TANIUM

Tanium Software Bill of Materials (SBOM)

Eine kritische Komponente für die Sicherheit der Software-Lieferkette

TANIUM

Tanium Software Bill of Materials (SBOM)

Eine kritische Komponente für die Sicherheit der Software-Lieferkette

Einführung

Eine starke Softwaresicherheit und -integrität war noch nie so wichtig wie heute, da Software die Triebfeder des modernen digitalen Unternehmens ist. In der Öffentlichkeit groß beachtete Schwachstellen, die in den letzten Jahren entdeckt wurden und das Potenzial hatten, zu Angriffen auf die Software nutzende Organisationen zu führen, haben die notwendige Wachsamkeit in Bezug auf das Management von Schwachstellen verdeutlicht.

Das vielleicht dramatischste Beispiel war in jüngster Zeit die Zero-Day-Schwachstelle, die im beliebten Open-Source-Logging-Dienst von Apache entdeckt wurde: **Log4j.** Das Dienstprogramm für die Protokollierung wird von Millionen von Java-Anwendungen verwendet, und der zugrunde liegende Fehler – Log4Shell genannt – kann relativ einfach ausgenutzt werden, um die Remote-Codeausführung auf einem kompromittierten Computer zu ermöglichen. Die Auswirkungen der Schwachstelle waren weltweit spürbar, und Sicherheitsteams mussten sich um das Problem bemühen und es abmildern.

Im November 2022 kündigten Open-Source-Toolkit-Entwickler zwei hochgradige Schwachstellen an, die alle Versionen von OpenSSL 3.0.0 bis 3.0.6 betreffen. OpenSSL ist ein Toolkit, das die sichere Kommunikation in Webservern und Anwendungen unterstützt. Daher ist es eine Schlüsselkomponente des TLS-Protokolls (Transport Layer Security), das für die Sicherheit der über das Internet gesendeten Daten sorgt.

SBOM als Lösung

Eines der effektivsten Tools zum Auffinden und Beheben derartiger Schwachstellen und zum Schutz der Software ist die Software Bill of Materials (SBOM, Software-Stückliste). SBOMs sind formelle, maschinenlesbare Aufzeichnungen. Sie enthalten die Details und Lieferkettenbeziehungen sowie Lizenzen aller verschiedenen Komponenten, die zur Erstellung eines bestimmten Softwareprodukts verwendet werden. Sie sind so konzipiert, dass sie sich organisationsübergreifend teilen lassen und transparenten Einblick in die Softwarekomponenten bieten, die von verschiedenen Akteuren in der Lieferkette bereitgestellt werden.

Viele Softwareanbieter bauen ihre Anwendungen auf der Grundlage von Open-Source- und kommerziellen Softwarekomponenten auf. Eine SBOM führt diese Komponenten auf und liefert ein „Rezept“ davon, wie die Software erstellt wurde.

Beispielsweise umfasst das OpenSSL-Toolkit Abhängigkeiten, die für herkömmliche Schwachstellenscanner schwierig oder in vielen Fällen unmöglich aufzudecken sind. Die Lösung erfordert einen mehrschichtigen Ansatz, der Sicherheitsteams bei der Identifizierung der mit einem Softwarepaket verbundenen Bibliotheken von Drittanbietern unterstützt. Hier kann eine SBOM hilfreich sein.

Das US-Handelsministerium hat angegeben, dass SBOMs den Personen, welche die Software produzieren, kaufen und betreiben, Informationen zur Verfügung stellen, die ihr Verständnis der Lieferkette verbessern. Das bringt mehrere Vorteile, insbesondere das Potenzial, bekannte neu aufgetretene Schwachstellen und Risiken nachzuverfolgen.

Diese Aufzeichnungen bilden ein Datenfundament, auf dem weitere Sicherheitstools, -praktiken und -zusicherungen aufgebaut werden können, so das Handelsministerium, und dienen als Grundlage für einen sich weiterentwickelnden Ansatz zur Softwaretransparenz.

Laut eines Berichts der Linux Foundation Research aus dem Jahr 2022, der auf einer Umfrage unter 412 Organisationen aus der ganzen Welt basiert, hatten 90 % der Organisationen die SBOM-Reise begonnen.

Über die Hälfte der Umfrageteilnehmer gab an, dass ihre Organisationen SBOMs in wenigen, einigen oder vielen Geschäftsbereichen ansprechen, und 23 % antworteten, dass sie SBOMs in nahezu allen Bereichen des Geschäfts ansprechen oder über Standardverfahren verfügen, die die Verwendung von SBOMs einschließen. Insgesamt hatten 76 % der Unternehmen zum Zeitpunkt der Umfrage ein gewisses Maß an SBOM-Bereitschaft.

