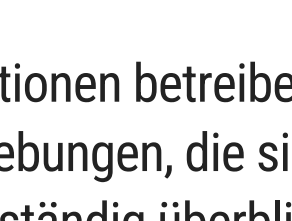


Zertifikatslücken sind ein Ausfallrisiko

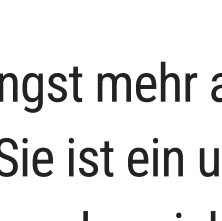
Laut dem DigiCert 2026 Global PKI Research Report verfügen nur 34% der Unternehmen über ein vollständiges Zertifikatsinventar.



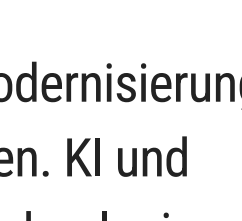
Organisationen sind nicht so gut vorbereitet, wie sie glauben. Neue Erkenntnisse von Omdia und DigiCert zeigen, warum.



Organisationen betreiben PKI-Umgebungen, die sie nicht vollständig überblicken können, bleiben jedoch für Ausfälle, Sicherheitsverletzungen und Verstöße gegen Compliance-Vorgaben verantwortlich.



PKI ist längst mehr als ein System. Sie ist ein umfassendes Ökosystem, das sich schneller fragmentiert hat, als Organisationen damit Schritt halten können.



Die PKI-Modernisierung kann nicht warten. KI und Quantentechnologie erhöhen den Handlungsdruck und machen den Übergang von Erkenntnis zu Umsetzung dringlicher.

Was man nicht sieht, kann man nicht steuern.

PKI-Risiken beginnen mit Transparenzlücken. Viele Unternehmen betreiben Zertifikatsumgebungen, die sie nicht vollständig erfassen können, und schaffen damit systemische Risiken.

Fast **zwei Drittel der Unternehmen verfügen nicht über ein vollständiges und aktuelles Verzeichnis ihrer digitalen Zertifikate.**

Wie lässt sich der aktuelle Stand Ihrer Organisation bei der Nachverfolgung digitaler Zertifikate am besten beschreiben?

34%

Vollständiges, aktuelles Verzeichnis aller digitalen Zertifikate

50%

Teilbestand, einige Zertifikate möglicherweise unbekannt

16%

Unklar, wie viele Zertifikate vorhanden sind oder wo sie verwendet werden.

Das PKI-Risiko ist bekannt. Es wird nicht ausreichend kontrolliert.

Zwischen Bewusstsein und Umsetzung besteht eine deutliche Diskrepanz. Die Organisationen erkennen das Risiko, aber ihre Betriebsmodelle haben sich nicht entsprechend angepasst.

Unternehmen, die äußerst oder sehr besorgt sind über:

73%

Risiko von Ausfällen oder Serviceunterbrechungen aufgrund abgelaufener Zertifikate

74%

Zunehmende Verbreitung von Zertifikaten bei wachsender Anzahl von Systemen oder Identitäten

PKI hat sich weiterentwickelt. Die Verwaltung nicht.

Manuelle Nachverfolgung und Tabellenkalkulationen sind nach wie vor die am weitesten verbreitete Methode zur Zertifikatsverwaltung.

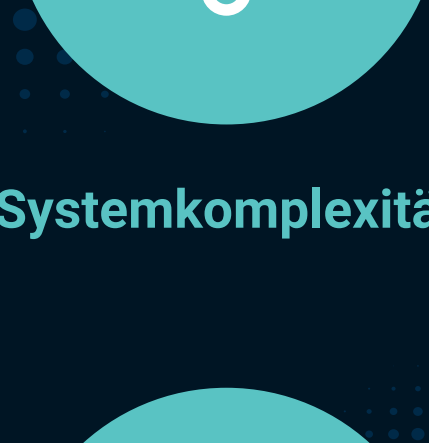
Komplexität ist der Feind der modernen PKI.

