eBook

# BEST PRACTICES FÜR TLS

digicert®

digicert®

# BESSERE GESCHÄFTE DANK BEST PRACTICES

Ein abgelaufenes Zertifikat kann schnell zum zeitaufwendigen Problem werden. Allein im vergangenen Jahr wurde der Geschäftsbetrieb von 60 % aller Unternehmen mindestens einmal beeinträchtigt, weil ein Zertifikat nicht verfügbar war. In diesem E-Book finden Sie einen ausführlichen und doch unkomplizierten Leitfaden für Best Practices in Bezug auf die Zertifikatsverwaltung – damit Sie nicht auch ein Fall für die Statistik werden.

# INHALT

## INVENTUR

Erstellen Sie eine Liste aller ausgestellten Zertifikate.

Ermitteln Sie, wo diese Zertifikate installiert sind.

Identifizieren Sie die Eigentümer aller Zertifikate und Domains.

Erfassen Sie die Webserver-, Betriebssystem - und Anwendungsversionen.

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

## FEHLERBEHEBUNG

Ersetzen Sie schwache Schlüssel, Cipher-Suiten und Hash-Algorithmen.

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

Nutzen Sie angemessene Zertifikatstypen.

Überprüfen Sie die Zertifikate aller standardmäßig genutzten Anbieter.

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

## SCHUTZ

Standardisieren und automatisieren Sie die Prozesse für die Ausstellung und Erneuerung von Zertifikaten.

Installieren und erneuern Sie alle Zertifikate rechtzeitig.

Achten Sie darauf, dass private Schlüssel nach der Erneuerung von Zertifikaten nicht weiter genutzt werden.

Installieren Sie Zertifikate und private Schlüssel auf sichere Art und Weise.

Achten Sie darauf, dass nicht mehr genutzte Zertifikate entfernt bzw. widerrufen werden.

## MONITORING

Durchsuchen Sie Netzwerke nach neuen Systemen und Änderungen.

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

Nutzen Sie die CAA, um nicht autorisierte Zertifikatsanforderungen zu verhindern.

# ERSTELLEN SIE EINE LISTE ALLER AUSGESTELLTEN ZERTIFIKATE

## Am besten beginnen Sie mit einer Inventur aller Zertifikate in Ihrer Umgebung. Erfassen Sie dabei alle Zertifikatseigentümer, Speicherorte, Domains, Versionen der Betriebssysteme und Anwendungen, Cipher-Suiten und TLS-Versionen.

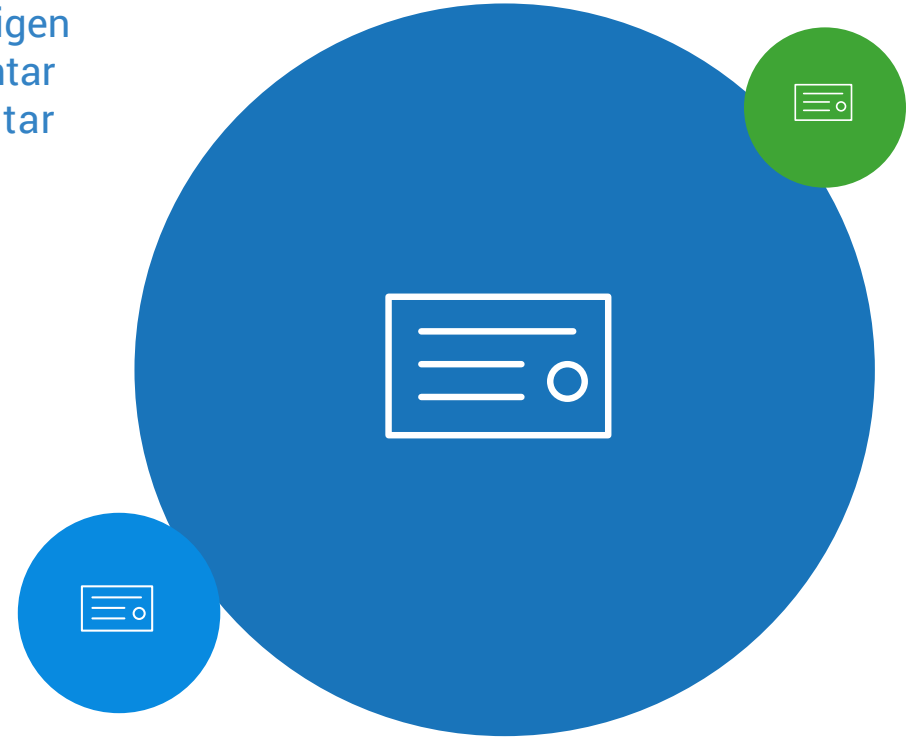
Wenn Sie nicht genau wissen, welche Zertifikate Ihr Unternehmen besitzt, setzen Sie sich Sicherheitsrisiken, wie ablaufenden Zertifikaten oder schwachen Schlüsseln und Hashes, aus. Ihr Inventar sollte detaillierte Zertifikatsangaben, wie Zertifikatstyp (DV, OV, EV usw.) aller ausstellenden CAs, sowie etwaige Probleme mit Ausstellern, Schlüssellängen, Algorithmen, Ablaufdaten und andere Zertifikatselemente enthalten.

Zum Einstieg empfiehlt es sich, eine Liste aller ausgestellten Zertifikaten von Ihren CAs anzufordern. Doch wie können Sie sicher sein, dass Sie nichts übersehen haben? Was ist mit internen CAs und Netzwerkgeräten mit TLS-Zertifikaten? Am besten verwenden Sie einen Netzwerkscanner zum Auffinden von TLS-Zertifikaten. Viele Unternehmen sind überrascht, wenn sie sehen, wie viele Zertifikate sie haben, von denen sie gar nichts wussten.

