

So sichern Sie Ihre Software-Lieferkette



Angriffe auf Software-Lieferketten verzeichnen einen Zuwachs im dreistelligen Prozentbereich, aber nur wenige Unternehmen haben Maßnahmen ergriffen, um die Risiken dieser Angriffe zu bewerten.

61%



der US-Unternehmen waren im 12-Monatszeitraum bis April 2023 direkt von einem Angriff auf die Software-Lieferkette betroffen.

60%



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

90%



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

Source: Gartner

Und dadurch ist die Lieferkette gefährdet



Eingeschränkte Transparenz und Kontrolle

Viele Unternehmen setzen mehrere verschiedene Security-Tools ein, so dass es fast unmöglich ist, einen vollständigen Überblick über die Software-Lieferkette zu erhalten.



Operationelle Komplexität und Overhead

Die tägliche und weltweite Bereitstellung neuer Softwareversionen zu den erwarteten Lieferzeiten stellt eine Herausforderung dar.



Wachsende Angriffsfläche

Bedrohungsakteure nehmen die Software-Lieferkette in jedem Schritt des Development-Lebenszyklus ins Visier, sogar in der Laufzeitumgebung.



Risiken von Open Source Software

Open Source ist leicht zugänglich und wird von Unternehmen jeder Größe und Branche eingesetzt, was sie zu einem direkten Ziel für Bedrohungsakteure macht.



Spannungen zwischen Development und Security Teams

Angriffe auf Software-Lieferketten verzeichnen einen Zuwachs im dreistelligen Prozentbereich, aber nur wenige Unternehmen haben Maßnahmen ergriffen, um die Risiken dieser Angriffe zu bewerten.

Was tun?



Hier sind 6 Schritte zur Sicherung der Software-Lieferkette



1. Kuratieren Sie alle Open-Source-Pakete beim Eintritt in Ihr Unternehmen sorgfältig



2. Scannen Sie Pakete (SCA) auf Open-Source Schwachstellen sowohl im Quellcode als auch in Binärdateien



3. Analysieren Sie proprietären oder Erstanbieter-Code (SAST)



4. Reduzieren Sie Fehlalarme und Schwachstellen durch Kontextanalyse



5. Erkennen Sie potenzielle Sicherheitslücken in Ihren Konfigurationen und bei der Verwendung von Open-Source Libraries im Code



6. Schützen Sie Ihre Geschäftsanwendungen vor kritischen Sicherheitslücken in der Laufzeitumgebung

Transformieren Sie Ihren Ansatz zur Sicherheit der Software-Lieferkette

mit umsetzbaren Erkenntnissen aus dem Report "Software-Lieferkette: Zum Stand der Dinge 2024", der auf Insights von mehr als 1.200 Branchenführern basiert.

Holen Sie sich den Report →

