ERGEBNISSE DER REIFEGRADBEWERTUNG IHRER TLS-AUTOMATISIERUNG

Eine Bewertung des Automatisierungsgrads, Risikoniveaus und Verbesserungspotenzials der TLS-Zertifikatsverwaltung in Ihrem Unternehmen

digicert®

MANUELLE PROZESSE SIND FEHLERANFÄLLIG

Entdecken Sie moderne Best Practices zur Verwaltung von TLS-Zertifikaten.

IT-Führungskräfte suchen heute nach effizienten und flexiblen Methoden zur Gewährleistung der digitalen Sicherheit, da der Zeitaufwand für die Verwaltung von TLS-Zertifikaten und das Management der damit verbundenen Risiken höher ist als je zuvor. Viele IT-Profis erwägen die Einführung von Lösungen zur Automatisierung von TLS-Zertifikaten, um mehr Struktur in dieses komplexe Aufgabengeflecht zu bringen.

Die Notwendigkeit der Automatisierung

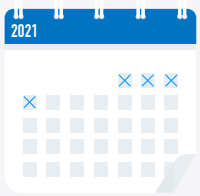
Experten für digitale Sicherheit sind sich einig, dass die TLS-Automatisierung die bewährteste Methode ist, zukünftigen Schwachstellen vorzubeugen. Einer der Hauptgründe dafür ist die Arbeitserleichterung durch die Automatisierung der Zertifikatsverwaltung. Dank Funktionen wie der Zertifikatssuche in DigiCert CertCentral® können Unternehmen jedes Zertifikat innerhalb und außerhalb des eigenen Netzwerks automatisch erfassen und zuordnen.

Gleichzeitig stärkt die Automatisierung des gesamten Lebenszyklus von TLS-Zertifikaten die IT-Sicherheit und verhindert Serviceunterbrechungen durch abgelaufene und nicht rechtzeitig erneuerte Zertifikate. Zudem versetzt eine automatisierte, den gesamten Zertifikatslebenszyklus umfassende Zertifikatsverwaltung Unternehmen in die Lage, schnell auf branchen- oder CA-spezifische Compliance-Vorfälle zu reagieren und ihre Zertifikate umgehend zu ersetzen oder sogar PQC-Lösungen (Post-Quanten-Kryptographie) zu implementieren. Aus diesen und anderen Gründen sind effiziente Prozesse zur Gewährleistung der digitalen Sicherheit unverzichtbar.

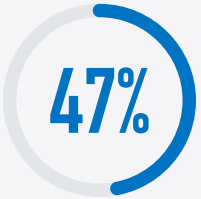
Wie steht es um Ihre Sicherheit?

Die von DigiCert bereitgestellte Reifegradbewertung der TLS-Automatisierung beleuchtet Ihre aktuelle Nutzung von Tools für die Erkennung und Automatisierung von TLS-Zertifikaten und zeigt auf, wie Sie Ihren Sicherheitsstatus verbessern können. Anhand der Bewertung können Sie entscheiden, welches Bereitstellungsmodell für Ihr Unternehmen geeignet ist. Unsere Lösungen decken ein breites Spektrum bezüglich der Art und Anzahl von Zertifikaten ab, um den Anforderungen großer, mittlerer und kleiner Unternehmen gerecht zu werden. Jedes Unternehmen ist einzigartig. Deshalb muss die für Sie passende Automatisierungslösung optimal auf die Anforderungen und Ressourcen Ihrer IT zugeschnitten sein.