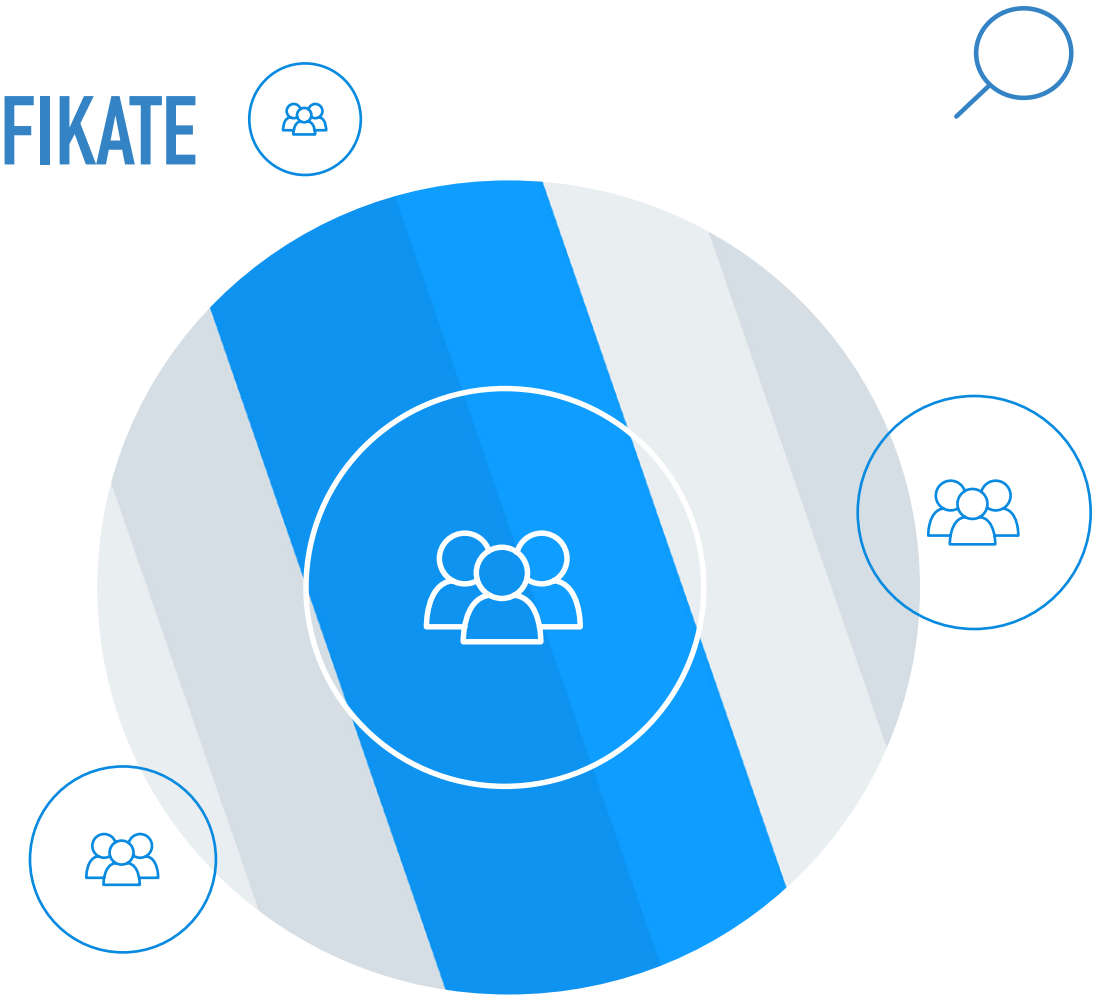
# ERMITTELN SIE, WO DIESE ZERTIFIKATE INSTALLIERT SIND

Nur weil Sie ein Zertifikat ausgestellt haben, heißt das nicht, dass es auch korrekt und an der richtigen Stelle installiert wurde. Mit Ihrem Zertifikatinventar als Ausgangspunkt sollten Sie auch ein Inventar verifizierter Serverstandorte erstellen.

Das kann manuell geschehen, doch größere Unternehmen überprüfen ihre Systeme in regelmäßigen Abständen automatisch darauf, dass alle Zertifikate dort installiert sind, wo sie hingehören. Nicht konforme Zertifikate können dazu führen, dass verschlüsselte Daten das Netzwerk unbemerkt verlassen.



# IDENTIFIZIEREN SIE DIE EIGENTÜMER ALLER ZERTIFIKATE UND DOMAINS



## Wer kauft sonst noch Zertifikate? Wer kümmert sich um deren Erneuerung? Wo gibt es Lücken?

Wenn ein Zertifikatseigentümer Ihr Unternehmen verlässt, kann es passieren, dass Zertifikate ablaufen und zu kostspieligen Ausfällen führen. Daher ist es wichtig, dass jedes Zertifikat einen bekannten Eigentümer hat und dass Prozesse für die Erneuerung und Eigentumsübergabe definiert sind. Auch wer für Domains verantwortlich ist, muss überprüft werden, damit eine CA Zertifikate für eine öffentliche Domain ausstellen kann.

# IDENTIFIZIEREN SIE DIE VERSIONEN DER BETRIEBSSYSTEME UND ANWENDUNGEN AUF DEM WEBSERVER.


## Ihr Inventar sollte auch Angaben zum Betriebssystem (z. B. Windows oder Linux) und zu Anwendungen (z. B. Apache) enthalten.

Dies ist wichtig, weil Ihr Unternehmen anfällig für Exploits sein könnte, die zum Beispiel Schwachstellen in bestimmten OpenSSL-Versionen ausnutzen (wie Heartbleed).

# IDENTIFIZIEREN SIE DIE VON DEN WEBSERVERN GENUTZTEN CIPHER-SUITEN UND SSL-VERSIONEN.

## Schließlich sollte Ihr Inventar auch die von den Webservern genutzten Cipher-Suiten und SSL-Versionen enthalten.

Diese sind normalerweise auf den Webservern konfiguriert. Viele SSL-spezifische Angriffe zielen auf ältere SSL-Versionen (z. B. der POODLE-Angriff auf SSL 3.0) oder ungeschützte Cipher-Suiten (z. B. der ROBOT-Angriff auf die RSA-Verschlüsselung) ab.

**Cipher-Suite:** Ein auf einem Webserver konfigurierter Algorithmensatz zum Schutz von SSL- oder TLS-Netzwerkverbindungen.

