Vereinfachte Verwaltung von SSL-Zertifikaten im gesamten Unternehmen

Vereinfachte Verwaltung von SSL-Zertifikaten im gesamten Unternehmen

Einleitung

SSL-Zertifikate sind längst nicht mehr nur für die Bezahlseite von Online-Shops, sondern auch für Kernfunktionen von Unternehmen erforderlich. So werden sie beispielsweise zum Schutz der Kommunikation mit Mitarbeitern und Partnern an anderen Standorten per E-Mail, Chat und Instant Messaging verwendet. Die Browser-Server-Kommunikation für cloudbasierte Dienste erfordert SSL-Zertifikate, wenn hierbei Kundendaten angezeigt, Transaktionen mit Geschäftspartnern vorgenommen oder Produktivitäts-Tools für Mitarbeiter eingesetzt werden. Nicht zuletzt werden SSL-Zertifikate zur Sicherung der Server-Server-Kommunikation von Anwendungen und der Datenübertragung verwendet.

Die Verwaltung einzelner Zertifikate in einem großen Unternehmen mit zahlreichen Standorten und Abteilungen, das zunehmend webbasierte Dienste einsetzt, wird schnell kompliziert. Durch das unbemerkte Ablaufen eines SSL-Zertifikats kann ein Unternehmen nicht nur Umsatz und das Vertrauen seiner Kunden verlieren, sondern möglicherweise sind auch Mitarbeiter und Geschäftspartner nicht in der Lage, ihre Arbeit zu erledigen, oder riskieren es, vertrauliche Informationen preiszugeben. Die Verwaltung von SSL-Zertifikaten in komplexen Netzwerken, um ablaufende Zertifikate rechtzeitig zu erneuern und den durchgängigen Schutz sicherzustellen, ist daher für alle Geschäfte von existenzieller Bedeutung.

Dieser Leitfaden zeigt fünf einfache Schritte auf, mit denen IT-Fachleute SSL-Zertifikate im gesamten Unternehmen überwachen können. Zudem enthält er Empfehlungen für eine Verwaltungsplattform, mit der sich volle Transparenz und die zentrale Verwaltung der Zertifikate während ihrer gesamten Lebensdauer erzielen lassen.

Überwachung von SSL- und Code Signing-Zertifikaten in fünf Schritten

Mit den folgenden fünf Schritten gelingt es IT-Administratoren, die Kontrolle über alle SSL-Zertifikate im Unternehmen zu erlangen:

1. Überprüfen aller Domänen und Zertifikate
2. Zusammenlegen aller Zertifikate in einem verwalteten Konto
3. Definieren eines Verwaltungsablaufs für das gesamte Unternehmen
4. Einrichten von Warnmeldungen und regelmäßige Berichte über verfügbare Einheiten und anstehende Erneuerungen
5. Bedarfsgesteuertes Widerrufen und Ersetzen von Zertifikaten

1. Überprüfen aller Domänen und Zertifikate

Wissen Sie, wo Ihre SSL-Zertifikate abgelegt sind? Für den Schutz von Online-Transaktionen, der Kommunikation im Internet und webbasierter Anwendungen ist es wichtig, dass Sie den Überblick über alle SSL-Zertifikate von Thawte in Ihrem Unternehmen haben. Unabhängig davon, ob Sie bei null anfangen oder eine Bestandsliste überprüfen möchten, können Sie den Prozess mithilfe eines Tools zur Zertifikatsuche automatisieren und einen Katalog mit Angaben zu Speicherort, Ablaufdatum, Gültigkeitszeitraum und Schlüssellänge Ihrer SSL- und Code Signing-Zertifikate erstellen.

Ergebnis: Echtzeitberichte über alle Zertifikate für gesicherte Domänen

Fallbeispiel: Das plötzliche Ablaufen eines Zertifikats

Ein E-Commerce-Server fällt aus und niemand weiß, warum. Stündlich bleiben Tausende von Verkaufschancen ungenutzt, während die IT-Abteilung die Ursache sucht. Ein SSL-Zertifikat, das bei einem nicht genehmigten Lieferanten erworben wurde, ist abgelaufen und der Administrator, der den Kauf abgewickelt hatte, ist nicht mehr im Unternehmen. Die Benachrichtigung über die anstehende Erneuerung ist nie beim jetzigen Administrator angekommen und niemand wusste, dass dieses SSL-Zertifikat überhaupt existierte. Mit dem Thawte Certificate Center Enterprise-Konto haben Administratoren alle Thawte-Zertifikate im Unternehmensnetzwerk im Blick.

