Die Grundlage von Softwareentwicklung sichern

Angesichts der rasanten Zunahme staatlich geförderter Cyberangriffe und böswilliger Akteure im Internet sind wir bei Google davon überzeugt, dass unsere Produkte und Dienstleistungen sicher sein müssen, damit sie den Menschen helfen. Unser Fokus liegt mehr denn je darauf, Gesellschaft, Wirtschaft, Staat und Verwaltung zu schützen, indem wir unser Fachwissen weitergeben und alle Menschen dabei unterstützen, mit den sich ständig weiterentwickelnden Cyberbedrohungen umzugehen. Wir arbeiten kontinuierlich daran, den Fortschritt der Technik im Bereich Onlinesicherheit voranzutreiben, um unsere Gesellschaft ein Stück weit sicherer zu machen.

Open-Source-Software – Code, der frei verfügbar ist und von allen genutzt, verändert und ausgebaut werden kann – ist die Grundlage des modernen Internets. Die Entwicklung von Open-Source-Software ermöglicht es, durch den freien Austausch von Lösungen besser zusammenzuarbeiten und Innovationen zu beschleunigen. Doch gerade diese Zugänglichkeit zur digitalen Welt macht sie auch anfällig für Sicherheitsbedrohungen.

Die Herausforderung

Open-Source-Software ist Teil unseres Alltags

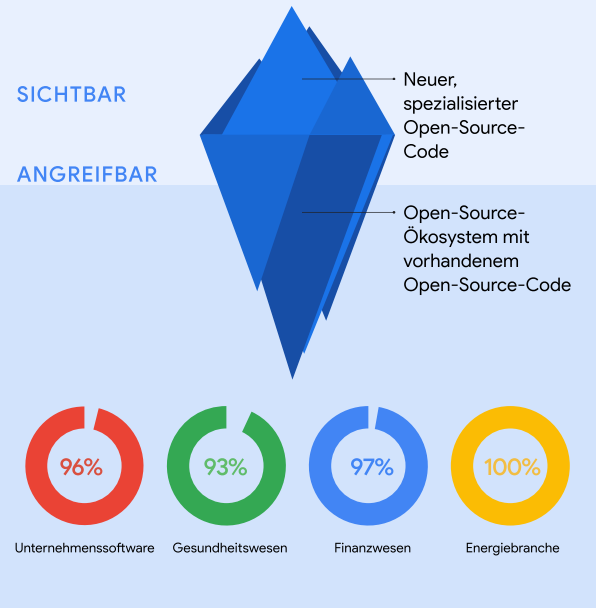
Die Open-Source-Community basiert auf Transparenz und Austausch. Die Entwickler:innen tragen eine enorme Menge an Code zu den meisten Anwendungen bei, die wir heute nutzen. Von medizinischen Geräten bis hin zum Stromnetz – wir verlassen uns täglich auf Open-Source-Software (OSS). Genau das macht sie zu einem bevorzugten Ziel für Cyberangriffe. In den letzten drei Jahren ist die Zahl der Angriffe auf Softwarelieferketten im Vergleich zum Vorjahr um 742 % gestiegen[1].

Open-Source-Software zeichnet sich durch eine äußerst komplexe, verschachtelte Struktur aus. Indirekte Abhängigkeiten, die nicht sofort ersichtlich sind, können Sicherheitslücken bergen und die verschiedenen Ebenen erschweren eine manuelle Erkennung von Schwachstellen. Inzwischen ist es weltweit zu einem dringenden Sicherheitsanliegen geworden, diesen Bereich der Softwareentwicklung zu schützen.

Alle Beteiligten müssen sensibilisiert werden:

- Open-Source-Entwickler:innen benötigen Wissen und Ressourcen, um ihre Projekte abzusichern.
- Unternehmen müssen die Risiken und Schwachstellen der Lieferkette kennen, um Pläne zur Milderung der Folgen im Fall eines Angriffs zu entwickeln.
- Wirtschaft, Staat und Verwaltung müssen zusammenarbeiten, um widerstandsfähige und effektive Sicherheitsstandards zu gewährleisten.[3]

PROZENTSATZ GEWERBLICH GENUTZTER SOFTWARE MIT OPEN-SOURCE-CODE[2]



[2] Quelle: 2022 Synopsys Open Source Security and Risk Analysis Report

Unsere Lösung

Sichere Open-Source-Software für alle

Google stellt sich dieser Herausforderung seit Jahren. Jedes Jahr beteiligt sich über 10 % der Belegschaft von Google an Open-Source-Softwareprojekten. Die Erfahrung zeigt, dass Transparenz tatsächlich die Voraussetzungen für moderne digitale Sicherheit schaffen kann. Offene Ansätze stellen sicher, dass die neuesten Innovationen schnell übernommen werden und mehr Menschen potenzielle Onlinebedrohungen abwenden können. Um aber den Wert von Open Source voll auszuschöpfen und mehr Sicherheit für alle zu schaffen, bedarf es stärkerer öffentlich-privater Partnerschaften und dynamischer politischer Rahmenbedingungen.

- Wir entwickeln zukunftsweisende Sicherheitstools und Frameworks, wie die Supply Chain Levels for Software Artifacts (SLSA)[4,5], die der gesamten Community Nutzen bringen.
- Dazu gehört auch der Graph for Understanding Artifact Composition (GUAC), der Software-Sicherheitsinformationen aus verschiedenen Quellen in einer einzigen abfragbaren Datenbank zusammenführt. Mit GUAC werden wir Sicherheitsinformationen allgemein verfügbar machen, sodass diese jedem Unternehmen frei zugänglich und nutzbringend zur Verfügung stehen.