# FAZIT

## Ihr TLS-Inventar sollte Folgendes enthalten:

**Ausgestellte Zertifikate**
- Zertifikatstyp
- Schlüssellänge
- Algorithmus
- Ablaufdatum

**Zertifikatsstandorte**

**Zertifikatseigentümer**

**Webserver-Konfiguration**
- Betriebssystem (mit Version)
- Anwendungsversion
- TLS-Version
- Cipher-Suiten

# ERSETZEN SIE SCHWACHE SCHLÜSSEL, CIPHER-SUITEN UND HASH-ALGORITHMEN

## Bei der Inventur kommen höchstwahrscheinlich einige ungelöste Probleme ans Licht. Nun können Sie mit der Behebung dieser Probleme beginnen.

Zertifikate enthalten öffentliche Schlüssel und Signaturen, die anfällig für Angriffe sein könnten. Zertifikate mit Schlüssellängen von weniger als 2048 Bit oder mit älteren Hashing-Algorithmen wie MD5 oder SHA-1 sind auf öffentlichen Webservern nicht mehr erlaubt. Sie können sie aber durchaus noch auf Ihren internen Websites finden. Sie sollten die entsprechenden Zertifikate unbedingt aktualisieren.

Noch wichtiger als die Identifizierung von Zertifikaten mit schwachen Schlüsseln oder Hashes ist die Überprüfung der auf Ihren Webservern unterstützten TLS/SSL-Versionen und Cipher-Suiten.

**Die folgenden Versionen sind veraltet und anfällig und sollten deaktiviert werden:**

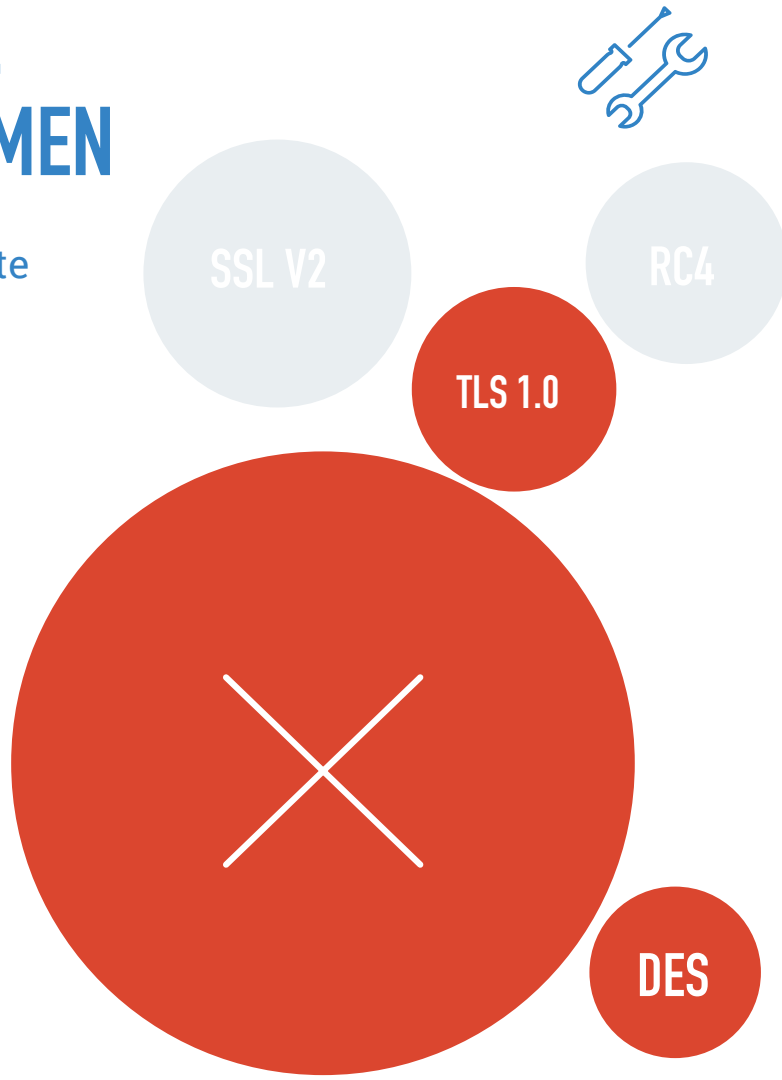
- SSL v2
- SSL v3
- TLS 1.0
- TLS 1.1

Aktivieren Sie stattdessen TLS 1.2 und TLS 1.3.

**Die folgenden Cipher-Suiten sind veraltet und anfällig und sollten deaktiviert werden:**

- DES
- 3DES
- RC4

Stattdessen sollten Sie moderne Cipher-Suiten wie AES verwenden.



digicert®

# BRINGEN SIE DIE AUSSTELLUNG UND VERTEILUNG VON WILDCARD-ZERTIFIKATEN UNTER KONTROLLE

## Wildcard-Zertifikate werden für einen Hostnamen mit Platzhaltern ausgestellt und schützen Systeme mit verschiedenen Hostnamen, die bestimmte Bedingungen erfüllen.

Das hat jedoch nicht nur Vorteile. Wenn der private Schlüssel eines Wildcard-Zertifikats gestohlen wird, können Angreifer ein System mit einem den Bedingungen entsprechenden Hostnamen aufsetzen und sich als legitimer Eigentümer der Domain ausgeben. So wurden gestohlene Wildcard-Schlüssel zum Beispiel schon für DNS-Spoofing oder zur Erstellung nicht konformer WLAN-Access-Points in einem Netzwerk genutzt.

Ein weiterer Nachteil ist, dass alle Kopie eines Wildcard-Zertifikats widerrufen und neu ausgestellt werden müssen, wenn das Zertifikat kompromittiert wurde. Davon können zahlreiche Systeme an verschiedenen Standorten betroffen sein. Je mehr Systeme mit einem Wildcard-Zertifikat geschützt sind, desto aufwendiger ist das. Und wenn die Zertifikate nicht gut dokumentiert sind, können Sie nicht sicher sein, dass Sie wirklich alle ersetzt haben.