2. Zusammenlegen aller Zertifikate in einem verwalteten Konto

Nach der Überprüfung verfügen Sie über alle Informationen, die Sie benötigen, um Ihren SSL-Schutz zu beurteilen und die Zusammenlegung der Zertifikate in einem einzigen verwalteten Konto in Angriff nehmen zu können. Kontrollieren Sie die Ergebnisse der Überprüfung unter den folgenden Gesichtspunkten:

- Wurden alle Zertifikate ordnungsgemäß installiert?
- Bieten die Zertifikate eine angemessene Verschlüsselung und Authentifizierung?
- Werden auf den erforderlichen Seiten Vertrauensmarken und Sicherheitssiegel angezeigt?
- Sind alle zu schützenden Server durch SSL-Zertifikate abgedeckt?
- Gibt es nicht autorisierte Zertifikate, die verwaltet werden müssen?

Heute sind eine Reihe von SSL-Zertifikaten mit unterschiedlicher Verschlüsselungsstärke und Authentifizierung erhältlich, doch viele Enterprise-Tools zur SSL-Verwaltung erfordern für jeden Zertifikatstyp ein anderes Konto. Wenn das Unternehmen wächst und die Zahl der Administratoren zunimmt, wird die Verwaltung verschiedener Konten für die unterschiedlichen SSL-Zertifikatstypen ohne eine zentrale Verwaltungsplattform unübersichtlich. Nutzen Sie die Erneuerung ablaufender Zertifikate, um sie in einem einzigen verwalteten Konto zusammenzufassen, das alle erforderlichen Zertifikatstypen unterstützt. Damit können Sie außerdem Mengenrabatte nutzen und Ihre Kosten senken.

Ergebnis: ein einziges verwaltetes Konto für alle Zertifikate in Ihrem Unternehmen

Fallbeispiel: Das Konsolidierungsprojekt

Im Rahmen einer Fusion fällt die Integration zweier Netzwerke an. Sie müssen fünf Premium- und fünf Standard SSL-Zertifikate anschaffen und in drei bestehenden Zertifikaten die Kontaktdaten für die Domäne aktualisieren. Die Anschaffung einzelner Zertifikate kostet wertvolle Zeit, die dann für andere Integrationsmaßnahmen fehlen würde. Der Kauf mehrerer Zertifikate über das Thawte Certificate Center Enterprise-Konto für Erneuerungen und die sofortige Ausgabe löst dieses Problem.

Thawte Certificate Center Enterprise-Konto

Merkmale	Vorteile
webgestütztes Managementportal	Eine funktionsreiche Schnittstelle für die Zertifikatsverwaltung während des gesamten Lebenszyklus erleichtert die Installation und Konfiguration.
zentrale Verwaltung	Die abteilungs- und standortübergreifende Konsolidierung von Einkauf und Verwaltung führt zu Kostensenkungen.
anpassbare Workflow- und Audit-Protokolle	Die Delegierung von Verwaltungsaufgaben und die Genehmigung von Domänen im Voraus ermöglichen bei Bedarf die verzögerungsfreie Ausgabe von Zertifikaten. Ausführliche Audit-Protokolle machen alle Maßnahmen nachvollziehbar.
große Auswahl an SSL-Zertifikaten	Alle Zertifikatstypen können über eine Konsole verwaltet werden: Extended Validation (EV), SGC, SAN für Unified Communications, Standard SSL und Code Signing.
umfassende Berichtsfunktionen	Rollenbasierte Echtzeit- und Monatsberichte, die online und offline verfügbar sind, erleichtern das Ressourcen- und Risikomanagement.
anpassbare Warnmeldungen und Benachrichtigungen	Dank automatisierter Warnmeldungen an mehrere Empfänger werden keine Mitteilungen mehr übersehen.
Support der Spitzenklasse	Telefonisch, im Internet, per E-Mail und im Online-Chat verfügbar.

3. Definieren eines Verwaltungsablaufs für das gesamte Unternehmen

Ein Enterprise-Account für die Zertifikatsverwaltung ermöglicht autorisierten Administratoren den Kauf mehrerer Zertifikatseinheiten in einer Transaktion. Diese können dann unternehmensweit nach Bedarf ausgegeben werden. Der Administrator definiert entsprechend dem gewünschten Maß an Kontrolle einen einheitlichen Verwaltungsablauf. Darin wird u. a. festgelegt, welcher Mitarbeiter welche Privilegien besitzt, wie die Anmeldung erfolgt und welche Art von Benachrichtigungen an welche Mitarbeiter versandt werden.

