Zertifikatsverwaltung: Der ultimative Leitfaden

Best Practices für SSL/TLS-Administratoren, die Hunderte oder Tausende von Zertifikaten verwalten

digicert®

Inhaltsverzeichnis

Einleitung

Wer für die Zertifikatsverwaltung verantwortlich ist, kann es sich nicht leisten, auch nur ein einziges Zertifikat durch das Netz rutschen zu lassen. Vergessene oder abgelaufene Zertifikate sind kostspielig und schädlich. Im Durchschnitt kostet jeder Zertifikatsausfall großen Unternehmen 15 Millionen US-Dollar.[1] Hinzu kommen die Auswirkungen auf die Sicherheit und den Markenruf sowie das Risiko eines Vertrauensverlustes bei Kunden mit entsprechendem Absatzrückgang.

Sie sind wahrscheinlich für mehrere Aspekte des Managements Ihrer Public Key Infrastructure (PKI) verantwortlich: die Verwaltung von Zertifikaten, die Einhaltung von Best Practices für SSL und zeitnahe Genehmigungen, um nur einige zu nennen.

Was in dieser Rolle häufig am meisten Kopfzerbrechen bereitet, ist die ständige Sorge, dass es irgendwo im Netzwerk ein Zertifikat gibt, das bei der Zertifikatsuche unentdeckt blieb. Eines Tages wird ein Server ausfallen und Chaos verursachen.

Wäre es nicht praktisch, eine umfassende Checkliste für das Zertifikatsmanagement zu haben? Eine Liste mit den entscheidenden Punkten, damit Sie sich darauf verlassen können, die wichtigsten Aspekte des Zertifikatslebenszyklus auch wirklich im Blick zu haben – die Aspekte, die für Netzwerksicherheit unerlässlich sind.

Da Netzwerke so unterschiedlich komplex sind, kann es keine allgemeingültige Checkliste geben. Es gibt jedoch einige Dinge, um die sich alle Zertifikatsmanager kümmern sollten, damit sie wissen, dass ihre Daten, ihr Unternehmen und ihre Mitarbeiter geschützt sind.

Dieser Leitfaden enthält alles, woran Sie beim Zertifikatsmanagement denken sollten. Er hilft Ihnen, die Kontrolle über alle Bereiche des Zertifikatslebenszyklus zu übernehmen und dabei APIs zu nutzen und Ihr Team zu optimieren.

Übernehmen Sie mit Best Practices die Kontrolle über Ihr PKI-Management

Die einzelnen Komponenten der PKI, von der Zertifizierungsstelle (CA) und der Registrierungsstelle (RA) über Zertifikatsrichtlinien bis hin zum Zertifikatsverwaltungssystem, unter einen Hut zu bekommen, ist nicht immer einfach. Die Bereitstellung von Zertifikaten ist oft einfach, doch um die Sicherheit zu gewährleisten, müssen sie auch richtig bereitgestellt und verwaltet werden.

SSL-Administratoren in großen Unternehmen verwalten Tausende (wenn nicht sogar Millionen) von Zertifikaten. Wie stellen Sie sicher, dass Zertifikate Tag für Tag, Woche für Woche richtig bereitgestellt und verwaltet werden?

Die Kontrolle zu behalten ist die Herausforderung – Best Practices sind die Lösung. Diese Best Practices verschaffen Ihnen einen Überblick, sparen Zeit und erleichtern Ihnen das Leben.

Wer sie befolgt, muss nicht rund um die Uhr an Zertifikate denken, sondern kann sich darauf verlassen, dass sein Netzwerk geschützt ist.

Best Practice: Nutzen Sie eine PKI-Management-Plattform

MPKI-Lösungen (Managed PKI) geben Unternehmen die Möglichkeit, Zertifikate ganz ohne kostspielige interne Zertifizierungsstelle (CA) zu bestellen und zu verwalten. Viele öffentlich vertrauenswürdige CAs bieten eine Managed-PKI-Lösung an und die meisten großen Unternehmen entscheiden sich unter anderem aus Kostengründen dafür.

Mit einer MPKI-Lösung übernimmt eine CA die Verwaltung eines großen Teils der PKI, während weiterhin Zertifikate für die Sicherheit sorgen.