PKI ist nicht nur technisch, sondern auch strukturell komplex geworden. Integration und organisatorische Reibungsverluste stellen heute die größten Hindernisse für den Fortschritt dar.

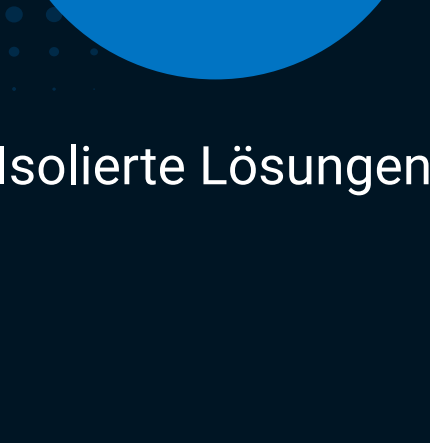
Aktuelle Herausforderungen bei der Zertifikatsverwaltung und -verifizierung:



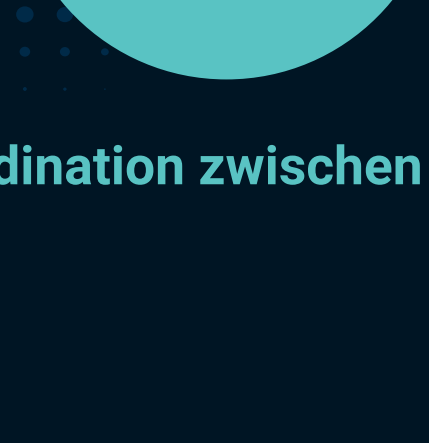
Mangelnde Sichtbarkeit



Systemkomplexität



Isolierte Lösungen



Koordination zwischen Teams

Die Identitätsexplosion stellt sowohl eine Herausforderung als auch eine Chance für PKI dar.

Der Übergang zu nicht-menschlichen Identitäten (NHIs) in großem Umfang überfordert herkömmliche PKI-Ansätze – insbesondere im Bereich agentenbasierter KI. Organisationen müssen ihre PKI-Abdeckung deutlich ausbauen, um den Bedarf zu decken.

