Abgelaufene Zertifikate sind kein Pech – sondern ein Prozessproblem

Montagmorgen, 08:30 Uhr.

Eine kritische Anwendung lässt sich nicht starten. Die Monitoring-Systeme schlagen Alarm, alles steht auf Rot – und dennoch scheint die Infrastruktur auf den ersten Blick völlig in Ordnung zu sein. Erst nach rund 40 Minuten intensiver Log-Analyse steht die Ursache fest: Ein TLS-Zertifikat ist abgelaufen.

Das eigentliche Problem in solchen Situationen ist nicht die Tatsache, dass die Gültigkeit von Zertifikaten abläuft. Das Problem ist, dass niemand im Team genau weiß, wer für dieses Zertifikat verantwortlich ist, wo der Private Key liegt oder warum es in keiner Übersicht **aufscheint**.

Kommt Ihnen das bekannt vor? Unsere Erfahrung zeigt: **Das ist kein technisches Problem. Es ist ein Prozessproblem.**

In einer IT-Welt aus Hybrid-Clouds, Microservices und tausenden Maschinen-Identitäten ist Certificate Lifecycle Management (CLM) längst kein Randthema mehr. Es ist ein kritischer operativer Bestandteil – und kein technisches Detail, an das man sich einmal im Jahr erinnert.

TL;DR – Das erwartet Sie in diesem Artikel

- Falls Sie gerade wenig Zeit haben, speichern Sie diesen Beitrag gerne für später. Sie finden darin:
    - ein **5-Bausteine-Framework** für funktionierendes CLM
    - typische **Warnsignale**, die auf ein hohes Ausfallrisiko hindeuten
    - ein **90-Tage-Playbook** vom Inventar bis zum stabilen Prozess
    - eine **Verantwortlichkeitsmatrix (RACI)**, die Zuständigkeitsfragen klärt
    - eine **Checkliste**, mit der Sie Ihre Umgebung realistisch einschätzen können

Warum Sie dieses Thema jetzt angehen sollten

Noch vor wenigen Jahren war Zertifikatsmanagement überschaubar: ein paar Domains, ein Anbieter, Erneuerung alle zwei Jahre. Heute sieht die Realität anders aus:

1. **Explosion der Zertifikatsanzahl:** Container, APIs, IoT, Multi-Cloud – jede Umgebung benötigt eigene Identitäten.
2. **Kürzere Laufzeiten:** Sicherheitsstandards erzwingen immer häufigere Rotationen. Manuelle Prozesse skalieren hier nicht mehr.
3. **Steigender Compliance-Druck:** In regulierten Umgebungen wird während eines Audits nicht hinterfragt, ob Sie Zertifikate einsetzen, sondern wie Sie den Erneuerungsprozess steuern.

Die Frage ist nicht, ob ein Zertifikat abläuft – das wird es definitiv. Die entscheidende Frage ist: **Erfahren Sie es rechtzeitig – und haben Sie einen Prozess, der eine Erneuerung ohne Chaos ermöglicht?**

Typische Anzeichen für organisatorisches Chaos

Bevor wir zu Lösungen kommen, prüfen Sie, ob Ihnen diese Situationen bekannt vorkommen:

- **Kein vollständiges Inventar:** „Wir wissen nicht genau, wie viele Zertifikate wir haben und wo sie überall im Einsatz sind."
- **Excel als „zentrales" System:** Erneuerungen werden in Tabellen oder über E-Mails verfolgt, die oft an ehemalige Mitarbeiter:innen adressiert sind.
- **Unklare Zuständigkeiten:** Die Infrastruktur-Abteilung sieht das Security-Team in der Verantwortung, die Security verweist wiederum auf die Applikationsteams.
- **Last-Minute-Incidents:** Der Prozess startet erst, wenn Anwender:innen bereits die Warnung „Verbindung nicht sicher" sehen und nicht mehr auf die Applikation zugreifen können.

Wichtig: Automatisierung ohne klar geregelte Verantwortlichkeiten ist ein sicherer Weg ins Chaos.