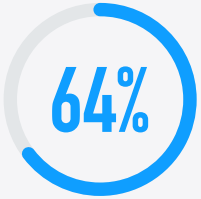
DIGITALE SICHERHEIT IN ZAHLEN



1–4 Arbeitstage pro Monat werden für die Verwaltung von Zertifikaten aufgewendet



Im Schnitt entfallen 47 % der Arbeitszeit von IT-Fachkräften auf die Zertifikatsverwaltung

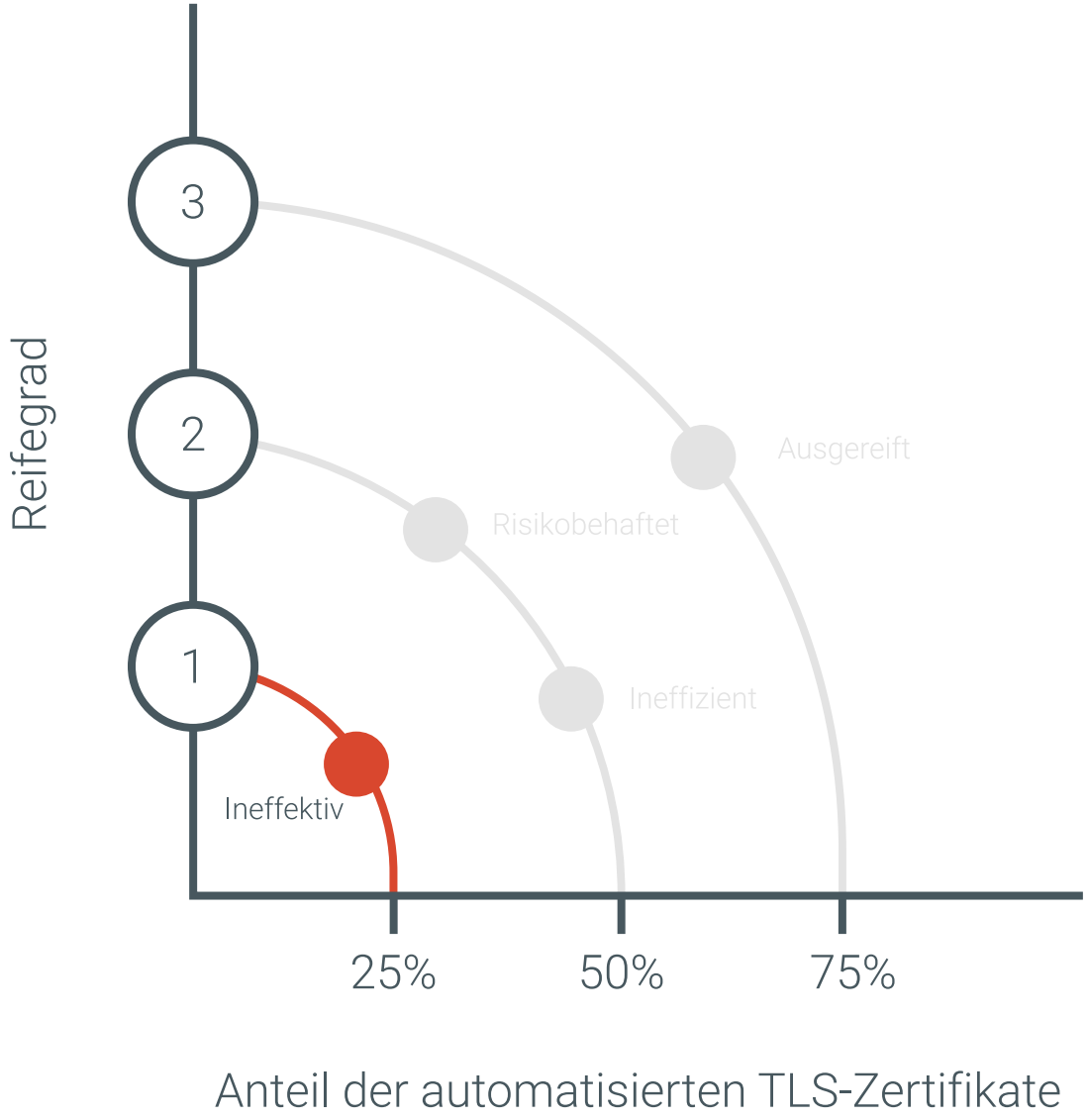


64 % der Befragten finden jeden Monat nicht erfasste Zertifikate

Für 38 % der Befragten ist der Zeitaufwand für die Zertifikatsverwaltung ein großes Problem