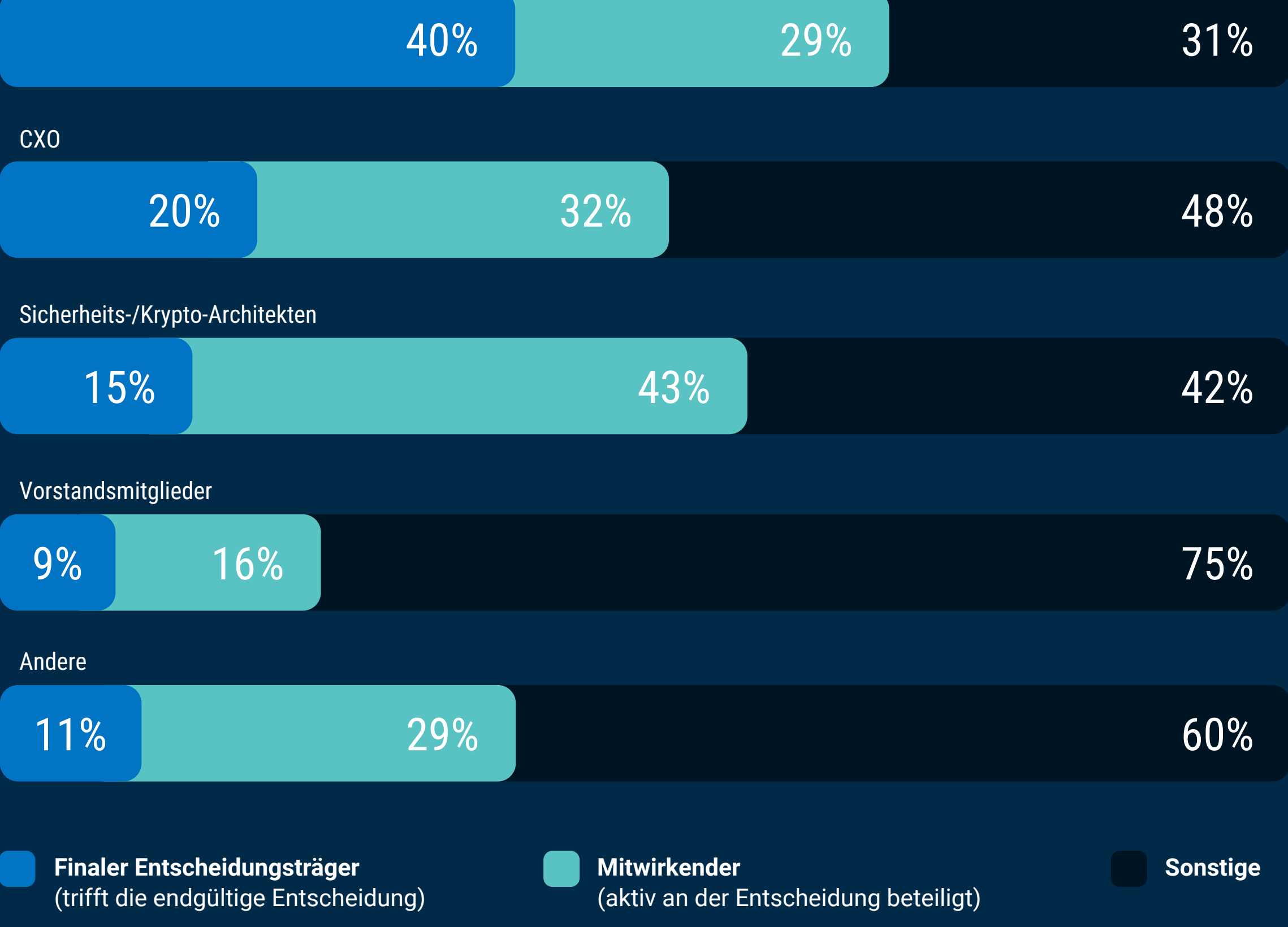
Aktuelle PKI-Abdeckung



Jeder nutzt PKI. Niemand trägt die Verantwortung.

Unklare Verantwortlichkeiten bremsen den Fortschritt. Die PKI-Modernisierung ist nicht nur eine technische Herausforderung, sondern auch eine Frage von Governance und Verantwortlichkeit.

Welchen Grad an Beteiligung haben die einzelnen Stakeholder an PKI-Entscheidungen in Ihrem Unternehmen?



Mit 40% sind die CISOs mit Abstand die wichtigsten Entscheidungsträger für PKI.



CIOs, CTOs und Sicherheitsteams leisten Unterstützung, doch auch der übrige CxO-Kreis muss stärker eingebunden werden.

