Enormer Anstieg bei Public-Key-Infrastrukturen und digitalen Zertifikaten

Jährliche Studie zu aktuellen Trends im Bereich PKI und IoT konstatiert weltweit eine starke Zunahme von Public-Key-Infrastrukturen, angetrieben durch das Internet of Things und Cloud-Dienste

Minneapolis und Düsseldorf – 13. Oktober 2020 – Weltweit vergrößern Unternehmen rapide den Umfang und das Ausmaß ihrer Datenschutzinfrastruktur, was sich laut Untersuchungen von Entrust in einer erheblichen Zunahme von Public-Key-Infrastrukturen (PKI) widerspiegelt. PKIs gewährleisten die Sicherheit wichtiger digitaler Initiativen wie zum Beispiel die Nutzung der Cloud, der Einsatz mobiler Geräte und digitaler Identitäten sowie das Internet of Things (IoT).

Die jährlich vom Ponemon Institut im Auftrag von nCipher Security, einem Unternehmen von Entrust, durchgeführte 2020 Global PKI and IoT Trends Study basiert auf den Antworten von über 1.900 IT-Security Experten aus 17 Ländern.

IoT, Authentifizierung und Cloud sind die wichtigsten Triebkräfte für PKIs
Unternehmen werden immer abhängiger von digitalen Informationen und sind mit immer raffinierteren Cyberangriffen konfrontiert. Hier schaffen PKIs Abhilfe, mit denen sich der Zugriff auf Daten kontrollieren und die Identität von Personen, Systemen und Geräten ermitteln lässt.
Den größten Zuwachs bei PKI-Anwendungen verzeichnet die aktuelle Studie im Bereich Internet of Things: 47% der Befragten gaben diesen Trend als Hauptgrund für das Wachstum ihrer PKI-Infrastruktur an (ein Anstieg von 26% innerhalb der letzten fünf Jahre). Die Nutzung Cloud-basierter Dienste steht mit 44% der Befragten an zweiter Stelle.

TLS/SSL-Zertifikate für öffentlich zugängliche Websites und Dienste sind der am häufigsten zitierte Anwendungsfall für PKI-Credentials (84% der Befragten). Public Cloud-basierte Anwendungsfälle verzeichneten im Jahresvergleich das schnellste Wachstum (82%, plus 27% gegenüber 2019), gefolgt von der Benutzerauthentifizierung in Unternehmen (70% der Befragten, ein Anstieg von 19% gegenüber 2019). Die Ergebnisse der Studie unterstreichen den entscheidenden Bedarf an PKI zur Absicherung zentraler Unternehmensanwendungen.

Rasanter Anstieg bei zu verwaltenden Zertifikaten
Die durchschnittliche Anzahl an Zertifikaten, die ein Unternehmen verwalten muss, stieg in 2020 um 43 Prozent im Vergleich zum Vorjahr, von 39.197 auf 56.192 Zertifikate. Dies unterstreicht die massiven Anforderungen an die Verwaltung von Unternehmenszertifikaten. Der enorme Anstieg in diesem Jahr lässt sich nach Meinung der Experten von Entrust auf den branchenweiten Übergang hin zu kürzeren Gültigkeitszeiträumen bei Zertifikaten und das starke Wachstum bei Anwendungen in den Bereichen Cloud und Benutzerauthentifizierung zurückführen.

Herausforderungen und Unsicherheit
Die aktuelle Studie zeigte auch neue Herausforderungen für IT-Sicherheitsexperten bei der Realisierung von PKI-Anwendungen. Mehr als die Hälfte der Befragten (52%) nannte dabei die mangelnde Sichtbarkeit der Sicherheitsfunktionen einer bestehenden PKI als größtes Problem (ein Anstieg von 16% gegenüber 2019). Dies unterstreicht den Mangel an Fachkenntnissen im Bereich Cybersicherheit und den Bedarf an PKI-Spezialisten, die auf der Grundlage bewährter Sicherheits- und Betriebspraktiken maßgeschneiderte unternehmensweite Roadmaps erstellen können. Problematisch erweist sich zudem das Ändern von Legacy-Anwendungen und die Adaption bestehender PKIs an neue Anwendungen (jeweils 51%).

