

IT-SECURITY

Ausweg aus dem Passwort-dilemma

Die Verwendung von Passwörtern birgt Sicherheitsrisiken und ist eine Kostenfalle. Deshalb setzt sich die Authentifizierung mittels Fingerprint immer mehr durch.



Passwörter sind nicht nur lästig, sondern auch ein Sicherheitsrisiko. Denn: Je schärfer die Passwortrichtlinien, desto eher finden die Benutzer Workarounds, um sich diesen zu entziehen. Wer will oder kann sich schon fünf, zehn oder noch mehr Passwörter mit acht bis zwölf Zeichen Mindestlänge und Sonderzeichen merken – vor allem wenn sie auch noch monatlich geändert werden? Kein Wunder also, dass gerade in mittleren und grossen Unternehmen die Helpdesk-Mitarbeiter alle Hände voll zu tun haben, ihren Benutzern bei vergessenen Passwörtern zu helfen.

Alternativen zum Passwort

Es gibt jedoch Alternativen: Mit Passwort Reset und Single-Sign-On (SSO) sollen vor allem die Helpdesk-Kosten reduziert werden. Die Sicherheitsproblematik bleibt jedoch ungenügend gelöst, da nach wie vor Passwörter den Zugang regeln. Smartcards und Tokens sind zwar fortschrittlicher, haben aber auch Nach-

teile: Die Einführung ist mit erheblichem Zeit- und Kostenaufwand verbunden, denn es wird eine Private Key Infrastructure (PKI) vorausgesetzt. Hinzu kommen Kosten für die Logistik und der Aufwand für die temporäre Ausstellung vergessener Karten oder Tokens. Als Faustregel kann man pro Tag von zehn Prozent vergessener Hardware der Mitarbeiter ausgehen. Ausserdem können die elektronischen Schlüssel leicht gestohlen werden, ein weiteres Sicherheitsrisiko. Einen anderen Weg schlagen biometrische Authentifizierungsmethoden ein. Das Authentifizierungsmerkmal trägt jeder bei sich und merken muss man sich auch nichts.

Sicherer Fingerabdruck

Es gibt eine Vielzahl von biometrischen Erkennungsmethoden, die unterschiedliche Charakteristika verwenden, zum Beispiel Fingerabdruck, Iris, Retina, Gesichts- und Handgeometrie, Handlinienstruktur oder Venenerkennung. Dabei hat sich der Fingerabdruck am erfolgreichsten durchgesetzt.

Die Authentifizierung per Fingerabdruck funktioniert heute zuverlässig, ist in Anschaffung und Unterhalt günstig und weist eine sehr hohe

Benutzerakzeptanz auf. Bei der Auswahl einer Fingerprintlösung sollte man das Zusammenspiel von Hardware und Software beachten.

Bei der Hardware spielt das Thema Sicherheit eine erhebliche Rolle. Die grösste Genauigkeit bieten hier optische 3D-Reader. Diese weisen mit Stempelfarbe oder Silikonabguss angefertigte Kopien von Fingerabdrücken zuverlässig ab. Von Vorteil ist auch, wenn

«Analysten sagen der Biometrie 15 Prozent jährliches Marktwachstum bis 2010 voraus.»

sich bereits vorhandene Reader, etwa in Notebooks, nahtlos integrieren lassen.

Bei der Software ist der Betriebsaufwand der Knackpunkt, denn wenn neue Server angeschafft und proprietäre Authentifizierungs-Datenbanken angelegt und unterhalten werden müssen, ist der Kostenvorteil gegenüber Passwörtern schnell dahingeschmolzen.

Integrierte Lösung

Im Idealfall baut die Lösung auf vorhandener Infrastruktur auf, beispielsweise auf das bei den meisten Unternehmen verwendete Microsoft Active Directory. Dabei sollte einer Lösung mit Integration ins Active Directory

der Vorzug gegeben werden und nicht nur mit einer Synchronisation. So umgeht man das Ausfallrisiko.

Ein weiterer Vorteil der Integration: Die Fingerprint-Software wird direkt auf den Domain Controllern installiert, was Anschaffungs- und Unterhaltskosten spart. Zudem werden so die bestehenden Richtlinien aus dem Active Directory von der Software direkt übernommen. Dies verkürzt die Einführungszeit erheblich, ausserdem sind keine Spezialkenntnisse für die Konfiguration notwendig.

Aus Datenschutzgründen ist darauf zu achten, dass keine Bilder der Fingerabdrücke gespeichert werden, sondern nur ein Hash-Code. Eine derartige Lösung wird beispielsweise vom Hersteller Digital Persona angeboten, der über eine installierte Basis von mehr als 90 Millionen Benutzern verfügt.

Analysten sagen der Biometrie 15 Prozent jährliches Marktwachstum bis 2010 voraus. Durch die bereits heute schon ausgereifte Technik ist davon auszugehen, dass der Authentifizierung per Fingerprint der grösste Teil des Kuchens zufallen wird. ■

 Mehr zur IT-Security:
www.computerworld.ch



DER AUTOR

Antonio Retica ist Leiter IT-Security beim Schweizer IT-Dienstleister Itrix Trading AG www.itrix.ch