FALLSTUDIE

TRUST LIFECYCLE MANAGER FÜR EINFACHERES ZUGRIFFSMANAGEMENT UND BESSER GESCHÜTZTE RESSOURCEN

Zusammenfassung

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

Die wichtigsten geschäftlichen Herausforderungen:

- Kontinuierlicher Zugriff auf Unternehmensanwendungen und -daten in einer hybriden Arbeitsumgebung für alle Mitarbeitenden weltweit
- Automatisierung verschiedener Zugriffsebenen für alle Phasen des Mitarbeiterzyklus – vom Onboarding bis zum Ausscheiden aus dem Unternehmen
- Reduktion der IT-Supportanfragen, damit IT-Teams sich Projekten widmen können, die dem Unternehmenswachstum zugute kommen

Die Lösungen

- DigiCert Trust Lifecycle Manager mit SCEP-Integrationen für MDM-Lösungen
- DigiCert ONE CA Manager

Die wichtigsten Vorteile:

- Das ServiceDesk-Team kann mithilfe von Vorlagen schnell und einfach Zertifikate generieren, die die Sicherheitsrichtlinien des Unternehmens erfüllen.
- SCEP-Integrationen ermöglichen die automatische Zertifikatsregistrierung über die unternehmenseigenen MDM-Lösungen.
- Automatisierungsfunktionen straffen die Zertifikatsverwaltung, reduzieren die Komplexität und mindern das Risiko von zertifikatsbedingten Unterbrechungen.
- Die proaktive Verwaltung des Zertifikatslebenszyklus setzt Service-Unterbrechungen ein Ende und reduziert die Anzahl von Support-Tickets.

Die Herausforderung

Kontinuierlicher Zugriff auf das Unternehmensnetzwerk für alle Mitarbeitenden von DigiCert weltweit

Das ServiceDesk-Team von DigiCert besteht aus 15 Mitarbeitenden, die für mehr als 1.600 Beschäftigte auf der ganzen Welt zuständig sind. Sie sorgen dafür, dass die gesamte Belegschaft des Unternehmens jederzeit und störungsfrei auf das Netzwerk, die Anwendungen und die Daten des Unternehmens zugreifen kann – sowohl von Bürostandorten als auch vom Homeoffice und unterwegs aus. Da Remote-Verbindungen gern von Angreifern ausgenutzt werden, stellt das Team außerdem sicher, dass eingehender Datenverkehr nur von authentifizierten Nutzern und Geräten zugelassen wird.

Der Versuch, ein Gleichgewicht zwischen einem hohen Sicherheitsniveau für IT-Systeme und kontinuierlichem Zugriff für die Mitarbeitenden und deren Geräte herzustellen, war mit mehreren Herausforderungen verbunden. Erstens war die Einrichtung von Nutzerkonten zum Verwalten der rollenbasierten Zugriffssteuerung sehr zeitaufwendig. Zweitens gab es eine Reihe von Konnektivitätsvoraussetzungen: Zum einen mussten sich die Endgeräte der Nutzer und die einzelnen Komponenten der Unternehmensinfrastruktur leicht miteinander verbinden können, zum anderen war die nahtlose Integration in MDM-Lösungen wie Intune (Windows) und Kandji (macOS und iOS) erforderlich. Drittens musste das Team die Lebenszyklen aller digitalen Zertifikate verwalten, die zum Authentifizieren von Nutzern und Geräten erforderlich waren.

„So wissen wir nicht nur, wer und was abgesichert ist, sondern können auch die entsprechenden Zertifikate problemlos verwalten und bei Bedarf in Echtzeit ausstellen bzw. erneuern, ohne dass die Anwender in irgendeiner Weise beeinträchtigt werden."

Leider konnte das Team oft nicht erkennen, dass ein Client-Zertifikat abgelaufen war, und wurde erst auf das Problem aufmerksam, wenn Mitarbeitende nachfragten, warum sie keinen Zugriff auf das Unternehmensnetzwerk mehr hatten. „Die Bearbeitung einer solchen Helpdesk-Anfrage nimmt mindestens zehn Minuten in Anspruch, weil bei jeder Anfrage eine Checkliste mit Fragen abgearbeitet werden muss", erklärt Rob Carnesecca, IT-Verantwortlicher bei DigiCert. „Das war besonders frustrierend, weil das Problem sehr häufig an einem abgelaufenen Zertifikat lag."

