Eine Welt ohne Passwörter?

Von Nadine Effert

Mit Cloud-Anwendungen oder der Nutzung von Mobile Devices wachsen die Cyber-Risiken – das verlangt nach einer starken Identitätsprüfung und intelligentes Management von Zugriffsrechten. Innovative Technologien und Nutzungskonzepte sind gefragt.

Authentisch ist, was echt und somit glaubwürdig ist. So die Definition. Unsere Glaubwürdigkeit – oder besser Identität – gilt es, ständig unter Beweis zu stellen. Sei es im Alltag am Bankautomaten oder am Arbeitsplatz durch die Eingabe des Passwortes am Rechner. Doch mit ein paar Klicks können gewiefte Hacker und Kriminelle in fremde, digitale Identitäten schlüpfen und sich unberechtigt Zugriff auf Netzwerke, Dienste und Daten verschaffen. Authentisch ist in diesem Fall nicht nur was echt, sondern vor allem sicher ist. Passwörter bieten dabei oftmals nur eine Scheinsicherheit: „Schwache oder nicht regelmäßig ausgewechselte Passwörter öffnen Hackern Tür und Tor. Sie können oft in Sekunden geknackt werden", sagt der Bonner Informatik-Professor Hartmut Pohl. Um gängige Angriffe auf Passwörter, wie Man-in-the-Middle- oder Phishing-Attacken, zu vermeiden, empfiehlt der Experte, einen weiteren Sicherheitsschlüssel hinzuzufügen.

Wissen allein? Kein ausreichender Schutz

Nicht zuletzt, weil die Sicherheitsanforderungen in Unternehmen, aber auch Behörden, ständig wachsen. Viele Anwendungen laufen heutzutage auf On-Premise-Systemen, extern gehosteten Plattformen und cloudbasierten Services. Mit ihnen entstehen neue Sicherheitslücken, die IT-Verantwortliche füllen müssen. Die Multi-Faktor-Authentifizierung steht dabei auf der Agenda vieler Unternehmen ganz oben. Laut der Studie „Global Annual Authentication Survey 2013" kommt sie bei 37 Prozent der befragten IT-Unternehmen zum Einsatz. Das sind sieben Prozent mehr als im Vorjahr. Nach dem Prinzip „Wissen und Besitz" kann eine Zwei-Faktor-Authentifizierung mit Smartcard oder Token erfolgen. Heißt: Das Wissen eines Passwortes oder einer PIN allein reicht nicht aus, um die Identität nachzuweisen.

nen-Sensor. Dennoch ist die biometrische Authentifizierung in deutschen Unternehmen bisher kaum angekom-