Ausgabe 2011 / 1

Erscheinungsart: ca. 4 x jährlich in elektronischer Form

Penetrations-Tests

In dieser Ausgabe:

- Kosten und Nutzen von Penetrationstests
- Das 7. Element - Security
- Links, Literatur, Zitate

Das 7. Element - Security (von Klaus Veselko)

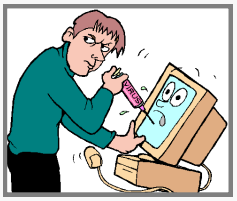
Das International Software Test & Qualification Board (ISTQB®) hat sich in den letzten Jahren mit seinen Ausbildungsmodulen und der Nomenklatur zu dem internationalen Standard auf dem Gebiet des Software-Testens entwickelt. Neben IEEE, dem TPI Standard und anderen wird immer öfter ISTQB als Referenz herangezogen.

Wenn wir die Lehrinhalte (Syllabus) von ISTQB betrachten, dann finden wir fein säuberlich definiert die Hauptmerkmale für Softwarequalität:

- Funktonalität (functionality)
- Zuverlässigkeit (relyability)
- Benutzbarkeit (usability)
- Effizienz (performance)
- Änderbarkeit bzw. Wartbarkeit (maintainability)
- Übertragbarkeit (portability)

Wenn es um den Bereich des Sicherheit geht, da klafft bei ISTQB eine riesige Lücke. Sicherheit bzw. Security wird nicht als eigenes Qualitätsmerkmal behandelt und dementsprechend wird auch die Disziplin Sicherheitstest nur sehr stiefmütterlich behandelt. Auf die Frage, warum das so ist, hatte keiner eine überzeugende Antwort.

Am wahrscheinlichsten ist die Annahme, dass das Thema sehr komplex und technisch kompliziert ist. Security zieht sich durch sämtliche Schichten der IT- und SW-Architektur. Außerdem steht man einem unsichtbaren, schier übermächtigem Gegner – dem unbekannten Angreifer – gegenüber. Da passiert es, dass man aufgrund des erwarteten hohen Aufwandes die Prioritäten anders verteilt.



Aus den genannten Gründen, darf Sicherheit bei der Testplanung und späteren -durchführung nicht vernachlässigt werden. Im Gegenteil: Durch die heutigen Bedrohungsszenarien im Internet und dem stetig wachsenden Cloud Computing muss der verantwortliche Testmanager das Thema Security mit Top-Priorität versehen. Heutzutage darf ein Security Test in keiner Teststrategie bzw. keinem Testplan fehlen. Dies bleibt jedoch oft auf die Funktionalität der Anmeldemaske oder Rollenvergabe und Berechtigungen beschränkt. Das Testen der Sicherheit gegenüber Angriffen, Datenklau oder gar betrügerische Manipulationen wird oft vergessen.

Aber wird das der Wichtigkeit des Themas Security gerecht? Ich denke, es ist gerechtfertigt, dass Security als eigenständiges Qualitätsmerkmal – quasi als das 7. Element – in die obenstehende Liste aufgenommen wird. Dafür plädiere ich.

Um diesem neuen, alten Qualitätsmerkmal mit seiner Komplexität den Schrecken zu nehmen, beleuchten wir in diesem Newsletter das Thema Penetration Test (kurz: PenTest) als praktikables Mittel zur Verbesserung der Applikationssicherheit. Wie geht man an die Sache heran? Was bringt es im SW-Erstellungsprozess? Und wie kann man die Kosten dafür im Griff behalten? Sie werden sehen und können hier lesen, dass es ein spannendes Thema ist. Viel Spaß bei der Lektüre!

Secure-Code
Ein frommer Wunsch?

Wir haben in unseren Projekten in der Software-Qualitätssicherung viel mit Software-Entwicklern und natürlich auch Software-Source-Code zu tun.

Wir analysieren oft Source-Code nach verschiedenen Gesichtspunkten und stellen dabei immer wieder fest, dass neben den typischen Qualitätsmängeln wie schlechte Testbarkeit, mangelnde Dokumentation, etc. auch zu wenig Wert auf sicheren Code gelegt wird.

Es treten dabei eklatante Mängel wie z.B. fehlende Input-Validierung sehr häufig auf, obwohl diese Schwachpunkte eigentlich meist recht einfach zu beheben wären.

Teilweise wird dies von den SW-Entwicklern mit mangelnder Zeit begründet, oft sind aber auch fehlendes Architektur- und Security-Wissen bzw. –Bewusstsein dafür verantwortlich.

