FORSCHUNG KOMPAKT

Schutz vor Cyberangriffen

Rechtschreibprüfung für Entwickler: Automatisierte Erkennung von Sicherheitslücken in Cloudanwendungen

Cloud Computing ist ein Wachstumsmarkt. Aber auch die Cyberangriffe auf Cloud-Softwaresysteme nehmen zu, denn die Anwendungen enthalten oft Sicherheitslücken, die Hacker ausnutzen. Die Software CodeShield des gleichnamigen Unternehmens entdeckt die Schwachstellen und behebt sie automatisiert. CodeShield ist ein Spin-off des Fraunhofer-Instituts für Entwurfstechnik Mechatronik IEM und des Heinz Nixdorf Instituts der Universität Paderborn.

Immer mehr Unternehmen verlagern ihre IT-Infrastruktur in die Cloud, nutzen die Speicher- und Rechenkapazitäten von Clouddiensten oder programmieren Applikationen direkt in der Cloud. Cloudsysteme bieten zahlreiche Vorteile, sie erfordern jedoch auch besondere Sicherheitsvorkehrungen. Viele Firmen sind darauf nicht vorbereitet – mit Folgen für die eigene Datensicherheit. »Oftmals sind es vulnerable Webinterfaces, falsch konfigurierte Schnittstellen oder verwundbare Zugangsprotokolle, die Cyberkriminelle ausnutzen. Dies kann beispielsweise zum Verlust sensibler Daten führen«, weiß Prof. Dr. Eric Bodden, Wissenschaftler am Fraunhofer IEM. Gemeinsam mit Kollegen des Heinz Nixdorf Instituts der Universität Paderborn hat er 2020 das Spin-off CodeShield gestartet und mit CodeShield ein Tool entwickelt, das die Sicherheit von Cloudanwendungen analysiert, bewertet und Schwachstellen behebt. Zu den Gründungsmitgliedern gehören neben Prof. Bodden Manuel Benz, Andreas Dann und Dr. Johannes Späth. Inzwischen zählt das Start-up neun Mitarbeiter. »Ziele von Hackerangriffen sind beispielsweise offen beschreibbare Buckets von Unternehmen. In dieser Art von Cloud-Containern werden Daten in Form von Objekten gespeichert. Die Attacken sind beispielsweise möglich, wenn das Bucket nicht schreibgeschützt ist und so öffentlich darauf zugegriffen werden kann«, erläutert Bodden. Bekannte Opfer dieser Art von Attacken sind die Tradingplattform BHIM und Autoclerc, eine Plattformvermittlung für Zimmer und Hotelgäste. Millionen von User- und Kontodaten gelangten in die Hände der Angreifer.

Sicherheitslücken automatisch erkennen

Mit CodeShield will das Start-up diesem cyberkriminellen Vorgehen einen Riegel vorschieben. Die Software analysiert automatisiert Schwachstellen im Programmcode, wobei der Fokus auf Cloud-Native-Anwendungen liegt, die derzeit einen Boom erleben. Prominente Beispiele für Cloud-Native-Technologien sind Spotify und Netflix. Auch

Kontakt
Janis Eitner | Fraunhofer-Gesellschaft, München | Kommunikation | Telefon +49 89 1205-1333 | presse@zv.fraunhofer.de
Kirsten Harting-Stuke | Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM | Telefon +49 5251 5465107 | Zukunftsmeile 1 | 33102 Paderborn | www.iem.fraunhofer.de | kirsten.harting-stuke@iem.fraunhofer.de

