Security Testing

Studiengang: MAS Information Technology
Betreuer: Lukas Ith
Experte: Lukas Ith (advact AG)

Funktionale Anforderungen an eine Web-Applikation müssen heutzutage mit aller Sorgfalt erarbeitet werden, damit für den Anwender der optimalste Nutzen daraus gewonnen werden kann. Nicht funktionale Anforderungen scheinen dabei etwas in den Hintergrund zu geraten. Gerade die Security, welche nicht so greifbar ist, verdient es mal genauer unter die Lupe genommen zu werden.

Ausgangslage und Ziel

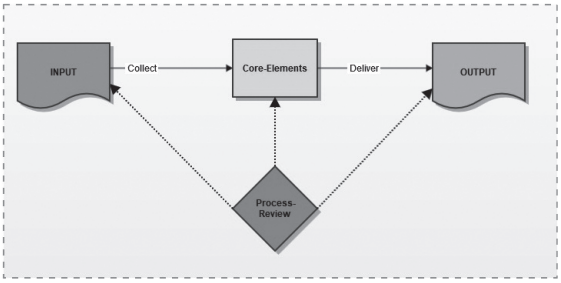
Die betreffende Firma ist im Bereich der individual Software-Entwicklung im Enterprise-Bereich tätig. Bis jetzt fehlte ein übergreifender Security Test-Prozess im Unternehmen. Mit zunehmenden Entwicklungen im öffentlichen Bereich und im Hinblick auf die ISO-27001 Zertifizierung, wird das Verlangen nach einem solchen Test-Prozess immer wichtiger. Ziel dieser Arbeit war es, einen Test-Prozess zu entwerfen, aufgrund dessen in Zukunft Security-Tests durchgeführt werden können. Web-Applikationen sollen so auf deren Sicherheit getestet werden, bevor diese produktiv zum Einsatz kommen.

Abgrenzung

Themen, wie sicherer Softwareentwurf, sichere Softwareentwicklungsmethoden, sicheres Programmieren und Codeschutz, ist nicht Teil dieser Arbeit. Der vorliegende Test-Prozess soll ein Hilfsmittel sein, um damit erste Erfahrungen zu sammeln und wo nötig dann Ergänzungen vorzunehmen.

Ergebnis

Der erarbeitete Security Test-Prozess besteht aus den folgenden vier Komponenten (siehe Abbildung):
In der ersten Komponente, dem INPUT, wird die notwendige Basis für die Komponente Core-Elements geschaffen. Der Input ist die Schutzanforderungsdefinition für eine Web-Applikation. Hierzu wird ein Risikomanagement-Prozess (inkl. Bedrohungsmodellierung) durchlaufen, welcher die Assets und deren Schutzbedarf bis hin zu den Massnahmen identifiziert. Die zweite und für das Testing grösste Komponente bilden die Kern-Elemente, welche aus Test-Dimensionen, Test-Strategie Modell, Test-Techniken, Test-Planung sowie Test-Durchführung besteht. Diese werden benötigt, um das Security-Testing in seiner Gesamtheit zu erfassen.



Security Test-Prozess

Die dritte Komponente ist der OUTPUT sprich das Test-Reporting. Der Test-Report bildet das finale Test-Produkt (mit Test-Resultaten, Bug-Report, Test-Scripts, verwendete Test-Daten usw.). Dieses Dokument präsentiert dem Projektteam und dem Kunden die durchgeführten Test-Aktivitäten. Der Test-Report soll dabei ebenfalls aufzeigen, inwiefern sich der Test-Aufwand gelohnt hat. Weiter lässt sich daraus die mögliche Weiterentwicklung des gesamten Security Test-Prozesses ableiten.

Die letzte Komponente ist das Process-Review. Diese hat die Aufgabe des Überwachens des gesamten Prozesses. Durch regelmässige Reviews soll der Test-Prozess kontinuierlich weiterentwickelt, optimiert und den aktuellen technischen Möglichkeiten sowie den Markt-Bedürfnissen angepasst werden.

Weiteres Vorgehen

Der für die Firma entworfene Test-Prozess soll nun in einem nächsten Schritt in einem Proof of Concept verifiziert werden. In Zukunft soll dieser in den Projekten eingesetzt werden können.

»Sichere Software ist Software, die gegen absichtliche Angriffe auf die Software geschützt ist. Jeder im Softwareentwicklungsprozess sollte an dieser Eigenschaft einer Software interessiert sein, da Software leider selten automatisch sicher ist.»
(Sachar Paulus)

Simon Berner