Schlimm dabei ist, dass es wegen zusätzlich meist fehlender systematischer Security-Analysen und Security-Tests im Unternehmen oft niemandem auffällt und die möglicherweise funktional ganz gute Software trotzdem als tickende Zeitbombe die Software-Entwicklung verlässt.

Ganz offensichtlich leidet das Thema Secure-Code an den selben Symptomen wie auch das Thema Code-Qualität oder Code-Dokumentation.

In der Ausbildung wird es leider oft nur als Nebenfach oder halbherzig vermittelt und in der Praxis hat dann keiner mehr die Zeit für diese Themen.

Dipl.-Ing. Johannes Bergsmann
Staatl. befugter und beeideter Ingenieurkonsulent für Informatik

Der Quality-Knowledgeletter ist ein periodisches Informationsmedium von Software Quality Lab und dessen Partnern mit den Schwerpunkten IT-Qualitätsmanagement, Projekt- und Prozess-Management.

Inhalt: fachliche Beiträge und Schwerpunktthemen, Vorstellung neuer Produkte und Leistungen, neue wissenschaftliche Erkenntnisse und andere Fachbeiträge aus unseren Themenbereichen.

Aktuelle Fach- und Forschungsbeiträge sind willkommen. Einsendungen an info@software-quality-lab.at .

Weitere Infos zu diesem und anderen Themen finden Sie auf http://www.software-quality-lab.at .

Kosten und Nutzen von Penetrationstests

Jürgen R. Plasser, Software Quality Lab

Einleitung

Eine wesentliche Zahl von Einbruchsversuchen in Unternehmensnetze und Webapplikationen bleibt verborgen und meist erfährt nicht einmal der Geschädigte von einem Einbruch. Erfahrene Angreifer hinterlassen wenig oder keine Spuren und lösen in der Regel auch keine Notifikationen von Warnsystemen aus.

Neben einer entsprechend ausgestatteten Sicherheitsinfrastruktur und einem Entwicklungsprozess mit Fokus auf Qualität bringt die Überprüfung der Sicherheit und Robustheit von Anwendungen gegenüber Angriffen einen hohen Sicherheitsgewinn. So lassen sich zwar über den Softwaretest viele Fehler (Defects) finden und eine planerische als auch konstruktive Qualitätssicherung ist Grundlage jeder Softwareentwicklung, jedoch ohne analytische Qualitätssicherung nicht vollständig.

In der Regel wird über eine analytische Qualitätssicherung – im Normalfall, der bekannte Softwaretest in all seinen Ausprägungen – eine funktionale als auch nichtfunktionale Fehlerminimierung angestrebt. Oft werden dabei jedoch ganz spezifische Sicherheitsaspekte nicht berücksichtigt, womit es in den finalen Anwendungen oft möglich ist diverse Angriffsszenarien über XSS (Cross-Site-Scripting), SQL-Injection, Buffer-Overruns, etc. durchzuführen.

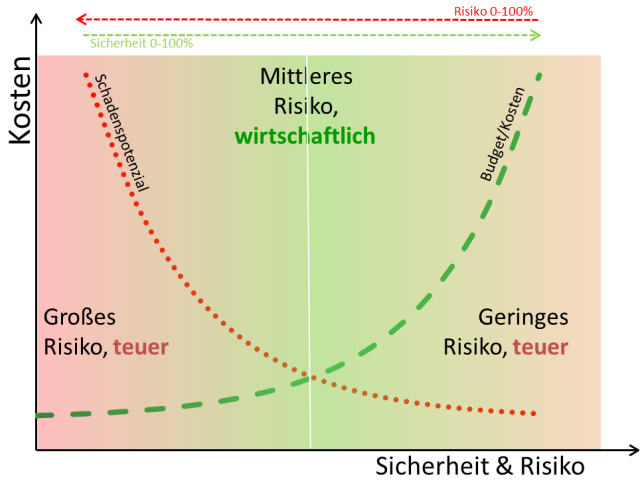


Abbildung 1—Kosten/Nutzen Penetrationstests
[Quelle: Software Quality Lab]

Ein Grund für das „Übersehen" solcher Lücken ist oft im Nichtvorhandensein von Risikoassessments und Sicherheitsanforderungen zu suchen. Wenn keine Sicherheitsanforderungen spezifiziert wurden, werden diese beim Test auch nicht berücksichtigt.