Am besten lässt sich das vermeiden, indem von vornherein jedes Wildcard-Zertifikat mit einem eigenen privaten Schlüssel ausgestellt wird. Dann müssen nicht alle Kopien des Zertifikats widerrufen werden, wenn eine kompromittiert wurde.

Aufgrund dieser Probleme sind Wildcard-Zertifikate bei der Extended Validation (EV) nicht zulässig Wenn Sie jedoch über gut strukturierte und dokumentierte Prozesse verfügen, ist gegen die Verwendung von Wildcard-Zertifikaten nichts einzuwenden.

digicert®

# NUTZEN SIE ANGEMESSENE ZERTIFIKATSTYPEN.

## Nicht alle TLS-Zertifikate sind gleich.

So können private TLS-Zertifikate beispielsweise für interne Systeme verwendet werden, doch dazu muss das private Root-Zertifikat erfolgreich an die Nutzer weitergeleitet werden. Zum Schutz Ihrer öffentlich zugänglichen Website empfehlen wir hingegen OV- oder EV-Zertifikate. DV-Zertifikate sind für Websites, über die vertrauliche Daten übermittelt werden, auf keinen Fall zu empfehlen.



**Extended Validation (EV)**
- Domain-Rechte
- gründliche Prüfung des Unternehmens
- höchste Sicherheit

**Organization Validation (OV)**
- Domain-Rechte
- Prüfung der Geschäftsregistrierung
- hohe Sicherheit

**Domain Validation (DV)**
- Domain-Rechte
- niedrige Sicherheit

**Private SSL-Zertifikate**
- privates Root-Zertifikat muss an Nutzer weitergeleitet werden

**Selbstsignierte SSL-Zertifikate**
- nicht vertrauenswürdig

digicert®

# ÜBERPRÜFEN SIE DIE ZERTIFIKATE ALLER STANDARDMÄßIG GENUTZTEN ANBIETER

## Anbieterzertifikate zeichnen sich vorrangig durch einfache Verwendung und nicht unbedingt durch starke Sicherheit aus.

Das Problem ist, dass diese Zertifikate nie für Unternehmensnetzwerke vorgesehen waren. Anbieterzertifikate sind in der Regel selbstsigniert, abgelaufen oder verwenden schwache Schlüssel. Daher werden sie von Browsern nicht als vertrauenswürdig eingestuft. In vielen Unternehmen gibt es Tausende von Anbieterzertifikaten, ohne dass irgendjemand von ihnen weiß. Jedes dieser Zertifikate sollte entfernt und durch ein vertrauenswürdiges Zertifikat (mindestens ein privates SSL-Zertifikat) ersetzt werden. Optimieren lässt sich dieser Austauschvorgang mit modernen Automatisierungstools, zum Beispiel einem ACME-Protokoll.

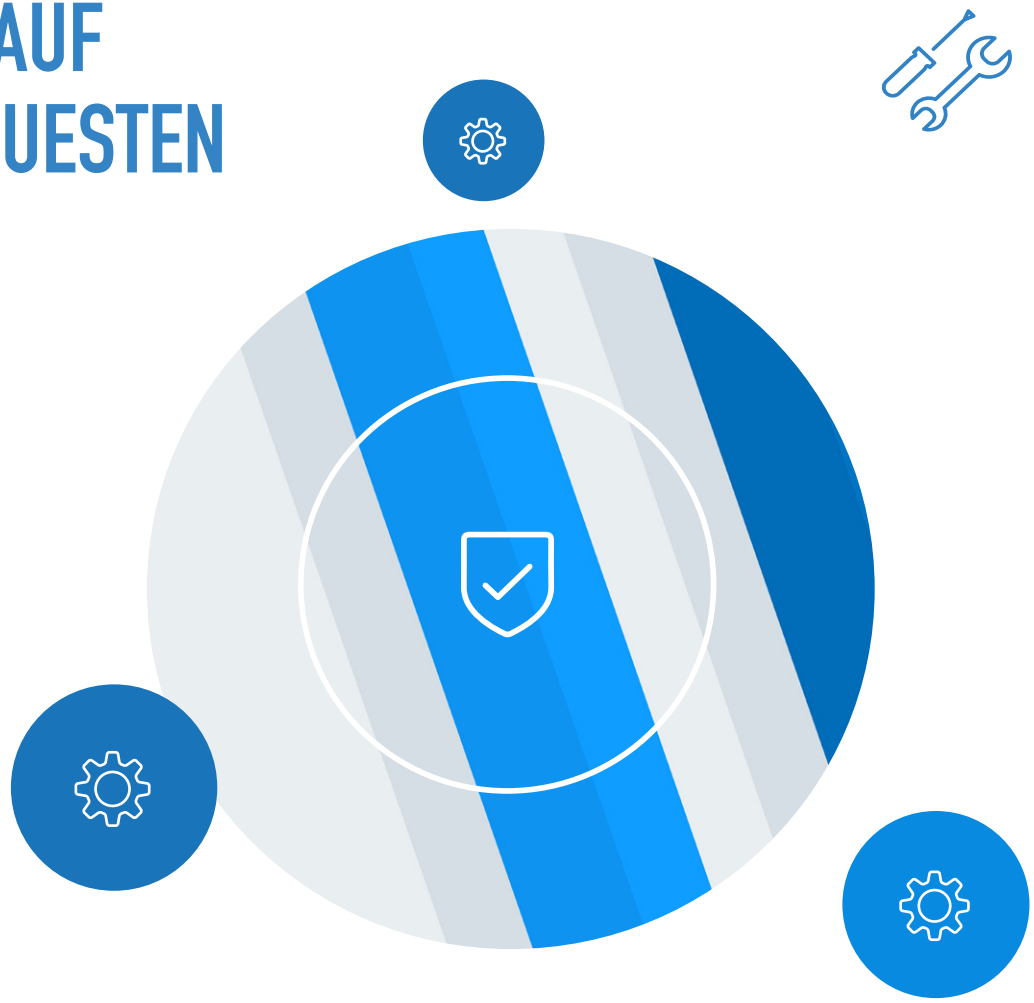
# STELLEN SIE SICHER, DASS AUF ALLEN WEBSERVERN DIE NEUESTEN PATCHES INSTALLIERT SIND

## Durch das Patchen der Betriebssysteme lassen sich einige der folgenschwersten internetbasierten Angriffe vermeiden.

Das gilt sowohl für Ihre Webserver, als auch Ihr Betriebssystem.

