FALLSTUDIE

digicert

DIGICERT TRUST LIFECYCLE MANAGER – AUTOMATISIERTE, SICHERE ZERTIFIKATS-VERWALTUNG FÜR ALLE ARTEN VON WORKLOADS

Zusammenfassung

Firmenname: DigiCert
Branche: Technologie
Hauptsitz: Lehi, Utah, USA

Die wichtigsten geschäftlichen Herausforderungen:

- Effektive Verwaltung digitaler Zertifikate auf den unternehmenseigenen VMs
- Straffung der Arbeitsschritte für die Bereitstellung und Installation von Zertifikaten für verschiedene Workloads
- Automatisierung aller Phasen der Verwaltung des Zertifikatslebenszyklus (CLM)

Die Lösung:

- DigiCert Trust Lifecycle Manager

Die wichtigsten Vorteile:

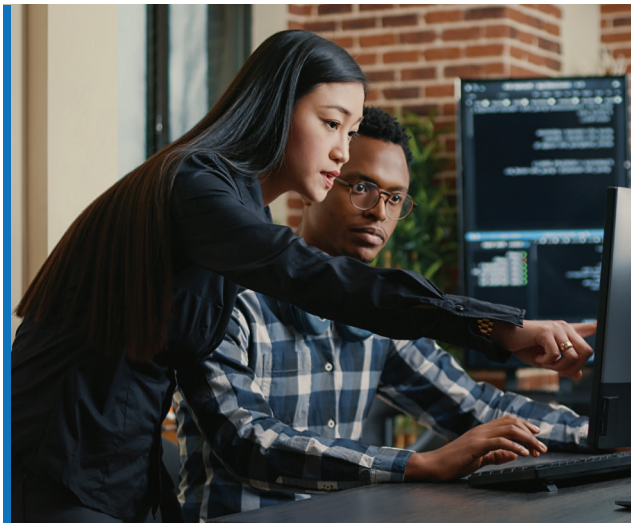
- Konfigurationsvorlagen ermöglichen dem SRE-Team, Zertifikate in DigiCert Trust Lifecycle Manager automatisch registrieren zu lassen. So können Zertifikate nun in wenigen Minuten – statt Stunden – bereitgestellt und installiert werden.
- Automatisierungsfunktionen straffen die Zertifikatsverwaltung, mindern das Risiko von zertifikatsbedingten Unterbrechungen und reduzieren die Wahrscheinlichkeit von Ausfällen aufgrund falsch konfigurierter oder abgelaufener Zertifikate.
- Sofort einsatzbereite Integrationen für externe Plattformen, Cloud-Umgebungen und Geräte decken alle Phasen des CLM-Prozesses ab und reduzieren den Aufwand für das IT-Team, wenn das Unternehmen wächst.

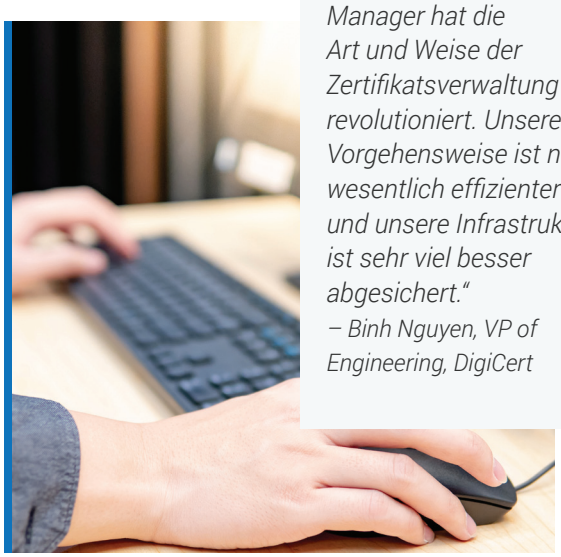
Die Herausforderung

Effektive Verwaltung der Host-Sicherheit und -Verfügbarkeit in einer heterogenen IT-Umgebung

Das SRE-Team (Site Reliability Engineering) von DigiCert ist dafür verantwortlich, dass die globale IT-Infrastruktur des Unternehmens kontinuierlich verfügbar ist und die erwartete Leistung bietet. Um diesem hohen Anspruch an die Verfügbarkeit gerecht zu werden, muss das SRE-Tam alle digitalen Zertifikate auf den Tausenden von virtuellen Maschinen (VMs) verwalten, die die Rechenzentren des Unternehmens in den USA, in Europa und in Japan unterstützen.

