Pressemitteilung

Contrast Security-Trendradar zu Anwendungssicherheit: Vor diesen Sicherheitsangriffen auf Webanwendungen sollten sich Unternehmen im Digitalisierungszwang schützen

München, den 15.4.2020 – Contrast Security, führender Anbieter von Sicherheitstechnologien zum serverseitigen Schutz von Webanwendungen und APIs, stellt die momentan relevantesten Anwendungsschwachstellen sowie Angriffstypen vor. Angesichts des Digitalisierungszwangs, unter dem Unternehmen aufgrund der COVID19-Pandemie weltweit stehen, können diese Informationen genutzt werden, um die Sicherheitsbedrohungen von Anwendungen besser zu verstehen, Sicherheitskontrollen anzupassen und den gesamten Sicherheitsstatus zu optimieren.

Als Basis für diese Übersicht dient der AppSec Intelligence Report von Contrast Security, eine Analyse der hauseigenen Contrast Labs über reale Anwendungsangriffe und Schwachstellendaten in den Monaten Januar und Februar 2020.

Entwicklerteams im Homeoffice durch Automatisierung entlasten

Unternehmen, Behörden und Verwaltungen sind durch die Krise gezwungen, analoge Geschäftsmodelle und Prozesse auf den Prüfstand und digitale Angebote bereitzustellen. Zu schnelle, wenig systematische Umsetzungen von Digitalisierungsmaßnahmen bieten eine hohe Risiko-Oberfläche für schädliche Angriffe auf sensible Kundendaten.

„Ressourcenprobleme, knappe Budgets für Security-Themen, mangelndes Problembewusstsein auf Entscheiderebene und unzureichend verzahnte Prozesse zwischen Sicherheitsteam, Entwicklung und Softwarebetrieb finden sich oft in der Praxis. So vielfältig die Gründe für die schlecht ausgeprägte Application-Security-Kultur sind, muss bei aktuellen Entscheidungen zwingend berücksichtigt werden, dass derzeit ganze Entwicklerteams aus dem Homeoffice heraus arbeiten und einem erhöhten Maß an Ablenkung ausgesetzt sind. Cyberkriminelle stehen gerade in Krisenzeiten in den Startlöchern, um jede sich bietende Schwachstelle in der Anwendungssicherheit auszunutzen", betont Daniel Wolf, Regional Director DACH bei Contrast Security.

Auf diese Angriffstypen und Schwachstellen sollten Unternehmen besonders achten:

Trend 1: Große Anzahl ernsthafter Schwachstellen auf Teilmenge von Anwendungen

Die Anzahl der entdeckten Schwachstellen ist von Anwendung zu Anwendung sehr unterschiedlich. Ein Indikator für diesen Trend: Im Durchschnitt wurden pro Anwendung 18 Cross-Site-Scripting (XSS)-Schwachstellen gefunden. Da aber nur 25 Prozent der Anwendungen diese Art von Schwachstellen enthalten, wird deutlich, dass eine Untergruppe von Anwendungen eine große Anzahl von ihnen aufweist. Ebenso existieren durchschnittlich 12 SQL-Injection-Schwachstellen pro Anwendung, aber solche Schwachstellen wurden nur in

9 Prozent der Anwendungen gefunden. Insgesamt hatten 11 Prozent der Anwendungen im Januar und Februar 2020 mehr als 15 Schwachstellen.

Trend 2: Cross-Site-Scripting ist der häufigste Typ von Anwendungsschwachstellen
Im Januar und Februar ist Cross-Site-Scripting **(**XSS) die bei weitem häufigste entdeckte Schwachstelle, die in 25 Prozent der Gesamtanwendungen und 31 Prozent der Java-Anwendungen auftritt.

Trend 3: Die überwiegende Mehrheit der erforschten Angriffe erreicht keine anvisierten Schwachstellen
Die Untersuchung von Contrast Labs ergab, dass das Volumen der Angriffe recht hoch ist, wobei die durchschnittliche Anwendung im Januar und Februar von mehr als 20.000 Angriffen betroffen war. Insgesamt erhielt die große Mehrheit der Anwendungen eingehende Angriffe, die auf Path Traversal, XSS- und SQL-Injection-Schwachstellen abzielten, und fast die Hälfte erlebte Command-Injection-Angriffe.

Trend 4: Angriffe mit Non-Library-Code, die sich auf Command-Injection und SQL-Injection konzentrieren
Während der Großteil des Codes, der in den meisten Anwendungen gefunden wird, aus Open-Source-Bibliotheken stammt, hat der Non-Library-Code laut Daten von Contrast Labs mehr Angriffe erlebt. Die überwiegende Mehrheit dieser Angriffe im Januar und Februar erfolgte in Form von SQL-Injection und Command-Injection.

Trend 5: Angriffe auf Open-Source-Code konzentrierten sich auf wenige CVEs
Für Standardcode aus Open-Source-Bibliotheken katalogisiert die Datenbank der Common Vulnerabilities and Exposures (CVEs) alle bekannten Schwachstellen – momentan sind mehr als 133.000 davon bekannt. Zwar wird die große Mehrheit dieser nie ins Visier genommen, jedoch können sie für ein Grundrauschen sorgen, welches das Auffinden von wirklich gefährlichen CVE-Schwachstellen erschwert. Alle der vier wichtigsten CVEs, die im Januar und Februar 2020 angegriffen wurden, waren Schwachstellen im Apache Struts Open-Source-Framework für Java-Webanwendungen.

Den vollständigen aktuellsten AppSec Intelligence Report finden Sie hier: https://www.contrastsecurity.com/appsec-report-feb20. Weiteren Informationen über die möglichen Schwachstellen, Angriffe und Tools zur Anwendungssicherheit sowie die werden im Contrast Security Influencers Blog regelmäßig veröffentlicht.

Über Contrast Security
Contrast Security ist ein weltweit führender Anbieter von Sicherheitstechnologien, die es Softwareanwendungen ermöglichen, sich eigenständig vor Cyberangriffen zu schützen. Durch den Einsatz von patentierter Instrumentierung sorgt Contrast Security bei der Softwareentwicklung, -ausführung und -produktion dafür, dass Schwachstellen und Datenschutzverletzungen in Unternehmen aufgedeckt und proaktiv verhindert werden können. Der Gartner Report für Application Security Testing 2019 hat Contrast Security als

einziges Unternehmen weltweit als visionär bezeichnet. Weitere Informationen finden Sie unter http://www.contrastsecurity.com

Pressekontakt

Agentur Frische Fische
Liubov Levkina
Tel: +49 (0)30 61675559
E-Mail: liubov.levkina@frische-fische.com