.

[1] „2015 Cost of Failed Trust Report: When Trust Online Breaks, Businesses Lose Customers“, Zugriff 26. Juni 2017, https://www.venafi.com/assets/pdf/wp/Ponemon-When-Trust-Online-Breaks-Businesses-Lose-Customers-white-paper.pdf

Darüber hinaus sollte eine MPKI-Plattform alle Aspekte der Zertifikatsverwaltung vereinfachen – von Ausstellung und Installation bis hin zu Inspektion, Reparatur und Erneuerung.

Insgesamt spart Ihnen eine MPKI Zeit und erleichtert die Verfolgung wichtiger Zertifikatsdetails:

- Ablaufdatum
- SSL-Fehler auf dem Endgerät
- Zertifikatsanfragen von Teammitgliedern
- Widerrufstatus
- Ausstellende CA

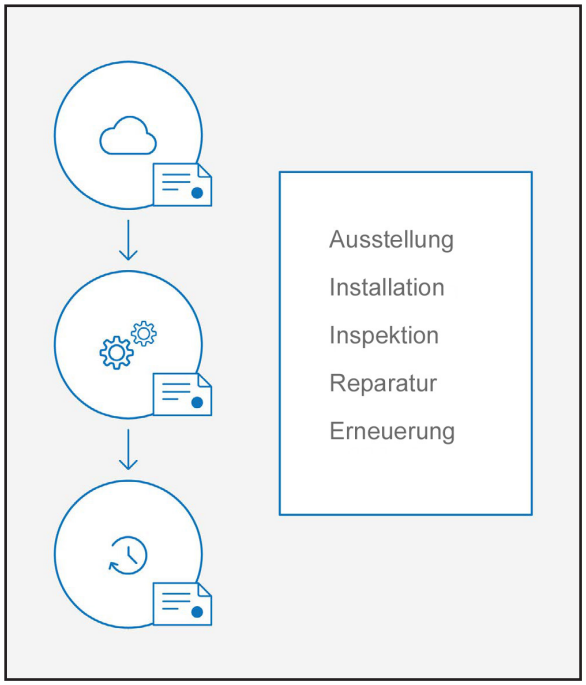
Bis vor wenigen Jahren verwalteten viele Unternehmen Zertifikate noch manuell mithilfe von Tabellen. TechTarget sagt – und Sie wissen das vielleicht aus eigener Erfahrung –, dass dies „zu Fehlern führen kann, wie verlorene, nicht übereinstimmende oder falsch beschriftete Zertifikate".[2]

Mit einer MPKI-Plattform ist es nicht mehr nötig, Zertifikatsdetails über Tabellen zu verfolgen und Anfragen per E-Mail zu jonglieren. Vielmehr werden diese Aufgaben größtenteils automatisiert und das Risiko von menschlichen Fehlern sinkt. Die Zertifikatsverwaltung wird damit einfacher und schneller.

Best Practice: Nutzen Sie Automatisierung über API

APIs ermöglichen eine unternehmensübergreifende Zusammenarbeit und ermöglichen es Entwicklern, bei der Erstellung von Anwendungen verschiedene Technologien zu nutzen. Genauer gesagt, kann eine API die Arbeitslast für IT-Teams verringern, die daran arbeiten, die Zertifikatsverwaltung zu automatisieren und anzupassen.

Eine MPKI-Plattform vereinfacht die Zertifikatsverwaltung



Während für kleinere Unternehmen die Benutzeroberfläche von SSL-Verwaltungstools oft völlig ausreicht, muss sie für große Unternehmen in der Regel angepasst werden. Einige PKI-Verwaltungstools bieten Ihnen Zugriff auf eine API, mit der Sie Funktionen und Workflows anpassen und Prozesse automatisieren können, um eine einfachere Zertifikatsverwaltung zu ermöglichen.

Mit einer API können Sie die SSL-Verwaltung wirklich personalisieren.

[2] R. Shapland, „SSL certificate management: Avoiding costly mistakes." Zugriff 26. Juni 2017, http://searchsecurity.techtarget.com/tip/SSL-certificate-management-Common-mistakes-and-how-to-avoid-them

Ja nach Branche lassen sich Tausende, wenn nicht sogar Millionen von Geräten überwachen. Automatisierung erleichtert Ihnen das Leben und ermöglicht es Ihnen, für Sicherheit zu sorgen, indem Sie menschliche Fehler und durch Zertifikate verursachte Ausfälle reduzieren.

