digicert®

CHECKLISTE: BEST PRACTICES FÜR DIE VERWALTUNG VON TLS-ZERTIFIKATEN

Allein im vergangenen Jahr wurden in 60 % der Unternehmen geschäftskritische Anwendungen mindestens einmal beeinträchtigt, weil ein TLS-Zertifikat nicht verfügbar war.[1] Solche Ausfälle können das Wachstum und den guten Ruf eines Unternehmens erheblich beeinträchtigen und verursachen im Durchschnitt Einbußen von 5.600 USD pro Minute.[2]

Deshalb ist es heute wichtiger denn je, kompromisslose Sicherheitsstandards für die Verwaltung Ihrer digitalen Zertifikate zu etablieren und konsequent anzuwenden.

Diese Checkliste von Best Practices soll Unternehmen wie Ihres dazu anregen, Wissenslücken im Bereich der Zertifikatsverwaltung zu füllen, Sicherheitsmaßnahmen netzwerkweit durchzusetzen und den Überblick über den gesamten Lebenszyklus Ihrer Zertifikate zu behalten, um betriebsschädigende Ausfälle zu vermeiden.

INVENTUR

Erstellen Sie eine Liste aller ausgestellten Zertifikate

Wenn Sie nicht genau wissen, welche Zertifikate im Einsatz sind, können Sie sie nicht hinreichend schützen. Erstellen Sie also eine detaillierte Liste sämtlicher von Ihrer Zertifizierungsstelle ausgestellten Zertifikate. Da eine solche netzwerkweite Bestandaufnahme Ihrer TLS-Zertifikate zeit- und ressourcenaufwendig sein kann, empfehlen wir Ihnen, einen Netzwerkscanner zu nutzen.

Ermitteln Sie, wo diese Zertifikate installiert sind

Doch damit ist die Arbeit noch nicht getan. Nicht konforme Zertifikate können die Übertragung verschlüsselter Daten gestatten, ohne Sie zu benachrichtigen. Ermitteln Sie also, wo Ihre Zertifikate installiert sind, und nehmen Sie die Serverstandorte in die Inventarliste auf.

Identifizieren Sie die Eigentümer aller Zertifikate und Domains

Abgelaufene Zertifikate sind eine häufige Ursache von Anwendungs- oder Serviceausfällen. Deshalb müssen Sie wissen, wer in Ihrem Unternehmen Zertifikate kauft, und Sie benötigen Prozesse zum Erneuern dieser Zertifikate und zur Änderung des Eigentümers, falls der Käufer Ihr Unternehmen verlässt.

Erfassen Sie die Betriebssystem- und Anwendungsversionen Ihrer Webserver

Hacker nutzen Schwachstellen aus, um in Betriebssysteme einzudringen. Ein Beispiel ist Heartbleed in der Kryptographiebibliothek OpenSSL, die für unbefugte Systemzugriffe über das Internet missbraucht werden kann. Daher sollte Ihr Zertifikatsinventar unbedingt auch Angaben zu Betriebssystemen und Anwendungen enthalten.

Identifizieren Sie die von den Webservern genutzten Cipher-Suiten und TLS-Versionen

Als Cipher-Suite wird eine Sammlung von Algorithmen bezeichnet, die dem Schutz einer auf TLS-Verschlüsselung basierten Netzwerkverbindung dienen. Veraltete TLS-Versionen und risikobehaftete Cipher-Suites sind beliebte Ziele für Hacker. Daher sollte Ihrem Zertifikatsinventar zu entnehmen sein, welche Versionen Sie nutzen.

[1] https://www.venafi.com/blog/majority-businesses-still-experience-outages-are-you-protecting-your-certificates
[2] https://www.venafi.com/blog/what-if-you-could-guarantee-eliminating-outages-your-organization

PROBLEMBEHEBUNG

Deaktivieren Sie schwache Schlüssel, Cipher-Suiten und Hash-Algorithmen

Prüfen Sie, ob veraltete Hash-Algorithmen wie MD5 oder SHA-1 immer noch auf Ihren internen Websites im Einsatz sind und aktualisieren Sie diese. Die einzigen empfohlenen TLS-Versionen sind TLS 1.2 und TLS 1.3, denn sie stellen sicher, dass Sie moderne Cipher-Suiten wie AES verwenden.

