

## **Digitale Transformation und hybride Arbeitsplätze kurbeln den Einsatz von PKI und digitalen Zertifikaten an**

*Studie von Entrust zu globalen PKI- und IoT-Trends 2021*

**Minneapolis und Düsseldorf – 10. November 2021** – Der Einsatz von Public-Key-Infrastrukturen (PKI) und digitalen Zertifikaten in Unternehmen war noch nie so hoch wie heute – die notwendigen Fähigkeiten zur Verwaltung von PKIs haben jedoch gleichzeitig einen historisch niedrigen Stand erreicht. Das fand eine Studie des Ponemon Instituts im Auftrag von [Entrust](#) heraus. Die [Studie zu globalen PKI- und IoT-Trends 2021](#) ergab, dass IT-Fachleute den Mangel an klaren Zuständigkeiten, Ressourcen und Kompetenzen weiterhin als die größte Herausforderung bei der Bereitstellung und Verwaltung von PKIs ansehen.

Als Herzstück einer unternehmensweiten IT-Infrastruktur ermöglicht eine PKI die Absicherung wichtiger digitaler Initiativen – hierzu zählen zum Beispiel die Cloud, der Einsatz mobiler Geräte, die Identitätsverwaltung und das Internet der Dinge (IoT). Sie ist somit der Schlüssel für den digitalen Wandel – was sich nicht zuletzt im Zuge der weltweiten Pandemie und ihrer Auswirkungen auf viele Arbeitsabläufe besonders deutlich gezeigt hat.

### **Treiber und Herausforderungen bei der Einführung von PKI**

Wenn es um die wichtigsten Faktoren geht, die den Einsatz von PKI-Anwendungen vorantreiben, bleibt das Internet der Dinge (IoT) mit 47 % der am schnellsten wachsende Bereich. Cloud-basierte Dienste werden von 44 % der Befragten als zweitwichtigster Treiber genannt, mobile Anwendungen stehen mit 40 % an dritter Stelle.

Als größte Herausforderung, die den Einsatz und die Verwaltung von PKI behindert, wurde von 71 % der Befragten das Fehlen klarer Zuständigkeiten genannt. Diese Tendenz blieb über die letzten fünf Jahre konstant – was darauf hindeutet, dass dieser Punkt für viele Unternehmen ein zentrales Problem darstellt.

Unzureichende Ressourcen und mangelhafte Kompetenzen wurden mit 51 % bzw. 46 % als zweit- bzw. drittwichtigste Herausforderungen genannt. Bei der Nutzung von PKI verursachen bestehende PKI, die nicht in der Lage sind, neue Anwendungen zu unterstützen (55 %), sowie unzureichende Kompetenzen (46 %) wiederum die größten Probleme.

Zu den Bereichen, von denen der größte zu erwartende Wandel und damit verbundene Unsicherheit ausgeht, gehören an erster Stelle (für 41 % der Befragten) das Internet der Dinge, an zweiter und dritter Stelle wurden externe Mandate und Standards (37 %) sowie Änderungen bei PKI-Technologien (27 %) genannt.



**ENTRUST**

SECURING A WORLD IN MOTION

„Im Laufe der Jahre, in denen wir diese Studie durchführen, wird die Kluft zwischen der steigenden Nachfrage nach PKI und den damit zusammenhängenden Herausforderungen immer deutlicher“, erklärt Dr. Larry Ponemon, Vorsitzender und Gründer des Ponemon Instituts. „Wir sehen ein Risiko, dass sich diese Probleme noch verstärken und damit Lücken in den Sicherheitssystemen von Unternehmen entstehen. Wenn man bedenkt, dass IT-Infrastrukturen durch Remote-Arbeit, Cloud und IoT immer verteilter werden, wird klar, dass viele Unternehmen auch mehr Transparenz, Automatisierung und zentrale Kontrolle benötigen.“

### **Anstieg maschineller Identitäten**

TLS/SSL-Zertifikate für öffentlich zugängliche Websites und Dienste sind der am häufigsten genannte Anwendungsfall für PKI-Berechtigungsnachweise (81 % der Befragten). Private Netzwerke und VPN-Anwendungen stehen an zweiter Stelle (67 %), die E-Mail-Sicherheit belegt den dritten Platz (55 %). Letztes Jahr waren noch öffentliche Cloud-Anwendungen und die Authentifizierung von Mitarbeitern an zweiter bzw. dritter Stelle. Dieser Wechsel unterstreicht den sich verändernden Fokus auf die Gewährleistung der Sicherheit von Remote-Mitarbeitern und verteilten IT-Workloads.