Quelle: Studienbericht von YouGov zur TLS-Automatisierung, Feb. 2021

REIFEGRADMODELL DER TLS-AUTOMATISIERUNG



IHR ERGEBNIS

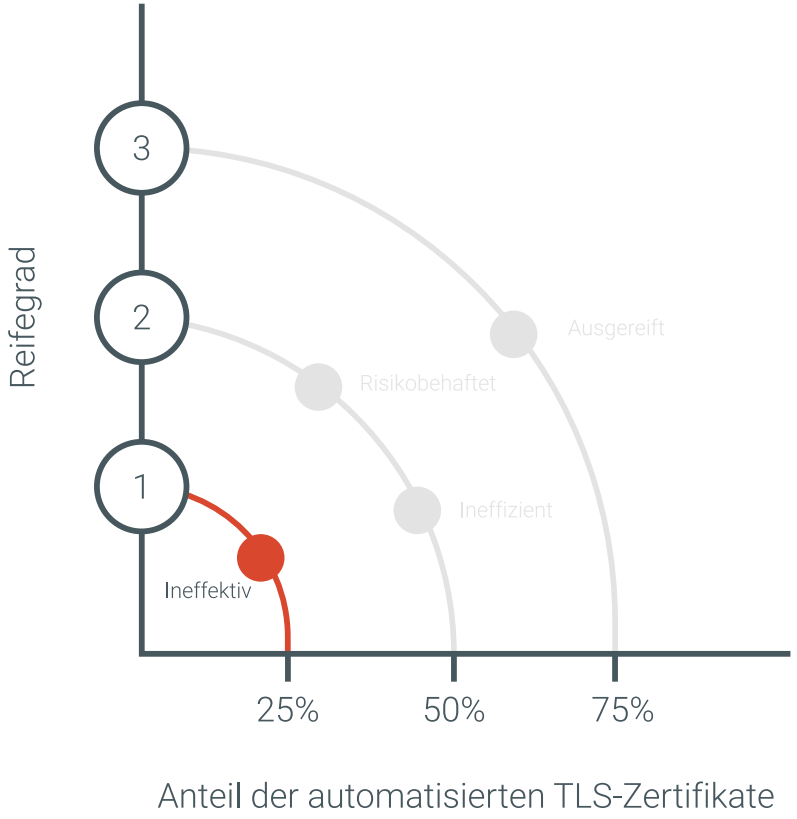
Leitfaden zur Beurteilung Ihres Sicherheitsstatus.

Sicherheitsstatus:
REAKTIV

IHR GESAMTRISIKO: HOCH

Ihre aktuelle Strategie für die Zertifikatsverwaltung führt zu einer reaktiven Haltung gegenüber zertifikatsbedingten Ausfällen, Gefährdungen und Problemen bei Zertifizierungsstellen (CA). Einer der wichtigsten Risikofaktoren ist, dass Sie keinen umfassenden Überblick über all Ihre Zertifikate haben und daher oft nicht rechtzeitig eingreifen können, wenn dies erforderlich ist. Zudem ist Ihr Unternehmen aufgrund ineffizienter, manueller Prozesse anfällig für Bedrohungen aller Art.

Kleinere Unternehmen in dieser Kategorie verfügen möglicherweise über eine Inventarliste ihrer Zertifikate, die aber keine Auskunft über weniger offensichtliche Probleme wie Fehlkonfigurationen bzw. schwache Schlüssel, Cipher-Suiten oder Hash-Algorithmen geben kann. Für größere Unternehmen ist es generell schwierig, den ganzen Zertifikatsbestand manuell zu verwalten. Wenn ohne Ihr Wissen nicht konforme Zertifikate installiert werden, entstehen tote Winkel, die als Einfallstore für Malwareangriffe ausgenutzt werden können. Unternehmen wie das Ihre sind einem hohen Risiko für kostspielige Serviceausfälle ausgesetzt.



