner überprüft werden, stehen Webanwendungen vorwiegend unkontrolliert Nutzern und somit auch Hackern zur Verfügung. Verwaltungen benötigen Lösungen, die Sicherheitsrisiken identifizieren und gegen diese vorbeugen. Derzeit finden 75 Prozent der Hackerangriffe auf der Anwendungsebene statt. Diese Angriffe werden durch Hacker mithilfe automatisierter Werkzeuge gestartet. Aus diesem Grund ist für die Abwehr dieser Bedrohungen ebenfalls eine automatische Fehlererkennung zwingend erforderlich.

Die öffentliche Verwaltung ist verpflichtet, sowohl die Vorgaben und Richtlinien des BSI (Bundesamt für Sicherheit in der Informationstechnik) als auch die Datenschutzgesetze einzuhalten. Der Sicherheit von Webanwendungen, der Daten sowie der Transaktionen kommt im Rahmen der Web 2.0-Maßnahmen eine essenzielle Bedeutung zu. Erfolgreiches E-Government basiert auf dem Vertrauen der Bürgerinnen und Bürger in die Sicherheit der Ihnen angebotenen Webservices. Serviceorientierung bedeutet nicht zuletzt, vertrauensvoll mit personenbezogenen Daten umzugehen. Eine Datenschutzerklärung alleine reicht dafür nicht aus.



Beschreibung der Lösung

Mit IBM Rational AppScan erhält die öffentliche Verwaltung ein leistungsstarkes Werkzeug zur Überprüfung der Sicherheit von Webanwendungen und -diensten. IBM Rational AppScan identifiziert, bewertet und meldet Schwachstellen in den Anwendungen, ermöglicht neue Methoden für Sicherheitsbeauftragte und berechtigt gleichzeitig verschiedene IT-Verantwortliche, kritische Webanwendungen auf ihre Sicherheit hin zu testen. Die Werkzeuge „Scan Expert“ und „State Inducer“ ermöglichen es den Entwicklern, Testern und IT-Verantwortlichen zudem, Schwachstellen nicht nur zu identifizieren, sondern diese auch gleich zu beheben.

Sie haben nicht nur die Möglichkeit, Sicherheit zu einem integralen Bestandteil der Anwendungsentwicklung und -bereitstellung zu machen. Sie können die erforderlichen Sicherheitstests bei der Entwicklung direkt in die Anwendung integrieren und so ereignisgesteuerte Tests durchführen. Hierzu ein Beispiel: Wenn ein Benutzer eine Anforderung stellt und die Anwendung antwortet, vergleicht die Testfunktion die Antwort mit einer erwarteten oder zuvor gespeicherten Antwort, um festzustellen, ob das System ordnungsgemäß arbeitet. In Abbildung 1 beispielsweise verwendet eine Anwendung eine Datenbank als Back-End-Komponente. Der Tester integriert einen „Spy Proxy“ und eine Prüffunktion in den Anforderungsablauf und die Prüffunktion erhält Informationen darüber, wie eine normale Anforderung aussehen sollte. Die Prüffunktion kann dann die tatsächlichen Anforderungen des „Spy Proxy“ mit diesen Informationen vergleichen.

Dadurch erhöht sich die Wahrscheinlichkeit, dass Sicherheitsprobleme schon in einem frühen Stadium erkannt werden, also bevor sie ein ernstzunehmendes Risiko für Ihre Verwaltung darstellen.

IBM Rational AppScan unterstützt Sie bei der Reduktion von Sicherheitslücken in drei Schritten:

- ***Automatisierte Scans:*** *Rational AppScan lokalisiert in Ihren Webanwendungen alle bekannten Schwachstellen wie SQL-Injection, Cross-Site Scripting oder Buffer Overflow.*
- ***Sicherheitsberichte:*** *Rational AppScan stellt Ihnen ein umfangreiches Security-Reporting zur Risikoanalyse und Unterstützung der Einhaltung gängiger Standards zur Verfügung.*
- ***Korrekturempfehlungen:*** *Rational AppScan zeigt anhand von Schulungsmodulen und Best Practise auf, wie Programmierer vorgehen müssen, um bestehende Schwachstellen zu schließen.*

Vorteil

Rational AppScan bietet folgende Vorteile:

- *Alle Eingabeparameter (z. B. Formularfelder, Abfragezeichenfolgen, Cookies und HTTP-Header) können automatisiert auf bekannte Sichherheitslücken überprüft werden. Die Sicherheitslücken werden protokolliert, beschrieben und nach Risiko klassifiziert. Zudem werden Empfehlungen zur Fehlerbehebung ausgegeben.*
- *Potenzielle Sicherheitsbedrohungen werden permanent überwacht. Dadurch ist es möglich, auf Angriffe direkt zu reagieren und bestehende Risiken abzuwenden. Dies geschieht durch eine umfassende Scan-Abdeckung, eine intigrierte Sicherheitsüberprüfung direkt im Entwicklungsprozess sowie eine effektive Kommunikation im Entwicklungsteam.*
- *Kosten können durch manuelle Sicherheitstest, computerbasierte Trainings sowie ein webbasiertes Angebot zur unternehmenweiten Einführung reduziert werden.*

Unser Angebot

Den Webscanner bieten wir Ihnen in zwei verschiedenen Versionen an: die Standard Edition und die Express Edition.

Für die Einführung (Installation, Schulung) bietet IBM zwei Tage Dienstleistungen vor Ort an.

Weitere Informationen

Die Bedrohungslage im Internet wächst Untersuchungen zufolge rasant. Wie genau sich die verschiedenen Angriffe auf die Inhalte Ihrer Webanwendungen auswirken, finden Sie in einer kurzen Abhandlung, die Sie auf unserer Produktseite im Internet herunterladen können:

ibm.com/software/de/rational/appscan/index.html

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

PUF03002-DEDE