Code Review

Ein Großteil der Sicherheitsprobleme entsteht durch kritische Schwachstellen in Applikationen. Code Reviews identifizieren Sicherheitslücken im Quellcode. Dadurch werden Risiken minimiert.

Besonders bei sicherheitskritischen Applikationen, durch die der Zugang zu sensiblen Daten möglich ist, sollten Sie einen Code Review in Betracht ziehen. Als Ergebnis erhalten Sie einen Bericht, der die im Quellcode analysierten Schwachstellen nach Kritikalität auflistet, sowie detaillierte Vorschläge zu deren Behebung.

Unsere Verfahren

Je nach Applikation verwenden wir statische oder manuelle Analyseverfahren. Dabei betrachten wir wahlweise einen Teilbereich oder Ihre komplette Applikation. Wir überprüfen die Einhaltung von anerkannten Secure Coding Guidelines und Best Practices. Unsere Verfahren unterstützen PHP, Java, C/C++, Bash, Perl, SQL, JavaScript und Python.

Statische Analyse

Beim statischen Analyseverfahren werden automatisierte Tools eingesetzt, um Schwachstellen zu identifizieren. Dabei wird der Quellcode der Applikation überprüft, ohne diese auszuführen. Als Ergebnis erhalten Sie den aus dem Analysetool erstellten Bericht.

Manuelle Analyse

Rein statische Analyseverfahren stoßen an ihre Grenzen, wenn Fehler auf Businesslogik beruhen. An dieser Stelle greift das dynamische Analyseverfahren durch einen unserer Experten. Die auf Tools gestützte manuelle Analyse identifiziert die kritischen Bereiche. Die Durchführung wird, sofern dies möglich ist, während der Ausführung der Applikation vorgenommen. Anschließend findet eine manuelle Überprüfung und Auswertung der gefundenen Schwachstellen durch einen unserer Experten statt.

Preis/Umfang

Der Umfang dieser Leistung wird individuell bestimmt. Er ist beispielsweise abhängig vom jeweiligen Untersuchungsobjekt. Kontaktieren Sie uns! Gerne erstellen wir ein individuelles Angebot.

Unsere Empfehlung für Sie

Ein ganzheitlicher Code Review kombiniert die statische und manuelle Analyse. Die Überprüfung der Ergebnisse durch einen Experten ist unabdingbar, um eine reale Einschätzung geben zu können. Wir suchen gezielt nach Fehlern in der Applikations- und Businesslogik, indem wir uns auf die typischen Schwachstellen wie Injection, Directory-Traversal, Buffer Overflow, Privilege Escalation etc. fokussieren. Ebenso analysieren wir die eingesetzten Kryptographiemethoden und überprüfen das Exception-Handling. Fehler in der Anwendung von Kontrollstrukturen lassen sich bei der umfangreichen Prüfung ebenfalls entdecken.

Code Review gemäß PCI DSS

Laut PCI DSS Anforderung 6.3.2 muss mittels einem Code Review ein benutzerdefinierter Code, der von intern und extern erreichbar ist, auf Verwundbarkeit überprüft werden.

Mit starkem Partner usd

Experten kennen die usd AG als einen der führenden Anbieter von technischen Sicherheitsanalysen in Deutschland. Das Sicherheitsteam der usd AG führt jährlich tausende automatisierte Schwachstellen-Scans sowie hunderte manuelle Pentests von IT-Systemen und Anwendungen durch. Die Sicherheitsexperten der usd AG sind dem Code of Ethics des EC-Councils verpflichtet, verfügen über zahlreiche Sicherheitszertifizierungen und umfangreiche Erfahrungen aus internationalen Projekten. Die usd AG ist eines der wenigen deutschen Unternehmen, das durch das PCI Security Standards Council (PCI SSC) autorisiert ist, europaweit Sicherheitsprüfungen gemäß den Standards PCI DSS, PCI PA-DSS, PCI P2PE und PCI 3DS durchzuführen.

Dieses Produktblatt hat Gültigkeit, sofern keine aktuellere Version veröffentlicht wurde. *Erstellungsdatum Produktblatt 25.05.2018*

usd AG
Frankfurter Straße 233, Haus C1 | 63263 Neu-Isenburg
www.usd.de

Sprechen Sie uns bei Fragen und Interesse gerne an.
Telefon: +49 6102 8631-190 | E-Mail: vertrieb@usd.de