WEITERE VORGEHENSWEISE

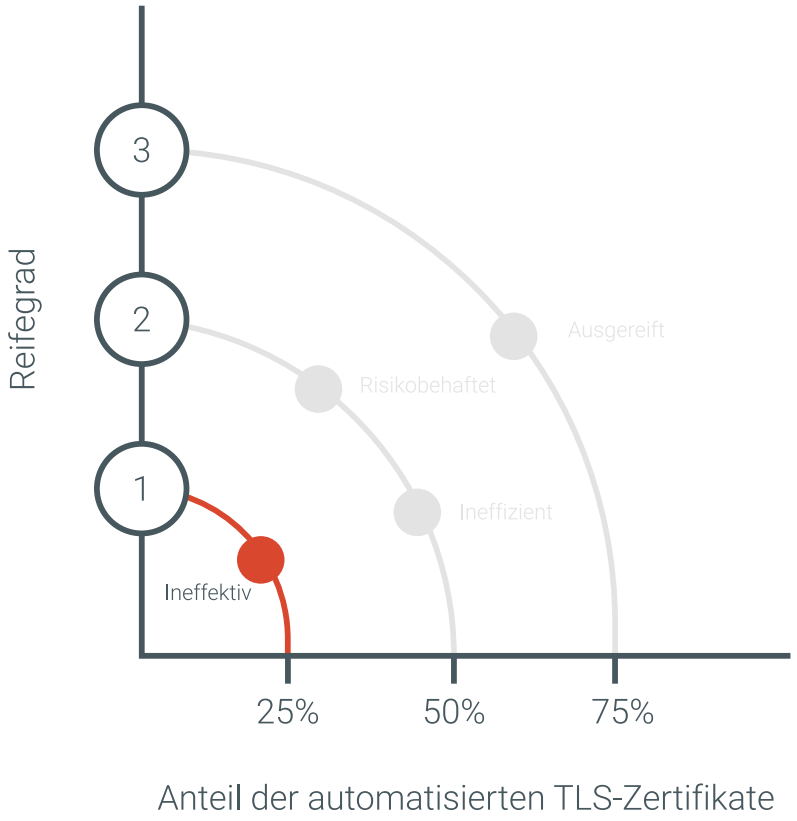
Die nächsten Schritte zu mehr Sicherheit.

Sicherheitsstatus:

REAKTIV

Wir empfehlen Ihnen, **innerhalb der nächsten 90 Tage** die folgenden Maßnahmen zu ergreifen:

- Einführung einer Lösung für die konsolidierte Verwaltung von Zertifikaten: Mit DigiCert CertCentral® können Sie alle Zertifikate über eine zentrale Konsole verwalten, ausstellen, widerrufen und ersetzen.
- Implementierung eines Tools für automatische Scans für das Monitoring Ihres gesamten Zertifikatsbestands: Durch gezielte Scans erkennen Sie Veränderungen in Ihrer IT-Umgebung und können rechtzeitig auf zertifikatsbedingte Probleme reagieren.
- Einführung von Best Practices für das TLS-Management: Veranlassen Sie Mitarbeiterschulungen zu sicherheitsrelevanten Themen wie Monitoring des Zertifikatsbestands, standardisierte Speicherung von Schlüsseln, Etappen des Zertifikatslebenszyklus, Prozesse für die Außerbetriebnahme und Monitoring mittels CT-Logs.
- Groß angelegte Ausweitung der Automatisierung: Nutzen Sie Profile, Zeitpläne, Benachrichtigungen und integrieren Sie Drittanbieterlösungen.
- Unser Automatisierungsassistent: Der intelligente Assistent von DigiCert unterstützt Sie bei der Auswahl des richtigen Bereitstellungsmodells und führt Sie durch die Installation und Einrichtung.
- Verwendung von APIs: Über REST APIs können beliebige Systeme und Anwendungen integriert werden. DigiCert bietet zudem vorkonfigurierte Integrationen von Drittlösungen.
- Für kleine und mittlere Unternehmen: Die Managed ACME-Funktion ist ein gehostetes, agentenbasiertes Tool, das eine benutzerfreundliche Zertifikatsverwaltung über das ACME-Protokoll in CertCentral ermöglicht.