Sie sparen Zeit und können viele Schritte im Lebenszyklus eines SSL-Zertifikats über eine API automatisieren, wie zum Beispiel:

- Anforderung von Zertifikaten
- Genehmigung von Anfragen
- Ablehnung von Anfragen
- Herunterladen von Zertifikaten
- Erneuerung von Zertifikaten
- Widerrufung von Zertifikaten
- Neuausstellung von Zertifikaten

Sich ändernde Branchenstandards und die Verkürzung der Gültigkeitsdauer von Zertifikaten werden dafür sorgen, dass Automatisierung in Zukunft nicht mehr nur eine Option, sondern eine Notwendigkeit sein wird.

Die Verwendung einer API reduziert die Komplexität, die mit der Verwaltung von Zertifikaten aus verschiedenen ausstellenden CAs verbunden ist. Indem Sie den Antragsteller aus dem Prozess nehmen, haben Sie mehr Kontrolle über die Zertifikatsverlängerung. Wenn sich Zertifikate mit 90, 60 oder 30 Tagen Laufzeit automatisch verlängern lassen, müssen Sie sich keine Gedanken mehr darüber machen, ob ein Teammitglied beim richtigen Anbieter bestellen wird oder nicht – die Entscheidung ist bereits getroffen.

APIs eignen sich hervorragend, um durch Automatisierung und eine flexible Zertifikatsverwaltung Zeit zu sparen.

Best Practice: Erkennen Sie, welche Zertifikate vernachlässigt wurden

Zertifikatsmanager machen sich häufig Sorgen darum, nicht richtlinienkonforme und unbekannte Zertifikate zu finden. Die Gründe dafür sind die Skalierung von Zertifikatslandschaften, die Bestellung und Installation von Zertifikaten durch verschiedene Einzelpersonen und der in großen Unternehmen übliche Mitarbeiterwechsel. Das Problem ist, dass man Zertifikate, von denen man nichts weiß, nicht verwalten kann.

Mit einem Inspektionstool für die Zertifikatsuche erhalten Sie einen umfassenden Überblick über Ihre Zertifikate und können genauere Angaben anzeigen, wenn Sie nähere Einzelheiten einsehen müssen. Viele CAs bieten ein Inspektionstool oder einen Agenten an, der Zertifikate entdeckt und die Daten aus jedem Prüfvorgang zusammenfasst. Im Idealfall findet das Tool alle in Ihrem Netzwerk verwendeten Zertifikate, unabhängig von der ausstellenden CA, sodass Sie über alle verwendeten Zertifikate informiert sind. Mit Tools zur Zertifikatsuche vermeiden Sie Fehler, die bei der manuellen Prüfung auftreten, und sparen Zeit bei der Bestandsführung.

Regelmäßige Überprüfungen (wir empfehlen mindestens eine pro Woche) gewährleisten, dass Sie einen vollständigen Überblick über alle verwendeten Zertifikate haben, geben Ihnen mehr Einblick in mögliche Schwachstellen und helfen Ihnen, nicht autorisierte Zertifikate, die Ihre Marke gefährden könnten, zu entdecken. Sobald Sie vergessene oder vernachlässigte Zertifikate finden, können Sie entsprechend eingreifen, um die entstandenen Schwachstellen zu beheben.

Best Practice: Organisieren Sie Ihr Team

Ein wesentlicher Bestandteil der Zertifikatsverwaltung ist das Management der an Ihrer PKI beteiligten Mitarbeiter.

Es ist wichtig, die richtigen Schlüsselpersonen zu identifizieren, sie in Abteilungen oder Teams aufzuteilen, jeder Person die richtigen Zugriffsrechte zuzuteilen und sicherzustellen, dass jeder weiß, wofür er verantwortlich ist und genau über alle Prozesse und Abläufe informiert ist.