**Fazit**

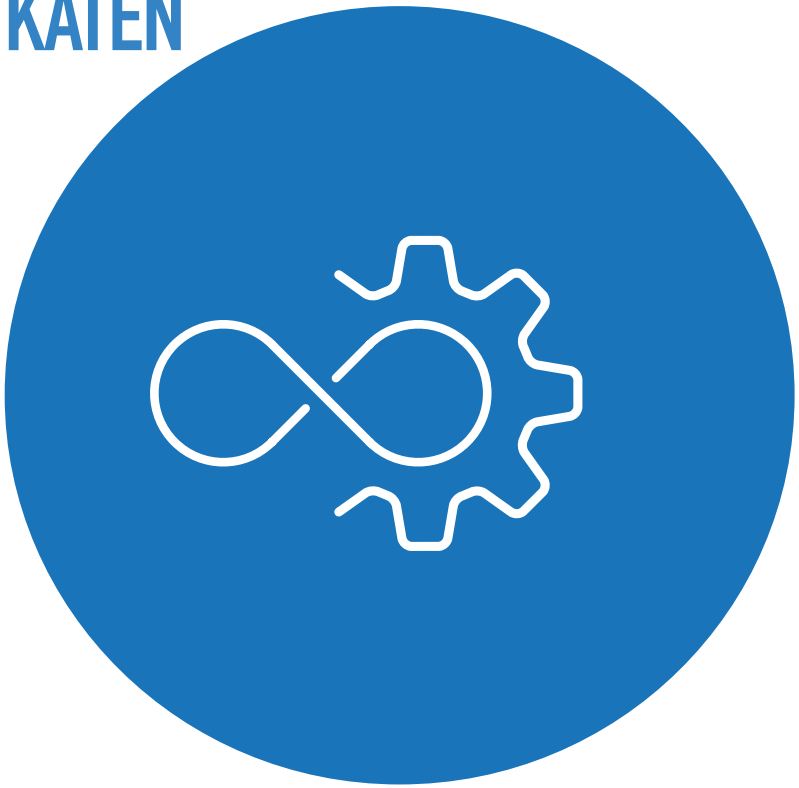
- Ersetzen Sie schwache Schlüssel und Hashes, wo das möglich ist.
- Deaktivieren Sie SSL v2 und v3 sowie TLS 1.0 und 1.1.
- Aktivieren Sie TLS 1.2, 1.3.
- Deaktivieren Sie schwache Cipher-Suiten von TLS 1.2.
- Behalten Sie Wildcard-Zertifikate unter Kontrolle.
- Verwenden Sie geeignete Zertifikatstypen.
- Ersetzen Sie Anbieterzertifikate.
- Sorgen Sie dafür, dass Webserver über die neuesten Patches verfügen.



# STANDARDISIEREN UND AUTOMATISIEREN SIE DIE PROZESSE FÜR DIE AUSSTELLUNG UND ERNEUERUNG VON ZERTIFIKATEN

## Nachdem Sie Probleme nun erkannt und behoben haben, können Sie damit beginnen, Richtlinien und Prozesse zu etablieren, um künftige Risiken zu mindern.

Erstellen Sie Standardprozesse für die Ausstellung und Erneuerung von Zertifikaten, um festzulegen, wer für was zuständig ist, um Nutzerfehler zu vermeiden und um SSL-Prozesse zu automatisieren. Die Bereitstellung von ACME-Protokollen, zum Beispiel, lässt sich in DigiCert® CertCentral für praktisch jeden Client- und Servertyp automatisieren.