Elektroroller, die seit einiger Zeit zum Straßenbild gehören, sind mit der Cloud verbunden. Die Anwendungen werden direkt beim Cloud Provider gehostet. Auch der Programmcode wird in der Cloud programmiert und liegt dann beispielsweise bei Amazon Web Services, einem bekannten Anbieter dieser Dienste. Die Crux: »Die von den Providern bereitgestellten Schnittstellen und Komponenten, man kann sie als eine Art Baukastensystem beschreiben, sind nicht einfach zu benutzen. Sie versetzen den Programmierer zwar in die Lage, in kurzer Zeit neue Applikationen zu entwickeln. Konfiguriert man die Schnittstellen jedoch falsch, können private Daten ungewollt veröffentlicht werden«, sagt der Informatiker. »CodeShield deckt diese Schwachstellen nicht nur automatisiert in Echtzeit auf, sondern visualisiert sie auch gleichzeitig.« Die Software stellt von der Webseite und App über den Code bis hin zum Datencontainer die komplette Cloud-Infrastruktur in Form von Diagrammen dar, sodass Programmierer mögliche Probleme und Angriffspunkte schnell erkennen. Auch Komponenten wie Open-Source-Bibliotheken von Drittanbietern lassen sich hier einbinden, anzeigen und prüfen.

Fingerprinting-Verfahren und Datenflussanalyse

Um die Sicherheitslücken im Code aufzudecken, nutzt das Werkzeug zum einen das sogenannte Fingerprinting-Verfahren. Dabei laden Bodden und sein Team die Open-Source-Komponenten aus der Cloud herunter und berechnen pro Komponente einen Fingerabdruck, anhand dessen unsicherer Code, wenn er zu einem späteren Zeitpunkt erneut in eine Applikation eingebunden wird, sofort wiedererkannt wird.

Zum anderen analysiert CodeShield den Programmcode, den der Entwickler selber schreibt, in der Cloud ablegt und permanent bearbeitet, um Funktionalitäten anzupassen und zu ergänzen. In diesem Fall führt CodeShield täglich hocheffiziente Datenflussanalysen durch, wobei unter anderem Nutzereingaben im Frontend geprüft werden, um Manipulationen schnell aufzuspüren. Eigens entwickelte Algorithmen ermöglichen die qualitativ hochwertigen Analysen. Die Rate an Falschmeldungen von CodeShield liegt bei unter fünf Prozent. »Viele IT-Sicherheitswerkzeuge liefern Falschmeldungen von 70 bis 80 Prozent, was ein großes Problem für Entwickler ist. Das ist vergleichbar mit einer Rechtschreibprüfung, die in jedem Satz Fehler markiert, wo keine sind«, so der Wissenschaftler. Hiervon hebt sich die CodeShield-Technologie ab, sie entdeckte etwa Sicherheitslücken in der Corona-Warn-App vor deren Launch.

Die CodeShield-Technologie wurde 2019 mit dem Ernst Denert Software Engineering Award ausgezeichnet. CodeShield wird gefördert durch das europäische Förderprogramm START-UP transfer.NRW. CodeShield wird darüber hinaus durch das BMBF-Programm StartUpSecure gefördert.

Abb. 1 Das Gründungsteam von CodeShield: Dr. Johannes Späth, Prof. Dr. Eric Bodden, Manuel Benz, Andreas Dann (von links nach rechts).

© CodeShield GmbH

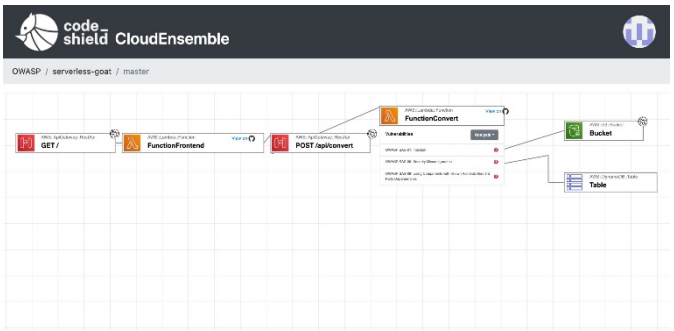

Abb. 2 CodeShield stellt Datenflüsse in einer übersichtlichen Visualisierung dar und ermöglicht hierdurch eine effiziente Einschätzung der Bedrohungslage.

© CodeShield GmbH