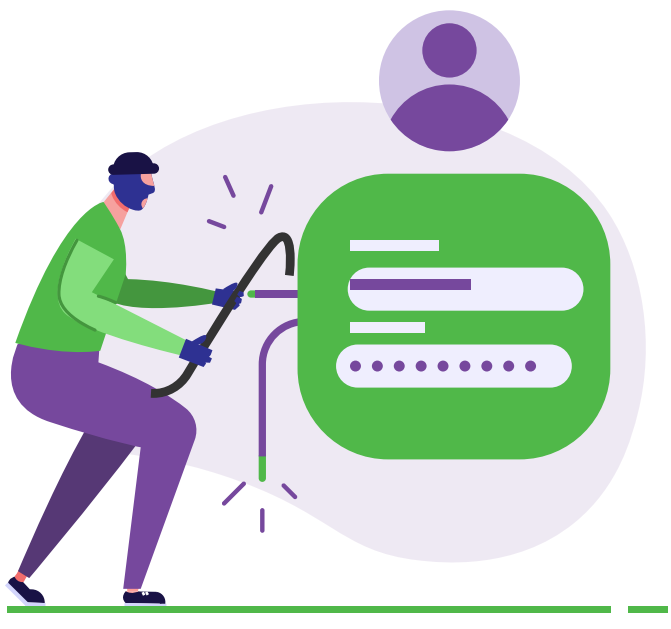
Warum Lieferketten gehackt werden



Ohne automatische Sicherheitsprüfungen im DevOps-Zyklus kann es leicht passieren, dass vielbeschäftigte Developer aus Versehen bösartigen Code, fehlerhafte Richtlinien/Governance oder Sicherheitsverstöße in ihren Code einschleusen. Im Folgenden sind fünf Datenpunkte aufgeführt, die die Auswirkungen des Problems zeigen und wie Sie es in Ihrer eigenen Software verhindern können.

Ungepatchte Schwachstellen

ÜBER 16,000

Die Anzahl neuer Sicherheitslücken, die dem National Institute of Standards and Technology NIST im Jahr 2023 gemeldet und von diesem analysiert wurden.
(bis Juli – https://nvd.nist.gov/general/nvd-dashboard)

2,548

davon werden als kritisch eingestuft. Die meisten können über das Netzwerk ausgenutzt werden, erfordern keine Zugriffsrechte oder Benutzerinteraktion und weisen eine geringe Angriffskomplexität auf.

Die Lösung für dieses Problem ist die ständige Überprüfung des gesamten Quellcodes und der Librarys durch ein System, das auf eine umfassende Datenbank mit dokumentierten Schwachstellen Zugriff hat.

Datenlecks

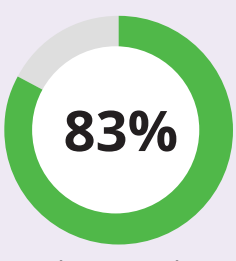
1 MILLIARDE

Die Anzahl der personenbezogenen Daten, größten Datenschutzverletzung der Geschichte durch "Exposed Secrets" offengelegt wurden.
(https://securityboulevard.com/2022/07/the-worlds-largest-breach-root-cause-secrets-in-code/)
Der in einem Blog des Chinese Software Developer Networks (CSDN) veröffentlichte Code „enthielt für jedermann sichtbare unverschlüsselte Zugangsdaten".

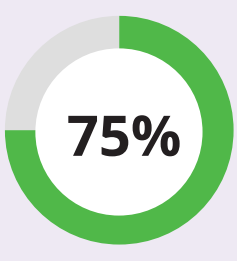
"Die Daten, die im Dark Web zum Verkauf angeboten werden, beinhalten „Namen, Adressen, Personalausweise, Handys, Strafregister und Krankenakten aus einem asiatischen Land".

Vertrauliche Daten, die von Entwicklern leichtfertig offengelegt werden, sind ein gravierendes Problem, das zur Gefahr für sensible Unternehmensdaten, Assets wie Quellcode und sogar das Build-Systems selbst werden kann.

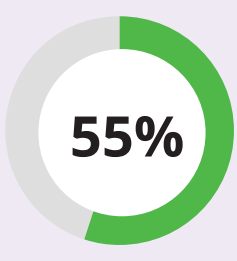
Besorgniserregende Statistiken hierzu sind leicht zu finden. Palo Alto Networks hat auf der Grundlage von Studiendaten ihres Bedrohungsanalyse-Teams Unit 42 herausgefunden, dass:



der Unternehmen in ihren Source-Control-Management-Systemen hartkodierte Anmeldedaten haben.



der Unternehmen über VM-Instanzen mit Nicht-HTTP-Ports verfügen, die über das Internet öffentlich zugänglich sind.



der Unternehmen die Verschlüsselung von AWS EBS-Volume nicht umsetzen.

https://start.paloaltonetworks.com/unit-42-cloud-threat-report-volume-7

Die Art und Weise, wie Developer versehentlich sensible Daten preisgeben, ist bekannt und ein intelligentes Scanning-Tool kann den Quellcode auf diese Probleme hin analysieren und sie erkennen, bevor sie das Unternehmen gefährden.

