BEST PRACTICES FÜR TLS 2022

Mit den fünf Grundprinzipien für die Verwaltung des Zertifikatslebenszyklus reduzieren Sie den administrativen Aufwand und mindern Risiken.

digicert®

DIE PROAKTIVE ZERTIFIKATSVERWALTUNG IST DAS A UND O

Die Anzahl von Websites, Geräten, Systemen, Servern und Benutzern, die eine digitale Identität benötigen und geschützt werden müssen, scheint ins Unermessliche zu steigen. Das führt zu immer mehr und neuen PKI-Anwendungsbereichen und macht eine effektive Verwaltung des Zertifikatslebenszyklus unerlässlich. Vor diesem Hintergrund bieten Best Practices, die die Effizienz und Wirksamkeit von Programmen zur Zertifikatsverwaltung verbessern, das erforderliche Maß an Schutz und die Flexibilität bei der Verschlüsselung, die moderne Unternehmen benötigen. Mit diesem E-Book erhalten Sie ein ausführliches und übersichtliches Framework, um in puncto digitale Sicherheit die Nase vorn zu behalten und konform zu bleiben – heute und in Zukunft.

INHALT

LEGEN SIE EIN VOLLSTÄNDIGES BESTANDSVERZEICHNIS IHRER KRYPTOGRAFISCHEN ASSETS AN

Zertifikatsuche: Das Fundament für Best Practices in PKIs

Wenn Sie keinen Überblick über Ihren Zertifikatsbestand haben, kann Ihr Unternehmen Risiken ausgesetzt sein, von denen Sie noch nicht einmal wissen, dass es sie gibt. Mit einem Zertifikatsuchservice lassen sich Schwachstellen wie nicht genehmigte oder auslaufende Zertifikate, schwache Schlüssel und Hashes sowie veraltete Versionen Ihrer Serversoftware erkennen. Das ist eine der effektivsten Methoden, um potenzielle Ausfälle und Störungen zu vermeiden.

Zum Einstieg empfiehlt es sich, eine Liste aller ausgestellten Zertifikaten von Ihren Zertifizierungsstellen (CAs) anzufordern. Doch wie können Sie sicher sein, dass Sie nichts übersehen haben? Was ist mit internen CAs und Netzwerkgeräten mit Zertifikaten? Ein guter erster Schritt ist, zunächst das Netzwerk nach Zertifikaten zu durchsuchen. Eine Bestandsaufnahme umfasst zudem das Lokalisieren von Geräte- und Benutzerzertifikaten, Schlüsseln und Algorithmen auf den Servern, das Importieren privater Root-Zertifikate und das Identifizieren von Zertifikaten, die über diese Root-Zertifikate ausgestellt wurden, sowie das Einspeisen von Daten aus anderen Erkennungstools.

Zusammenfassung:

Zertifikatsuchservices sind das Fundament eines Best-Practice-Ansatzes beim PKI-Management, denn sie ermöglichen Ihnen, sich einen vollständigen und detaillierten Überblick über alle kryptografischen Assets im Unternehmen zu verschaffen. Such-, Prüf- und andere Erkennungsvorgänge können mit der Regelmäßigkeit ausgeführt werden, die Ihrer Risikominderungsstrategie entspricht. So werden Schwachstellen schnell entdeckt und können zeitnah behoben werden.

SO SCHAFFEN SIE EINE EINHEITLICHE BESTANDSANSICHT:

- Durchsuchen des Netzwerks
- Server- und Dateiprüfungen
- Ermittlung privater Root-Zertifikate
- Importieren von Daten aus Drittanbietertools

ERMITTELN SIE, OB IHR UNTERNEHMEN BEKANNTEN BEDROHUNGEN AUSGESETZT IST

Schützen Sie Ihr Unternehmen vor systemspezifischen Angriffen.

Ihr Inventar sollte auch Angaben zum Betriebssystem (z. B. Windows oder Linux) und zu Anwendungen (wie Apache) enthalten. Prüfen Sie alle Systeme, um sicherzugehen, dass alles auf dem neuesten Stand ist

Dies ist wichtig, damit Ihr Unternehmen vor Exploits wie Heartbleed, POODLE (SSLv3), FREAK, Logjam oder DROWN geschützt ist. Vergessen Sie auch nicht die auf Ihren Webservern ausgeführten Betriebssysteme und die dort installierten Zertifikate.

Zusammenfassung:

Indem Sie die Versionen Ihrer Server, Load-Balancer, Anwendungsframeworks, Cloud-Infrastrukturen, Datenbanken und anderen IT-Komponenten identifizieren, können Sie Ihre Umgebung proaktiv vor Exploits und Schwachstellen schützen.

