3 SCHRITTE ZUR SICHERUNG DER SOFTWARE-LIEFERKETTE

JEDES GLIED IN DER KETTE STELLT EINEN POTENZIELLES EINFALLSTOR FÜR ANGREIFER DAR. WIR ZEIGEN, WAS SIE DAGEGEN TUN KÖNNEN.

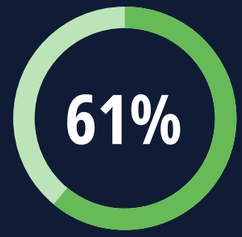


EINFÜHRUNG

Die Software-Lieferkette eines Unternehmens umfasst alle Komponenten, Werkzeuge und Prozesse, die für die Entwicklung und Distribution von Software erforderlich sind. Von Abhängigkeiten von Drittanbietern bis hin zu internen Prozessen stellt jedes Glied in der Kette ein potenzielles Einfallstor für Angreifer dar.

Jüngste Analysen von Gartner zeigen, dass die Zahl der Angriffe auf Code, Tools, Open-Source-Komponenten und Entwicklungsprozesse, bei denen die Unternehmen keine Übersicht haben und nicht geschützt sind, im dreistelligen Prozentbereich steigt. Fast zwei Drittel (61 %) der US-Unternehmen waren laut Gartner in den letzten 12 Monaten vor April 2023 direkt von einem Angriff auf die Software-Lieferkette betroffen.

Die Kosten von Angriffen auf die Software-Lieferkette sind hoch und belaufen sich laut einem Bericht des Cyentia Institute auf durchschnittlich 1,7 Millionen US-Dollar. Dies umfasst sowohl direkte Kosten, wie die Reaktion auf Vorfälle und deren Behebung, als auch indirekte Kosten, wie Produktivitäts- und Umsatzeinbußen.



der US-Unternehmen waren in den 12 Monaten vor April 2023 direkt von einem Angriff auf die Software-Lieferkette betroffen.



der Organisationen, die geschäftskritische Softwarelösungen beziehen, werden bis 2025 SBOMs verlangen, gegenüber einem Anteil von weniger als 20 % im Jahr 2022.



der SCA-Tools werden in der Lage sein, SBOMs zu generieren und zu verifizieren, um eine sichere Nutzung von Open-Source-Software zu ermöglichen, gegenüber 30 % im Jahr 2022.

1. ALLE OPEN-SOURCE-PAKETE BEIM EINTRITT SORGFÄLTIG KURATIEREN

Durch die Umsetzung dreier grundlegender Maßnahmen können Security-Teams ihre Organisationen gegen die missbräuchliche Ausnutzung ihrer Software-Lieferkette schützen.

Die Verwendung von Open-Source-Software ist in der modernen Softwareentwicklung immer weiter verbreitet, und viele Organisationen nutzen eine Vielzahl von Open-Source-Bibliotheken und -Komponenten. OSS bietet viele Vorteile, erhöht aber auch die Komplexität der Software-Lieferkette, da Organisationen diese Pakete sorgfältig verwalten und pflegen müssen, um ihre Sicherheit, Compliance und Qualität zu gewährleisten.

Ein präventiver Sicherheitsansatz anstelle eines reaktiven Ansatzes hilft dabei, Bedrohungen schon frühzeitig im Entwicklungslebenszyklus zu erkennen und zu beheben, bevor die Entwickler mit der Programmierung beginnen. Schwachstellen, die früh im Entwicklungsprozess erkannt werden, können schneller und kostengünstiger behoben werden.

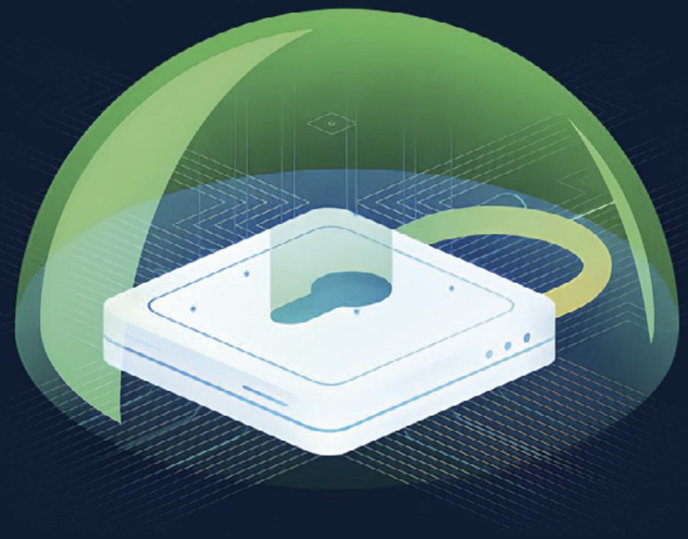


2. SECURITY KONSEQUENT IN JEDE PHASE DES SDLC INTEGRIEREN

Die konsequente Anwendung von Sicherheitsmaßnahmen in jeder Phase des SDLC (Software Development Lifecycle) ist für die Sicherheit der Software-Lieferkette von entscheidender Bedeutung. Dies heißt, dass man sowohl vorbeugende Maßnahmen (Shift-Left-Ansatz) als auch reaktive Methoden (Shift-Right-Ansatz) ergreift.