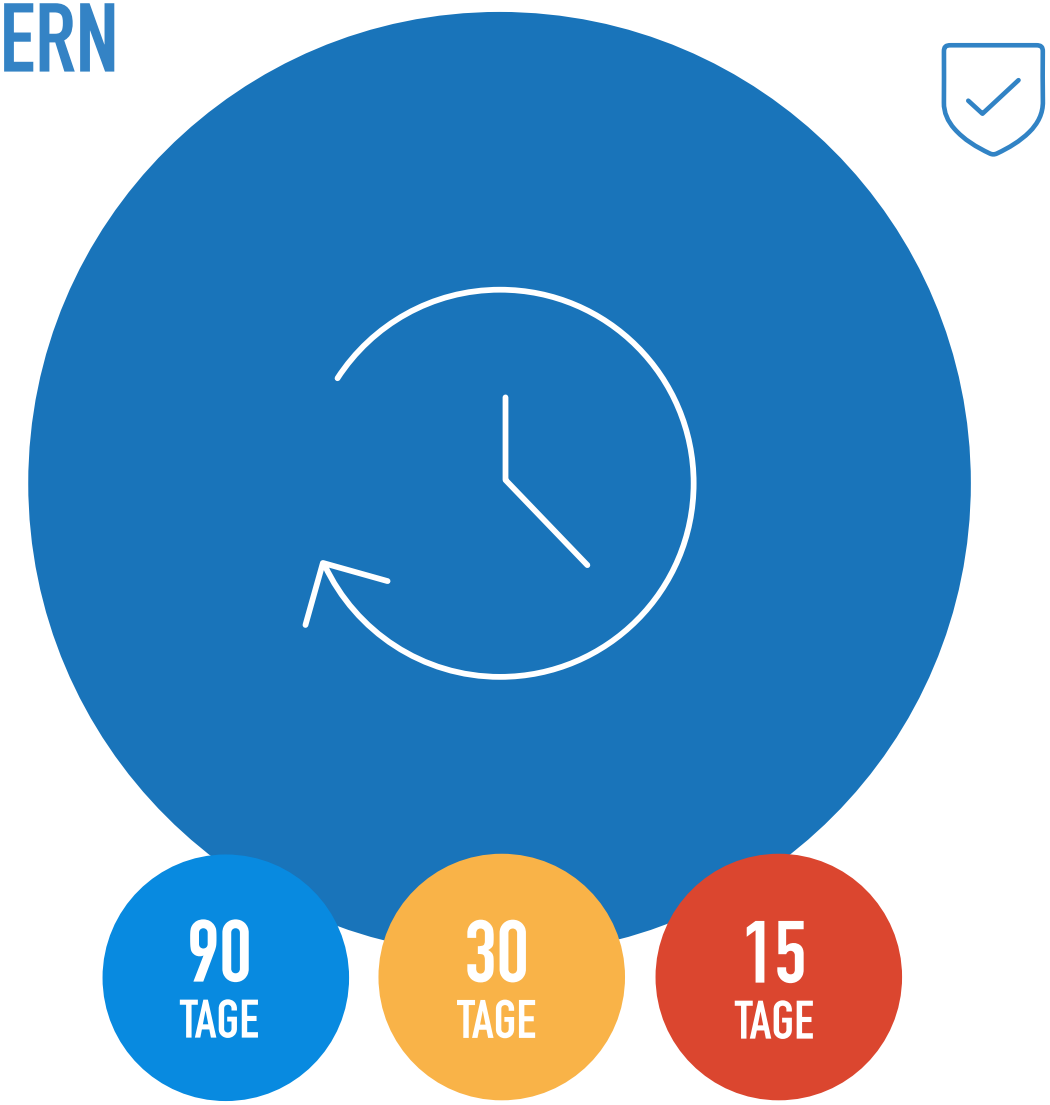


# INSTALLIEREN UND ERNEUERN SIE ALLE ZERTIFIKATE RECHTZEITIG

## Je nach Unternehmen stehen Sie vermutlich mehr oder weniger unter Zeitdruck.

Wir empfehlen, Zertifikate mindestens 15 Tage vor dem Ablaufdatum zu erneuern, um genügend Zeit für Tests zu haben und im Notfall auf das vorherige Zertifikat zurückgreifen zu können. Wenn Ihre Prozesse für das Änderungsmanagement besonders aufwendig sind, sollten Sie eventuell sogar 30 Tage vor Zertifikatsablauf verlängern.

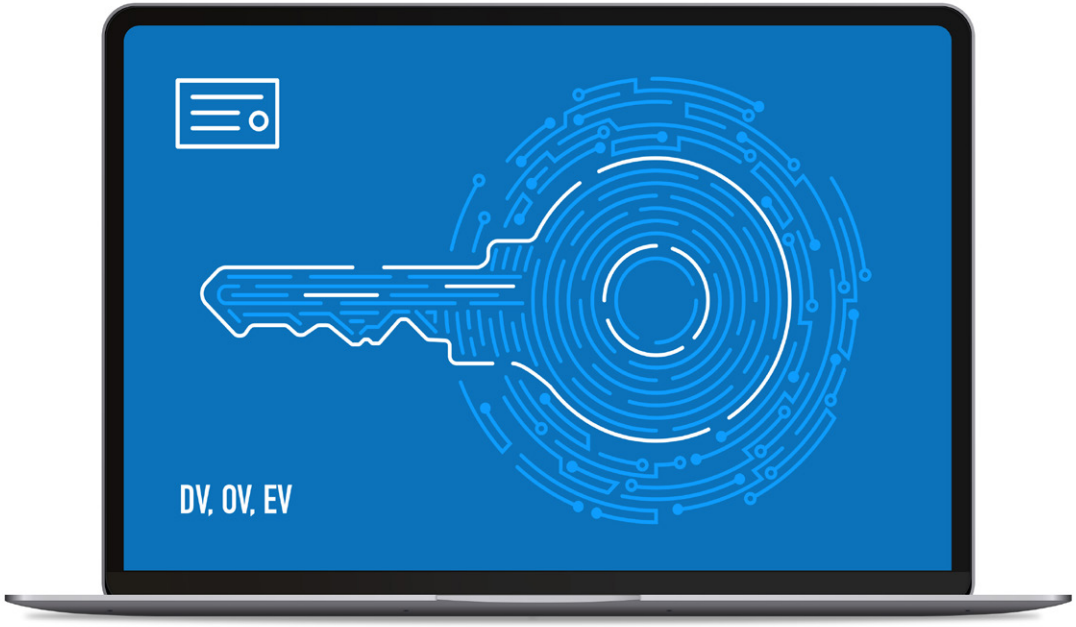
Unabhängig davon, welches System Sie verwenden, sollten die Nutzer mit Benachrichtigungen auf demnächst ablaufende Zertifikate hingewiesen werden. Das System sollte Nutzer automatisch und in regelmäßigen Abständen (z. B. 90, 60, 30, 15 Tage vor Ablauf) benachrichtigen.