Doch wie Binh Nguyen, Vice President of Engineering bei DigiCert, erklärt, werden Zertifikate zunehmend als Identitäten für die Workloads auf den VMs genutzt, wodurch sich diese Aufgabe zu einem kaum zu bewältigenden Kraftakt entwickelt hat. „Die Zertifikatsverwaltung war schon immer eine Herausforderung, aber seitdem wir deutlich mehr Zertifikate nutzen, ist es kaum noch möglich, alle im Blick zu behalten“, so Nguyen. „Die Bereitstellung und Installation eines einzigen Zertifikats war mit so vielen Schritten verbunden, dass der Prozess oft mehrere Stunden in Anspruch nahm.“





„DigiCert Trust Lifecycle Manager hat die Art und Weise der Zertifikatsverwaltung revolutioniert. Unsere Vorgehensweise ist nun wesentlich effizienter und unsere Infrastruktur ist sehr viel besser abgesichert."
– Binh Nguyen, VP of Engineering, DigiCert

Früher war die Registrierung von Zertifikaten kompliziert und zeitaufwendig: Zunächst musste eine Signaturanforderung (Certificate Signing Request, CSR) erstellt und genehmigt werden. Dann wurde ein Zertifikat ausgestellt, das manuell vom Team heruntergeladen und auf dem Hostsystem installiert wurde – ein Prozess mit mehreren Schritten, der von Host zu Host unterschiedlich ablief. Anschließend musste das Team das Zertifikat noch testen. Nguyen erklärt: „Diese Schritte mussten für jedes Zertifikat ausgeführt werden und mit jedem Schritt stieg das Potenzial für menschliche Fehler. Wir brauchten eine Möglichkeit, diese Prozesse zu automatisieren, denn DigiCert ist genauso wenig gegen Ausfälle durch abgelaufene Zertifikate gefeit wie jedes andere Unternehmen, das seine Umgebung mit einer PKI schützt."

Die Lösung

Effiziente Verwaltung des Zertifikatslebenszyklus auf VMs – mit DigiCert Trust Lifecycle Manager

Für Nguyen konnte die Einführung von DigiCert Trust Lifecycle Manager (TLM) gar nicht schnell genug kommen. TLM bietet einen Überblick über sämtliche Zertifikate, mit denen die Tausenden von VMs und die darauf unterstützten Workloads geschützt werden. Die vielfältigen mit der Zertifikatslebenszyklusverwaltung verbundenen Prozesse konnten gestrafft werden und die zahlreichen integrierten Automatisierungsfunktionen von TLM beschleunigen die Beschaffung von Zertifikaten. Außerdem sorgt TLM dafür, dass der Betrieb nicht mehr durch abgelaufene oder falsch konfigurierte Zertifikate beeinträchtigt wird.

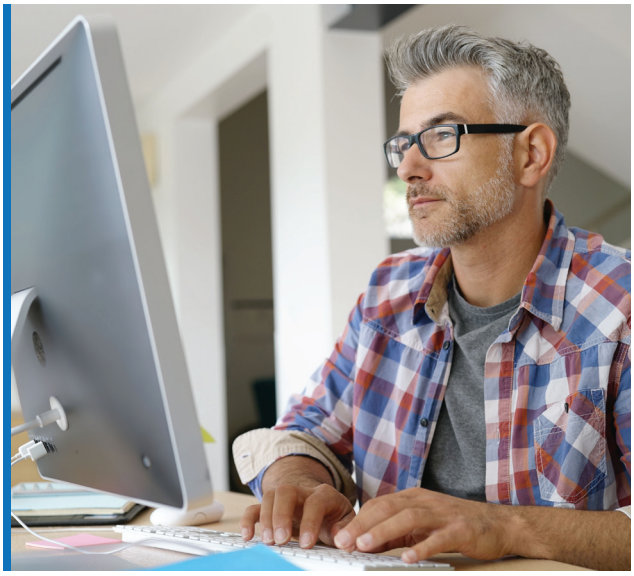
„DigiCert Trust Lifecycle Manager hat die Art und Weise der Zertifikatsverwaltung revolutioniert. Unsere Vorgehensweise ist nun wesentlich effizienter und unsere Infrastruktur ist sehr viel besser abgesichert", freut sich Nguyen.