PRÜFEN SIE CIPHER-SUITEN UND TLS-VERSIONEN AUF SCHWACHSTELLEN

Kontrollieren Sie Cipher-Suiten und TLS/SSL-Versionen.

Diese Elemente sind normalerweise auf den Webservern konfiguriert. Viele TLS/SSL-spezifische Angriffe zielen auf ältere SSL-Versionen (z. B. der POODLE-Angriff auf SSL 3.0) oder ungeschützte Cipher-Suiten (wie der ROBOT-Angriff auf die RSA-Verschlüsselung) ab. Wir empfehlen, die aktuellen Versionen von TLS zu verwenden (einschließlich TLS 1.2 und 1.3).

Was ist eine Cipher-Suite?

Eine Cipher-Suite ist ein auf einem Webserver konfigurierter Algorithmensatz zum Schutz von SSL- oder TLS-Netzwerkverbindungen.

SCHÜTZEN SIE PRIVATE SCHLÜSSEL

Bei der wiederholten Nutzung desselben Schlüssels, genau wie beim Wiederverwenden eines Kennworts, gilt: Die eingesparte Zeit ist das Risiko einfach nicht wert.

Bei einem privaten Schlüssel handelt es sich um eine separate Datei, die bei der Ver- und Entschlüsselung des Datenverkehrs zwischen Ihrem Server und damit verbundenen Clients zum Einsatz kommt. Er wird vom Zertifikatsinhaber während der Signaturanforderung (Certificate Signing Request, CSR) erstellt – nicht von der Zertifizierungsstelle (Certificate Authority, CA), die Ihr Zertifikat ausstellt (und die den privaten Schlüssel auch nicht speichert). Tatsächlich sollte niemand außerhalb Ihres Administratorenteams jemals Zugang dazu haben. Am besten sollte für jedes Zertifikat immer ein neues Schlüsselpaar erstellt werden. Auch CSRs sollten nie wiederverwendet werden, weil dadurch automatisch der private Schlüssel mehrfach genutzt wird.

Weitere wichtige Schritte:

- Suchen Sie nach schwachen Schlüsseln.
- Suchen Sie gezielt nach Schlüsseln, von denen Sie wissen, dass sie kompromittiert wurden.
- Verwenden Sie einen digitalen Tresor (Vault), Token oder Hardware-Sicherheitsmodule (HSM) zur Aufbewahrung von Schlüsseln.

Zusammenfassung:

Aus Zeitgründen kann es verlockend sein, CSRs mehrfach zu nutzen. Doch das führt zur Wiederverwendung von Schlüsseln und zu einem wesentlich höheren Risiko. Stattdessen sollten Sie Zertifikatsanforderungen und -erneuerungen automatisieren, um den manuellen Aufwand bei der Erstellung von CSRs und der Ausstellung von Zertifikaten zu reduzieren.

PRIORISIEREN SIE DIE PROBLEMBEHEBUNG

Aktualisieren oder deaktivieren Sie schwache Schlüssel, Chiffren und Hashes sowie veraltete Assets.

Zertifikate enthalten öffentliche Schlüssel und Signaturen, die anfällig für Angriffe sein könnten. Zertifikate mit Schlüssellängen von weniger als 2048 Bit oder mit älteren Hashing-Algorithmen wie MD5 oder SHA-1 sind auf öffentlichen Webservern nicht mehr erlaubt. Unternehmen können sie aber durchaus noch auf ihren internen Websites finden und sollten die entsprechenden Zertifikate unbedingt sofort aktualisieren.

Noch wichtiger als die Identifizierung von Zertifikaten mit schwachen Schlüsseln oder Hashes ist die Überprüfung der auf Ihren Webservern unterstützten TLS/SSL-Versionen und Cipher-Suiten. Es ist wichtig, stets die aktuellen Versionen von TLS zu aktivieren (einschließlich TLS 1.2 und 1.3). Für Cipher-Suites sollten Sie immer moderne Standards wie AES verwenden. Hier finden Sie eine Liste mit veralteten Cipher-Suiten.

Veraltete und anfällige TLS/SSL-Versionen:

- SSL v2
- TLS 1.0
- SSL v3
- TLS 1.1

BEHALTEN SIE DIE KONTROLLE ÜBER AUSGEGEBENE UND VERTEILT GESPEICHERTE WILDCARD-ZERTIFIKATE

Wildcard-Zertifikate vereinfachen die Zertifikatsausstellung, verursachen jedoch Sicherheitsrisiken.

