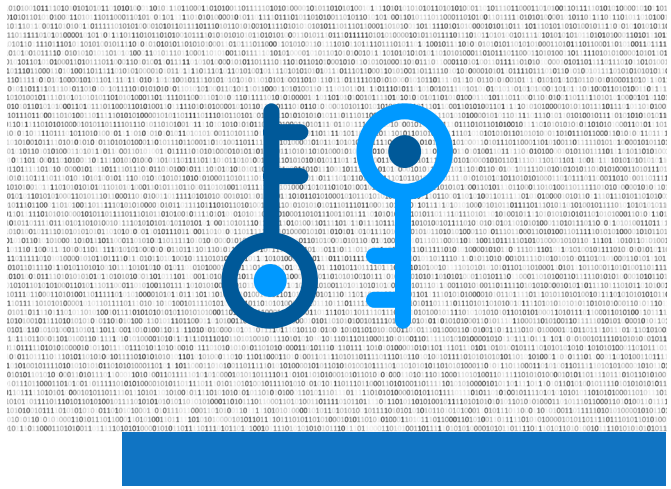
DIE ZEHN WICHTIGSTEN FRAGEN, DIE CISOS ZUM THEMA DEVOPS STELLEN SOLLTEN – ABER NICHT STELLEN

digicert®

01 SICHERE SCHLÜSSELVERWALTUNG

Stellen wir durch konkrete Maßnahmen sicher, dass der Zugriff auf Signaturschlüssel unternehmensweit nachverfolgt und verwaltet wird?

Ohne solche Maßnahmen können gültige Schlüssel in die Hände böswilliger Akteure geraten. Die Folgen wären katastrophal: Cyberkriminelle könnten mit Malware infizierte Software mit diesen Schlüsseln signieren und Ihre Kunden so in der falschen Sicherheit wiegen, die Software sei vertrauenswürdig. Wenn Sie Ihre Kunden schützen, Ihr Ansehen wahren und finanziellen Schaden für Ihr Unternehmen vermeiden wollen, kommen Sie um eine Nachverfolgung sämtlicher Signaturschlüssel und Speicherorte nicht herum.



02 EFFEKTIVE DURCHSETZUNG VON SIGNIERBERECHTIGUNGEN

Wissen wir, wer zum Signieren von Software berechtigt ist und die Nutzung der entsprechenden Signaturschlüssel regeln kann?

Sichere Signiervorgänge setzen strenge Richtlinien zur Schlüsselnutzung voraus. Wird die Einhaltung solcher Richtlinien nicht überwacht und effektiv durchgesetzt, können Personen Softwareprogramme signieren, ohne sich an die internen und gesetzlichen Vorschriften zu halten. Haben Ihre Administratoren aber den Überblick darüber, wie die Schlüssel verwendet werden, können sie entsprechende Zugriffsberechtigungen einrichten und bei missbräuchlicher Verwendung eingreifen.

03 ÜBERWACHUNG DER SCHLÜSSELERZEUGUNG

Wissen wir, welche Code-Signing-Zertifikate mit unseren Signaturschlüsseln ausgestellt werden?

Signierte Software schafft eine Vertrauensbasis zwischen Ihrem Unternehmen und Ihrer Kundschaft. Bedingung dafür ist jedoch, dass Ihre Administratoren im Blick haben, wer mit Signaturschlüsseln Zertifikate ausstellt. Anderenfalls könnte jemand gültige Zertifikate ausstellen und den guten Ruf Ihres Unternehmens ausnutzen, um mit diesen Zertifikaten Malware oder nicht autorisierte Softwareversionen zu signieren.

04 ROLLENVERWALTUNG UND ENTZUG VON ZUGRIFFSBERECHTIGUNGEN

Sind wir in der Lage, Nutzern den Zugriff auf Schlüssel und Zertifikate zu entziehen, wenn ein Nutzer die Rolle wechselt oder unser Unternehmen verlässt?

Scheidet ein Mitarbeiter aus Ihrer Organisation aus, müssen Sie ihm die Signierberechtigungen entziehen. Auch wenn sich ein Mitarbeiter lediglich intern verändert, ist es notwendig, die Berechtigungen an die Signieranforderungen der neuen Rolle anzupassen. Eine effektive Nutzerverwaltung ermöglicht es Ihnen, Signierberechtigungen je nach Rolle, Zuständigkeit oder Projekt festzulegen, damit die richtige Person zur richtigen Zeit Zugriff auf Schlüssel und Zertifikate hat.

05 MULTIFAKTOR-AUTHENTIFIZIERUNG

Ist die Multifaktor-Authentifizierung zum Signieren, Erzeugen von Schlüsselpaaren oder Ausstellen von Zertifikaten für unsere Nutzer obligatorisch?

Das Signieren von Software, das Erzeugen von Schlüsselpaaren und das Ausstellen von Zertifikaten sind kritische Prozesse, die unbedingt abgesichert werden müssen. Schließlich kann es zu Sicherheitsverletzungen kommen, wenn ein nicht autorisierter Nutzer diese Vorgänge ausführt. Mit Malware infizierte Software könnte so signiert und freigegeben werden und Supply-Chain-Angriffe zur Folge haben. Die Multifaktor-Authentifizierung ermöglicht eine verlässliche Identitätsprüfung, damit nur autorisierte Nutzer Zugriff auf Signatur-Tools haben.

