Neue Studie: Unternehmen haben Aufholbedarf bei sicherer Authentifizierung

Datum: 20.10.2017 18:37
Kategorie: IT, New Media & Software
Pressemitteilung von: KeyIdentity GmbH

Studie in Zusammenarbeit mit IDG offenbart große Lücken im Identitäts- und Access-Management. / Risiken beim Einsatz von Passwörtern werden weiterhin unterschätzt.

Weiterstadt, 19. Oktober 2017 – Trotz massiver Vorfälle von Datendiebstahl und Hacks tun sich viele Unternehmen noch immer schwer bei der Umsetzung von sicheren Logins und Transaktionen. Dies hat die neue Identity Access Management Studie von IDG Research Services in Zusammenarbeit mit KeyIdentity ergeben.

Passwörter nicht mehr ausreichend für sichere Authentifizierung

Für 61,6 Prozent der befragten Unternehmen ist das klassische Passwort noch immer die wichtigste Methode zur Authentifizierung, gefolgt von PINs (39,2 Prozent) und E-Mails (35,3 Prozent). Die Studienteilnehmer gehen allerdings auch davon aus, dass Passwörter in den kommenden fünf Jahren an Bedeutung verlieren und andere Authentifizierungsmethoden wie Fingerabdruck (+18,2 Prozent), Gesichtserkennung (+15,4 Prozent) oder Smartphone-Apps (+13,3 Prozent) häufiger zum Einsatz kommen.

„Regelmäßige Hacks und Vorfälle von Datendiebstahl belegen, dass selbst komplexe Passwörter heute nicht mehr für die Authentifizierung von digitalen Identitäten geeignet sind“, erklärt Dr. Amir Alsbih, CTO/COO von KeyIdentity. „Unternehmen müssen ihre Logins und Transaktionen daher dringend um eine leicht nutzbare, sichere Multi-Faktor-Authentifizierung ergänzen, um in der fortschreitenden Digitalisierung auch die Sicherheit zu garantieren. Hierbei wird etwa ein Passwort um einen zweiten Authentifizierungsfaktor – ein sogenanntes Token – ergänzt, das nur dem berechtigten Nutzer vorliegt. Ein Missbrauch durch externe Angreifer ist damit ausgeschlossen.“

Multi-Faktor-Authentifizierung insbesondere für Kunden unzureichend

Obwohl eine Multi-Faktor-Authentifizierung (MFA) inzwischen unverzichtbar für den sicheren Umgang mit digitalen Identitäten ist, gibt es laut aktueller IDG-Studie noch deutlichen Nachholbedarf beim Einsatz der MFA-Lösungen: 69,2 Prozent der befragten Firmen nutzen die Methode für die eigenen Mitarbeiter. Nur bei 26,7 Prozent der Unternehmen müssen sich Geschäftspartner, Dienstleister und Zulieferer per MFA authentifizieren. Und geringe 13,7 Prozent aller befragten Firmen in Deutschland bieten die Multi-Faktor-Authentifizierung für Kunden etwa in Portalen oder eigenen Cloud-Anwendungen an.

„Gerade Webportale für Kunden sind häufig Angriffspunkte für Kriminelle und sollten deshalb besonders umfassend gesichert werden“, ergänzt Dr. Amir Alsbih. „Globale Player wie Apple, Google oder Microsoft haben diese Anforderung bereits erkannt und setzen zunehmend auf eine MFA-basierte Authentifizierung. Wenn Unternehmen die sensiblen Daten ihrer Kunden und Partner nicht aufs Spiel setzen wollen, sollten sie sich dringend mit der Einführung dieser Sicherheitslösungen auseinandersetzen. Das Gleiche gilt für die Zusammenarbeit mit Partnern, Dienstleistern und Zulieferern.“

Die Möglichkeiten für die Multi-Faktor-Authentifizierung sind heute bereits sehr vielfältig. Es lassen sich je nach Anforderung und Sicherheitsstufe des Nutzers passende Token-Typen auswählen. So hat die Identity Access Management Studie von IDG Research Services in Zusammenarbeit mit KeyIdentity ergeben, dass Smartphones (44,9 Prozent), Smartcards (43,6 Prozent) und USB-Lösungen (37,2 Prozent) aktuell am häufigsten für MFA eingesetzt werden.

Durch ihre leichte Anwendbarkeit und den hohen Sicherheitsstandard bieten die unterschiedlichen MFA-Authentifizierungsmöglichkeiten Unternehmen heute eine wichtige Grundlage, um zudem die Anforderungen der ab Mai 2018 geltenden EU-Datenschutz-Grundverordnung sowie der EU-Zahlungsrichtlinie PSD2 zu erfüllen. Der IDG-Studie zufolge gilt die Umsetzung dieser Vorgaben heute als größte Compliance-Herausforderung für Unternehmen.

Die Identity Access Management Studie von IDG Research Services wurde im Juli 2017 durchgeführt. Im Rahmen der zugrundeliegenden Online-Befragung wurden 385 qualifizierte Interviews mit obersten IT- und Security-Verantwortlichen von Unternehmen in der DACH-Region geführt.

Diese Pressemitteilung wurde auf openPR veröffentlicht.

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

KeyIdentity ist ein globaler Anbieter von hoch skalierbaren, einfach einsetzbaren Multi-Faktor-Authentifizierungslösungen (MFA) auf Open-Source-Basis. Die KeyIdentity LinOTP Suite ermöglicht eine sichere und zuverlässige Authentifizierung digitaler Identitäten und Transaktionen bei Unternehmen und Behörden. Die MFA-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 kann KeyIdentity LinOTP durch den API-First-Ansatz in kürzester Zeit in jede verfügbare IT-Infrastruktur integriert werden. KeyIdentity bietet „Security made in Germany“: Die MFA-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.

Link zur PM:
https://www.openpr.de/news/975639/Neue-Studie-Unternehmen-haben-Aufholbedarf-bei-sicherer-Authentifizierung.html