Wildcard-Zertifikate bieten klare Vorteile für Administratoren, allerdings ist das Absichern mehrerer Domains mit ein und demselben privaten Schlüssel mit ebenso klaren Sicherheitsrisiken verbunden. Wenn ein Schlüssel beispielsweise verloren geht oder gestohlen wird, bietet er dem „Finder" dann Zugang zu jedem Server, für den das entsprechende Zertifikat ausgestellt wurde. Wird derselbe Schlüssel mehrfach im gesamten Netzwerk oder von verschiedenen Abteilungen genutzt, ist die Gefahr groß, dass er plötzlich nicht mehr auffindbar ist. Und dann müssen alle mit diesem Schlüssel verbundenen Zertifikate ersetzt werden. Und sollte das Wildcard-Zertifikat widerrufen werden, muss der zugehörige private Schlüssel auf allen Servern aktualisiert werden, die dieses Zertifikat nutzen. Ein solcher Aktualisierungsvorgang muss für jeden Server einzeln erfolgen, um Betriebsstörungen infolge von Datentransfers zu vermeiden.

Dasselbe gilt, wenn Wildcard-Zertifikate erneuert werden. Zwar sparen Unternehmen durch die Verwendung von Wildcard-Zertifikaten anfangs Zeit und Geld, aber das Erneuern oder Ersetzen dieser Zertifikate kann beträchtlichen Mehraufwand bedeuten.

Zusammenfassung:

Wenn Sie ein Wildcard-Zertifikat verwenden, müssen Sie den zugehörigen privaten Schlüssel unbedingt schützen. Sie können das Risiko, das mit der gemeinsamen oder mehrfachen Nutzung eines privaten Schlüssels für Wildcard-Zertifikate verbunden ist, jedoch minimieren, indem Sie einen separaten privaten Schlüssel für jede Kopie des Wildcard-Zertifikats verwenden und Ihre privaten Schlüssel an einem sicheren Ort aufbewahren. Zudem empfehlen wir, auf allen Servern, auf denen das Wildcard-Zertifikat installiert ist, automatisierte Funktionen zu nutzen. So sparen Sie Zeit, vermeiden Bedienfehler und reduzieren das Risiko, dass ein Schlüssel abhanden kommt.

NUTZEN SIE ANGEMESSENE TLS-ZERTIFIKATSTYPEN

Wählen Sie den richtigen Validierungsgrad für Ihr Unternehmen.

Wenn Sie eine öffentlich zugängliche Website schützen, auf der Benutzerdaten in Formularen oder Anmeldedaten und Kennwörter erfasst werden, sollten Sie ein High-Assurance-Zertifikat verwenden. So schützen Sie Ihre Marke und verhindern Imitationen durch Unbefugte.

Das Zertifikat mit dem höchsten Grad an Marken- und Identitätsschutz ist ein TLS-Zertifikat mit Extended Validation (EV). EV-Zertifikate werden in der Regel von Behörden, internationalen Konzernen, Banken und Finanzdienstleistern verwendet. EV-Zertifikate werden dem anspruchsvollsten Validierungsprozess unterzogen. In 16 Schritten werden unter anderem die Details der anfordernden Person geprüft, darunter Kontaktangaben, Position im Unternehmen und das Beschäftigungsverhältnis. Zudem wird geprüft, wo und unter welcher Nummer das Unternehmen gerichtlich eingetragen ist, und es erfolgt ein Abgleich mit Sperrlisten, eine Überprüfung auf Domain-Betrug sowie die Prüfung des Zustellungsbevollmächtigten.

Das Zertifikat mit der zweithöchsten Validierungsstufe ist das TLS-Zertifikat mit Organization Validation (OV). Für dieses Zertifikat werden der Domain-Inhaber sowie alle Kontaktdetails für das Unternehmen überprüft, unter anderem durch die Bestätigung der Postanschrift und durch einen Telefonanruf zum Nachweis der Zertifikatsanforderung. Darüber hinaus werden Betrugs-, Sperrlisten- und Malwareprüfungen durchgeführt.

Die dritte Option sind TLS-Zertifikate mit Domain Validation (DV). Diese Zertifikate bieten das niedrigste Maß an Identitätsschutz und werden nicht für Websites empfohlen, über die sensible Daten übertragen werden, da sie am leichtesten gefälscht werden können. Private TLS-Zertifikate werden oft für interne Systeme verwendet, doch sie bieten nur Schutz, wenn das private Root-Zertifikat erfolgreich an die Nutzer weitergeleitet wird.

ANWENDUNGSBEREICHE FÜR ZERTIFIKATE:

EXTENDED VALIDATION (EV)

- Unternehmen im Bank- und Finanzdienstleistungssektor
- Fortune-500-Unternehmen
- Global-2000-Unternehmen
- E-Commerce
- Compliance (z. B. HIPAA, PCI)

ORGANIZATION VALIDATION (OV)

- Anmeldebildschirme
- Unternehmenswebsites
- Compliance (z. B. HIPAA, PCI)

DOMAIN VALIDATION (DV)

- Blogs
- Persönliche Websites
- Websites, die keine Transaktionen durchführen und keine Daten erfassen

KONTROLLIEREN SIE VON ANBIETERN BEREITGESTELLTE ZERTIFIKATE

Anbieterzertifikate zeichnen sich durch Benutzerfreundlichkeit, aber nicht durch starke Sicherheit aus.

