Die Open Source-Bestie mit einem effizienten Programm für Anwendungssicherheitsprüfungen bändigen

4. Mai 2017 | Von David Marshak

Nette Angriffe mit akuter Auswirkung auf die Prüfeffizienz Ihrer Anwendungssicherheit

Es ist wieder so weit: Ein weiterer Angriff mit einem netten Namen macht die Runde. Über den Angriff, der gefährlicher als ein Ghost, POODLE, FREAK, Heartbleed, Shellshock oder die anderen mehr als 6.000 Angriffe ist, die jedes Jahr auftauchen, wissen wir immerhin zwei Dinge:

1. Er wird wahrscheinlich über eine verwundbare Open Source-Komponente angreifen.
2. Es ist sehr wahrscheinlich, dass Sie die Open Source-Komponente in Ihren Anwendungen finden.

Bewältigung der Open Source-Herausforderung

Sollten Sie Ihre Entwickler davon abhalten, Open Source zu verwenden? Das können Sie nicht, zumindest nicht, wenn Sie wollen, dass sie produktiv sind. Tatsächlich ist immer mehr Software auf Open Source-Komponenten als je zuvor angewiesen. Der Forrester-Bericht mit dem Titel ‘Secure Applications at the Speed of DevOps’ besagt, dass ‘etwa 80 bis 90 Prozent des Codes von modernen Anwendungen aus Open Source-Komponenten stammen.’

Offensichtlich soll Open Source bleiben. Um sich selbst zu schützen, müssen Sie Ihren Code proaktiv testen, um sicherzustellen, dass Sie keine verwundbaren Bibliotheken haben. Und da es sehr wahrscheinlich ist, dass Ihre Organisation in gewisser Weise verwundbar ist, sollten Sie sich auf zwei spezifische Erfolgsfaktoren konzentrieren.

Erfolgsfaktor 1: Open Source-Tests in DevOps integrieren

Das Wichtigste, auf das Sie sich konzentrieren sollten, sind die Open Source-Pakete Ihrer Entwickler und insbesondere solche mit Schwachstellen, die ausgenutzt werden können. Es ist extrem wichtig, dass diese Überprüfung in der Entwicklungsphase so früh wie möglich und kontinuierlich durchgeführt wird, da sich die Bedrohungen ständig ändern.

Forrester empfahl ausdrücklich Folgendes: ‘Fügen Sie so früh wie möglich ein Tool zur Analyse der Softwarezusammensetzung (SCA) in das SDLC ein und analysieren Sie weiterhin Anwendungen und auch ältere Anwendungen mit inkonsistenten oder langen Release-Zyklen, um neu entdeckte Schwachstellen aufzuspüren.’ Dazu sollten Sie die Erkennung von Open Source direkt in die von Ihnen bereits implementierten Anwendungssicherheitsüberprüfungen integrieren, und dies zu einem wesentlichen Bestandteil Ihrer DevOps-Strategie machen.

IBM® hat diesen Prozess einfach und transparent gemacht. Mit der Einführung des IBM Application Security Open Source Analyser, Teil von IBM Application Security on Cloud, erfolgt die Identifizierung von Open Source-Komponenten automatisch während der statischen Anwendungssicherheitsprüfung (SAST). Diese Komponenten werden mit einer Liste bekannter Schwachstellen verglichen, und die Ergebnisse werden zurückgegeben. Die Ergebnisse sind nicht nur umsetzbar, sondern beinhalten auch spezifische Korrekturempfehlungen, wie z. B. das Ersetzen durch neuere Versionen der Komponenten. Die Ergebnisse werden direkt in Berichte integriert, die die Identifizierung und Behebung von in Ihrem benutzerdefinierten Code gefundenen Schwachstellen enthalten, wodurch ein nahtloses Anpassungs- und Nutzungsmodell entsteht, das Ihren Erfolg garantiert.