Durch „Shift Left“ und der Suche nach Bedrohungen schon in frühen Entwicklungsstadien, können Korrekturen vorgenommen werden, sobald sie erforderlich sind, und größere Risiken werden vermieden.

In Kombination mit „Shift Right“ entsteht so eine Software, die von Anfang an mehr Sicherheit bietet und gewährleistet, dass alle Schwachstellen, die nach dem Release auftreten, leicht identifiziert und schnell behoben werden können.



3. NOCH ENGERE ZUSAMMENARBEIT ZWISCHEN DEVOPS UND SECOPS FÖRDERN

Es sollte eigentlich selbstverständlich sein, aber um die Software-Lieferkette wirklich zu stärken, müssen Unternehmen jegliche Reibung zwischen DevOps- und Security-Teams beseitigen und eine kollaborative Workflow-Umgebung schaffen, in der Bedrohungen effektiv identifiziert, priorisiert und behoben werden können.

Für die Bereitstellung sicherer Anwendungen müssen DevOps- und Security-Teams aufeinander abgestimmt sein und zusammenarbeiten. Ermöglicht wird dies durch Software-Supply-Chain-Plattformen, die eine vollständige Überwachung des Software-Entwicklungszyklus (SDLC) bieten und die Umsetzung einheitlicher Security-Policies ermöglichen.



WIE HITACHI VANTARA EINE KONSTANT HOHE SICHERHEIT GEWÄHRLEISTET

Hitachi Vantara, eine hundertprozentige Tochtergesellschaft von Hitachi, Ltd., ist ein Anbieter von Data Storage Systemen für mehr als 6.300 Kunden in über 100 Ländern, darunter über 80 % der Fortune-100-Unternehmen.

Mit 30 Teams, die über mehrere Akquisitionen hinweg entstanden waren und die in isolierten Systemen sowohl on-premise als auch in der Cloud arbeiteten, konnten Entwickler keine großen, gemeinsamen Artefakte über die verschiedenen Standorte hinweg mit der nötigen Geschwindigkeit austauschen, was komplexe Workflows verlangsamte. Und ohne einen einheitlichen Ansatz für die Verwaltung der Software-Lieferkette des Unternehmens war es auch unmöglich, eine konsistente Schutzstrategie gegen Open-Source-Schwachstellen über alle Pipelines hinweg aufrechtzuerhalten.

Hitachi Vantara entschied sich für JFrogs Software Supply Chain Platform als zentrale Schaltzentrale für DevOps, über die Binaries mit Metadaten für alle 14 erforderlichen Pakettypen über verschiedene Standorte hinweg verwaltet und gemeinsam genutzt werden. Drei on-premises JFrog-Plattform-Implementierungen bedienen bis zu 700 Techniker, indem wichtige Repositories für die Lokalisierung an jedem Standort repliziert werden.

Das Ergebnis: Die Built-Zeiten wurden um **25 - 30 % verkürzt.**

Die erhöhte Sicherheit bietet ein Remote-Caching von Open-Source-Komponenten (z. B. von DockerHub) für alle Standorte und schützt die gesamte Hitachi Vantara-Software-Lieferkette vor bekannten Sicherheitslücken.

"Etwas, das automatisch alles in diesem zentralen Repository of Truth scannt, ohne dass eine Anpassung erforderlich ist, ist wirklich extrem mächtig", sagt Larry Grill, DevSecOps Senior Manager von Hitachi Vantara.

ZUSAMMENFASSUNG & NEXT STEPS

Angriffe auf Software-Lieferketten und die sich daraus ergebenden Kosten werden in absehbarer Zukunft weiter steigen. Daher sind die drei Best Practices zur Kuratierung von Open-Source-Paketen an ihrem Eintrittsort, zur konsequenten Integration von Sicherheitsmaßnahmen in den SDLC und zu einer engeren Zusammenarbeit zwischen DevOps und SecOps noch wichtiger als je zuvor.

Verbessern Sie die Sicherheit Ihrer Software Supply Chain mit den Erkenntnissen von über 1.200 Branchenexperten im JFrog Software Supply Chain State of the Union 2024 Report. Meistern Sie den Umgang mit der Flut an Open-Source-Paketen, priorisieren Sie Ihre Remediation Maßnahmen effizient und durchbrechen Sie den Wildwuchs an Sicherheitstools, um die Produktivität Ihrer Entwickler zu steigern. Profitieren Sie von den besten Strategien für die Verwaltung kritischer CVEs und erfahren Sie, wie KI die Sicherheitspraktiken beeinflusst.

Jetzt Bericht herunterladen



ÜBER JFROG

JFrog's Software Supply Chain Platform ist ein Single System of Record, das es Unternehmen ermöglicht, Software schnell und sicher zu erstellen, zu verwalten und zu verteilen und dabei sicherzustellen, dass sie verfügbar, nachvollziehbar und manipulationssicher ist. Die integrierten Security Features helfen auch, Bedrohungen und Schwachstellen zu identifizieren, zu vermeiden und zu beheben. JFrog's hybride, universelle, Multi-Cloud-Plattform ist sowohl als selbstgehosteter als auch als SaaS-Service über die wichtigsten Cloud-Service-Anbieter verfügbar. Millionen von Nutzern und mehr als 7.000 Kunden weltweit, einschließlich der Mehrheit der Fortune 100, verlassen sich auf JFrog-Lösungen, um die digitale Transformation sicher zu bewältigen.



Folgen Sie uns: