# Neuer KeyIdentity Schwachstellen-Scanner identifiziert und priorisiert IT-Sicherheitslücken

Datum: 06.03.2018 08:15
Kategorie: IT, New Media & Software
Pressemitteilung von: KeyIdentity GmbH

KeyIdentity GmbH

KeyIdentity Schwachstellen-Scanner gibt Unternehmen einen Überblick über ihre aus dem Internet erreichbare IT-Infrastruktur. / IT-Sicherheitslücken können schneller erkannt und geschlossen werden.

Weiterstadt, 5. März 2018 – KeyIdentity, ein globaler Anbieter von hoch skalierbaren, einfach einsetzbaren Identity- und Access-Management-Lösungen (IAM) auf Open-Source-Basis, hat eine neue IT-Sicherheitslösung für Unternehmen entwickelt. Mit dem KeyIdentity Schwachstellen-Scanner können Nutzer ihre gesamte, aus dem Internet erreichbare IT-Infrastruktur auf Sicherheitslücken überprüfen und deren Behebung priorisieren. So können Schwachstellen schneller erkannt und geschlossen werden. Ebenso lassen sich Prozessfehler identifizieren, die für die Schwachstellen verantwortlich sind. Dadurch steigt langfristig das Sicherheitsniveau der gesamten Organisation. Die Kombination des Schwachstellen-Scanners mit der flexiblen KeyIdentity Multi-Faktor-Authentifizierung (MFA) hilft dabei, grundlegende IT-Sicherheitsmaßnahmen umzusetzen, die von nationalen Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und internationalen Institutionen empfohlen werden. Dies bringt Unternehmen einen großen Schritt bei der Einhaltung von Compliance- und Regulierungsvorgaben weiter.

Der KeyIdentity Schwachstellen-Scanner ermittelt aus dem Internet erreichbare Angriffspunkte. Dabei listet er unter anderem fehlende Sicherheitspatches oder unsichere Konfigurationsparameter auf. Im Zuge des Reportings erhalten Unternehmen eine Übersicht der identifizierten Schwachstellen und deren Verlauf. Zudem werden die Lücken priorisiert, sodass Verantwortliche die gravierendsten Fehler als erstes beseitigen können. Unternehmen bekommen auch einen Bericht mit Empfehlungen zum Schließen der Lücken sowie eine Einschätzung zur Verfügung gestellt, wie sich die Bedrohungslage für ihre IT-Infrastruktur seit dem letzten Scan verändert hat.

"Jedes Unternehmen und jeder IT-Verantwortliche sollten ein effektives Schwachstellen-Management für ihre IT-Infrastruktur nutzen. Nur dadurch lassen sich Angriffe aus dem Internet effektiv bekämpfen und die Hürden für eine erfolgreiche Kompromittierung durch Angreifer erhöhen", erklärt Dr. Amir Alsbih, CEO von KeyIdentity. "In der Realität ist aber oft das Gegenteil der Fall: Ohne Strategie und Struktur werden verschiedene Infrastrukturgeräte und -dienste installiert, aber im Anschluss nicht mehr richtig verwaltet, gewartet oder gepatched. Nutzer verlieren die Übersicht über verwendete Komponenten und Software-Versionen. Gerade bei Diensten, die aus dem Internet erreichbar sind, ist dies höchst fahrlässig. Denn es öffnet potenziellen Angreifern Tür und Tor."

Angriffe über IT-Sicherheitslücken werden – wenn überhaupt – oftmals erst nach mehreren Monaten bemerkt. Der entsprechende Schaden durch Datendiebstahl, Manipulationen oder Imageverlust ist enorm. Spätestens mit dem Inkrafttreten der EU-Datenschutz-Grundverordnung (EU-DSGVO) am 25. Mai 2018 stehen Unternehmen in der Pflicht, solche Risiken für alle personenbezogenen Daten auszuschließen. Ansonsten drohen empfindliche Strafen.

Diese Pressemitteilung wurde auf openPR veröffentlicht.

Pressekontakt:
PSM&W Kommunikation GmbH
Beatrice Gaczensky & Jens Eßer
Clemensstr. 10
60487 Frankfurt am Main
Tel.: +49 69 970705-42 / -32
E-Mail: keyidentity@psmw.de
www.psmw.de

Über KeyIdentity

KeyIdentity ist ein globaler Anbieter von hoch skalierbaren, einfach einsetzbaren Identity-und Access-Management-Lösungen (IAM) auf Open-Source-Basis für die Absicherung und Verwaltung digitaler Identitäten über Netzwerk- und Cloud-Umgebungen. Der Fokus von KeyIdentity liegt auf den Bereichen Transaktionssicherheit, Identitätsmanagement und der starken Authentifizierung mittels Multi-Faktor-Authentifizierung (MFA). Die Lösungen von KeyIdentity zeichnen sich durch ihre hohe Usability und Skalierbarkeit aus und lassen sich mit jedem am Markt verfügbaren Authentifizierungstoken (OTP-Token) nutzen – von Software-Token wie Push-, QR- und SMS-Token über Hardware-Token bis hin zu Biometrie-Token. Darüber hinaus können die Lösungen der KeyIdentity IAM-Plattform durch den API-First-Ansatz in kürzester Zeit in jede verfügbare IT-Infrastruktur integriert werden. Die IAM-Lösungen werden von Anfang bis Ende in Deutschland entwickelt und bereitgestellt und erfüllen höchste Sicherheitsstandards nach deutschem Recht. Durch den Open-Source-Ansatz lassen sich zudem kryptografische Backdoors ausschließen. KeyIdentity bietet seit 2002 "Security made in Germany" und hat seinen Sitz in Weiterstadt bei Darmstadt. Weitere Informationen stehen auf der KeyIdentity Website, im Blog sowie über LinkedIn, Twitter und Facebook zur Verfügung.

Link zur PM:
https://www.openpr.de/news/995267/Neuer-KeyIdentity-Schwachstellen-Scanner-identifiziert-und-priorisiert-IT-Sicherheitsluecken.html