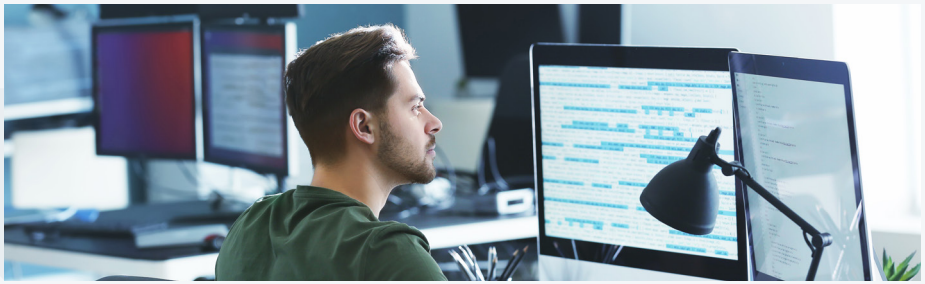
Hierbei handelt es sich um Zertifikate, die von externen Hardwareanbietern ausgestellt werden und auf Geräten vorinstalliert sind. Das Problem ist, dass diese Zertifikate nie für Unternehmensnetzwerke vorgesehen waren. Standardmäßige Anbieterzertifikate sind oft selbstsigniert, abgelaufen oder verwenden schwache Schlüssel. Daher werden sie von Browsern nicht als vertrauenswürdig eingestuft. In vielen Unternehmen gibt es Tausende von Anbieterzertifikaten, ohne dass irgendjemand von ihnen weiß. Jedes dieser Zertifikate sollte entfernt und durch ein vertrauenswürdiges Zertifikat (mindestens ein privates TLS/SSL-Zertifikat) ersetzt werden. Optimieren lässt sich dieser Austauschvorgang mit modernen Automatisierungstools wie APIs oder einer ACME-URL.

STELLEN SIE SICHER, DASS ALLE SYSTEME GEPATCHT SIND

Durch das Patchen der Systeme lassen sich einige der folgenschwersten internetbasierten Angriffe vermeiden.

Mit Patches werden Betriebssysteme, Server, Anwendungsframeworks, Datenbanken und andere Software- und Systemkomponenten aktualisiert, um Schwachstellen im Produkt auszumerzen. Dabei kann es sich zum Beispiel um Windows- oder Linux-Betriebssysteme, Webserver oder Load-Balancer handeln.

Diese Updates können Bedrohungen wie den Heartbleed-Exploit verhindern, der auf eine Sicherheitslücke in der OpenSSL-Bibliothek zurückzuführen war. Jedes System, auf dem die anfällige Version der OpenSSL-Software ausgeführt wurde, war für Angreifer zugänglich: Hacker konnten Kommunikation abfangen oder Daten von den Services und Nutzern stehlen.



SCHÜTZEN SIE DEN ZUGANG ZU ZERTIFIKATS-VERWALTUNGSSYSTEMEN

Nutzen Sie gängige Methoden wie die Zwei-Faktor-Authentifizierung und Single Sign-On (SSO).

Die Zwei-Faktor-Authentifizierung (2FA) oder Multi-Faktor-Authentifizierung (MFA) erfordert, dass sich Benutzer über mehr als eine Methode authentifizieren. Diese Methode nutzt meist etwas, das Ihnen bekannt ist, und etwas, das in Ihrem Besitz ist. Schützen Sie Ihre Plattformen für die Zertifikatsverwaltung durch eine zusätzliche Sicherheitsebene, um zu vermeiden, dass bei der Kontrolle Ihres Zertifikatsbestands Sicherheitsverletzungen auftreten.