WIE STEHT ES UM IHRE TLS-SICHERHEIT?

Informieren Sie sich über Ihren Sicherheitsstatus in dieser Vergleichsansicht aller drei Bewertungen.

Sicherheitsstatus:
REAKTIV

IHR GESAMTRISIKO: HOCH

Ihre aktuelle Strategie für die Zertifikatsverwaltung führt zu einer reaktiven Haltung gegenüber zertifikatsbedingten Ausfällen, Gefährdungen und Problemen bei Zertifizierungsstellen (CA). Einer der wichtigsten Risikofaktoren ist, dass Sie keinen umfassenden Überblick über all Ihre Zertifikate haben und daher oft nicht rechtzeitig eingreifen können, wenn dies erforderlich ist. Zudem ist Ihr Unternehmen aufgrund ineffizienter, manueller Prozesse anfällig für Bedrohungen aller Art.

Kleinere Unternehmen in dieser Kategorie verfügen möglicherweise über eine Inventarliste ihrer Zertifikate, die aber keine Auskunft über weniger offensichtliche Probleme wie Fehlkonfigurationen bzw. schwache Schlüssel, Cipher-Suiten oder Hash-Algorithmen geben kann. Für größere Unternehmen ist es generell schwierig, den ganzen Zertifikatsbestand manuell zu verwalten. Wenn ohne Ihr Wissen nicht konforme Zertifikate installiert werden, entstehen tote Winkel, die als Einfallstore für Malwareangriffe ausgenutzt werden können. Unternehmen wie das Ihre sind einem hohen Risiko für kostspielige Serviceausfälle ausgesetzt.

Sicherheitsstatus:
VERBESSERUNGSFÄHIG

IHR GESAMTRISIKO: DURCHSCHNITTLICH

Ihr Unternehmen nutzt unter anderem eine Lösung für die zentrale Verwaltung von TLS/SSL-Zertifikaten und ist daher auf dem richtigen Weg. Bei der Behebung von Ausfällen und anderen Problemen könnte Ihr Team allerdings schneller und agiler sein. Ohne Automatisierungstools ist die Fehlerbehebung oft mühsam, ineffizient und zeitaufwendig, besonders in verteilten oder komplexen Umgebungen. Ihre Prozesse für Routineaufgaben wie den Ersatz von Herstellerzertifikaten (die oft selbstsigniert bzw. schwach verschlüsselt sind) durch ein geeignetes anderes Zertifikat könnten ebenfalls gestrafft werden.

Automatisierung ist keine Einheitslösung. Im Sinne einer optimalen Effizienz sollten Sie verschiedene Bereitstellungsoptionen wie On-Premises, Cloud oder hybride Lösungen gegeneinander abwägen.

Sicherheitsstatus:
PROAKTIV UND AUSGEREIFT

IHR GESAMTRISIKO: NIEDRIG

Ihre automatisierten Prozesse sind effizient und stimmig. Sie haben einen guten Überblick über alle TLS/SSL-Zertifikate in Ihrer IT-Umgebung und Ihr Unternehmen schützt sich durch proaktive Maßnahmen vor Compliance-Problemen, zukünftigen Veränderungen in der Branche und potenziellen zertifikatsbedingten Ausfällen. Ausgereifte Unternehmen haben ihren gesamten Zertifikatsbestand unter Kontrolle und bis zu 75 Prozent der Zertifikate werden automatisiert verwaltet. Zudem ist die Automatisierung in diesen Betrieben in den internen Sicherheitsrichtlinien verankert.

Erwägen Sie die vollständige Automatisierung Ihres gesamten Zertifikatsbestands, damit Sie gegen zukünftige Bedrohungen gewappnet sind, bei Serviceausfällen alle Zertifikate schnell ersetzen können und auch auf den Übergang zur Post-Quanten-Kryptographie vorbereitet sind.