Die richtige Aufteilung

Die Verwaltung nationaler oder internationaler Zertifikatsanfragen wird sehr viel einfacher, wenn Sie die mit deren Bearbeitung betrauten Personen in Abteilungen, Einheiten oder Teams unterteilen. Ganz gleich, welche Option Sie wählen, können Sie Anfragen nach Standort, IP-Adresse, internem Team oder einer anderen Klassifizierung aufteilen.

Das ist zwar ein kleiner Schritt, ist jedoch sehr hilfreich, wenn Anfragen mit unvollständigen Angaben eingehen – Sie wissen dann sofort, an wen Sie sich wenden müssen, um die fehlenden Informationen zu erhalten. Außerdem wird es einfacher, den richtigen Ansprechpartner zu finden, wenn ein Zertifikat abgelaufen ist.

Zuweisung von Benutzerrollen

Die Zuweisung von Benutzerrollen für jedes Mitglied Ihres Teams ist wichtig, um Ihre PKI im Griff zu behalten. Wenn jede Person über die richtigen Zugriffsrechte für Verwaltungsplattform verfügt, sorgt dies für eine reibungslosere Zertifikatserneuerung und Überprüfung.

Überlegen Sie sich für jede Person, welche Rolle sie im gesamten Prozess spielt. Ganz gleich, ob es sich um einen regulären Nutzer handelt oder um einen Administrator, der Anfragen genehmigt, stellt die Zuweisung von Benutzerrollen innerhalb der Zertifikatsverwaltungsplattform sicher, dass jeder Beteiligte automatisch über die richtigen Funktionen verfügt. Verringern Sie Ihren Zeitaufwand, indem Sie Benutzern die Möglichkeit geben, Anfragen selbstständig zu stellen, und dann einige damit verbundenen Aufgaben einem anderen fähigen Teammitglied zuteilen.

Es kann vorkommen, dass ein einmaliger Benutzer eine Anfrage stellen muss. In diesem Fall können Sie dem Mitarbeiter Gastzugang gewähren, der nur vorübergehend und begrenzt Zugang ermöglicht. Dies sorgt für zusätzlichen Schutz Ihrer Zertifikate, da Mitarbeiter nur Zugriff auf Informationen haben, wenn es tatsächlich nötig ist.

Mitarbeiter informieren

Sorgen Sie dafür, dass Ihr Team ständig über Prozesse, genutzte Technologien und neue Implementierungen auf dem Laufenden gehalten wird.

Ihre Systemadministratoren und Entwickler benötigen den technischen Hintergrund, um Zertifikate effizient verwalten und bereitstellen zu können. Sie sind ein Team und Sie sollten sich mit den Teammitgliedern absprechen und ihren Rat einholen, wenn es angebracht ist.

Zudem müssen sie über alle Änderungen an Anforderungen oder Richtlinien Bescheid wissen. Sie selbst können sich über Branchentrends und sich ändernde Standards informieren, indem Sie das CA/Browser-Forum sowie den Blog Ihres bevorzugten SSL-Anbieters verfolgen.

Best Practice: Beschleunigen Sie den Genehmigungsprozess

Ein optimierter und schneller Genehmigungsprozess ist ebenfalls wichtig bei der Ausstellung größerer Mengen an Zertifikaten und auch ein entscheidender Teil des effektiven PKI-Managements. Angenommen, Sie arbeiten mit einer CA mit kurzen Validierungszeiten – dann ist der einzige Nachteil üblicherweise, dass die Anfrage von einem Zertifikatsadministrator genehmigt werden muss.

Sobald Sie Ihre Benutzer und Abteilungen organisiert haben, sollten Verifizierungs-E-Mails an die zuständigen Administratoren gesendet werden, damit Zertifikate schnell genehmigt und ausgestellt werden können. Dieses System beschleunigt den Genehmigungsprozess, da der Administrator nur die Richtigkeit der Informationen überprüfen muss und die Genehmigung dann erteilen kann. Dies spart Zeit und treibt die Bereitstellung voran, da Sie niemandem hinterherlaufen müssen, um Antworten zu erhalten.