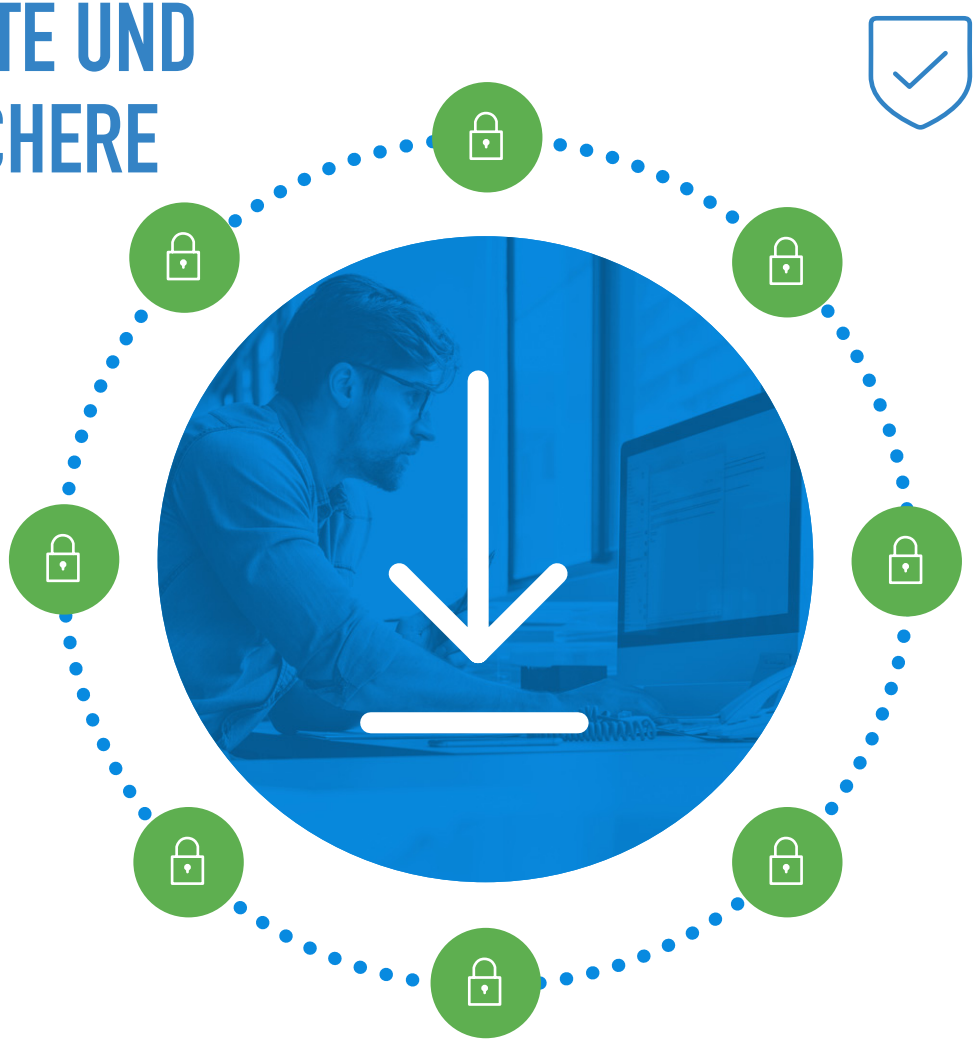
# ACHTEN SIE DARAUF, DASS PRIVATE SCHLÜSSEL NACH DER ERNEUERUNG VON ZERTIFIKATEN NICHT WEITER GENUTZT WERDEN

## Die Wiederverwendung privater Schlüssel erhöht das Risiko, dass diese Schlüssel geknackt werden.

Am besten sollte immer ein neues Schlüsselpaar erstellt werden. Auch CSRs sollten nie wiederverwendet werden, weil dadurch automatisch der private Schlüssel wiederverwendet wird.



# INSTALLIEREN SIE ZERTIFIKATE UND PRIVATE SCHLÜSSEL AUF SICHERE ART UND WEISE.



## In vielen Unternehmen gibt es Probleme mit dem sicheren Generieren und Speichern privater Schlüssel.

- Erzeugen Sie private Schlüssel auf einem sicheren und vertrauenswürdigen Computer.
- Geben Sie anderen nur Zugriff auf private Schlüssel, wenn dies absolut notwendig ist.
- Erzeugen Sie einen neuen privaten Schlüssel, wann immer ein Zertifikatseigentümer das Unternehmen verlässt.
- Verschlüsseln Sie E-Mails, wenn Sie private Zertifikate und Schlüssel versenden.
- Sorgen Sie dafür, dass Ihr E-Mail-System E-Mails automatisch löschen und entsorgen kann.
- Erfordern Sie Zwei-Faktor-Authentifizierung für den Zugang zu diesen Systemen.
- Dokumentieren Sie den Prozess für das Exportieren und Verschieben privater Schlüssel.

# ACHTEN SIE DARAUF, DASS NICHT MEHR GENUTZTE ZERTIFIKATE ENTFERNT BZW. WIDERRUFEN WERDEN.

## Das sollte im Rahmen des Änderungsmanagements und der Außerbetriebnahme von Systemen am Ende ihrer Nutzlebensdauer automatisch geschehen.

**Fazit**

- Standardisieren und automatisieren Sie die Ausstellung und Erneuerung von Zertifikaten.
- Installieren und erneuern Sie alle Zertifikate rechtzeitig.
- Installieren Sie Zertifikate und private Schlüssel auf sichere Art und Weise.
- Verwenden Sie private Schlüssel nie mehrmals.
- Achten Sie darauf, dass das Entfernen bzw. Widerrufen nicht mehr genutzter Zertifikate Teil des Prozesses für die Entsorgung von Geräten ist.

# DURCHSUCHEN SIE NETZWERKE NACH NEUEN SYSTEMEN UND ÄNDERUNGEN.

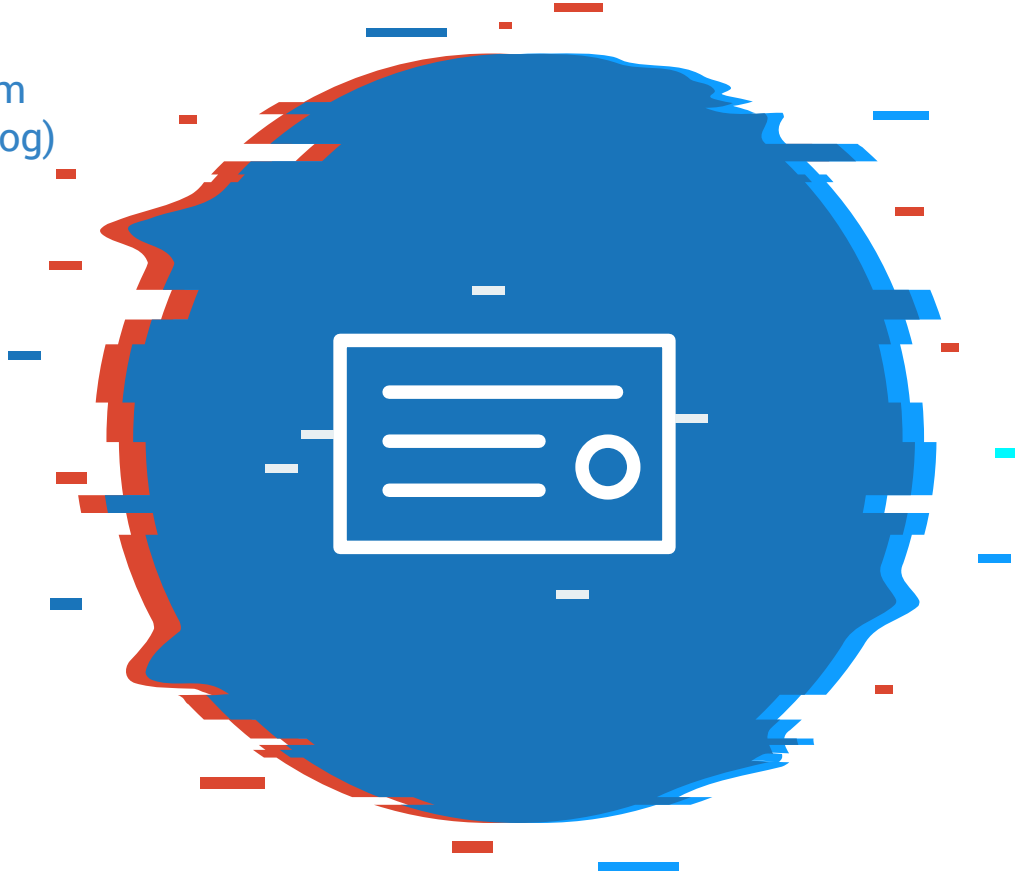
## Verwalten Sie Ihre TLS-Zertifikate nicht manuell, sondern führen Sie einfach regelmäßig Prüfungen auf etwaige Risiken durch.

