digicert®

Bewertung von Signing-Software & Einführung einer Code-Signing-Richtlinie

Best Practices zur Stärkung der Sicherheit im Release-Prozess für Software – ohne Verlangsamung der CI/CD-Pipeline

KAUFLEITFADEN

Einleitung

Angriffe auf die Softwarelieferkette und andere Formen der Malwareverbreitung können das Kundenvertrauen erschüttern und ihre Behebung kann viel Zeit und Geld kosten. Solche aufsehenerregenden Angriffe können zu Datendiebstahl und Lösegeldforderungen führen und ganze Systeme lahmlegen.

Gleichzeitig ist die Anzahl der angreifbaren Komponenten in der Softwaresicherheit gestiegen. Durch die agile Entwicklung hat sich die Frequenz der Build-Zyklen erhöht. Bereitstellung und Orchestrierung in der Cloud haben den Ort der Softwarebereitstellung verschoben. Nicht zuletzt macht die Verbreitung vernetzter Geräte sichere Firmware-Updates und Kommunikation notwendig.

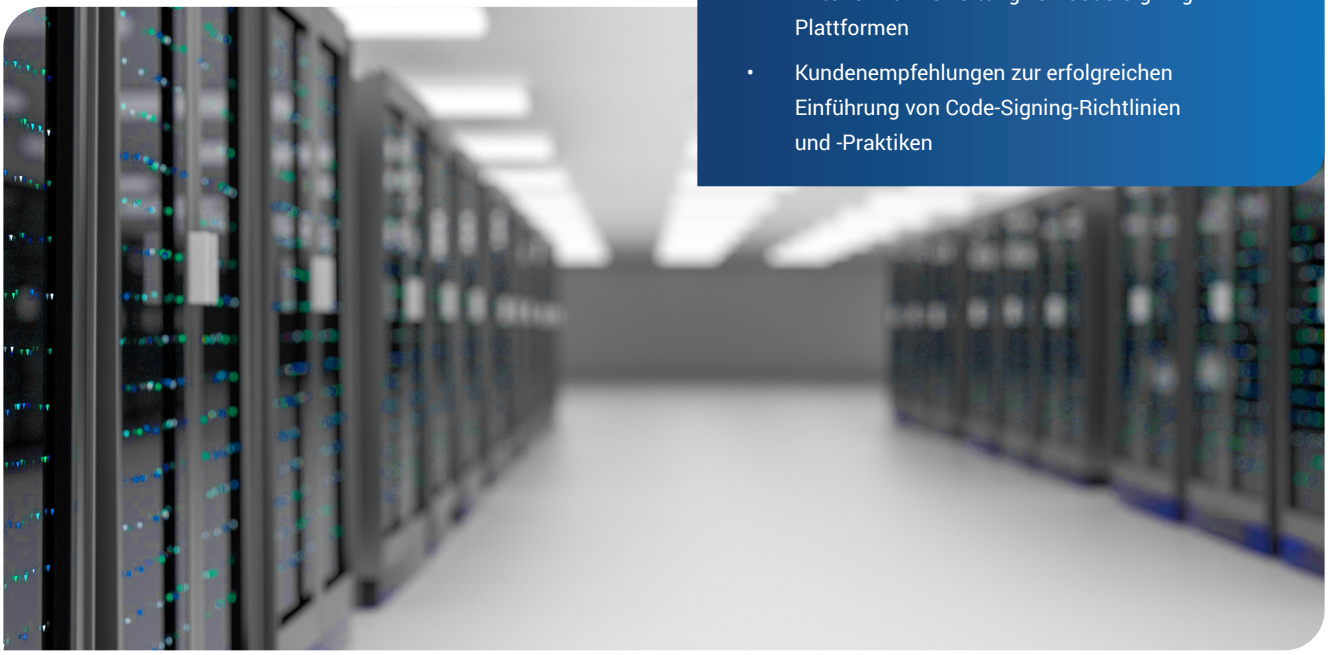
Für Unternehmen heißt das, dass sie nun mehr als je zuvor die Sicherheit ihrer Softwareentwicklungszyklen verbessern müssen. Code-Signing-Software zentralisiert die Verwaltung von Code-Signing-Aktivitäten und führt dadurch zur Standardisierung und Durchsetzung der Code-Signing-Richtlinien und -Praktiken, die Schwachstellen in Software reduzieren.