Das Zertifikatsverwaltungssystem sollte so flexibel und anpassungsfähig sein, dass es auf die jeweilige Umgebung zugeschnitten werden kann. Rollenbasierter Zugriff und die dynamische Zuweisung von Privilegien unterstützen die Durchsetzung des festgelegten Verwaltungsablaufs. Wenn sich Administratoren mit ihren eindeutigen Login-Daten anmelden, können sie Zertifikate je nach ihrer Rolle und Geschäftseinheit verwalten.

Fordert ein Administrator ein SSL- oder Code Signing-Zertifikat an, kann das Zertifikat je nach den vorher festgelegten Administrationsregeln umgehend genehmigt, abgelehnt oder als ausstehende Anforderung eingestuft werden.

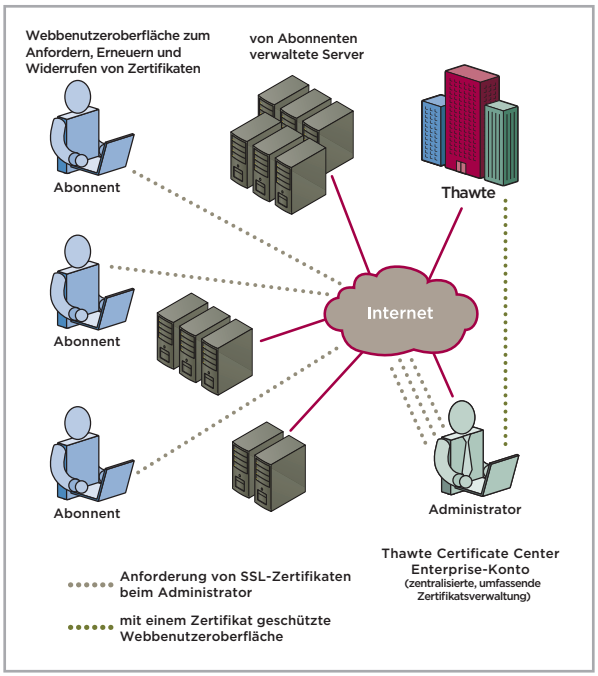
Während des Anmeldeverfahrens für die meisten SSL-Zertifikate muss der Käufer die Kontaktdaten eines technischen Mitarbeiters, wie Name, Telefonnummer und E-Mail-Adresse, angeben. Die Standardkontaktdaten und Benachrichtigungseinstellungen sollten dem festgelegten Verwaltungsablauf entsprechen. E-Mail-Benachrichtigungen über ablaufende Zertifikate können an mehrere Administratoren verschickt werden sowie an eine Alias-Adresse wie zum Beispiel ssladmin@yourdomain.com. Voreingestellte Benachrichtigungen tragen dazu bei, das Verfahren zu vereinheitlichen und die Administratoren stets auf dem Laufenden zu halten. Einige Beispiele:

- Wenn die Anzahl der verfügbaren Zertifikatseinheiten unter einen voreingestellten Wert sinkt, erhält der Administrator eine Benachrichtigung und kann weitere Einheiten bestellen.
- Benachrichtigungen über ausstehende Anforderungen informieren Administratoren, wenn sie neue Zertifikatsanforderungen überprüfen müssen.
- Bestätigungsmeldungen benachrichtigen Administratoren über sofort ausgestellte Zertifikate.

Ergebnis: ein klar definierter, in das Managementsystem integrierter Verwaltungsablauf

Fallbeispiel: Lokale Kontrolle, globaler Überblick

Stellen Sie sich vor, Ihre Niederlassung in Indien muss lokal ein Zertifikat ausstellen, um einen Entwicklungsserver online stellen zu können, aber der Zeitunterschied führt dazu, dass man dort 24 Stunden auf Ihre Genehmigung warten muss. Die Verzögerung ist unökonomisch, insbesondere wenn es sich um die vorab genehmigte Verwendung eines Zertifikats in einer autorisierten Domäne durch einen authentisierten Benutzer handelt. Mit dem Thawte Certificate Center Enterprise-Konto können Sie einem Mitarbeiter Administrationsrechte einräumen und so die sofortige Ausstellung des Zertifikats ermöglichen.