Wenn es um die Einführung und die Verwaltung einer PKI geht, sind IT-Sicherheitsexperten vor allem durch organisatorische Probleme wie fehlende klare Zuständigkeiten, unzureichende Kenntnisse und mangelnde Ressourcen herausgefordert. Die Zahlen der Studie zur PKI-Bereitstellung deuten eindeutig auf einen Trend zu diversifizierteren Ansätzen hin, in einigen Ländern sind As-a-Service-Varianten sogar weiter verbreitet als On-Premise Modelle.

Die beiden größten Bereiche, die beim Thema PKI für Unsicherheit sorgen, sind das IoT (52% der Befragten) und externe Standards und Richtlinien (49%). Letztere treiben den Einsatz von PKI-Anwendungen ebenfalls zunehmend voran, was von 24% der Befragten bestätigt wurde.

IoT: Sicherheit hinkt Wachstum hinterher
Die Verschlüsselung von IoT-Geräten, -Plattformen und -Datenspeichern nimmt zwar zu, liegt aber insgesamt nur bei 33% – ein Risiko für sensible Daten. Die Befragten sehen verschiedene Gefahren für die Sicherheit ihrer IoT-Geräte, darunter Funktionsstörungen durch Malware oder andere Angriffe (68%) und die Fernsteuerung eines Geräts durch einen nicht autorisierten Benutzer (54%). Allerdings rangieren Kontrollmechanismen zum Schutz vor Malware – wie die sichere Bereitstellung von Patches und Updates für IoT-Geräte – nur auf Platz 5 der wichtigsten PKI-Funktionen im Zusammenhang mit dem IoT.

Fazit:
„Wir beobachten eine zunehmende Abhängigkeit von PKIs und damit größere Herausforderungen für interne IT-Abteilungen, ihre Infrastrukturen an neue Bedürfnisse anzupassen – was wiederum Änderungen bei traditionellen PKI-Bereitstellungsmodellen und -methoden vorantreibt", so John Grimm, Vice President Strategy for Digital Solutions bei Entrust. „In neueren Bereichen wie dem Internet of Things versäumen es Unternehmen größtenteils, Sicherheitsmechanismen wie das digitale Signieren von Firmware zu priorisieren – diese würden aber den dringendsten Bedrohungen wie zum Beispiel Malware entgegenwirken. Eine weitere Erkenntnis der Studie ist die massive Zunahme ausgestellter und zu verwaltender Zertifikate. Damit nimmt die Bedeutung einer automatisierten Zertifikatsverwaltung und flexibler PKI-Bereitstellungsmodelle rasant zu – aber auch die Notwendigkeit starker Sicherheitsmechanismen zur Schlüsselverwaltung, einschließlich der Nutzung von Hardware-Sicherheitsmodulen."

Die komplette Studie zum Herunterladen: 2020 Global PKI and IoT Trends Study

###

„2020 Global PKI & IoT Trends" – Methodik der Studie
Die 2020 Global PKI and IoT Trends Studie erfasst aktuelle Entwicklungen und Herausforderungen beim Thema PKI sowie den Einfluss des IoT. Für den Bericht wurden 1.934 IT-Sicherheitsexperten in den folgenden 17 Ländern/Regionen befragt: Australien, Brasilien, Frankreich, Deutschland, Hongkong, Indien, Japan, Mexiko, Naher Osten (Saudi-Arabien und die Vereinigten Arabischen Emirate), Niederlande, Russische Föderation, Südkorea, Südostasien (Indonesien, Malaysia, Philippinen, Thailand und Vietnam), Schweden, Taiwan, Vereinigtes Königreich und die Vereinigten Staaten.

Die Studie 2020 ist der fünfte Jahresbericht über globale PKI- und IoT-Trends im Auftrag von nCipher Security, einem Unternehmen von Entrust. nCipher Security ist ein führender Anbieter von universellen Hardware-Sicherheitsmodulen (HSM) und unterstützt weltweit Unternehmen dabei, Vertrauen, Integrität und Kontrolle für ihre geschäftskritischen Informationen und Anwendungen zu schaffen.

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.

###

Pressekontakte D/A/CH:
Alexandra Maiberger, amaiberger@pr-am.com, Tel: +49 179 4674 310
Lisa Ostermaier, sternschmiede@email.de, Tel: +49 152 0865 2080