digicert®

TLS/SSL-Zertifikatsverwaltung Checkliste: Best Practices

Wenn Sie sich einen besseren Überblick über Ihren Zertifikatsbestand verschaffen, menschliches Versagen vermeiden und nicht konforme Zertifikate aufspüren wollen, ist eine Checkliste empfehlenswert.

1. 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 TLS/SSL-Versionen.

2. Problembehebung

- ☐ Deaktivieren Sie schwache Schlüssel, Cipher-Suiten und Hash-Algorithmen.
- ☐ Bringen Sie die Ausstellung und Verteilung von Wildcard-Zertifikaten unter Kontrolle.
- ☐ Nutzen Sie angemessene Zertifikatarten.
- ☐ Überprüfen Sie die Zertifikate aller standardmäßig genutzten Anbieter.
- ☐ Stellen Sie sicher, dass auf allen Webservern die neuesten Patches installiert sind.

3. 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.

4. 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.