Benutzertypen	Vorteile
Primärer Kontoadministrator	Zuweisen von Rollen, Einrichten von Administratorprivilegien und Zugriff auf Assistenten für andere Administratoren
Sekundärer oder Abteilungs-administrator	Verwaltung des Zertifikatslebenszyklus einer bestimmten Domäne, Geschäftseinheit oder Abteilung: Genehmigen bzw. Ablehnen von Zertifikatsanforderungen, Widerrufen von Zertifikaten, Zuweisen von Anforderungen an andere Administratoren
Lesezugriff	Einsicht in Berichte über aktuelle Anforderungen, Zertifikatsdaten und Protokolldateien

4. Einrichten von Warnmeldungen und regelmäßige Berichte über verfügbare Einheiten und anstehende Erneuerungen

Die Zertifikatsverwaltungsplattform sollte die regelmäßige Erstellung von Berichten ermöglichen, um Administratoren beim effektiven Zeit- und Ressourcenmanagement zu unterstützen. Berichte über alle unternehmensweit angeforderten und bestehenden Zertifikate, aufgeschlüsselt nach Status (angefordert, genehmigt, abgelehnt, gültig, widerrufen, deaktiviert, abgelaufen, in Kürze ablaufend), können jederzeit sofort ausgegeben werden. Berichte über Ablauffristen und Warnmeldungen 90, 60 und 30 Tage vor dem Zertifikatsende erleichtern dem Administrator die Planung der Erneuerung von SSL-Zertifikaten und die Nutzung von Mengenrabatten. Protokolle über die vergangene Nutzung von Zertifikaten geben wertvolle Einblicke, die die zukünftige Planung und Verwaltung vereinfachen.

Das Berichtstool sollte verschiedene Dateiformate unterstützen und flexibel anpassbar sein, um die optimale Einbindung in individuelle Administrationsabläufe und -Tools zu ermöglichen. Es sollte Administratoren die Option bieten, detaillierte, auf ihre Anforderungen zugeschnittene Berichte über die Zertifikatsnutzung durch Abteilungen oder Administratoren zu erstellen sowie automatisierte Berichte zur Weiterleitung an wichtige Ansprechpartner einzurichten. Verschiedene Dateiformate wie pdf, html und cvs ermöglichen die Nutzung anderer Software zur Ansicht und Analyse der Daten.

Ergebnis: jährliche Ressourcenbereitstellung und Budgetzuweisung für SSL

5. Bedarfsgesteuertes Widerrufen und Ersetzen von Zertifikaten

Tools zur Bestandskontrolle und -verwaltung erleichtern das Widerrufen und Erneuern von Zertifikaten. Wenn Server aus dem Netzwerk entfernt, verschoben oder ersetzt werden, müssen die entsprechenden SSL-Zertifikate ebenfalls ordnungsgemäß geändert werden. Dies erfolgt durch Widerrufen und Ersetzen. Bei Verlust oder Preisgabe des privaten Schlüssels, oder wenn das Zertifikat bei einem Serverabsturz gelöscht wurde, muss der Administrator die Möglichkeit haben, das Zertifikat zu widerrufen und ein Ersatzzertifikat auszustellen. Thawte bietet Unternehmenskunden die Möglichkeit, Zertifikate ohne Zusatzkosten zu widerrufen und zu ersetzen. Dadurch können Zertifikate ohne Verlust der verbliebenen Laufzeit neu zugewiesen werden.

Ergebnis: bessere Kontrolle über verlorene Zertifikate

Fallbeispiel: Umzug

Sie wollen Rechenzentren zusammenlegen und müssen daher Zertifikate von einem physischen Standort zu einem anderen verschieben. Sie möchten für den neuen Standort keine neuen Zertifikate kaufen und dadurch die restliche Laufzeit verlieren, können sich aber auch keine Ausfallzeit erlauben. Mit einem Thawte Certificate Center Enterprise-Konto können Sie über „widerrufen und ersetzen“ Zertifikate von einem Serverstandort zu einem anderen verschieben.

Zentrale Steuerung und vollständiger Überblick mit einer einzigen Plattform

Ohne geeignete Werkzeuge kann die Verwaltung umfangreicher SSL-Installationen in komplexen Infrastrukturen viele manuelle Eingriffe erfordern, was zeitraubend und fehleranfällig ist. Die Entwicklung einer Zertifizierungsstelle zur Selbstsignierung bietet zwar bessere Kontrolle an einer zentralen Stelle, doch erfordert eine interne Lösung erhebliche Vorabinvestitionen, Zeit für die Entwicklung sowie die kontinuierliche Erweiterung, um neue SSL-Zertifikatstypen wie zum Beispiel Extended Validation einzubeziehen.