Best Practice: Setzen Sie Benachrichtigungen zu Ihrem Vorteil ein

Fehlende Benachrichtigungen sind ein häufiges Problem für SSL-Manager und beeinträchtigen oft die Sicherheit, wenn es an der Zeit ist, ein Zertifikat zu erneuern. Sie sollten auf jeden Fall zumindest über ablaufende Zertifikate benachrichtigt werden. Doch auch an anderen Punkten des Zertifikatslebenszyklus können Benachrichtigungen hilfreich sein, zum Beispiel bei ausstehenden Zertifikatsanfragen, aktuellen Widerrufen oder wenn Zertifikate neu ausgestellt werden müssen.

Die Verwaltung von Zertifikaten in Tabellen ist nicht skalierbar und es gibt keinen Benachrichtigungsprozess. Manche Manager richten sich „Reminders“ im Outlook-Kalender ein, um rechtzeitig an die fällige Erneuerung von Zertifikaten erinnert zu werden, aber das hat mehrere Nachteile: So kann die Einrichtung einer solchen Erinnerung schnell einmal vergessen werden, es kann passieren, dass die Informationen bei einem Personalwechsel nicht weitergegeben werden oder es können andere technische Probleme auftreten. Tabellen sind nicht 100 % zuverlässig.

Wenn die Verlängerung eines Zertifikats ansteht und der Eigentümer es nicht innerhalb des festgelegten Zeitraums erneuert hat, müssen Sie sofort wissen, wer der Eigentümer ist, ob das Zertifikat aktiv ist und auf welchem Server es installiert wurde. Je früher Sie über die anstehende Erneuerung Bescheid wissen, desto eher können Sie handeln.

Legen Sie einen Eskalationspfad für spezifische potenzielle Zertifikatsprobleme fest. Zum Beispiel sollten Sie direkt benachrichtigt werden, wenn ein Zertifikat innerhalb der nächsten sieben Tage abläuft. Eskalation zur richtigen Zeit sorgt dafür, dass mögliche Probleme erkannt werden, bevor es zu spät ist. Solche Prüfungen helfen Ihnen, Ausfälle zu vermeiden, die durch abgelaufene Zertifikate verursacht werden.

Best Practice: Überwachen Sie Ihr Netzwerk und erstellen Sie Berichte

Mangelnde Transparenz in Ihrem Netzwerk kann zu Problemen führen. Manche MPKI-Plattformen bieten die Möglichkeit, Zertifikatsinformationen aus Ihren Netzwerkscans in einer umfassenden Dashboard-Übersicht zu bündeln. Nutzen Sie dieses Dashboard, um die Daten genau zu überprüfen.

Eine Dashboard-Ansicht gibt Ihnen einen schnellen Überblick über Ihr Zertifikatsnetzwerk. Mit nur einem Blick können Sie Ihren gesamten Netzwerkzustand beurteilen. Zudem lassen sich in Kürze ablaufende Zertifikate, gefährdete Zertifikatsendgeräte und ausstehende Zertifikatsanfragen von anderen Teammitgliedern überprüfen. Dies sind nur einige Beispiele der Erkenntnisse, die ein Dashboard zur Überwachung Ihres Netzwerks bieten kann.

Wenn Sie Ihr Netzwerk auf diese Weise überwachen, mit kontinuierlicher Zertifikatsuche und Überprüfung der jeweiligen Ergebnisse, sind Sie auf dem Weg zu mehr Transparenz einen großen Schritt weiter. Zertifikatsuche und Berichterstellung sind zwei Komponenten, die zusammenwirken, um Ihnen den größtmöglichen Einblick in und die größtmögliche Kontrolle über Ihre Zertifikatslandschaft zu geben.

Die folgenden Tipps helfen Ihnen bei der Überwachung:

- Setzen Sie zur Netzwerkprüfung einen Agenten ein, und lassen Sie diesen mindestens einmal alle 30 Tage einen Bericht erstellen.
- Automatisieren Sie diese Netzwerkprüfungen, wenn möglich, mit einem Skript.
- Beheben Sie Probleme auf gefährdeten Endgeräten sofort nach jeder Prüfung.
- Genehmigen Sie Zertifikatsanfragen so schnell wie möglich.
- Ermöglichen Sie automatische Verlängerungen, um Ausfälle zu vermeiden.

Für die ständige Überwachung Ihrer Zertifikate ist es wichtig, die Zertifikatslandschaft aus der Vogelperspektive überblicken und bei Bedarf alle Einzelheiten genauer inspizieren zu können.