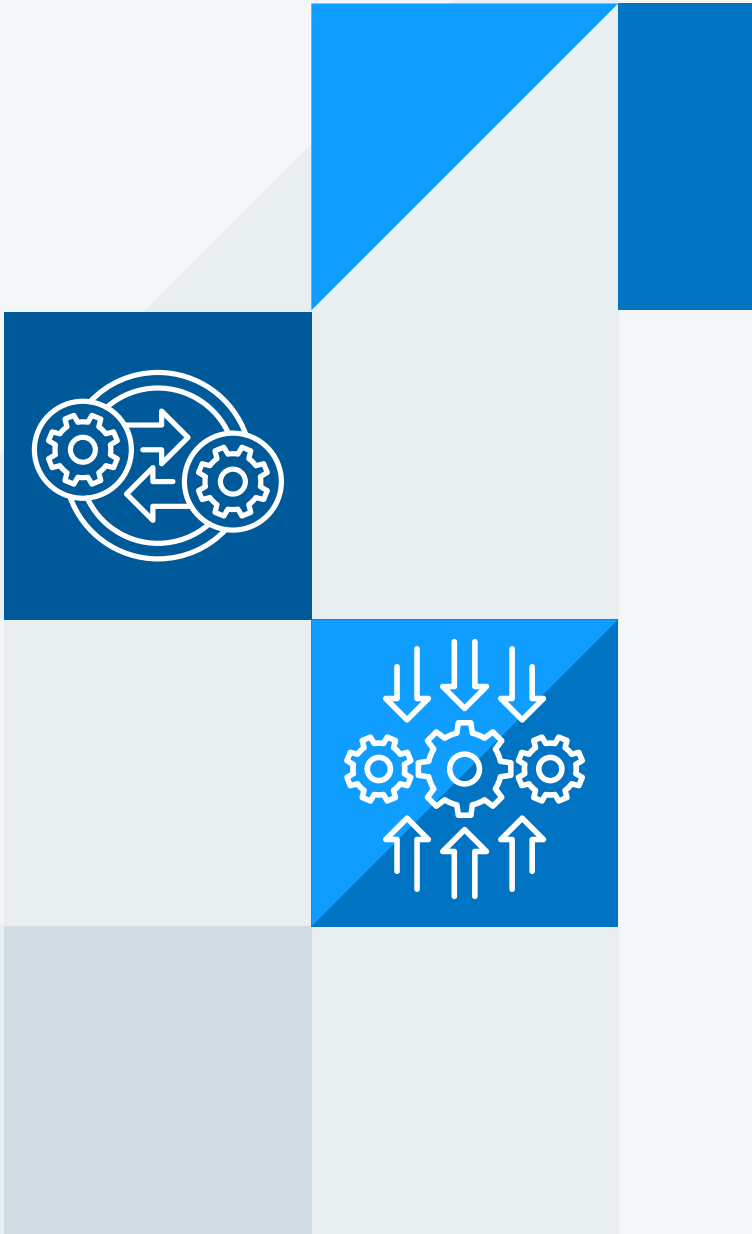
Beispiele für die Zwei-Faktor-Authentifizierung:

- 2FA über ein Mobilgerät
- 2FA über eine Authentifizierungs-App
- 2FA per Token

INTEGRIEREN SIE DIE ZERTIFIKATSVERWALTUNG IN ITSM-SYSTEME

Plattformen für die Zertifikatsverwaltung können in andere Softwarelösungen wie ServiceNow integriert werden, um eine reibungslose Einbindung in IT-Abläufe sicherzustellen.

In komplexeren IT-Umgebungen sollte die Zertifikatsverwaltungsplattform in ein ITSM-Tool (Information Technology Services Management) wie ServiceNow integriert werden, damit Prozesse für die Genehmigung von Zertifikaten eingerichtet werden können, die den Abläufen in Ihrem Unternehmen gerecht werden. So können Mitarbeiter TLS-Zertifikate anfordern, ohne direkten Zugang zum Zertifikatsverwaltungssystem zu besitzen. Zudem lassen sich durch die Nutzung eines ITSM-Systems für Eskalationsprozesse menschliche Fehler reduzieren und die Verfügbarkeit steigern.



ÜBERPRÜFEN SIE WARNMELDUNGEN AUF HANDLUNGSBEDARF

Nutzen Sie Dashboards für die Anzeige von Elementen, die Ihre Aufmerksamkeit erfordern.

Ein zentrales Dashboard zur Nachverfolgung des Status von Elementen, die bei der Zertifikatsuche erfasst wurden, ist ein wichtiger erster Schritt. Doch ebenso wichtig ist es, dass die Daten übersichtlich präsentiert werden und praxistauglich sind.

Ein geeignetes Berichtssystem sollte Folgendes ermöglichen:

- Übersicht über alle Zertifikate und zugehörigen Elemente auf einer zentralen Konsole
- Erstellen, Herunterladen, Planen und Integrieren detaillierter Berichte
- Einfaches Identifizieren konkreter Probleme und Aktionspunkte wie nicht konforme Zertifikate, anstehende Ablaufdaten und Compliance-Verletzungen
- Intuitive Datenvisualisierung und Diagramme, die sich leicht weiterleiten lassen und Maßnahmenempfehlungen enthalten

RICHTEN SIE BENACHRICHTIGUNGS- UND ESKALATIONS-HIERARCHIEN EIN

Definieren und automatisieren Sie Benachrichtigungsmethoden und -ziele.