Das Thawte Certificate Center Enterprise-Konto vereint die besten Eigenschaften einer vertrauenswürdigen Zertifizierungsstelle und einer Lösung für die Selbstsignierung: zentrale Verwaltung über eine äußerst zuverlässige, skalierbare Infrastruktur und Ermittlung aller SSL- und Code Signing-Zertifikate von Thawte im gesamten Unternehmen. Zudem haben Administratoren, sobald ein Zertifikat erworben und ein Konto eröffnet wurde, ohne weiteren Zeit- oder Kostenaufwand für die Einrichtung der Infrastruktur die Möglichkeit, Benutzerkonten einzurichten und Zuständigkeiten zu delegieren.

- Das Thawte Certificate Center Enterprise-Konto für SSL ist ein cloudbasierter Service, der keine Vorabinvestitionen erfordert und nur geringe Wartungskosten verursacht. Die äußerst zuverlässige Thawte-Infrastruktur wächst mit Ihrem Unternehmen mit.
- Dank der zentralen Verwaltung und flexiblen Zuweisung von Aufgaben können die Administrationseinstellungen an die Unternehmensabläufe angepasst werden. Zugelassene Administratoren, die vorab genehmigte Domänen verwalten, können bedarfsgerecht SSL-Zertifikate für mehrere Server ausstellen und Versuche blockieren, außerhalb des genehmigten Prozesses Zertifikate zu erwerben.

Hauptvorteile

Niedrigere Gesamtbetriebskosten

Senkung der Kosten und Komplexität der unternehmensweiten Verwaltung mehrerer SSL-Zertifikate durch zentrale Steuerung, Zertifikatsermittlung und Mengenrabatte

Flexible Verwaltungsoptionen

Durchsetzung der adäquaten Kontrolle für die Verwaltung des Zertifikatslebenszyklus durch Funktionen zur Delegierung von Administrationsaufgaben, rollenbasierte Zugangskontrolle und dynamische Zuweisung von Privilegien

- Die Optionen für Thawte SSL-Zertifikate umfassen neben dem Thawte Trusted Site-Siegel mehrere Stufen für Verschlüsselung, Authentifizierung und Laufzeit, so dass Sie sie flexibel an Ihre geschäftlichen Anforderungen anpassen können.
- Durch größere Transparenz und Kontrolle sinkt das Risiko eines Ausfalls der Kommunikations- oder Betriebsfunktionen durch das unbemerkte Ablaufen von Zertifikaten und können nicht genehmigte SSL-Zertifikate entdeckt werden.

Fazit

Die unternehmensweite Verwaltung von SSL-Zertifikaten ist ein komplexes Unterfangen. Das Thawte Certificate Center Enterprise-Konto bietet eine einfache, aber leistungsfähige Plattform zur kostengünstigen Erkennung und Verwaltung von SSL-Zertifikaten. Mit der cloudbasierten Plattform können IT-Administratoren bei der unternehmensweiten Verwaltung von SSL-Zertifikaten geschäftskritische Aufgaben automatisieren sowie die Kosten und Risiken senken.

Falls Sie weitere Fragen haben, wenden Sie sich an einen unserer Verkaufsberater:

- **Telefonisch**
  - **USA: +1 888 484 2983**
  - **Großbritannien: +44 203 450 5486**
  - **Südafrika: +27 21 819 2800**
  - **Deutschland: +49 69 3807 89081**
  - **Frankreich: +33 1 57 32 42 68**
- **Per E-Mail an Enterprisesales@thawte.com**
- **Besuchen Sie unsere Website: http://www.thawte.de/ssl/volume-discount-ssl-certificates/index.html**

Mit den renommierten digitalen Zertifikaten des führenden internationalen Online-Sicherheitsexperten Thawte schützen Sie Ihr Unternehmen und bauen so bei Ihren Kunden Vertrauen auf. Seit 17 Jahren bietet Thawte seinen Kunden Stabilität, Zuverlässigkeit, eine bewährte Infrastruktur und erstklassigen Kunden-Support. Deshalb entscheiden sich Kunden weltweit für Thawte als ihren internationalen Sicherheitspartner.

UID 192/2/13