Lassen Sie sich bei der Bewertung und Implementierung von Code-Signing-Softwarelösungen von den folgenden Kriterien leiten:

1. flexible Konfigurationsmöglichkeiten
2. umfassende Methoden zur Aufbewahrung und Handhabung von Schlüsseln
3. Integration und Automatisierung von Workflows
4. zentralisierte und flexible Berichterstellung
5. Kontrollfunktionen für den Release-Prozess
6. flexible und skalierbare Bereitstellung

Dieser Kaufleitfaden wendet sich an Kunden, die größere Sicherheit bei der Softwareveröffentlichung anstreben. Sie erhalten folgende Hilfestellungen:

- Kriterien zur Bewertung von Code-Signing-Plattformen
- Kundenempfehlungen zur erfolgreichen Einführung von Code-Signing-Richtlinien und -Praktiken



Flexible Konfigurations-möglichkeiten

Die feingranulare Konfigurierbarkeit von Kontostrukturen, Benutzerrollen und Berechtigungen ermöglicht es Unternehmen, Systemfunktionen an ihre individuellen organisatorischen Anforderungen anzupassen.

Zielsetzungen

- Unternehmensweite Zentralisierung der Verwaltung von Signierschlüsseln und Zertifikaten
- Anpassung der Kontostrukturen und Funktionen an Sicherheitsanforderungen
- Beschränkung des Systemzugriffs auf ausgewählte Nutzer
- Beseitigung von Schwachstellen, deren Ausnutzung allein ausreicht, um einen erfolgreichen Angriff auf geschäftskritische Funktionen durchzuführen
- Durchsetzung des Zero-Trust-Prinzips für den Kontozugriff
- Verbesserung der Effizienz bei der Zuweisung und Zurücknahme von Systemprivilegien

Erforderliche Merkmale

- Import von Schlüsseln und Zertifikaten zur Konsolidierung sämtlicher Schlüssel und Zertifikate
- zentrale Verwaltung von Kontokonfiguration und Nutzerstrukturen, einschließlich Einrichtung von ICAs und ICA-Attributen
- granulare Definition von Nutzerrollen und Berechtigungen mit Steuerungen gemäß der Zugriffsrichtlinie
- Quorumberechtigungen für Funktionen, die eine Genehmigung von zwei Parteien erfordern
- Unterstützung von Multifaktor-Authentifizierung
- Profile auf Gruppenebene

Code-Signing-Richtlinie und -Praxis – Tipp 1

Kunden berichteten von unterschiedlichen Vorgehensweisen zur Verbindung ihrer Code-Signing-Richtlinie mit der Nutzung von Code-Signing-Software. Manche gaben an, ein formelles Richtliniendokument erstellt zu haben. Andere setzten auf Leitlinien und Schulungen als Anleitung zu Code-Signing-Praktiken und wieder andere auf den Einsatz von Software zur zentralen Durchsetzung der Richtlinie.

Code-Signing-Richtlinie und -Praxis – Tipp 2

Kunden nannten die folgenden Punkte als die drei wichtigsten Fragen beim Umgang mit Schlüsseln: Wer verwaltet die Schlüssel? Welche Schlüssel werden gespeichert? Wie werden Signierberechtigungen definiert und durchgesetzt?

Umfassende Methoden zur Schlüsselaufbewahrung und Handhabung

Mit feingranularen Steuerungen für die Schlüsselspeicherung und Handhabung können Unternehmen Inkonsistenzen beim Umgang mit Schlüsseln innerhalb des Unternehmens beseitigen und dem Zugriff und der Nutzung durch Unbefugte oder aus Versehen vorbeugen.