Die Lösung

DigiCert Trust Lifecycle Manager für automatisierte, in MDM-Plattformen integrierte CLM-Workflows

Glücklicherweise hatte Carneseccas Team Zugang zu DigiCert Trust Lifecycle Manager (TLM), einer zuverlässigen Plattform für die Verwaltung der PKI und des Zertifikatslebenszyklus (Certificate Lifecycle Management, CLM). Im Gegensatz zu anderen Lösungen auf dem Markt übernimmt Trust Lifecycle Manager das Generieren und Verwalten der Client-Zertifikate, die für die Authentifizierung von Nutzern und Geräten notwendig sind, und bietet darüber hinaus einsatzfertige Integrationen für MDM-Lösungen.

Mit TLM konnten alle Aspekte der Zertifikatsverwaltung automatisiert werden – von der Ausstellung über die Erneuerung bis hin zum Widerruf von Zertifikaten.

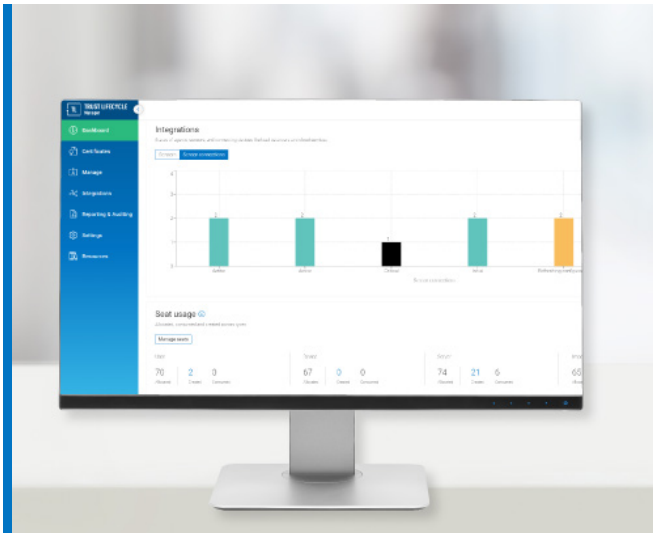
Carnesecca zeigt sich begeistert: „Trust Lifecycle Manager benachrichtigt uns, wenn Zertifikate ablaufen, und kann sie sogar automatisch erneuern – vorausgesetzt, der Nutzer ist in unserem System aktiv. So wissen wir nicht nur, wer und was abgesichert ist, sondern können auch die entsprechenden Zertifikate problemlos verwalten und bei Bedarf in Echtzeit ausstellen bzw. erneuern, ohne dass die Anwender in irgendeiner Weise beeinträchtigt werden."

Integrationen und Profile für effiziente CLM-Workflows

Damit die für die Authentifizierung von Geräten erforderlichen Zertifikate ordnungsgemäß installiert werden können, muss das ServiceDesk-Team bestimmte Abläufe in den MDM-Lösungen des Unternehmens durchführen. Da Trust Lifecycle Manager die SCEP-Integration unterstützt, können private Zertifikate automatisch über den DigiCert ONE CA Manager registriert werden. Dies geschieht selbstgesteuert über Kandji oder Intune, ohne dass die zahlreichen, für diesen Schritt erforderlichen Prozesse manuell konfiguriert oder überwacht werden müssen.

Zudem kann das ServiceDesk-Team die zahlreichen, vom Trust Lifecycle Manager bereitgestellten Profile nutzen, die sich ganz einfach mithilfe von anwenderfreundlichen Vorlagen einrichten lassen. „Ich kenne mich mit Zertifikaten wirklich nicht gut aus und wäre damit normalerweise überfordert gewesen. Doch mit der Vorlage in TLM ist die SCEP-Integration ein Kinderspiel", freut sich Jordan Wilcox, Systemadministrator bei DigiCert. „Man wählt einfach nur das entsprechende Simple Certificate Enrollment-Protokoll oder SCEP für die Intune-Vorlage aus, beantwortet ein paar Fragen und schon wird das Profil in TLM eingerichtet!"

Außerdem bietet Trust Lifecycle Manager vorlagenbasierte Profile für die automatische Einbindung von Integrationen in Netzwerkressourcen und die automatisierte Einrichtung von rollenbasiertem Zugriff. Wilcox erläutert: „Es gibt Vorlagen, mit denen man die Gültigkeitsdauer von Zertifikaten konfigurieren und festlegen kann, dass Zertifikate rechtzeitig vor dem Ablaufdatum erneuert werden."