Durch das Festlegen von Benachrichtigungs- und Eskalationshierarchien verhindern Sie, dass Zertifikate unvorbereitet ablaufen und Sicherheitsverletzungen auftreten. Dabei sollten folgende Angaben für Zertifikatsgruppen gemacht werden:

- Wann Benachrichtigungen ausgelöst werden
- Auf welche Weise Benachrichtigungen übermittelt werden (E-Mail, Warnmeldungen, Slack, ITSM)
- An welche Funktion (Tätigkeitsbereich) Benachrichtigungen gesendet werden
- Schwellenwerte für eine Eskalation

Stellen Sie zudem sicher, dass die in der ausstellenden Zertifizierungsstelle gespeicherten E-Mail-Adressen für Ihre Kontakte auf dem aktuellen Stand sind, damit die erforderlichen Personen alle Benachrichtigungen über Erneuerungen oder Vorfälle erhalten.

LEGEN SIE SCHWELLENWERTE FÜR BENACHRICHTIGUNGEN FEST

Erhalten Sie automatisierte Benachrichtigungen 90, 60 oder 30 Tage vor Ablauf eines Zertifikats.

Abgelaufene Zertifikate müssen nicht sein: Legen Sie fest, dass bestimmte Schwellenwerte (z. B. 90, 60 oder 30 Tage vor dem Ablaufdatum) Benachrichtigungen auslösen. Wir empfehlen, Zertifikate mindestens 15 Tage vor dem Ablaufdatum zu erneuern, um genügend Zeit für Test- und Validierungsprozesse zu haben. Wenn Ihre Prozesse für das Änderungsmanagement besonders aufwendig sind, sind eventuell sogar 32 Tage angemessen.

Für abgelaufene Zertifikate sollten ähnliche Benachrichtigungen auf der Basis von Schwellenwerten eingerichtet werden.

ÜBERWACHEN SIE ZERTIFIKATSTRANSPARENZ-LOGS

Jedes öffentliche Zertifikat, das nicht in einem öffentlichen CT-Log (Zertifikatstransparenz-Log) erfasst ist, wird von Browsern als nicht vertrauenswürdig eingestuft.

Nutzen Sie ein CT-Log-Monitoring-Tool, um nicht konforme Zertifikate schnell zu ermitteln und entsprechende Maßnahmen einzuleiten. CT-Logs dienen als Rechenschaftsnachweis gegenüber Zertifizierungsstellen, wenn diese vertrauenswürdige TLS/SSL-Zertifikate ausstellen. Wenn eine andere Person ein Zertifikat für eine Ihrer Domains ausstellt – ob mit böser Absicht oder unter Missachtung der Richtlinien – erkennt das CT-Log-Monitoring-Tool diese Anomalie und benachrichtigt Sie sofort.

RICHTEN SIE CAA-WARNUNGEN EIN UND VERHINDERN SIE NICHT AUTORISIERTE ZERTIFIKATS-ANFORDERUNGEN

Eine Certificate Authority Authorization (CAA) zur Autorisierung von Zertifizierungsstellen ist ein DNS-Eintrag, der angibt, welche Zertifizierungsstellen (CAs) dazu berechtigt sind, Zertifikate für Ihre Domain auszustellen.

Im Jahr 2017 führte das CA/Browser Forum den „Ballot 187“ ein, der von allen CAs verlangt, die CAA-DNS-Einträge zu überprüfen und sich an alle für die fragliche Domain gefundenen Einträge zu halten. So können Domain-Inhaber festlegen, welche CAs ein Zertifikat für ihre Domain ausstellen dürfen. Der CAA-Eintrag kann auch dazu genutzt werden, dass die verantwortlichen Personen benachrichtigt werden, wenn ein Zertifikat von einer nicht autorisierten CA angefordert wird.

AUTOMATISIEREN SIE DIE ZERTIFIKATSVERWALTUNG ÜBER DEN GESAMTEN LEBENSZYKLUS HINWEG

Straffen Sie die Abläufe für die Erneuerung und Installation von Zertifikaten und die Generierung einer Signaturanforderung (Certificate Signing Request, CSR).

Unternehmen, die eine große Anzahl von Zertifikaten effizient verwalten möchten, müssen die Zertifikatsverwaltung automatisieren. Indem Sie verschiedene manuelle Abläufe der Zertifikatsverwaltung automatisieren, können Sie menschliche Fehler vermeiden und den Zeit- und Ressourcen-aufwand reduzieren – insbesondere bei kürzeren Zertifikatslaufzeiten.

Vorteile der automatisierten Zertifikatsverwaltung:

- Weniger Aufwand bei der Ausstellung, dem Austausch und der Erneuerung von Zertifikaten
- Weniger Ausfälle und Unterbrechungen aufgrund von Bedienfehlern oder Fehlkonfigurationen
- Weniger IT-Supportanfragen dank der automatisierten Bereitstellung
- Schnellere Problembehebung, da nicht konforme Zertifikate leicht ersetzt werden können

NUTZEN SIE AUTOMATISIERUNG FÜR MEHR FLEXIBILITÄT BEI DER VERSCHLÜSSELUNG

Die Post-Quanten-Kryptografie rückt in greifbare Nähe.

