Deloitte.

Enterprise Risk Services

Webapplikationssicherheit
Risiken webbasierter Software

Risikofaktor Webapplikationen

Kaum ein Unternehmen kann heute noch auf den Einsatz webbasierter Applikationen verzichten, um erfolgreich am Markt zu bestehen.

Schlagwörter wie Webservices, Service-orientierte Architekturen (SOA) und Web 2.0 sowie die einfache Bedienung von webbasierten Anwendungen mittels eines Webbrowsers führen zu einer immer stärkeren Verdrängung klassischer Client/Server-Anwendungen.

Doch mit der Verbreitung dieser Technologien und ihrer vereinfachten Anwendung steigt auch die Motivation von Angreifern, Schwächen in diesen Technologien aufzuspüren und auszunutzen.

Wer ist betroffen?

Fast täglich sind den Medien sicherheitsrelevante Vorfälle zu entnehmen, deren Ursachen im unsicheren Betrieb und in der Entwicklung von Webanwendungen zu finden sind.

Nachrichten über Phishing-Attacken und die typischen Implementierungsfehler sind immer noch regelmäßig in den Schlagzeilen. Angreifer kommen dadurch illegal in den Besitz tausender Konto- und Benutzerdaten und missbrauchen sie auch. Zudem können skriptbasierte Würmer die Fehler in Webanwendungen ausnutzen, um unbedarfte Endanwender, während sie im Internet surfen, auszuspionieren.

Vom Web-Shop bis zum Lieferantenportal

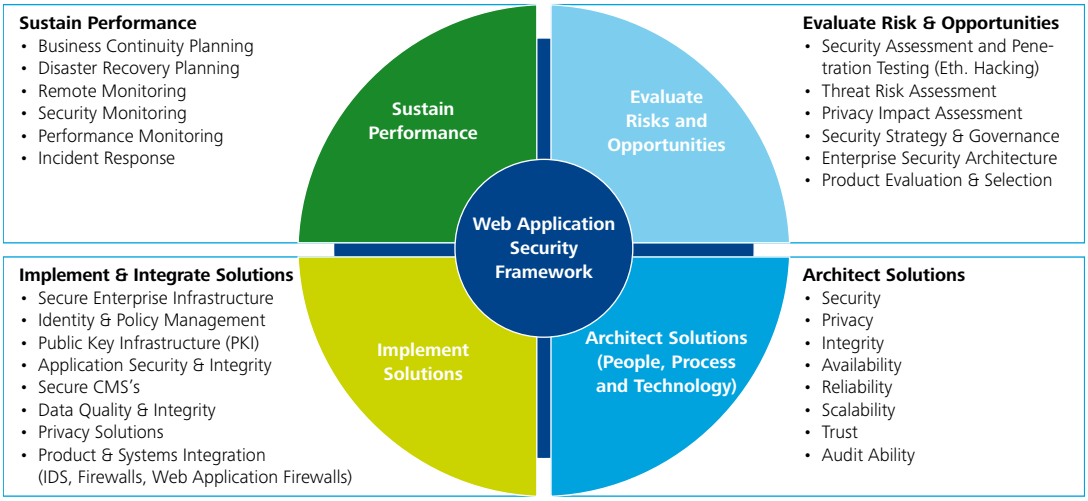
Besonders Unternehmen sind gefährdet, da sie häufig Webanwendungen über die eigenen Firmengrenzen hinweg betreiben, um Endkunden, Partner oder Lieferanten über Web-Shops und Lieferantenportale direkt in die Geschäftsprozesse einbinden zu können.

Hierbei kann bereits die kleinste Unachtsamkeit bei der Entwicklung oder Integration der Webapplikationen dazu führen, dass Unberechtigte Zugriff auf interne Systeme wie Datenbanken und File-Server erhalten.

Web Application Security and LifeCycle Framework

Das von Deloitte angewandte Web Application Security Framework basiert in seinen Grundbestandteilen auf gängigen Standards, wurde jedoch für die speziellen Anforderungen von Webanwendungen angepasst. Nur durch eine umfängliche Betrachtung der Anwendungen einschließlich der Prozesse sowie der Infrastruktur, in der die Anwendungen betrieben werden, können die relevanten Risiken identifiziert und minimiert werden.