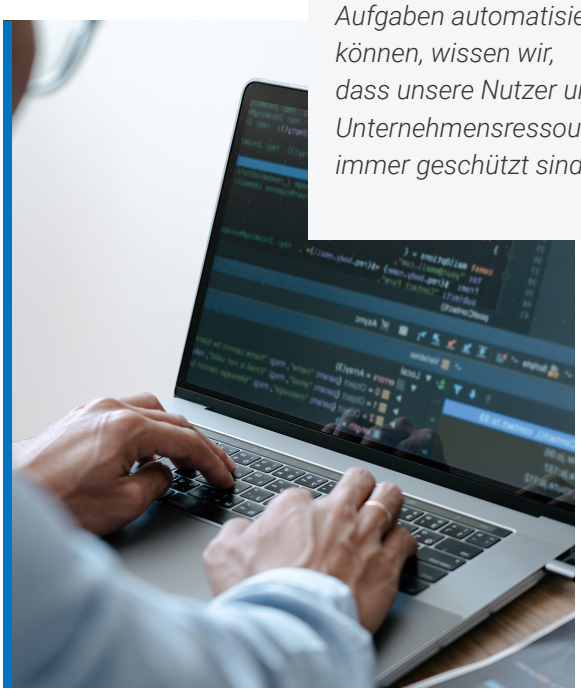
Vollständig automatisierte Verwaltungsfunktionen und Skalierbarkeit

Da so viele Aspekte der Zertifikatsverwaltung automatisierbar sind, kann Carneseccas Team das Potenzial der PKI nun voll ausschöpfen und sämtliche Aspekte der Nutzer- und Gerätesicherheit schnell und mit minimalem Aufwand abwickeln. „TLM ist enorm zuverlässig. Wir können einfach ein Gerät mit einem Zertifikat versehen und wissen, dass das Gerät von DigiCert geschützt wird. Mit einem anderen Zertifikat, das die Anbindung an unsere Netzwerkinfrastruktur sichert, wird dann geprüft, ob das Gerät Zugriff auf eine bestimmte Ressource hat. Auch Anwendungen lassen sich über ein Zertifikat absichern“, so Carnesecca. „Nun ist dafür gesorgt, dass die Automatisierungsfunktionen von TLM das alles für uns übernehmen. Damit müssen wir uns also nicht weiter befassen.“

Da DigiCert über eine geografisch stark verteilte Belegschaft verfügt, wäre es für Carnesecca und sein Team ohne eine Plattform wie Trust Lifecycle Manager enorm schwierig gewesen, den Bedürfnissen des Unternehmens gerecht zu werden. Carnesecca bringt es auf den Punkt: „Ein wichtiger Vorteil von TLM ist, dass es sich um eine weltweit nutzbare Lösung handelt. Das ist für uns besonders relevant, da unsere Standorte und Mitarbeitenden über so viele verschiedene Zeitzonen verteilt sind. Da wir einen Großteil der Aufgaben automatisieren können, wissen wir, dass unsere Nutzer und Unternehmensressourcen immer geschützt sind. Außerdem können wir jederzeit zusätzliche Ressourcen und Nutzer betreuen, ohne meinem Team nennenswerte Mehrarbeit zu verursachen.“

„Es ist eine echte Erleichterung, dass TLM die Zertifikatserneuerung übernimmt. So kommt es nicht mehr zu Service-Unterbrechungen. Wenn die Automatisierungsfunktionen einmal eingerichtet sind, muss ich mich nicht weiter darum kümmern. Und wenn alles rund um die Uhr laufen muss, hilft es sehr, wenn man eine Sorge weniger hat.“

„Da wir einen Großteil der Aufgaben automatisieren können, wissen wir, dass unsere Nutzer und Unternehmensressourcen immer geschützt sind.“



Stärkere Sicherheit, besseres Zugriffsmanagement und wesentlich weniger Aufwand

DigiCert Trust Lifecycle Manager hat dem Team gleich zwei Sorgen genommen. Nun können DigiCert-Ressourcen mit Hochverfügbarkeitsanspruch geschützt werden, während den Mitarbeitenden die Arbeit erleichtert wird. Außerdem wurde der Aufwand für das IT-Personal erheblich reduziert, sodass Teammitglieder, die früher Tag für Tag stundenlang mit der Beantwortung von Supportanfragen beschäftigt waren, ihre Zeit nun für Projekte nutzen können, die einen geschäftlichen Mehrwert bieten.

„Es ist eine echte Erleichterung, dass TLM die Zertifikatserneuerung übernimmt. So kommt es nicht mehr zu Service-Unterbrechungen. Wenn die Automatisierungsfunktionen einmal eingerichtet sind, muss ich mich nicht weiter darum kümmern. Und wenn alles rund um die Uhr laufen muss, hilft es sehr, wenn man eine Sorge weniger hat“, kommentiert Wilcox.

Sie möchten DigiCert® Trust Lifecycle Manager sofort nutzen? Dann wenden Sie sich an sales@digicert.com.