Alle Netzwerke sind dynamisch und ändern sich ständig. Aus diesem Grund müssen Sie immer nach neuen Systemen oder Änderungen Ausschau halten. Am einfachsten geht das mit Tools für Netzwerkscans. Solche Tools sollten SSL-Sicherheitsprobleme aufzeigen, auf ablaufende Zertifikate hinweisen und andere Netzwerkänderungen erkennen.

# DURCHSUCHEN SIE CT-LOGS NACH NICHT KONFORMEN ZERTIFIKATEN

Jedes öffentliche Zertifikat, das nicht in einem öffentlichen CT-Log (Zertifikatstransparenz-Log) festgehalten ist, wird von Browsern als nicht als vertrauenswürdig eingestuft.

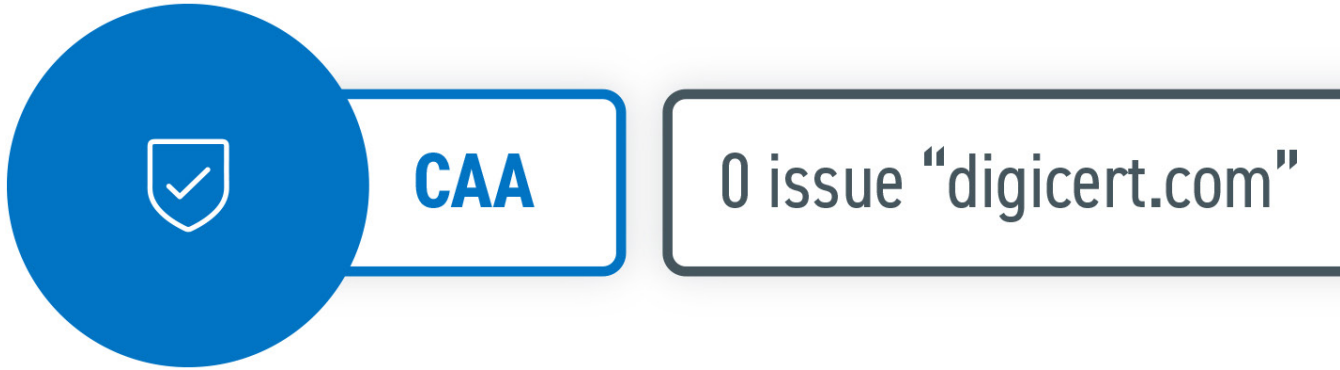
Mit einem Tool zum CT-Monitoring lassen sich nicht konforme Zertifikate schnell und einfach identifizieren und korrigieren.



# NUTZEN SIE DIE CAA, UM NICHT AUTORISIERTE ZERTIFIKATSANFORDERUNGEN ZU VERHINDERN

## Eine Certificate Authority Authorization (CAA) ist ein DNS-Eintrag, der angibt, welche CAs dazu berechtigt sind, Zertifikate für Ihre Domain auszustellen.

Im Jahr 2017 führte das CA/Browser Forum den „Ballot 187“ ein, der von allen CAs verlangt, die CAA-DNS-Einträge zu überprüfen und sich an alle für die fragliche Domain gefundenen Einträge zu halten. So können Domaininhabern festlegen, welche CAs ein Zertifikat für ihre Domain ausstellen dürfen. Mithilfe der CAA bietet können die Verantwortlichen auch benachrichtigt werden, wenn ein Zertifikat von einer nicht autorisierten CA angefordert wird.



# FAZIT

## Nun wissen Sie, was zu tun ist, und es wird Zeit für die einfachste und schnellste Möglichkeit, dieses Wissen in die Praxis umzusetzen.

**DigiCert® CertCentral** bietet Ihnen all die Funktionen, die Sie brauchen, um Ihre gesamte Zertifikatsinfrastruktur zu schützen, zu überwachen und vor allem auch anzupassen und zu automatisieren.

- Durchsuchen Sie Netzwerke nach neuen Systmen und Änderungen.
- Überprüfen Sie CT-Logs auf nicht autorisierte Zertifikate.
- Nutzen Sie die CAA, um nicht autorisierte Zertifikatsanforderungen aufzuspüren und zu verhindern.

# DIE NUTZUNG VON TOOLS ZUR ZERTIFIKATSVERWALTUNG IST IN DER PRAXIS WEIT VERBREITET. FÜR ALLES NUR EINE PLATTFORM ZU VERWENDEN DAGEGEN NICHT.

Weitere Informationen dazu, wie DigiCert® CertCentral die Umsetzung von Best Practices unterstützt, finden Sie unter **digicert.com/certificate-management**