Bringen Sie die Ausstellung und Verteilung von Wildcard-Zertifikaten unter Kontrolle

Wildcard-Zertifikate können sehr nützlich sein, da sie Schutz für zahlreiche Sub-Domains, Flexibilität und Benutzerfreundlichkeit bieten. Doch wenn Ihre privaten Schlüssel in die falschen Hände geraten, können Hacker sie nutzen, um sämtliche über diese Domains verwalteten Systeme zu manipulieren und Ihnen die Zertifikatswiderrufung und -neuausstellung erheblich zu erschweren. Sorgen Sie also dafür, dass Ihre Wildcard-Zertifikate strengen Sicherheitskontrollen unterliegen.

Nutzen Sie angemessene Zertifikatstypen

Zertifikate sollten zweckgebunden sein. Das bedeutet, dass Sie für interne Systeme private TLS-Zertifikate ausstellen können, aber für öffentliche Umgebungen die strengere Organization Validation (OV) oder Extended Validation (EV) nutzen sollten. Einfache DV-Zertifikate (Domain Validation) bieten nur wenig Sicherheit und sollten daher nicht für den Schutz von sensiblem Datenverkehr eingesetzt werden.

Überprüfen Sie die Zertifikate aller standardmäßig genutzten Anbieter

Die Zertifikate vieler Anbieter lösen Browser-Warnmeldungen aus, weil sie oft nicht von einer validierten Zertifizierungsstelle signiert wurden, abgelaufen sind oder schwache Verschlüsselungsmethoden nutzen und somit nicht für den Schutz von Produktionsumgebungen geeignet sind. Trotzdem sind in vielen Unternehmen Tausende dieser Zertifikate installiert. Wir empfehlen Ihnen dringend, solche Standardzertifikate aus Ihrem Netzwerk zu entfernen und Ihre Zertifikatsverwaltung mit modernen Automatisierungstools und einer branchenführenden Management-Plattform auf den neuesten Stand zu bringen.

Stellen Sie sicher, dass auf allen Webservern die neuesten Patches installiert sind

Spielen Sie regelmäßig die neuesten Patches auf Ihren Betriebssystemen und Webservern ein, um sie vor den schädlichsten Angriffen zu schützen.

SCHUTZ

- [ ] **Standardisieren und automatisieren Sie die Prozesse für die Ausstellung und Erneuerung von Zertifikaten**

  Indem Sie die TLS-Zertifikatsverwaltung automatisieren und standardisieren, können Sie menschliche Fehler vermeiden und gleichzeitig wertvolle Zeit sparen. Nutzen Sie dazu eine bedienfreundliche, hochwertige Zertifikatsmanagementplattform.

- [ ] **Installieren und erneuern Sie alle Zertifikate rechtzeitig**

  Passen Sie die Zertifikatserneuerung an Ihren Geschäftsrhythmus an. Wir empfehlen Ihnen, Ihre Zertifikate in regelmäßigen Zeitabständen zu erneuern und einen Puffer von mindestens 15 Tagen zwischen Erneuerungs- und Ablaufdatum einzuplanen. Das hängt jedoch von vielen Faktoren ab – einige Unternehmen benötigen möglicherweise einen Puffer von bis zu 90 Tagen.

- [ ] **Stellen Sie sicher, dass private Schlüssel nach der Erneuerung von Zertifikaten nicht weiter genutzt werden**

  Ganz gleich, ob Sie DV-, OV- oder EV-Zertifikate einsetzen: Wenn Sie private Schlüssel wiederverwenden, entsteht eine Schwachstelle, die von Hackern ausgenutzt werden kann. Erstellen Sie bei der Zertifikatserneuerung also immer ein neues Schlüsselpaar.

- [ ] **Installieren Sie Zertifikate und private Schlüssel auf sichere Art und Weise**

  Private Schlüssel sollten prinzipiell auf einem sicheren Computer erstellt und über verschlüsselte E-Mails verteilt werden. Außerdem sollte es möglich sein, diese Schlüssel automatisch vom System zu entfernen.

- [ ] **Achten Sie darauf, dass nicht mehr genutzte Zertifikate entfernt bzw. widerrufen werden**

  Stellen Sie sicher, dass geeignete Prozesse zum Entfernen und Widerrufen vorhandener Zertifikate in den Prozeduren für die Übergabe und Entsorgung von Systemen enthalten sind.