Zielsetzungen

- Auswahl des Verfahrens zur Schlüsselspeicherung, das den Sicherheitsanforderungen am besten entspricht (z. B. öffentliche oder private Vertrauenslösung)
- Implementierung strengerer Steuerungen für sensible Projekte
- Zugriffsbeschränkung während der Untersuchung möglicher Bedrohungen
- Getrennte Praktiken der Schlüsselnutzung für Produktions- und Testumgebungen
- Anwendung des für die Anforderungen der Zielsoftware-plattform geeigneten Schlüsselnutzungsmodells
- Reduzierung der Nutzung von Schlüsseln mit veralteten, schwachen oder nicht vorschriftsgemäßen kryptografischen Elementen
- Steigerung der Effizienz und Reduzierung menschlicher Fehler

Erforderliche Merkmale

- Optionen für die Schlüsselspeicherung in Hardware-Sicherheitsmodulen (HSM) oder verschlüsselten Speichern
- Schlüsselzugriffsprofile steuern, wer wann auf welche Schlüssel zugreifen kann
- Online- und Offline-Schlüsselmodi für eine schnelle und fallorientierte Verarbeitung
- Verschiedene Schlüsselarten für Produktion und Test
- Statische, dynamische und rotierende Schlüsselnutzungs-modelle
- Granulare Profilsteuerungen für Schlüsselpaare
- Vorlagen für Zertifikatsprofile und Workflows für die Erzeugung mit einem Klick

Code-Signing-Richtlinie und -Praxis – Tipp 3

Kunden gaben an, dass geschäftliche bzw. gesetzliche Compliance sowie Anforderungen von Kunden und Plattformen die wichtigsten Beweggründe für die Entwicklung einer Code-Signing-Richtlinie und -Praxis waren.

Integration und Automatisierung von Arbeitsabläufen

Integration und Automatisierung verhindern manuelle Fehler, verbessern die Effizienz, fördern eine konsistente Signierpraxis und unterstützen die Markteinführungsziele der agilen Entwicklung.

Zielsetzungen

- Sicherheit, ohne den Entwicklungsprozess zu verlangsamen
- ein höheres Niveau der Unternehmenssicherheit und Compliance durch Verbesserung der Benutzerfreundlichkeit im Vergleich zu manuellen Signierprozessen
- Minimierung des Risikos, dass Quellcode während des Signiervorgangs abgefangen wird

Erforderliche Merkmale

- Verknüpfung mit CI/CD-Pipelines, mit Befehlszeile, Konsole oder API als Optionen
- Unterstützung mehrerer CI/CD-Plattformen
- Zentralisierung und Vorkonfigurierung von Zugriff und Privilegien für Entwickler und Build-Server
- Vorkonfigurierte Zertifikatsvorlagen und Zertifikatserzeugung
- Hash-Signing zur Beseitigung der Notwendigkeit, Quellcode zu übermitteln

Code-Signing-Richtlinie und -Praxis – Tipp 4

Kunden berichteten, dass ihre Code-Signing-Richtlinie, durchgesetzt durch eine Code-Signing-Software und unter Governance einer verantwortlichen Sicherheits- oder IT-Abteilung, sehr effektiv ist.

Code-Signing-Richtlinie und Praxis – Tipp 5

Kunden wiesen darauf hin, dass sowohl Sicherheits- als auch IT-Teams bei der Erstellung der Code-Signing-Richtlinie eine wichtige Rolle spielten. Zu den von den Kunden erwähnten Beteiligten zählten der CISO, das Compliance- und Risikomanagement, DevOps, SecOps, Produktmanagement sowie die Teams für Cybersicherheit und IT.

Steuerung des Release-Prozesses

Steuerungsfunktionen für den Release-Prozess stellen zusätzliche Prüfungen bereit, die dazu beitragen können, der Einschleusung von Malware während des Build-Prozesses vorzubeugen.