Unkomplizierte, automatische Zertifikatsregistrierung über Profile

Als Erstes musste das SRE-Team die automatische Registrierung von Zertifikaten optimieren. Das betraf alle Phasen, von der Erstellung einer CSR über die Installation der Zertifikate bis hin zum Testen. Diese Schritte ließen sich mit den Konfigurationsvorlagen von DigiCert Trust Lifecycle Manager vereinfachen. Diese – auch Profile genannten – Vorlagen bieten vorkonfigurierte Regeln für das Ausstellen, Installieren und Verwalten von digitalen Zertifikaten. Da Trust Lifecycle Manager standardmäßig eine Vielzahl gängiger Profile enthält, zum Beispiel für die automatische Registrierung auf Webservern, fiel dem Team von Nguyen die Einrichtung sehr leicht. „Wir konnten ein Profil für unseren ACME-Agenten konfigurieren, über den wir das Zielsystem zentral überwachen können. Dieser Agent führt selbsttätig alle erforderlichen Schritte für die Erneuerung ablaufender Zertifikate aus, ohne dass wir eingreifen müssen", legt Nguyen dar.

Mit den anwenderfreundlichen Vorlagen von TLM können Nutzer außerdem selbst Profile erstellen, ohne sich mit den Einzelheiten einer PKI auszukennen. Über die festgelegten Vorlagenkonfigurationen, mit denen beispielsweise Zertifikatseigenschaften wie Typ, Gültigkeit und Vertrauenshierarchie vorgegeben werden, kann das SRE-Team zudem Profile anlegen, die die Konfigurationen für einen bestimmten Anwendungsfall automatisch durchsetzen.

Selbst die Laufzeit eines Zertifikats kann mit DigiCert Trust Lifecycle Manager konfiguriert werden. Nguyen führt aus: „Man muss kein PKI-Experte sein, um diese Abläufe zu konfigurieren, da Trust Lifecycle Manager alle Schritte vom Ausstellen der Signaturanforderung bis zum Installieren und Ersetzen von Zertifikaten übernimmt. Was uns früher Stunden gekostet hat, ist nun in wenigen Minuten erledigt, da TLM alles automatisiert."

