CHECKLISTE: BEST PRACTICES FÜR DIE VERWALTUNG VON ZERTIFIKATEN

Allein im vergangenen Jahr wurden in 60 % der Unternehmen geschäftskritische Anwendungen mindestens einmal beeinträchtigt, weil ein TLS-Zertifikat nicht verfügbar war.[1]

Deshalb ist es heute wichtiger denn je, kompromisslose Sicherheitsstandards für die **Verwaltung Ihrer digitalen Zertifikate zu etablieren und konsequent anzuwenden.**

Diese Checkliste von Best Practices soll Unternehmen wie Ihres dazu anregen, Wissenslücken im Bereich der Zertifikatsverwaltung zu füllen, Sicherheitsmaßnahmen netzwerkweit durchzusetzen und den Überblick über den gesamten Lebenszyklus Ihrer Zertifikate zu behalten, um betriebsschädigende Ausfälle zu vermeiden.

PROBLEMBEHEBUNG

MONITORING

FAZIT

Nun wissen Sie, wie Sie Ihre Zertifkate und somit Ihr Unternehmen online besser schützen. Um Ihnen diese wichtige Aufgabe zu erleichtern, möchten wir Ihnen dazu gern unsere branchenführende Lösung empfehlen:

CertCentral von DigiCert

Zertifkatsverwaltung leicht gemacht

Mit DigiCert CertCentral® stehen Ihnen alle Tools und Funktionen zur Verfügung, die Sie benötigen, um Ihre Zertifkate zu identifzieren, zu schützen und zu überwachen und um effektiv auf Vorfälle zu reagieren. Außerdem erleichtert Ihnen CertCentral die Anpassung und Automatisierung Ihrer gesamten Zertifkatsinfrastruktur. Mit dieser Plattform können Sie ...

- Ihre Netzwerke nach neuen Systemen und Änderungen durchsuchen,
- CT-Logs nach nicht autorisierten Zertifkaten durchsuchen und
- die CAA nutzen, um nicht autorisierte Zertifkatsanforderungen aufzuspüren und zu verhindern.

Alles von einer zentralen Konsole aus.

Weitere Informationen fnden Sie unter digicert.com/certifcate-management