Zielsetzungen

- Reduzierung der Gelegenheiten für schädliche Aktivitäten während des Release-Prozesses

Erforderliche Merkmale

- Attribute und Steuerungen für das Release-Zeitfenster zur Definition des Nutzerzugriffs, vorgegebener Zeitfenster und anderer Kriterien zur Beschränkung des Zugriffs auf befugte Benutzer
- Funktionen für den Release-Vergleich, die auf der Basis des Prinzips reproduzierbarer Builds einen „Goldstandard" definieren, der dann als Vergleichsgröße für spätere Builds herangezogen wird

Zentralisierte und flexible Berichterstellung

Zentralisierte Berichterstellung trägt dazu bei, Probleme schneller zu beheben, Audit-Anforderungen zu erfüllen und mögliche Probleme oder Bedrohungen zu identifizieren.

Zielsetzungen

- vollständiger Überblick und Kontrolle über Code-Signing-Aktivitäten
- schnellere Problemlösung, da bekannt ist, wer wann was signiert hat
- Compliance und Audit-Fähigkeit

Erforderliche Merkmale

- Zentralisierte Protokollierung und Berichterstellung zur Unterstützung von Audits und Nachverfolgung
- Berichtsfilter mit Export der Rohdaten oder formatierten Dateitypen

Code-Signing-Richtlinie und -Praxis – Tipp 6

Kunden identifizierten zwei wichtige Maßnahmen: die Standardisierung des Code-Signing-Prozesses, wodurch dieser dokumentiert, nachvollziehbar, verfolgbar und sicher wird, sowie die Gewährleistung der Authentizität der Quelle und der Integrität der Softwarepakete des Unternehmens gegenüber dessen Kunden und Benutzern.

Flexible und skalierbare Bereitstellung

Unternehmen sollten auf Auswahlmöglichkeiten beim Bereitstellungsmodell achten, damit sie innerhalb des Unternehmens verschiedene Bereitstellungsanforderungen erfüllen können, und die Skalierbarkeit von Lösungen im Hinblick auf ihre voraussichtlichen Signieranforderungen prüfen.

Zielsetzungen

- Fähigkeit der Bereitstellung auf die gewünschte Art
- Unterstützung eines großen Volumens und Durchsatzes von Signierungsvorgängen
- effiziente Einrichtung und Skalierbarkeit im Bedarfsfall

Erforderliche Merkmale

- On-Premises-, Cloud- und Hybridoptionen zur umfassenden Unterstützung der Bereitstellungsanforderungen im gesamten Unternehmen
- schnelle und effiziente Einrichtung von ICAs für Abteilungen mit besonderen Anforderungen an die Sicherheitskonfiguration
- containerbasierte Architektur mit Orchestrierung zur schnellen und effizienten Skalierung

Zusammenfassung

Code-Signing-Software kann die Anzahl der angreifbaren Elemente in Veröffentlichungsprozessen für Software signifikant reduzieren. Lösungen auf Enterprise-Niveau, die flexibel konfigurierbar sind und umfassende Funktionen bieten, sind am besten geeignet, um die Ziele, die ein Unternehmen mit seiner Code-Signing-Richtlinie und -Praxis verfolgt, zu erreichen. Diese Lösungen bieten Folgendes:

Schutz

- Beseitigung von Schwachstellen, die zu Diebstahl oder Missbrauch von Schlüsseln führen können
- Verhinderung der Einschleusung von Malware während des Release-Prozesses

Verwaltung

- Förderung von Konsistenz des Sicherheitsstatus und der Compliance über Build-Teams hinweg
- zentralisierte Übersicht und Kontrolle über Code-Signing-Aktivitäten

Produktivität

- Verbesserung der Effizienz und Vermeidung menschlicher Fehler
- Erlangung von Flexibilität für die Reaktion auf veränderte Kryptografie- und Compliance-Anforderungen

Sind Sie bereit für den Einstieg?

Als vertrauenswürdiger Sicherheitspartner bietet DigiCert weltweit eine breite Palette an SSL-, PKI- und IoT-Sicherheitslösungen auf Enterprise-Niveau zum Schutz der geschäftskritischen Daten vieler führender Unternehmen. Sprechen Sie mit unseren Experten über Ihre Anforderungen.

Weitere Informationen erhalten Sie unter der E-Mail-Adresse pki_info@digicert.com oder unter digicert.com/de/software-trust-manager