Die 5 Bausteine eines funktionierenden CLM

Damit Zertifikatsmanagement nicht zum permanenten Feuerlöschen wird, braucht es ein stabiles Framework. Bei Bacher Systems arbeiten wir mit fünf zentralen Bausteinen:

1. **Inventory & Discovery:** Nur was Sie kennen, können Sie auch schützen. Der erste Schritt ist die kontinuierliche Erfassung aller Zertifikate – öffentlich wie intern.
2. **Ownership:** Jedes Zertifikat braucht eine klar definierte verantwortliche Person. Geteilte Verantwortung führt fast immer zu Ausfällen. Kurz: Es muss klar sein, **wer den Hut aufhat**.
3. **Policy & Governance:** Klare Regeln schaffen Verlässlichkeit. Welche CAs sind erlaubt? Welche Schlüssellängen gelten? Ziel ist eine „Minimum-Viable-Policy“ – kurz, verständlich und umsetzbar.
4. **Renewal & Rotation:** Automatisieren Sie Beantragung, Verteilung und Installation dort, wo Prozesse stabil und klar definiert sind.
5. **Monitoring & Reporting:** Dashboards zeigen den Zustand der Zertifikate und potenzielle Risiken. Weg vom reaktiven Feuerwehrmodus, hin zu vorausschauendem Betrieb.

Implementierungsplan: Ihr 90-Tage-Playbook

Tag 0-30: Bestandsaufnahme (Sichtbarkeit)

- Durchführung eines vollständigen Discovery-Scans und Erstellung des Inventars
- Klassifizierung der Kritikalität (was kann das Business stoppen?)
- Einrichtung sofortiger Alarme für 30/60/90 Tage vor Ablauf

Tag 31-60: Regeln festlegen und Risiken minimieren (Governance)

- Erstellung einer einfachen Policy und technischer Standards
- Einführung eines Prozesses für Beantragung und Erneuerung
- Identifizierung der Ownder für die 20 kritischsten Services

Tag 61-90: Vom Projekt zum Prozess (Operations)

- Implementierung von Automatisierung in den stabilsten Bereichen
- Erstellung von KPI-Dashboards für Management und Security
- Entwicklung von Runbooks - Anleitungen für den Fehlerfall bei der Erneuerung

Tage 0–30: „Sehen, was da ist“ (Sichtbarkeit)

- Vollständiger Discovery-Scan und Aufbau des Inventars.
- Klassifizierung nach Kritikalität (Was kann das Business stoppen?).
- Automatische Alarme bei 30 / 60 / 90 Tagen vor Ablauf der Gültigkeit.

Tage 31–60: „Regeln festlegen und Risiken minimieren“ (Governance)

- Erstellung einer einfachen Policy und technischer Standards.
- Definition eines klaren Erneuerungsprozesses.
- Festlegung der Owner für die 20 kritischsten Services.

Tage 61–90: „Vom Projekt zum Prozess“ (Operations)

- Automatisierung dort, wo Prozesse stabil und gut vorhersehbar sind.
- KPI-Dashboards für Management und Security.
- Runbooks für Zertifikatsfehler und Ausfälle.

Wer ist wofür verantwortlich? (Mini RACI)

Die größte Herausforderung im CLM sind nicht die Tools, sondern die Menschen.
Hier ein Vorschlag für die Rollenverteilung:

Aufgabe	IT Ops / Infra	Security / CISO	App Owner	Partner (z.B. Bacher)
Inventarisierung	R	A	I	S
Policy-Definition	C	R/A	I	S
Erneuerung / Rotation	R	I	A	S
Incident Response	R	C	A	S

Praxisbeispiel: Vom Ausfall zur Betriebssicherheit

In einem Unternehmen, mit dem wir gearbeitet haben, dauerte die Zertifikatserneuerung im Schnitt fünf Arbeitstage und beanspruchte vier Personen. E-Mails, Tickets und manuelles Kopieren von Schlüsseln machten den Prozess fehleranfällig. Ein vergessenes Zertifikat legte beinahe das gesamte Zahlungssystem lahm.

Nach Einführung eines vollständigen CLM-Zyklus reduzierte sich der Aufwand auf wenige Minuten. Die Transparenz stieg auf 100 %.

