Zertifikatsausfälle betreffen alle

Laut Security Magazine erlebten 72 % der Unternehmen im vergangenen Jahr mindestens einen zertifikatsbedingten Ausfall – häufig verursacht durch abgelaufene oder ungültige Zertifikate. Diese Vorfälle führen zu Sicherheitsrisiken und Betriebsunterbrechungen. Das Zertifikatslebenszyklusmanagement (CLM) verhindert solche Ausfälle, indem es Zertifikate stets aktuell hält. Durch die Automatisierung von CLM unterstützt Sectigo Unternehmen dabei, Ausfälle zu vermeiden und Geschäftskontinuität, Sicherheit sowie Kundenvertrauen sicherzustellen. Hier einige der jüngsten zertifikatsbedingten Ausfälle, die Schlagzeilen gemacht haben:

Erfahren Sie Mehr

2020

Spotify

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

Microsoft Teams

Über 20 Millionen Nutzer pro Tag waren betroffen, viele wechselten zum Konkurrenten Slack.

2021

Shopify

Direkter Umsatzverlust aufgrund geringerer Neukundenakquise und höherer Kosten für den Kundensupport.

Fortinet

Direkter Umsatzverlust aufgrund geringerer Neukundenakquise und höherer Kosten für den Kundensupport.

Xero

Über 3,95 Millionen Abonnenten und mehr als 1.000 Drittanbieter-Apps waren betroffen. Infolge des Ausfalls erhielten Mitarbeiter von Xero-Kunden in diesem Monat kein Gehalt.

Google Voice

Über 4 Stunden Ausfallzeit, während der Kunden keine Dienste oder Produkte nutzen konnten.

2022

Spotify

9 Stunden Ausfallzeit, während der keine Podcasts zugänglich waren.

Tailscale.com

Ein abgelaufenes Zertifikat verursachte einen 90-minütigen Ausfall.

2024

Microsoft Azure

Eine fehlerhafte Zertifikatsverwaltung führte zu Dienstunterbrechungen in den gesamten USA, von denen Unternehmen betroffen waren, die auf die Cloud-Infrastruktur von Microsoft angewiesen sind.

Microsoft Teams

Einige Minuten Ausfallzeit führten zu mehrstündigen Unterbrechungen, sodass viele Nutzer zu Plattformen von Mitbewerbern wechselten.

Outlook

Obwohl die Ausfallzeit nur wenige Minuten betrug, kam es für die Nutzer zu mehrstündigen Unterbrechungen, bevor die Dienste wieder normal funktionierten.

GitHub

Eindringlinge verschafften sich unbefugten Zugriff auf einige der Code-Repositorys von GitHub und stahlen Code-Signaturzertifikate für die Desktop- und Atom-Anwendungen von GitHub.

Cisco *(zweimal im Jahr 2023)*

Über 20.000 Kunden waren betroffen, Cloud-, Datenspeicher-, E-Commerce-Tools und andere Dienste waren gestört.

2023

Starlink

Mehrere Stunden Ausfallzeit mit weltweiter Medienberichterstattung.

Real Debrid

Ein abgelaufenes Zertifikat verursachte einen 45-minütigen Ausfall des Dienstes.

ServiceNow

Ein Fehler im Stammzertifikat führte zu einer Unterbrechung der Dienste für über 600 Unternehmen und löste weit verbreitete Frustration bei den Kunden aus.

Bank of England

Ein kritisches Zahlungssystem stürzte aufgrund eines abgelaufenen Zertifikats ab und verursachte einen 90-minütigen Ausfall von CHAPS und des Einzelhandelsabrechnungsdienstes.

2025

Google Chromecast

Chromecast-Geräte fielen aus, nachdem ein 2015 ausgestelltes Zertifikat abgelaufen war und die Geräte unbrauchbar machte.

Starlink

Ein abgelaufenes Root-Zertifikat verursachte 2023 einen weltweiten Ausfall, von dem 60.000 Kunden betroffen waren.

Microsoft

Verschiedene Microsoft 365- und Azure-Verwaltungsportale waren weltweit betroffen.

League of Legends

Die Spieler konnten sich stundenlang nicht einloggen, weil Riot vergessen hatte, das SSL-Zertifikat des Clients zu erneuern. Dies geschah ebenfalls vor 10 Jahren.