Ein weiterer Grund, warum Penetrationstests nicht (oder nur rudimentär) durchgeführt werden, sind die entstehenden zusätzlichen finanziellen Aufwände. Penetrationstests werden häufig outgesourct. Einerseits, weil das eigene Personal damit überfordert ist (sowohl zeitlich als auch fachlich), immerhin handelt es sich um ein sehr spezielles Testthema, und andererseits, weil solche Tests von unabhängigen Dritten durchgeführt werden sollten.

Dennoch lautet die häufigste Frage unserer Kunden: „Rechnet sich ein Penetrationstest?".

Kosten-/Nutzenanalyse von Penetrationstests

Die Optimierung von Sicherheit und Risiko unter Berücksichtigung der Kosten lässt sich wie in Abbildung 1 darstellen. Das Optimum findet sich dort wo sich die Kurven „Schadenspotenzial" und „Budget/Kosten" schneiden. In der näheren Umgebung dieses Punktes erwarten wir ein finanziell vertretbares Risiko.

Leider lässt sich das Budget nicht analytisch bestimmen, da sich der aus einer Entscheidung (z. B. „Verzicht auf Penetrationstests") zu erwartende Schaden nicht ohne weiteres quantifizieren lässt. Sinnvollerweise wird ein pragmatischer Ansatz gewählt, so kann beispielsweise das aktuelle Budget ähnlich angesetzt werden, wie für ein älteres und ähnliches Projekt. Die in der Abbildung 1 gezeigten Kurven gelten natürlich auch für den Penetrationstest selbst. Auch beim Penetrationstest wird versucht die risikoreichen Bereiche wirtschaftlich optimal abzudecken. Es macht wenig Sinn zu versuchen alle Schwachstellen in einem System zu finden, da dies generell unmöglich ist. Eine konkrete Fokussierung auf potenzielle Vulnerabilities ist der zielführende Ansatz. Weniger ist mehr, lautet auch hier die Devise!

Return on Investment

Der *Return on Investment* (ROI) ist im Security-Umfeld traditionell schwierig zu berechnen. Zu viele Unbekannte und Variablen machen eine Quantifizierbarkeit der Auswirkungen von Sicherheitslöchern und Investitionen beinahe unmöglich. Der Penetrationstest aber ist ein probates Mittel zur Feststellung des Status Quo. Daraus lassen sich unmittelbar geeignete Maßnahmen ableiten, um das Sicherheitsrisiko zu mindern oder völlig zu beseitigen.

Beim Penetrationstest einer Webapplikation wird der Fokus auf jene Bereiche der Anwendung gelegt, in denen durch ein vorgelagertes Risikoassessment die höchsten Risiken zu erwarten sind. In der Regel sind das Ein-/Ausgabeschnittstellen, im Authentifizierungscode, Datenbankzugriffscode, Bereiche in denen sensible Daten verwaltet oder finanzielle Transaktionen abgewickelt werden.

Wichtige Punkte bei Penetrationstests

Penetrationstests werden im Rahmen der Qualitätssicherung durchgeführt, aber nicht nur. Oft sind sie auch Bestandteil der Abnahme des Kunden zur Dokumentation des Sicherheitsniveaus oder dienen zur Entscheidungsfindung für Investitionen im Bereich IT-Sicherheit.

Penetrationstests werden in der Regel nicht von Bera-

Vollständiger Knowledge Letter Zugang

Wir freuen uns, dass Sie an diesem Thema Interesse haben und den Knowledge Letter von Software Quality Lab bis hierher gelesen haben.

Dieser Knowledge Letter ist eine Vorschau (gekürzte Version des gesamten Artikels).

Wenn Sie den ungekürzten Knowledge Letter lesen möchten, registrieren Sie sich bitte unter
http://www.software-quality-lab.com/download/knowledge-letter/anfrage-knowledge-letter/

Sie erhalten nach der Registrierung vollen Zugang zu allen bisherigen Knowledge Lettern von Software Quality Lab und erhalten automatisch künftige Knowledge Letter per E-Mail.

Software Quality Days — Die größte Konferenz zum Thema „Software Qualität“ in Europa!

Besuchen Sie die Top-Konferenz mit allen Infos rund um Software Qualität.

Beste Qualität der Vorträge und Tutorials sowie eine Mischung aus praktischen und wissenschaftlichen Beiträgen machen die Software Quality Days zum Top-Event.

In den 3 praktischen Tracks werden anwendungsorientierte Vorträge präsentiert. Der wissenschaftliche Track zeigt Beiträge mit hohem Innovationsgrad und praktischer Anwendbarkeit, basierend auf Forschungs-ergebnissen. Im Solution Provider Forum präsentieren Aussteller ihre neuesten Tools mit Praxis-Beispielen.

Nähere Infos unter

www.software-quality-days.com