06 SICHERHEIT PHYSISCHER SCHLÜSSEL

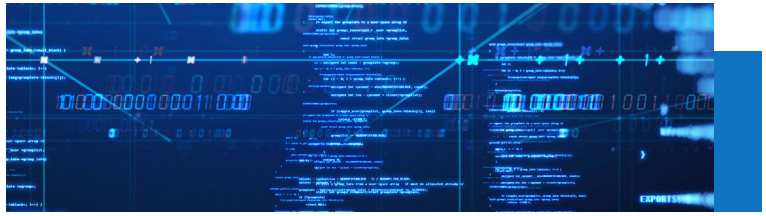
Ist für eine Nachverfolgung und Sicherung von physischen Token, USB-Geräten und Hardware-Sicherheitsmodulen gesorgt?

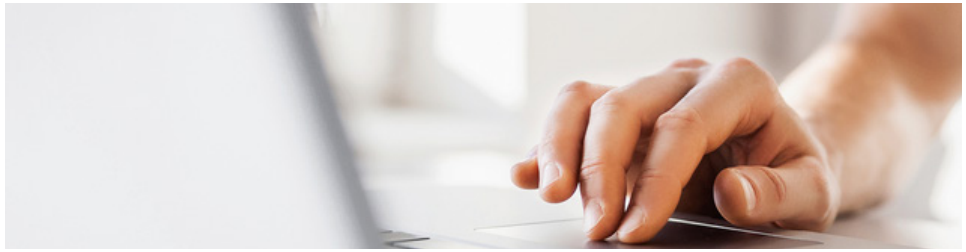
Physische Code-Signing-Schlüssel können ebenso verloren gehen oder in falsche Hände geraten wie Haus- oder Autoschlüssel. Deshalb ist es eine lückenlose Nachverfolgung erforderlich, damit Sie jederzeit wissen, wer die Schlüssel wann verwendet hat und wo sie sich aktuell befinden.

07 VERWENDUNG EINMALIGER SCHLÜSSEL

Teilen unsere Entwickler Code-Signing-Schlüssel?

Schlüssel zu teilen, ist unter DevOps eine weit verbreitete, aber riskante Praxis, die sogar in vielen gängigen Repositorys empfohlen wird. Wenn mehrere Entwickler gemeinsam dieselben Schlüssel verwenden, verlieren Sie jedoch schnell den Überblick darüber, wer was signiert hat und wann. Müssen Sie dann aus irgendeinem Grund ein Zertifikat widerrufen, wird Ihren Anwendern jede Software, die irgendwann mit dem entsprechenden Schlüssel signiert wurde, als unsicher angezeigt.





08 REPRODUZIERBARER CODE

Schreiben wir einen reproduzierbaren Code, um sicherzustellen, dass während des Programmierens keine Malware eingeschleust wird?

Reproduzierbarer Code bedeutet, dass Sie den Schreibvorgang replizieren und verschiedene Versionen gegeneinander abgleichen können. Ist der Binärcode identisch, enthält die Software sehr wahrscheinlich keine Malware, sodass Sie sie guten Gewissens signieren und veröffentlichen können. Dies ist eine der effektivsten Schutzvorkehrungen gegen Supply-Chain-Angriffe, insbesondere wenn Sie mit Open-Source-Software und Bibliotheken aus dritter Hand arbeiten.

09 PROTOKOLLIERUNG VON SIGNIERVORGÄNGEN

Werden alle Signiervorgänge im Unternehmen überwacht und protokolliert?

Sicherheit ist nur nicht für Software-Releases wichtig. Auch interne CI/CD-Prozesse sind ebenso sorgfältig abzusichern wie Software vor der Markteinführung. Daher muss innerhalb der Organisation stets nachvollziehbar sein, wer was zu welchem Zeitpunkt signiert hat, selbst wenn die Software nicht für externe Nutzer bestimmt ist. Dadurch können Sie Zwischenfälle und Missbrauch reduzieren sowie die Einhaltung von Vorschriften besser durchsetzen – beides kommt der Sicherheit in Ihrem Unternehmen zugute.

10 KONSEQUENTES SIGNIEREN OHNE AUSNAHMEN

Wird nachverfolgt, ob Code und Software-Releases überhaupt signiert werden?

Signierte Software signalisiert Ihren Partnern und Kunden, dass sie sich auf die Integrität Ihres Produkts verlassen können. Code und Docker-Container müssen in der Erstellungsphase geprüft und mit sicheren Schlüsseln, auf die nur autorisierte Nutzer zugreifen können, geschützt werden. Die fertige Software ist vor dem Release zu signieren. Die Signatur schützt Ihr Softwareprodukt auf dem Übermittlungsweg, wird durch einen Auditeintrag dokumentiert und beweist Ihrem Partner oder Kunden, dass Sie die Software vor dem Release sorgfältig geprüft haben. Mit verwalteten Code-Signing-Services und automatischen Tools können Signiervorgänge noch weitaus effizienter erledigt werden, ohne Unterbrechung oder Verzögerung Ihrer agilen CI/CD-Prozesse.

Vorsorge ist besser als Nachsorge – das gilt auch für DevOps. Wenn Sie von Beginn an die richtigen Fragen stellen, können Sie Ihre CI/CD-Prozesse und damit die gesamte Lieferkette proaktiv schützen.

Wir helfen Ihnen gern dabei, Sicherheitslücken in Ihren DevOps-Prozessen zu schließen. Wenden Sie sich einfach an uns. PKI_info@digicert.com