Die Studie zeigte, dass die Nutzung von Open-Source-Software weit verbreitet ist und dass die Softwaresicherheit eine der obersten Unternehmensprioritäten ist. Angesichts der weltweiten Bemühungen um die Softwaresicherheit haben sich SBOMs zu einem Schlüsselfaktor entwickelt, so die Studie. Es wurde erwartet, dass sich das Wachstum der SBOM-Produktion bzw. des SBOM-Verbrauchs im Jahr 2022 um etwa 66 % beschleunigen wird, was zu einer SBOM-Produktion oder einem SBOM-Verbrauch von 78 % der Organisationen führt.

Die drei wichtigsten Vorteile der SBOM-Erstellung, die von den Umfrageteilnehmern identifiziert wurden, war die Erleichterung für die Entwickler durch SBOMs, Abhängigkeiten zwischen Komponenten einer Anwendung zu verstehen, Komponenten auf Schwachstellen zu überwachen und die Lizenzkonformität zu verwalten.

- **Abhängigkeiten zwischen Komponenten einer Anwendung verstehen**
- **Komponenten auf Schwachstellen überwachen**
- **Lizenz-Compliance verwalten**

Zu berücksichtigende Hauptmerkmale

SBOMs sind ein entscheidender Faktor, um Schwachstellen schnell zu finden und zu beheben, bevor es zu spät ist. Der Grund dafür ist, dass sie tief in die verschiedenen Abhängigkeiten zwischen Softwarekomponenten blicken und die komprimierten Dateien mit Anwendungen für die effektive Risikoverwaltung untersuchen. Es kann Tage oder Wochen dauern, bis ein Softwareanbieter mit seinen Entwicklern bestätigt, ob seine Produkte betroffen sind. Das ist ein zu großes Zeitfenster, in dem Cyberkriminelle Schwachstellen ausnutzen können.

Fast alle SBOM-Lösungen bieten nur Informationen zum Build-Zeitpunkt. Der Build-Zeitpunkt liefert nur Details zu Anwendungen während der Entwicklungsphase und es fehlen aktuelle Informationen zu in der Umgebung eines Unternehmens installierten Anwendungen.

Mit SBOMs wissen Sicherheitsteams genau, wo eine betroffene Komponente in den Anwendungen ihrer Organisationen genutzt wird.

Unternehmen müssen verstehen, dass nicht alle SBOM-Angebote der Anbieter gleich sind. Eine ideale Lösung bietet kritische Echtzeit-Visibilität in die Softwareumgebungen eines Unternehmens und ermöglicht das Treffen fundierterer Entscheidungen zum Risikomanagement.

SBOMs sollten Fragen beantworten können, wie z. B.:

- Wo genau befindet sich ein bestimmtes Softwarepaket?
- Welche Open-Source-Abhängigkeiten hat eine Anwendung?
- Welche Version des Softwarepakets wird ausgeführt?
- Nutzen andere Anwendungen das Softwarepaket?

Zu den wichtigsten Funktionen gehört die Fähigkeit, jede Softwarekomponente bei der Laufzeit zu verstehen, Softwarepakete aufzudecken und aufzuteilen und alle Komponenten zu untersuchen, ohne den Softwareanbieter beauftragen zu müssen.

Eine Laufzeit-SBOM liefert die genauesten, aktuellen Informationen, da sie Details zu den in der Umgebung installierten – nicht nur zu den laufenden – Anwendungen enthält. Das ist eine wichtige Funktion, da es Versionen einer Anwendung geben kann, die ein Entwickler ändert oder verbessert. Mit einer Laufzeit-SBOM erhalten Sie Informationen darüber, was in Ihrer Umgebung jetzt passiert – und nicht Tage oder Wochen später.

SBOMs sollten auch alle Schwachstellen oder Fehlkonfigurationen in den verschiedenen Softwarekomponenten beheben, schnelle Maßnahmen für ein geringeres Risiko in der Lieferkette ergreifen, sogar Anwendungen vollständig über die betroffenen Endpunkte hinweg entfernen und die Investitionen eines Unternehmens in Tools von Drittanbietern optimieren können, indem sie sie mit granularen, genauen und Echtzeit-SBOM-Daten auffüllen.

Fazit

Digitale Unternehmen verlassen sich heute auf Software für die Unterstützung aller Arten von Prozessen. Tatsächlich ist es schwierig, sich ein Unternehmen vorzustellen, das ohne Anwendungen arbeitet. Dauerhaft sichere und zuverlässige Software ist heute für den Erfolg unerlässlich.

Mit Lösungen wie SBOM können Sicherheitsteams in Unternehmen darauf vertrauen, dass sie alle Komplexitäten der Softwarewelt gut im Griff haben und über alle für die Sicherheit der Anwendungen zu behebenden Fehler auf dem Laufenden sind.

Erfahren Sie, wie die XEM-Plattform (Converged Endpoint Management) von Tanium SBOM umsetzen kann, um Ihrem Unternehmen Echtzeit-Transparenz zu bieten – selbst in den komplexesten Softwareumgebungen.

WEITERE INFORMATIONEN