

Zertifikatsausfälle betreffen jedes Unternehmen



Laut Security Magazine erlebten 72 % der Unternehmen im vergangenen Jahr mindestens einen zertifikatsbedingten Ausfall; 67 % sind monatlich und 45 % wöchentlich betroffen. Solche Ausfälle entstehen durch abgelaufene oder ungültige Zertifikate und können erhebliche Sicherheits- und Betriebsstörungen verursachen. Automatisiertes Certificate Lifecycle Management (CLM) hilft, sie zu verhindern und Geschäftskontinuität, Netzwerksicherheit und Kundenvertrauen zu schützen. Hier eine Übersicht prominenter Zertifikatsausfälle der letzten Jahre:

Erfahren Sie mehr

Spotify

286 Millionen aktive Nutzer; bis zu 10 Millionen Kunden waren von einem 30-minütigen Ausfall betroffen.

Microsoft Teams

Über 20 Millionen tägliche Nutzer betroffen; viele Anwender wechselten zur Konkurrenzplattform Slack.

Shopify

Direkter Umsatzverlust durch verlangsamte Neukundengewinnung und gestiegene Supportkosten.

Fortinet

Direkte finanzielle Einbußen durch geringere Neukundenakquise und überlastete Support-Teams.

Xero

Über 3,95 Millionen Abonnenten betroffen und mehr als 1.000 integrierte Drittanbieter-Apps blockiert. Mitarbeiter von Kundenunternehmen erhielten in diesem Monat keine Gehaltszahlungen.

Google Voice

Über 4 Stunden Ausfallzeit, in denen Kunden die Dienste nicht nutzen konnten.

Spotify

9 Stunden kompletter Systemausfall, bei dem keinerlei Podcasts erreichbar waren.

2020

2021

2022

Tailscale.com

Ein abgelaufenes Zertifikat verursachte einen 90-minütigen Ausfall.

Microsoft Azure

Fehlerhaftes Zertifikatsmanagement führte zu Dienstunterbrechungen in den USA und traf Unternehmen, die auf die Microsoft-Cloud vertrauen.

Microsoft Teams

Ein Ausfall von wenigen Minuten führte zu stundenlangen Beeinträchtigungen, woraufhin viele Kunden zu Konkurrenzprodukten wechselten.

Outlook

Obwohl der totale Ausfall nur wenige Minuten dauerte, erlebten Nutzer über mehrere Stunden hinweg erhebliche Störungen.

GitHub

Angreifer verschafften sich unbefugten Zugriff auf Code-Repositories und stahlen Code-Signing-Zertifikate für die Anwendungen GitHub Desktop und Atom.

Cisco (Deux en 2023)

Über 20.000 Kunden betroffen; Störungen bei Cloud-Diensten, Datenspeichern und E-Commerce-Tools.

Starlink

Mehrständiger globaler Ausfall mit weltweiter Medienberichterstattung.

2024

2023

Bank of England

Ein kritisches Zahlungssystem fiel wegen eines abgelaufenen Zertifikats aus und stoppte das CHAPS-Netzwerk sowie den Zahlungsverkehr für 90 Minuten.

ServiceNow

Großer Unmut bei Kunden, nachdem ein Root-Zertifikatsfehler die Dienste von über 600 Unternehmen unterbrach.

Real Debrid

Ein abgelaufenes Zertifikat führte zu einem 45-minütigen Dienstausschlag.

Google Chromecast

Massiver Ausfall machte Chromecast-Geräte unbrauchbar – Ursache war das Ablaufdatum eines 2015 ausgestellten Zertifikats mit 10-jähriger Laufzeit.

Starlink

Ein abgelaufenes Zertifikat einer Bodenstation verursachte einen globalen Blackout für 60.000 Kunden (bereits 2023 gab es einen ähnlichen Vorfall).

Microsoft

Verschiedene Verwaltungsportale von Microsoft 365 und Azure waren weltweit von Störungen betroffen.

League of Legends

Spieler konnten sich stundenlang nicht einloggen – wegen eines abgelaufenen SSL-Zertifikats (das ist bereits vor 10 Jahren passiert)

2025