MONITORING

Durchsuchen Sie Netzwerke nach Änderungen

Moderne Netzwerkumgebungen unterliegen ständigen Veränderungen und die Anzahl der in Unternehmen verwendeten Zertifikate steigt rasant. Somit wird es für Administratoren immer schwieriger, den Überblick zu behalten. Scanning-Tools melden Änderungen und andere Umstände, die ein Eingreifen erforderlich machen, in Echtzeit, sodass Sie viel Zeit sparen und zudem Ihre Zertifikate besser schützen und den Verwaltungsprozess erheblich vereinfachen können.

Durchsuchen Sie die CT-Logs (Zertifikatstransparenz-Logs) nach nicht konformen Zertifikaten

Öffentliche Zertifikate, die nicht in diesen Logs verzeichnet sind, werden Kunden als nicht vertrauenswürdig gemeldet. Funktionen für die Prüfung der Zertifikatstransparenz ermöglichen es Ihnen, solche nicht konformen Zertifikate zu erkennen und zu entfernen, bevor sie Ihren Daten oder Ihrem Ruf schaden.

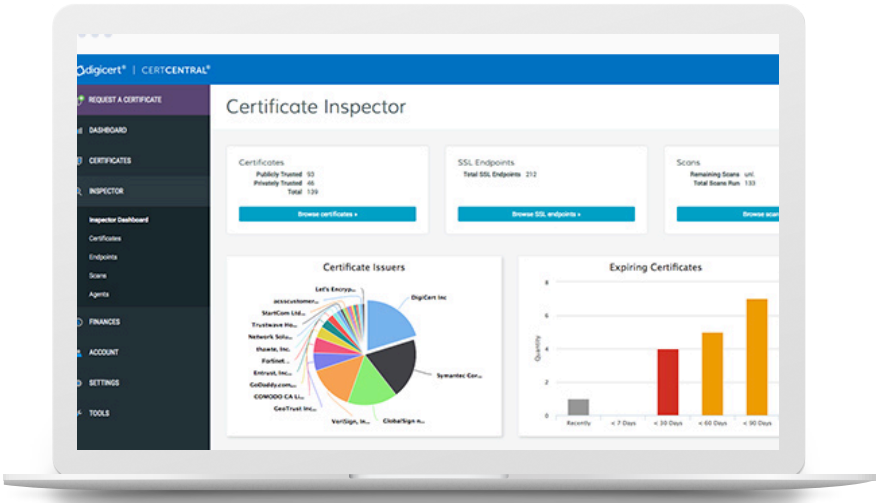
Nutzen Sie die CAA, um nicht autorisierte Zertifikatsanforderungen zu verhindern

Mithilfe von DNS Certification Authority Authorization (CAA) können Sie festlegen, welche Zertifizierungsstellen Zertifikate für Ihr Unternehmen ausstellen dürfen. Dadurch können Sie die Zertifikatausstellung auf vertrauenswürdige Zertifizierungsstellen beschränken und nicht von Ihnen autorisierte Stellen automatisch blockieren.

FAZIT

Nun wissen Sie, wie Sie Ihre Zertifikate und somit Ihr Unternehmen online besser schützen. Um Ihnen diese wichtige Aufgabe zu erleichtern, möchten wir Ihnen dazu gern unsere branchenführende Lösung empfehlen:

CertCentral von DigiCert



Zertifikatsverwaltung leicht gemacht

Mit DigiCert CertCentral® stehen Ihnen alle Tools und Funktionen zur Verfügung, die Sie benötigen, um Ihre Zertifikate zu identifizieren, zu schützen und zu überwachen und um effektiv auf Vorfälle zu reagieren. Außerdem erleichtert Ihnen CertCentral die Anpassung und Automatisierung Ihrer gesamten Zertifikatsinfrastruktur. Mit dieser Plattform können Sie ...

- Ihre Netzwerke nach neuen Systemen und Änderungen durchsuchen,
- CT-Logs nach nicht autorisierten Zertifikaten durchsuchen und
- die CAA nutzen, um nicht autorisierte Zertifikatsanforderungen aufzuspüren und zu verhindern.

Alles von einer zentralen Konsole aus.

Weitere Informationen finden Sie unter digicert.com/certificate-management