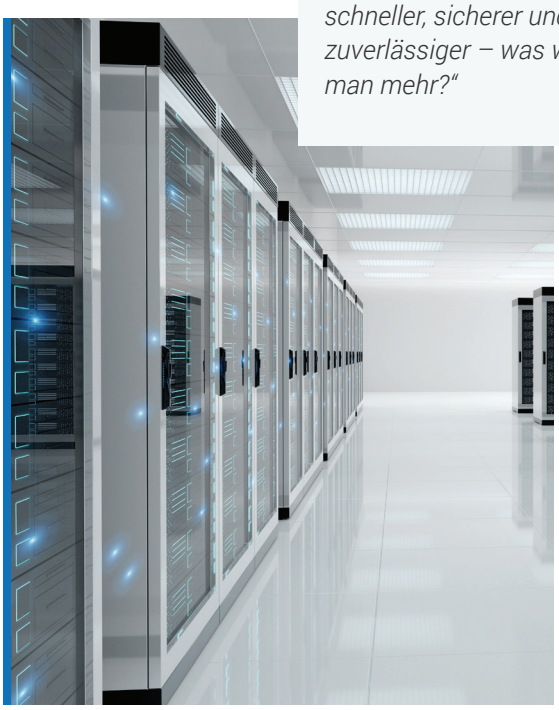


Automatisiertes CLM – von der Zertifikatsuche bis zur Erneuerung

Nguyens Team profitiert nicht nur von den Vorteilen der Profile, sondern auch von der integrierten Automatisierungsarchitektur von DigiCert Trust Lifecycle Manager, die es den SRE-Experten ermöglicht, sämtliche Aspekte der Zertifikatslebenszyklusverwaltung (CLM) zu automatisieren. Nguyen betont, dass diese Funktionen den Verantwortungsbereich seines Teams völlig revolutioniert haben. „Damit entfällt für uns ein Großteil des Aufwands, da wir uns nicht mehr um die Nachverfolgung der Zertifikate auf den VMs kümmern müssen. TLM übernimmt nicht nur die Suche und Bestandsaufnahme sämtlicher Zertifikate – ganz gleich, von welcher Zertifizierungsstelle sie ausgestellt wurden –, sondern informiert uns auch darüber, wem sie zugewiesen sind, wann sie ablaufen und ob sie unseren Sicherheitsrichtlinien entsprechen."

Doch das ist noch nicht alles. Die auf Automatisierung ausgerichtete Lösung ermöglicht es dem SRE-Team, Automatisierungsabläufe zu erstellen, die ganz ohne menschliche Unterstützung bestimmte Prozesse auslösen. So konnte das Team zum Beispiel einen Workflow entwickeln, der dafür sorgt, dass jedes Zertifikat, das falsch konfiguriert ist, Sicherheitslücken enthält oder von einer nicht autorisierten CA ausgestellt wurde, automatisch widerrufen wird. Ein solches Zertifikat wird dann automatisch und in Abhängigkeit vom Zertifikatstyp durch ein genehmigtes Zertifikat ersetzt, das von CertCentral oder vom DigiCert ONE CA Manager stammt.

„Unsere Prozesse sind schneller, sicherer und zuverlässiger – was will man mehr?"



Nahtlose Einbindung von Drittanbietergeräten und -Workloads im Netzwerk

Ein abschließender wichtiger Punkt für DigiCert ist, dass sich DigiCert Trust Lifecycle Manager nahtlos in die verschiedenen Workloads integrieren lässt, die von den VMs des Unternehmens unterstützt werden (einschließlich Load-Balancern und Webservern). Mithilfe von Sensoren und Agenten verwaltet Trust TLM zuverlässig alle Zertifikate auf diesen Netzwerkgeräten, und zwar ganz ohne zusätzliche Skripte oder andere Prozesse, die die Komplexität erhöhen oder anderweitig ein Problem für das SRE-Team darstellen würden. „Es ist eine echte Erleichterung zu wissen, dass unsere Apache-Server nicht plötzlich wegen eines Zertifikats ausfallen, von dem wir nichts wussten", bekräftigt Nguyen.

Er weiß auch zu schätzen, wie übersichtlich die Verwaltung und Automatisierung aller Zertifikate ist, die als Geräteidentitäten für die vielen Anwendungen und Microservices auf den Webservern und Load-Balancern des Unternehmens genutzt werden. „Jede dieser Komponenten benötigt ein Zertifikat für die Authentifizierung, um mit den anderen Komponenten zusammenwirken zu können. Wenn man darüber nachdenkt, wie komplex diese Verzweigungen sind, wird einem ganz schwindelig, aber dank TLM müssen wir uns darüber keine Gedanken mehr machen", begeistert sich Nguyen.

Nguyens Team hat bereits damit begonnen, die Zertifikatsverwaltung in den Cloud-Instanzen an DigiCert Trust Lifecycle Manager zu übertragen. Ein weiteres Plus neben den überzeugenden CLM- und PKI-Funktionen von Trust Lifecycle Manager ist die Fähigkeit der Lösung, ganz nach Bedarf Zertifizierungsstellen für Zwischenzertifikate (Intermediate Certificate Authorities, ICAs) zu erstellen. „Mit Trust Lifecycle Manager erhalten wir die Agilität, die wir benötigen, damit unsere Infrastruktur auch dann sicher bleibt, wenn wir wachsen", bekräftigt Nguyen. „Unsere Prozesse sind schneller, sicherer und zuverlässiger – was will man mehr?"

Sie möchten DigiCert® Trust Lifecycle Manager sofort nutzen? Dann wenden Sie sich hier an uns.