Best Practice: Nutzen Sie ein Tool zur Erkennung von Schwachstellen

Eine neue Schwachstelle kann jederzeit auftauchen, was die Behebung zu einem zeitkritischen Aspekt im Zertifikatslebenszyklus macht.

Laut einem Bericht von Bay Dynamics aus dem Jahr 2017 fühlen sich 74 % der Sicherheitsteams von ihrer Arbeit an Schwachstellen in sehr großen Unternehmen überfordert. Es ist durchaus möglich, dass Sie es zu jedem beliebigen Zeitpunkt mit mehr als einer Million Schwachstellen in Ihren Systemen zu tun haben.

„Dafür zu sorgen, dass alle Schwachstellen entsprechend bearbeitet und behoben werden, sorgt für erheblichen Druck.“[3]

[3] D. Monahan, „A Day in the Life of a Cyber Security Pro“, Zugriff 26. Juni 2017, https:// baydynamics.com/content/uploads/2017/05/4-19-17-FINAL-EMA-A-Day-in-the-Life-of-a-Security-Pro.pdf

Einige dieser Schwachstellen können bereits jetzt Ihr SSL-Netzwerk unsicher machen. Ein Zertifikat reicht nicht aus, um einen SSL-Dienst zu schützen, wenn Sie veraltete Verschlüsselungen oder gefährdete Versionen von SSL/TLS verwenden. Sie können den Aufwand für die Verwaltung von Schwachstellen für SSL-Endgeräte reduzieren, wenn Sie ein Tool nutzen, das Ihr Netzwerk überprüft, nach Schwachstellen sucht und Informationen über diese Schwachstellen liefert.

Solche Tools sind besonders hilfreich, wenn sie bestimmte Schwachstellen identifizieren und mit den betroffenen Endgeräten abgleichen, damit Sie sie schnell und problemlos korrigieren können.

Best Practice: Wählen Sie eine Plattform, die alles kann

Erleichtern Sie sich die Zertifikatsverwaltung und wählen Sie dafür eine Plattform, die Ihnen Folgendes ermöglicht:

- Einsatz einer MPKI-Lösung
- umfassendes Dashboard
- Automatisierung über API
- Zertifikatsuche
- Aufteilung und Zuweisung von Benutzerrollen
- Einrichtung von Benachrichtigungen und Eskalationspfaden
- Suche nach Schwachstellen

Die Plattform ist der Schlüssel zur effektiven Kontrolle über Ihre PKI und zur Verwaltung des Zertifikatslebenszyklus von der Ausstellung über die Installation, Inspektion und Reparatur bis hin zur Erneuerung.

Die CertCentral®-Plattform von DigiCert ist eine Software-Suite der Enterprise-Klasse zur Verwaltung von Zertifikaten. Sie wurde entwickelt, um die Verwaltung zu vereinfachen, Arbeitsabläufe anzupassen und die Ausgabe von Zertifikaten zu automatisieren.

Sie sollten alle Bereiche Ihres Netzwerks überwachen. Hinsichtlich Ihrer Zertifikate sollten Sie Berichte erstellen für:

Mit der DigiCert Services-API können SSL-Manager praktisch jeden beliebigen Prozess automatisieren. Die API lässt sich in Anwendungen von Drittanbietern integrieren und kann mit eigenem Branding versehen werden, um auch optisch zu Ihren anderen Tools zu passen.

Die Verwendung einer Paketlösung zur Überwachung, Verwaltung, Entdeckung und Prüfung von Schwachstellen, sorgt dafür, dass Sie immer genau wissen, was in Ihrem Netzwerk vor sich geht.

Sie ermöglicht mehr Transparenz. Die Organisation Ihrer Teammitglieder, die Zuweisung von Rollen und bei Bedarf die Aufteilung sorgen für umfassendere Kontrolle.

Wenn Sie sicherstellen wollen, dass keine Zertifikate durch das Netz rutschen, dann ist CertCentral Ihr wertvollstes Werkzeug.

Fragen zu CertCentral® oder unserer API? Unseren Vertrieb erreichen Sie telefonisch unter +1 855 800 3444 oder per E-Mail an sales@digicert.com.

digicert®