Abb. 1 – Secure LifeCycle Framework



Unsere Leistungen

Deloitte verfügt über ein Spezialistenteam, das Sie bei der Bewertung der Risiken, der sicheren Entwicklung und dem sicheren Betrieb von webbasierten Softwareanwendungen unterstützt.

Mit einem erprobten und auf Ihr Unternehmen maßgeschneiderten Lösungsansatz führt Deloitte zu einer umfassenden Erhöhung der Sicherheit der eingesetzten Applikationen und hilft, die vorhandenen Risiken in den Griff zu bekommen.

Hierbei wird anhand eines speziell auf die Sicherheit von Applikationen entwickelten Kennzahlensystems die Grundlage geschaffen, den Reifegrad der Anwendungen zu bestimmen und Veränderungen in der Sicherheit messbar zu machen.

Anschließend wird bereits bestehende oder geplante Software auf offensichtliche Entwicklungs- und Konfigurationsfehler geprüft, die negative Auswirkungen auf die Sicherheit haben können.

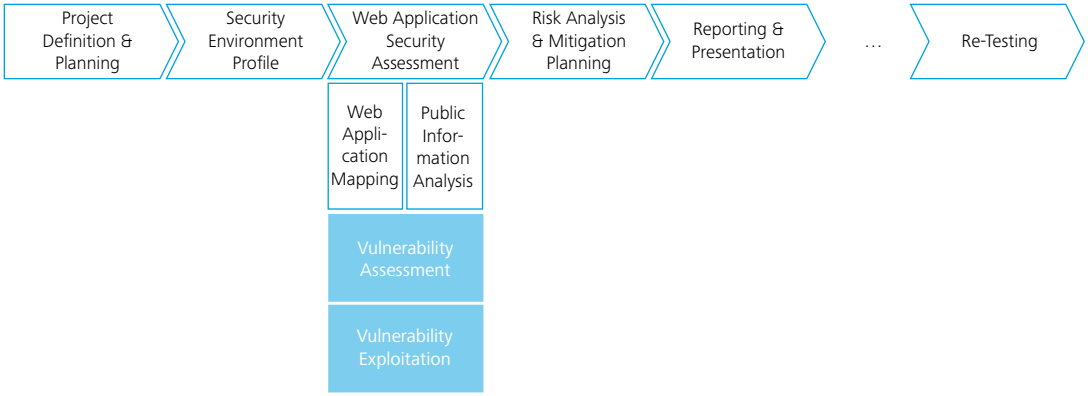
Hierbei reicht die Bandbreite der Deloitte-Leistungen von der Simulation eines Angriffs über eine Bewertung der Architektur der Anwendungsumgebung sowie einer detaillierten Prüfung des Quellcodes auf sicherheitsrelevante Entwicklungsfehler bis hin zu gezielten Entwickler- und Mitarbeiter-Schulungen für sichere Entwicklung und den sicheren Betrieb von Webanwendungen, um bestehende und zukünftige Unternehmensanwendungen und die zugehörigen Geschäftsprozesse effektiv zu schützen.

Mit Methode zum Ziel

Für die Prüfung des Sicherheitsniveaus Ihrer Anwendungen wenden wir unsere Methode an, die auf anerkannten Standards wie bspw. dem Open Source Security Testing Methodology Manual, dem OWASP Application Security Verification Standard sowie eigenen Erweiterungen basiert und unsere langjährige Erfahrung im Bereich der Webanwendungssicherheit einbezieht.

Da die Informationen und Daten, die in Ihren Anwendungen verarbeitet und transferiert werden, immer nur so sicher sind wie das schwächste Glied in der datenverarbeitenden Kette, verfolgen wir einen erprobten Ansatz, der die Anwendungsumgebungen mit in die Betrachtung einschließt.

Abb. 2 – Projektstufen



Application Environment Security

Eine Anwendung kann nur dann sicher betrieben werden, wenn die Umgebung, in der diese betrieben wird, auch abgesichert ist. Zur Anwendungsumgebung gehören sämtliche beim Anwendungsbetrieb und bei der Administration verwendeten Komponenten – von den Netzwerkgeräten bis hin zu den Anwendungsservern und Frameworks.