Unternehmen können ihre Abläufe zukunftssicher gestalten, indem sie schon heute Automatisierungstools einsetzen. So sind sie für jede branchen- und verschlüsselungstechnische Änderung gewappnet. Die automatisierte Ausstellung und Erneuerung von Zertifikaten spart langfristig Zeit, wenn Sie Zertifikate im Rahmen eines Sicherheitsvorfalls verwalten, nachverfolgen oder ersetzen müssen. Darüber hinaus vereinfachen automatisierte Prozesse das Aktualisieren von Verschlüsselungsalgorithmen.

AUTOMATISIEREN SIE GESCHÄFTSPROZESSE

Definieren Sie Zugriffsregeln, Workflows, Vorlagen und Integrationen.

Die Automatisierung der Zertifikatsverwaltung geht über die einfache Bereitstellung, Installation und Erneuerung von TLS-Zertifikaten hinaus. Automatisierte Geschäftsprozesse straffen das PKI-Management für Ihren gesamten Bestand an Zertifikaten und Schlüsseln, machen Ihren Betrieb effizienter und können Ihr Sicherheitsniveau stärken – nicht zuletzt durch vordefinierte Zugriffsregeln, automatisierte Genehmigungs-, Benachrichtigungs- und Registrierungsabläufe, geschützte Schlüssel und die Integration in Unternehmenssysteme.

NUTZEN SIE APIS FÜR MAßGESCHNEIDERTE INTEGRATIONEN

Integrieren Sie Ihre Plattform für die Zertifikatsverwaltung direkt in Ihre Unternehmenssysteme.

Nutzen Sie API-Integrationen, um die Zertifikatsverwaltung in Ihre Tools, Prozesse und Produkte zu integrieren. Viele Unternehmen nutzen auf diese Weise ihre ITSM-Systeme, um zertifikatsbezogene Abläufe in Änderungsprozesse einzubinden, und Erkennungstools, um ein einheitliches Bestandsverzeichnis anzulegen.

STELLEN SIE ROOT-VERFÜGBARKEIT IM GESAMTEN NETZWERK SICHER

Neuere oder kleinere Zertifizierungsstellen speichern Root-Zertifikate nicht immer im Root-Store des Browsers. Das kann insbesondere bei älteren Browsern zu Problemen führen.

Ihr Unternehmen sollte daher nur Zertifikate von einer bewährten Zertifizierungsstelle mit einer hohen Root-Verfügbarkeit nutzen. Dann stehen die Zertifikate in den Schlüsselspeichern neuer und älterer Browser zur Verfügung und sind mit 99,9 Prozent aller in Unternehmen verwendeten Plattformen und Browser kompatibel.

Unsere Erfahrungen zeigen, dass bestimmte Root-Zertifikate bei neuen Browserversionen nicht berücksichtigt werden, was zu Fehlermeldungen für Websitebesucher führt. Ein solches Problem kann ernsthafte negative Auswirkungen auf Konversionsraten und den Ruf einer Website haben.

NUTZEN SIE CA-UNABHÄNGIGE SUCH- UND IMPORTSERVICES

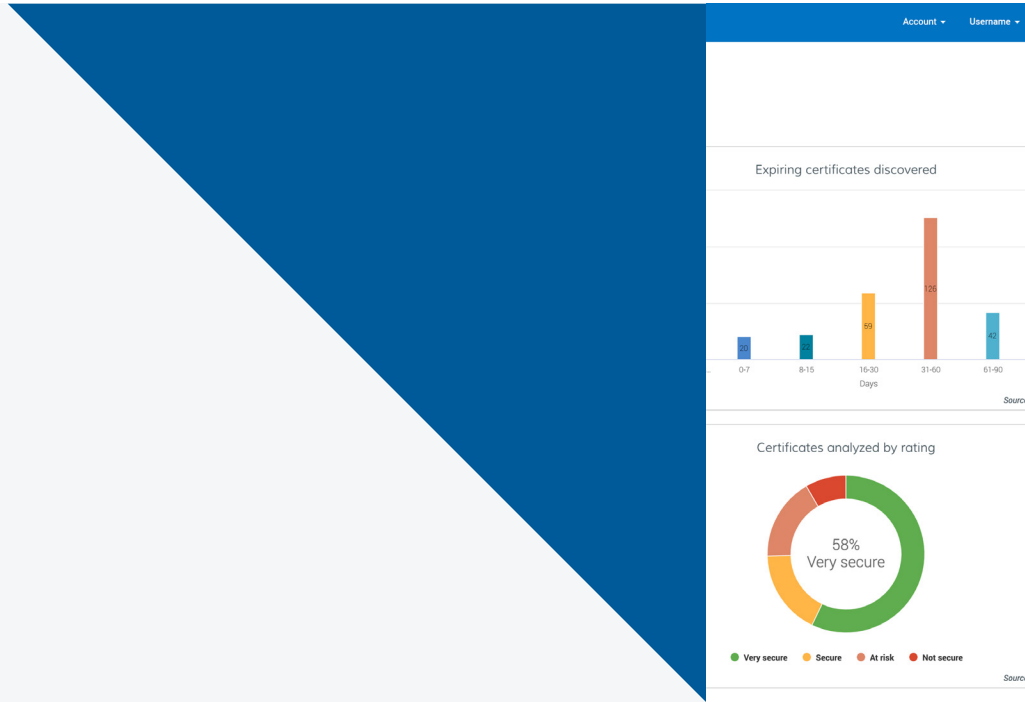
Entscheiden Sie sich für eine Zertifikatsverwaltungsplattform, die mehrere Zertifikate von verschiedenen CAs unterstützt.