Die durchschnittliche Anzahl der Zertifikate, die Unternehmen ausstellen oder erwerben, steigt der Studie zufolge weiter an – und zwar um 4,3 % (von 56.192 in 2020 auf aktuell 58.639). Seit 2019 stieg die Anzahl sogar um 50 %. Während die Menge der zu sichernden menschlichen Identitäten in den letzten Jahren relativ konstant geblieben ist, überholt die Zahl maschineller Identitäten (Geräte und Workflows) dieses Jahr erstmals die der menschlichen. Dieser Zuwachs ist vor allem auf die steigende Nutzung von IoT und Cloud-Diensten zurückzuführen.

Ganz unabhängig von den Gründen für den Anstieg, wird mit der Zunahme an Zertifikaten deren verantwortungsbewusste Verwaltung umso wichtiger. Ein Fünftel (20 %) aller Befragten verwendet jedoch eine manuelle Liste für die Aufhebung von Zertifikaten, und fast ein Drittel (32 %) gibt zu, dass hierfür gar kein Verfahren existiert. Diese Unternehmen sind anfällig für Angriffe und den Ausfall kritischer Systeme – was wiederum Unterbrechungen von Geschäftsabläufen und damit verbundene Kosten mit sich bringen kann.

„Noch nie war die Nachfrage nach PKI so groß wie in diesem Jahr – sei es durch den Druck, Remote- oder Hybrid-Arbeitsplätze zu sichern, oder durch das anhaltende Wachstum von IoT und Cloud-basierten Diensten“, so John Metzger, Vice President of Product Marketing, Digital Security bei Entrust. „Gleichzeitig bleiben die Fähigkeiten und Ressourcen, die für den Einsatz und die Verwaltung von PKI erforderlich sind, weiterhin knapp – ein Problem, welches durch den Mangel an klarer organisatorischer Verantwortung für den PKI-Einsatz verschärft wird. Um diese Komplexität zu bewältigen, benötigen Unternehmen erstens eine Strategie, und zweitens die passenden Produkte. Bei Entrust können wir beides leisten, da wir nicht nur über die technologischen Fähigkeiten, sondern auch über langjährige Erfahrung und Know-how in diesem Bereich verfügen.“



**ENTRUST**

SECURING A WORLD IN MOTION

## **Weiterführende Informationen**

Landing page: [Globale Studie zu PKI- und IoT-Trends 2021](#)

Blog: [Ist Ihre PKI bereit für die Möglichkeiten unserer vernetzten Welt?](#)

## **Methodik der Studie "Globale PKI- und IoT-Trends 2021"**

Die jährliche „Entrust Global PKI and IoT Trends Study“ wird von den Meinungsforschern des Ponemon Instituts durchgeführt und basiert auf dem Feedback von mehr als 1.900 IT-Sicherheitsexperten in 17 Ländern: Australien, Brasilien, Frankreich, Deutschland, Hongkong, Japan, Mexiko, Naher Osten (Saudi-Arabien und die Vereinigten Arabischen Emirate), Niederlande, Russische Föderation, Spanien, Südostasien, Südkorea, Schweden, Taiwan, Vereinigtes Königreich und Vereinigte Staaten.

---

## **Über Entrust**

Mit der Schaffung vertrauenswürdiger Identitäten, Zahlungen und Daten setzt sich Entrust für sichere Transaktionen in einer sich laufend verändernden Welt ein. Die Ansprüche an nahtlose und hochsichere Anwendungen steigen stetig – sei es beim Grenzübertritt, beim Einkaufen, bei der Nutzung von E-Government-Diensten oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet eine einzigartige Bandbreite an Lösungen für die digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen, welche die Grundlage all dieser Interaktionen darstellen. Weltweit vertrauen die angesehensten Organisationen und Unternehmen auf 2.500 Mitarbeiter und ein Netzwerk globaler Partner und Kunden in über 150 Ländern. Weitere Informationen unter [www.entrust.com](http://www.entrust.com).

## **Pressekontakt D/A/CH**

Alexandra Maiberger

[amaiberger@pr-am.com](mailto:amaiberger@pr-am.com)

+49 179 46 74 310