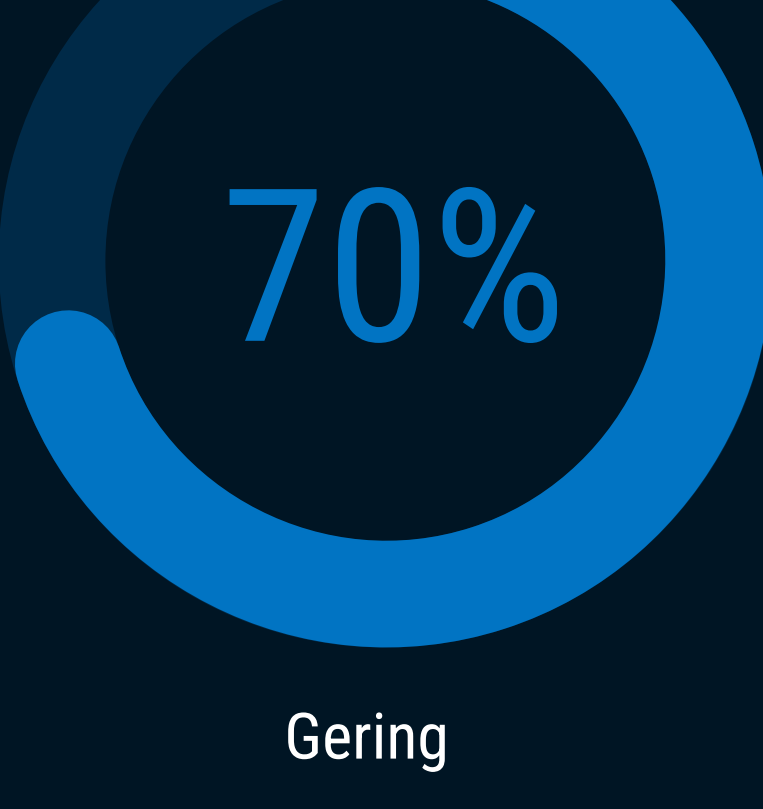


Lediglich 9% der PKI-Entscheidungen werden vom Vorstand getroffen.

Die Zukunft des Vertrauens ist bereits da. Die Organisationen sind nicht bereit.

Die nächste Nachfragewelle, angetrieben von KI, Quantenrisiken und Zero Trust, beschleunigt sich schneller als die organisatorische Bereitschaft.

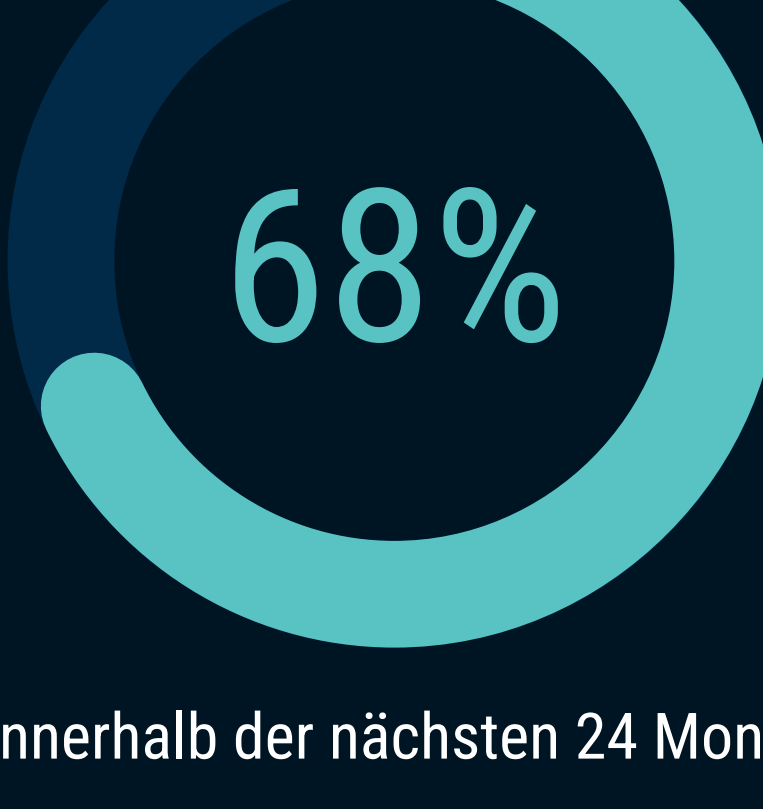
Aktuelles Verständnis der PKI-Modernisierung:



Gering

Umfasst „Grundkenntnisse“, „erste Lernphase“ und „kein Verständnis“.

Pläne zur vollständigen Modernisierung der PKI-Infrastruktur:



Innerhalb der nächsten 24 Monate

Organisationen können diesen Wandel nicht allein bewältigen. Das Fachwissen und die Unterstützung von Anbietern und Partnern im Bereich Digital Trust helfen ihnen, diese Transformation erfolgreich umzusetzen.

Organisationen, die ihre PKI modernisiert haben, verzeichnen eine Reduzierung der Ausfälle um **mehr als 60%**.

Vollständigen Bericht herunterladen