Unsere Ziele:

- 100 Millionen US-Dollar in Open-Source-Sicherheit, Führungsrollen in der Open Source Security Foundation und in die direkte Zusammenarbeit mit Entwickler:innen investieren.
- Entwicklung von praxistauglichen Sicherheitsstandards, Anleitungen, kostenlosen Tools und Best Practices, die wir auch intern verwenden und mit der gesamten Open-Source-Community teilen.
- Frühzeitige Erkennung von Bedrohungen und automatisiertes Triaging vorantreiben sowie Lösungen finden, wie Schutzfunktionen in den ersten Entwicklungsstadien eingebaut werden können.
- Tools automatisieren, um Sicherheitslösungen für Unternehmen kostenlos und für alle zugänglich zu machen.

Anwendungen

Google OSS Fuzz
Unsere Antwort auf den Heartbleed-Bug

Der Heartbleed-Bug war eine schwerwiegende Open-Source-Schwachstelle, die so gut wie alle Internetnutzer:innen hätte betreffen können. Im Jahr 2014 wurden bei einem Cyberangriff die Namen, Adressen, Geburtsdaten, Telefonnummern und Sozialversicherungsnummern von etwa 4,5 Millionen Patient:innen aus der Datenbank eines der größten US-Krankenhäuser gestohlen.

Als Reaktion darauf startete Google die kostenlose Open-Source-Initiative OSS-Fuzz. Fuzzing-Tests lokalisieren unbekannte Sicherheitslücken innerhalb von Minuten, während manuelle Tests dagegen Monate in Anspruch nehmen können. Zugleich hat Google in den Aufbau von Infrastruktur investiert, in der Hunderte Open-Source-Projekte automatisch getestet werden können. Mit OSS-Fuzz werden jetzt regelmäßige Code-Scans durchgeführt und ständig Innovationen entwickelt, um weitere Cyberbedrohungen zu finden.

Über 800 bedeutende Open-Source-Projekte werden von Fuzzing-Tests in sechs Sprachen gescannt.

Unsere Meilensteine und Investitionen in die Branche

2020 – AUGUST
Beitritt zur Open Source Security Foundation (OpenSSF), um die Sicherheit von Open-Source-Software zu verbessern.

2021 – JUNI
Veröffentlichung von SLSA mit OpenSSF. Das interne Sicherheits-Framework von Google diente als Grundlage, damit alle sichere Software entwickeln können.

AUGUST
Bereitstellung von 100 Millionen US-Dollar zur Verbesserung und Sicherung von Open-Source-Software. Ein Schwerpunkt der Initiative sind Partnerschaften mit Entwickler:innen mit dem Ziel, Schwachstellen zu finden und zu beheben.

2022 – MAI
Ankündigung der „Open Source Maintenance Crew“ von Google während des DC Summits: Ein Team von Vollzeitentwickler:innen, das direkt mit Open-Source-Projekten zusammenarbeitet, um deren Sicherheit zu verbessern.

MAI
Ankündigung von Assured Open-Source-Software. Der Service ermöglicht die Integration der gleichen vertrauenswürdigen Open-Source-Pakete, die Google in Entwickler-Workflows verwendet.

Sicherheitsempfehlungen von Google für öffentliche und private Organisationen

- Implementation von SLSA, um die Sicherheit der Software-Lieferkette zu erhöhen
- Kryptografische Signierung und Verifizierung der Authentizität von Software mittels Sigstore
- Automatisierung von Erkennung, Tracking und Triage von Schwachstellen mit OSS-Fuzz und OSV.dev
- Nutzung von Scorecards, um das Sicherheitsrisiko von Abhängigkeiten automatisch zu bewerten

Unser Ansatz

Jede Software ist nur so sicher wie ihr schwächstes Glied. Wir investieren unser Fachwissen und unsere finanziellen Ressourcen in die Verbesserung der Sicherheit des gesamten Open-Source-Systems. So können unsere Entwicklungs- und Sicherheits-Teams noch mehr öffentliche und private Organisationen schützen:

Unsere Teams prüfen jede Phase des Produktlebenszyklus – so werden Schwachstellen kontinuierlich gescannt, analysiert und mit Fuzzing getestet.

Wir setzen uns für ein offenes Internet ein, indem wir unser Wissen mit der Entwickler-Community teilen. So leisten wir unseren Beitrag zu mehr Onlinesicherheit für alle.

Wir bereiten uns auch auf zukünftige Sicherheitsprobleme vor, indem wir komplexe Bedrohungen erkennen, innovative automatisierte Tools bereitstellen und stets auf neue Entwicklungen reagieren.

Für sichere Open-Source-Software zu sorgen, ist eine gemeinsame Verantwortung. Unser Ziel ist eine kontinuierliche Zusammenarbeit an diesem dringenden und wichtigen Problem. g.co/security/gosst

Quellen: 1. 2022 State of the Software Supply Chain. 2. 2022 Synopsys Open Source Security and Risk Analysis Report. 3. CISA Goes on Tour to Get Feedback on Cyber Incident Reporting Rules. 4. Wissenstransfer (d. h. die Veröffentlichung von SLSA, die Begleitung von OpenSSF) bedeutet, dass alle, die Software herstellen, von der Erfahrung und den bewährten Sicherheitspraktiken von Google profitieren können. 5. SLSA ist ein Sicherheits-Framework, das Organisationen helfen kann, die Sicherheit ihres Softwareentwicklungsprozesses zu verbessern. Es hilft dabei, die Anforderungen des Secure Software Development Framework zu erfüllen. Diese wurden von der US-Regierung als Reaktion auf die Executive Order zur Cybersicherheit festgelegt. Daraus folgt, dass Organisationen bei der Einhaltung der US-Bundesrichtlinien unterstützt werden, um Software für alle sicherer zu machen.