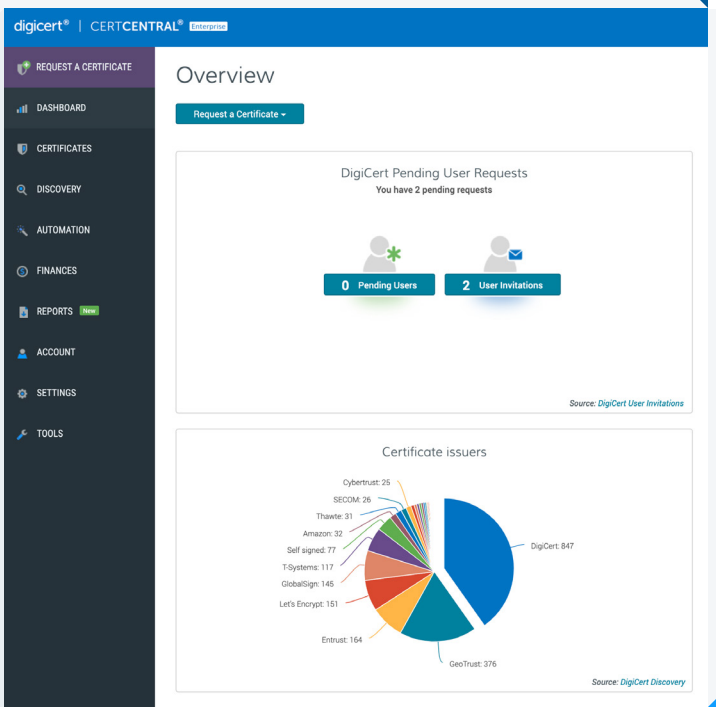
Mit einer CA-unabhängigen Lösung können Sie jedes Zertifikat unabhängig vom Zertifikatstyp und der ausstellenden Zertifizierungsstelle auf einer zentralen Plattform verwalten. Zudem ist wichtig, dass Ihr Erkennungstool private Root-Zertifikate importieren kann, damit auch Zertifikate erkannt werden, die über diese Root-Zertifikate ausgestellt werden. Auf diese Weise erhalten Sie eine umfassende, einheitliche Übersicht über Ihren gesamten Zertifikatsbestand.

FAZIT

Eliminieren Sie aufwendige Abläufe bei der Zertifikatsverwaltung.

Mit den DigiCert-Lösungen für das Lebenszyklusmanagement von Zertifikaten haben Sie alle erforderlichen Funktionen zur Hand, um die fünf Grundprinzipien der Best Practices für TLS zu implementieren: Zertifikatsuche, Verwaltung und Berichte, Benachrichtigungen, Universalität und vor allem die Automatisierung des Zertifikatsbestands. Unser umfassender, intuitiver Ansatz ermöglicht Ihnen, Ihre Zertifikate proaktiv zu verwalten.





ZERTIFIKATE VERWALTEN SICH NICHT VON ALLEINE – WERDEN SIE PROAKTIV!

Straffen Sie die Verwaltung des Zertifikatslebenszyklus und nutzen Sie die gewonnene Zeit für andere geschäftsfördernde Prozesse. Informieren Sie sich, wie die Produkte von DigiCert Ihnen helfen, Best Practices für Zertifikate zu implementieren: Senden Sie eine E-Mail an contactus@digicert.com, um Ihre Anforderungen an die Zertifikatsverwaltung zu besprechen, oder melden Sie sich unter digicert.com/de/tls-ssl/certcentral-tls-ssl-manager für eine ausführliche Demo an.