Unser Ansatz bei Bacher Systems: der Adoption Cycle

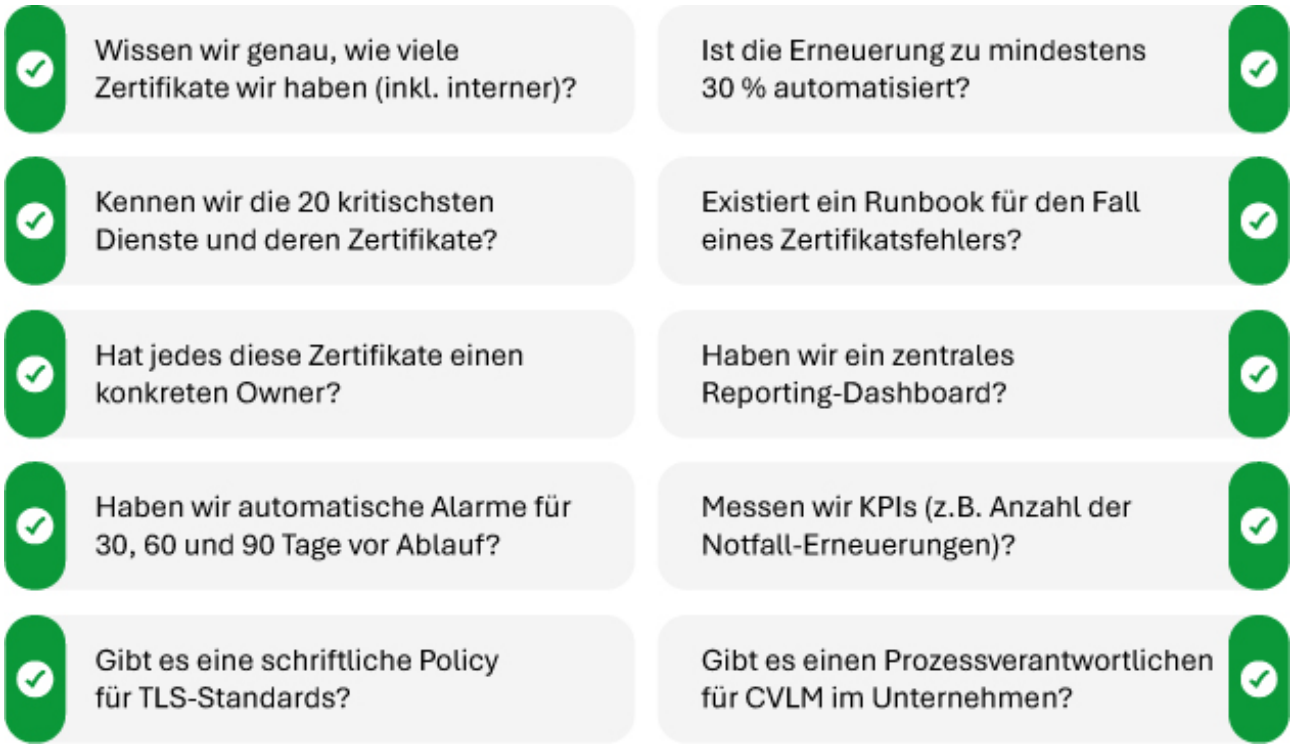
Zertifikatsmanagement ist keine einmalige Tool-Einführung, sondern kontinuierliche operative Arbeit. Im **Adoption-Cycle-Modell** bedeutet das:

- **Consulting:** Analyse des Ist-Zustands und der bestehenden Lücken.
- **Implementierung:** Auswahl der passenden Tools und Mitgestaltung der Prozesse.
- **Betrieb:** Unterstützung im operativen Betrieb, Updates und Patching.
- **Optimierung:** Laufende Reduktion von Ausnahmen und Ausbau der Automatisierung und Optimierung des Services.

Wir übernehmen Mitverantwortung für das Ergebnis – nicht nur für die Technologie.

Checkliste: Haben Sie Ihr CLM unter Kontrolle?

Stellen Sie sich selbst und Ihrem Team diese zehn Fragen:



Wenn Sie viele dieser Fragen mit „Nein“ beantwortet haben, ist jetzt der richtige Zeitpunkt, Struktur in den Prozess zu bringen – bevor der nächste Ausfall Sie überrascht.

Wie geht es weiter?

Was ist aktuell Ihre größte Herausforderung – die fehlende Übersicht, unklare Zuständigkeiten oder die Hürden bei der Automatisierung?

Möchten Sie direkt starten? Melden Sie sich gerne mit dem Stichwort **„CLM“** bei uns – und wir besprechen gemeinsam, wie wir Ihren Prozess nachhaltig absichern können.

Alexander Cornea

Business Owner Digital Identities

identity@bacher.at
+43 664 60126 - 376

Wir leben Mitverantwortung!

Bacher Systems EDV GmbH
Wienerbergstraße 11/B9 – 1100 Wien
info@bacher.at | Tel: +43 1 60 126-0 | www.bacher.eu