Produktivität von DevSecOps

6,7 MILLIONEN $

Der Mehrwert an erhöhter betrieblicher Effizienz durch automatisierte Schwachstellen- und Compliance-Workflows mit Open-Source-Software, laut der von Forrester Consulting im Auftrag von JFrog durchgeführten Studie „The Total Economic Impact of the JFrog Platform".
(https://jfrog.com/de/tei/)

Forrester hat herausgefunden, dass die Automatisierung dieser Prozesse die Softwarebereitstellung beschleunigt, die betrieblichen Effizienz erhöht, die Produktivität steigert und die Kosten für das Cloud-Engineering-Management senkt.

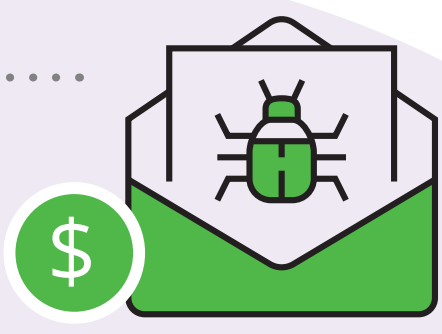
In herkömmlichen DevOps-Systemen wird die Produktivität durch separate Prozesse zur Überprüfung von Schwachstellen und Compliance-Problemen behindert. Die Automatisierung dieser Überprüfungen erhöht die Produktivität des gesamten Entwicklungszyklus, da die Developer weiterhin ihre Arbeit ausführen können.

Der Return on Investment betrug **393%**

Der Preis für das Fehlen von DevSecOps

4,45 MILLIONEN $

Die durchschnittlichen Gesamtkosten einer Datenschutzverletzung im Jahr 2023 laut dem „Cost of a Data Breach Report 2023" von IBM.
(https://www.ibm.com/reports/data-breach)



Sie wollten der Sache auf den Grund gehen und haben 27 Faktoren hinsichtlich ihrer positiven und negativen Auswirkungen auf die Kosten von Datenschutzverletzungen untersucht.

Die größten Einsparungen

($249,278)

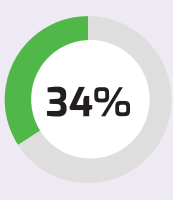
wurden durch einen DevSecOps-Ansatz erzielt.

Dann untersuchten sie die Auswirkungen jener Angriffsziele mit dem höchsten und dem niedrigsten Grad von DevSec-Ops-

Die Einsparungen bei denjenigen mit dem höchsten Grad an DevSecOps-Implementierung beliefen sich auf

1,68 MIO.$

bzw.



von jenen mit dem niedrigsten Grad.

Jedes Mal, wenn es zu einer Datenschutzverletzung kommt, bedeutet dies, dass jemand einen Fehler gemacht hat – und Software-Sicherheitsfehler stehen ganz oben auf der Liste dieser Fehler. Alles, was Sie tun können, um die Development-Security zu erhöhen, wird die Wahrscheinlichkeit von Datenschutzverletzungen verringern.

Kuratierte Open Source

9,074,000

Die Anzahl der in den 12 Monaten vor dem 3. Juli 2023 auf npm erstellten Versionen, dem beliebten Paketmanager für Open-Source-JavaScript-Code, der von Developern auf der ganzen Welt verwendet wird.
(https://blog.sandworm.dev/state-of-npm-2023-the-overview#-heading-packages-created-per-month)

Und das sind nur die neuen Pakete. Es gibt insgesamt 3,3 Millionen Pakete in npm, was Developern nicht gerade dabei hilft, zu entscheiden, welche sicher sind oder welche überhaupt das tun, was sie zu tun vorgeben.

Die Lösung besteht darin, den Developern eine kuratierte Open Source von Librarys zur Verfügung zu stellen, die sie verwenden können und die Code enthalten, der auf Sicherheitsprobleme geprüft wurde. Dennoch sollte der DevOps-Zyklus den gesamten Code auf bekannte und unbekannte Schwachstellen scannen. Das spart nicht nur Zeit bei der Recherche, sondern verhindert auch, dass viel Zeit und Geld für die Behebung von Schwachstellen verschwendet wird, die in die Codebasis importiert wurden. Stellen Sie außerdem sicher, dass eine aktuelle Liste der Importe für den CSO oder einen anderen Verantwortlichen zur Verfügung steht.

Quellen

- **National Vulnerability Database Dashboard:** https://nvd.nist.gov/general/nvd-dashboard
- **The World's Largest Breach. Root cause: Secrets in Code (Security Boulevard):** https://securityboulevard.com/2022/07/the-worlds-largest-breach-root-cause-secrets-in-code/
- **Palo Alto Networks Unit 42 Cloud Threat Report, Volume 7:** https://start.paloaltonetworks.com/unit-42-cloud-threat-report-volume-7
- **Forrester Consulting Report - Total Economic ImpactTM of the JFrog Software Supply Chain Platform:** https://jfrog.com/tei/
- **IBM - Cost of a Data Breach Report 2023:** https://www.ibm.com/reports/data-breach
- **State of Npm 2023 - Packages Created Per Month (Sandworm blog):** https://blog.sandworm.dev/state-of-npm-2023-the-overview#heading-packages-created-per-month

DARKReading

Sponsored By JFrog