audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Sichere Softwareentwicklung – Implementierung von Sicherheitsmodellen

Zusammenfassung

Security Breaches, die zu schwerwiegenden finanziellen und reputatorischen Schäden führen, finden sich täglich in den Schlagzeilen der Nachrichten. Neben Social-Engineering-Techniken bilden Schwachstellen in der Software für Angreifer das primäre Einfallstor in private Netzwerke und Systeme. Die Ursachen und Möglichkeiten zur Vermeidung des überwiegenden Teils der Software-Schwachstellen sind öffentlich bekannt. Zudem existiert eine Vielzahl von Vorgehensmodellen, die die Integration von Maßnahmen zur Vermeidung von Schwachstellen strukturieren und zusammenfassen. Solche Modelle werden als Security Development Lifecycle (kurz: SDL) bezeichnet. Trotz dieser Ausgangslage und der zentralen Bedeutung von Sicherheit während der Softwareentwicklung konnten sich diese SDL-Modelle bisher nicht etablieren.

Um die Ursache dieser Problematik zu verstehen, wurden drei Einstiegsmodelle in der Praxis evaluiert und Hindernisse bei der Implementierung dokumentiert. Mithilfe dieser Informationen konnten wir eine Methodologie entwickeln, mit der auch kleine und mittelständische Unternehmen Modelle zur sicheren Softwareentwicklung effektiv und effizient implementieren können.

Problemstellung

Die Bedeutung von Sicherheit in der Softwareentwicklung nimmt stetig zu. Die Menschheit ist zunehmend abhängig von softwarebasierten Systemen, die sensible Daten verarbeiten. Theoretische Modelle zur sicheren Softwareentwicklung, die in der Praxis nicht umgesetzt werden können, sind nicht ausreichend, um diesen Trend abzusichern. Die Wissenschaft beschäftigt sich nun seit fast 20 Jahren mit grundlegenden Fragestellungen im Bereich der sicheren Softwareentwicklung und hat mit der Entwicklung und Erweiterung von SDL-Modellen einen wesentlichen Grundstein gelegt. Dabei stand primär die Entwicklung, Definition und Kategorisierung von Sicherheitsaktivitäten und entsprechenden Umsetzungshinweisen im Vordergrund. Eine ausgezeichnete Komposition von Sicherheitsaktivitäten erzielt jedoch keinen effektiven Mehrwert, falls diese nicht oder nur schwer in der Praxis implementiert werden kann.

Laut einer Studie von Veracode aus dem Jahr 2016 berücksichtigen nur etwa 9.6% der untersuchten Unternehmen Sicherheitsaspekte in allen Phasen der Softwareentwicklung.[1] Die meisten Unternehmen stützen sich auch heute noch auf nachgelagerte Sicherheitsmaßnahmen, wie z.B. Penetrations- oder allgemeine Security-Tests. Dass dieser Ansatz zu keinem zufriedenstellenden Ergebnis führt, ist schon lange bekannt. Die mangelnde Adoption von SDL-Modellen und die damit einhergehende Vernachlässigung von Sicherheitsaktivitäten während der Softwareentwicklung haben in Kombination mit der stetig steigenden Anzahl von Softwareprojekten dazu geführt, dass sich die Anzahl der gefundenen Software-Schwachstellen in den letzten Jahren stark erhöht hat.[2] Es stellt sich also die zentrale Frage: Warum konnten sich SDL Modelle bislang nicht in der Masse durchsetzen?

[1] Vgl. Veracode 2016.

[2] Vgl. WhiteSource 2020;

Lösungsansatz

Zur Beantwortung dieser Frage wurden von uns drei Vorgehensmodelle[3] zur sicheren Softwareentwicklung in Zusammenarbeit mit drei Softwareentwicklungs-Unternehmen evaluiert. Keines der untersuchten Unternehmen besaß Praxiserfahrung mit SDL-Modellen und beschränkte sich auf sporadische Sicherheitstests und Code-Reviews. Die Vorgehensmodelle wurden einleitend allen Mitarbeitern des Unternehmens präsentiert und vorgestellt. Anschließend wurden die konkret vorgeschlagenen Sicherheitsaktivitäten in typischen Projektgruppen (etwa 3-6 Personen) genauer untersucht und mögliche Implementierungswege erarbeitet.

Ergebnis

Alle untersuchten Unternehmen bemängelten den Praxisbezug der Vorgehensmodelle. Die Sicherheitsaktivitäten und Umsetzungshinweise der Vorgehensmodelle waren zwar verständlich und nachvollziehbar, jedoch blieb unklar, wie diese in der Praxis umgesetzt werden sollten. Eine Implementierung ohne externe Unterstützung war somit größtenteils nicht möglich. Zudem enthielten alle Modelle eine Vielzahl von Sicherheitsaktivitäten, welche für die Tätigkeit der Unternehmen nur geringe oder keine Relevanz besaßen. Letzteres Problem wurde durch die Erarbeitung einer gekürzten und praxisorientierten Methodologie gelöst, welche auf erster Ebene in sechs Kategorien unterteilt werden kann:

1. Allgemeiner Sicherheitsmanagement Prozess
2. Schulungs- und Führungsmaßnahmen
3. Muster und Standards
4. Design
5. Verifizierung
6. Absicherung der operationalen Umgebung

Im Rahmen von Schulungsmaßnahmen wurde anschließend untersucht, welche Grundfähigkeiten die Mitarbeiter besitzen müssen, um die Aktivitäten dieser Methodologie effektiv und effizient umsetzen zu können. Dabei kamen wir zu folgendem Ergebnis:

Jeder Softwareentwickler benötigt ein Grundverständnis von potenziellen Bedrohungen. Die Betonung liegt an dieser Stelle auf Grundverständnis, die Entwickler müssen nicht wissen wie komplexe Angriffsmethoden konkret durchgeführt werden. Stattdessen müssen sie sich nur ihrer Existenz bewusst sein und in groben Zügen verstanden haben, wie sie funktionieren. Die zweite Anforderung liegt in dem Verständnis von grundsätzlichen Prinzipien zur sicheren Softwareentwicklung und dem jeweiligen Zusammenspiel mit den zuvor erwähnten Angriffsmethoden. Mithilfe von diesem Grundverständnis konnte unsere Methodologie schnell und effizient in die Softwareentwicklungsprozesse der untersuchten Unternehmen implementiert werden.

Unabhängig von dieser nachgelagerten Implementierung, empfanden alle Teilnehmer der Praxis-Evaluation den Aufbau der Grundfähigkeiten als sehr wertvoll. Daher

[3] Microsoft-SDL, SAFECode Fundamentals und BSIMM

haben wir uns entschlossen, dieses Wissen komprimiert in einem Basis Workshop zur sicheren Softwareentwicklung zusammenzufassen und anzubieten.

Autor und Ansprechpartner

Marcel Albrink
Consultant Informationssicherheit

Schwerpunkte: IT-Schwachstellenanalyse, Sichere Softwareentwicklung

Mail: m.albrink@audatis.de
Fon: 05221 87292-06
XING **Linkedin**

Haben Sie noch Fragen?

Wir haben versucht alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Dieses Whitepaper wird Ihnen von der audatis Consulting GmbH zur Verfügung gestellt und darf gerne unverändert weitergegeben oder veröffentlicht werden.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Datenschutz und Informationssicherheit CONSULTING

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de