Application Security

Robuste und vor allem sichere Anwendungen sind die Stützpfeiler einer erfolgreichen Organisation. Daher werden im Rahmen der Deloitte Application Security Services Dienstleistungen angeboten, um Risiken in Anwendungen zu identifizieren, zu klassifizieren und zu minimieren. Vom Blackbox-Anwendungstest bis zum Quellcode Review.

Network Security

Die Basis einer jeden IT-Infrastruktur bildet das Netzwerk. Hierüber laufen in der Regel alle Transaktionen – vom Mitarbeiter, der sich den aktuellen Speiseplan anschaut, bis hin zu Buchungen mithilfe des SAP-Systems. Um sicherzustellen, dass alle Daten auch ihrer Kritikalität entsprechend geschützt transportiert und voneinander getrennt übertragen werden, muss vom Design bis zur technischen Komponente Sicherheit implementiert sein.

System Security

Die heute meist zum Einsatz kommenden Systeme, hard- sowie software-seitig, sind oft wesentlich leistungsstärker als für ihren eigentlichen Verwendungszweck notwendig. Diese Tatsache verleitet dazu, mehrere Dienste oder virtuelle Maschinen auf dem gleichen System zu betreiben. Hieraus resultieren neue Angriffsvektoren und somit Risiken, die bei den Ihren Anwendungen zugrundeliegenden Systemen berücksichtigt werden müssen.

Configuration Security

Auch eine nicht ausreichend gesicherte Konfiguration einer Anwendung, eines Anwendungsservers, einer Netzwerkkomponente oder eines Betriebssystems birgt enorme Gefahren. Im Rahmen von Konfigurationsanalysen können mögliche Sicherheitsbedrohungen effizient erkannt und zielgerichtete Empfehlungen ausgesprochen werden.

Secure Data Management

Hinter beinahe jeder Anwendung verbergen sich Datenhaltungssysteme wie bspw. Datenbanken oder File-Server. Mit wachsendem Unternehmen wächst auch die Menge der Daten, die vorgehalten werden müssen. Diese Daten müssen, je nach Art und Kritikalität, vor Manipulation, Diebstahl und Missbrauch geschützt werden. Mit einem ganzheitlichen Ansatz – Discover/Classify/Control/Audit – helfen wir Ihnen, Herr über Ihre Daten zu bleiben.

Sieben Argumente für Deloitte

1. Weltweit über 12.000 Mitarbeiter im Bereich Security & Privacy, davon 1.100 CISSPs (Certified Information Systems Security Professionals) – mehr als in jeder anderen Service Organisation.
2. Strategisches Vorgehen basierend auf aktuellen Standards und den Erfahrungen von zahlreichen IT-Sicherheitsprojekten.
3. Aktive Mitwirkung in Organisationen, die sich mit dem Thema IT-Sicherheit befassen: Information Security Forum (ISF), Informations Systems Audit & Controls Association (ISACA), International Information Systems Security Certification Consortium (ISC)2, Information Systems Security Association (ISSA), CyLab, I-4, IAPP, American Society for Industrial Security (ASIS), International Standards Organization (ISO) und Open Web Application Security Project (OWASP).
4. Breite und Tiefe von Fachwissen und Fähigkeiten – wir verfügen über umfassendes und detailliertes Fachwissen. Dies ermöglicht es uns, alle Anforderungen an sichere Anwendungen in Ihrer Organisation umzusetzen.
5. Praktische Umsetzungserfahrung – wir haben Erfahrung in der Entwicklung komplexer Sicherheitsprogramme, in denen Menschen, Prozesse und technologischer Wandel ganzheitlich betrachtet werden.
6. Ausgezeichnete Projektmanagementfähigkeiten – Deloitte setzt seine langjährige und umfangreiche Erfahrung im Projektmanagement wirksam ein, um Ihren Projektaufwand zu reduzieren.
7. Gemeinschaftliche Herangehensweise – für Deloitte hat die enge Zusammenarbeit mit Kunden und deren Partnern hohe Priorität und stellt einen wichtigen Baustein für den Erfolg der Projekte dar.

Ihre Ansprechpartner

Peter J. Wirnsperger
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Für weitere Informationen besuchen Sie unsere Webseite auf www.deloitte.com/de/cyber

Stand 05/2013