UNSERE EMPFEHLUNGEN

Diese TLS-Lösungen sollten Sie implementieren.

Sicherheitsstatus:
REAKTIV

Wir empfehlen Ihnen, **innerhalb der nächsten 90 Tage** die folgenden Maßnahmen zu ergreifen:

- Einführung einer zentralen Lösung für die Verwaltung aller Zertifikate: Mit DigiCert CertCentral® können Sie alle Zertifikate über eine zentrale Konsole verwalten, ausstellen, widerrufen und ersetzen.
- Implementierung eines Tools für automatische Scans für das Monitoring Ihres gesamten Zertifikatsbestands: Durch gezielte Scans erkennen Sie Veränderungen in Ihrer IT-Umgebung und können rechtzeitig auf zertifikatsbedingte Probleme reagieren.
- Einführung von Best Practices für das TLS-Management: Veranlassen Sie Mitarbeiterschulungen zu sicherheitsrelevanten Themen wie Monitoring des Zertifikatsbestands, standardisierte Speicherung von Schlüsseln, Etappen des Zertifikatslebenszyklus, Prozesse für die Außerbetriebnahme und Monitoring mittels CT-Logs.
- Groß angelegte Ausweitung der Automatisierung: Nutzen Sie Profile, Zeitpläne, Benachrichtigungen und integrieren Sie Drittanbieterlösungen.

Sicherheitsstatus:
VERBESSERUNGSFÄHIG

Wir empfehlen Ihnen, **innerhalb der nächsten sechs Monate** die folgenden Maßnahmen zu ergreifen:

- Maßgeschneiderte Automatisierungsprozesse: Von ACME-URLs über APIs, Managed ACME-Agenten und Sensor-Automatisierung bis hin zum brandneuen Automation Manager bieten wir zahlreiche Lösungen an, die genau auf Ihre Sicherheitsanforderungen zugeschnitten werden können.
- Planen Sie regelmäßige, monatliche Discovery Scans aller primären Domains und FQDNs (vollständig qualifizierte Domainnamen) ein.
- Sehen Sie sich Ihren TLS-Stack an und erwägen Sie, ob sich bestimmte Systeme oder andere Ressourcen konsolidieren lassen: Konzentrieren Sie sich dabei auf Innovationen, Prozessverbesserungen und Effizienzgewinne.
- Integrieren Sie die Automatisierung als Standardkonzept in Ihre Richtlinien für die Verwaltung des Lebenszyklus von TLS/SSL-Zertifikaten.
- Unser Automatisierungsassistent: Der intelligente Assistent von DigiCert unterstützt Sie bei der Auswahl des richtigen Bereitstellungsmodells.

Sicherheitsstatus:
PROAKTIV UND AUSGEREIFT

Wir empfehlen Ihnen, **im Laufe des nächsten Jahres** die folgenden Maßnahmen zu ergreifen:

- Behalten Sie die Richtlinien bei, in denen die Automatisierung als Standardlösung empfohlen wird.
- Automatisieren Sie mehrere Implementierungen mithilfe verschiedener Bereitstellungsmodelle (gehostet bzw. On-Premises).
- Planen Sie regelmäßige, monatliche Discovery Scans aller primären Domains und FQDNs (vollständig qualifizierte Domainnamen) ein.
- Erwägen Sie den Einsatz von Automation Manager, wenn eine größere Anzahl von Zertifikaten implementiert werden muss.
- Bleiben Sie krypto-agil und nutzen Sie weiterhin Automatisierungstools, um zukünftigen Anforderungen wie der Quantenkryptographie gewachsen zu sein.

DIE BESTE BERATUNG IN DER BRANCHE

Unsere Automatisierungstools sind keine Einheitslösung. Sprechen Sie mit Ihrem Account Manager oder schreiben Sie an contactus@digicert.com. Wir unterstützen Sie gern bei der Auswahl einer für Ihr Unternehmen geeigneten Lösung.

digicert®