Stehen Sicherheit und Komfort im Widerspruch?

Es gibt unterschiedliche Bezeichnungen und Technologien für ein und dasselbe Bestreben: den Zugriff auf Daten und Applikationen zu schützen und die zugriffsberechtigten Personen bei deren Anmeldung sicher zu identifizieren. Thomas Boll

Thomas Boll
ist Geschäftsführer der BOLL Engineering AG

Ob gesicherter Zugang zu Anwendungen und Daten im Unternehmen, ob E-Banking oder Remote Access auf das Firmennetzwerk, ob Zugriffssicherheit bei Notebooks im Offlinebetrieb – der Schutz von Daten, Applikationen und IT-Ressourcen ist ein schwieriges Unterfangen. Zwar stehen innovative und wirksame Security-Technologien zur Verfügung. Deren integrale Nutzung ist in der Praxis jedoch nur selten anzutreffen. Die Probleme, die sich zeigen, sind vielfältig. Die Vielzahl notwendiger Passwörter führt dazu, dass die User einfache Identifikationscodes verwenden, keine regelmässige Änderung vornehmen oder ein Passwort für sämtliche Anwendungen verwenden. Die Verwaltung der Benutzerdaten («Authentication Management») sowie das Monitoring und Reporting (auch für Compliance-Auflagen wichtig) erweisen sich als aufwendig und fehleranfällig. Das Fehlen zusätzlicher Identifikationskomponenten wie Einmalpasswort-Token (OTP – One Time Password) oder biometrische Authentisierungsoptionen verhindert eine sogenannte «starke Authentisierung». Und schliesslich schaffen die getrennten Welten der physischen und logischen Zugangskontrolle Sicherheitslücken.

Integrale Lösungen schaffen Sicherheit und Komfort

Bisher galt es als Faktum, dass ein hohes Mass an (Zugriffs-) Sicherheit zwingend einhergeht mit einer hohen Komplexität bezüglich der User-Authentisierung, des Passwort-Managements und Reportings. Diese «Gesetzmässigkeit» wird dank innovativer AIM- und ESSO-Lösungen aufgebrochen. So sind Plattformen erhältlich, die folgende drei Funktionen in einem System vereinen: «Single Sign-On» (SSO) beziehungsweise «Enterprise Single Sign-On» (ESSO), Authentication Management und Physical/Logical. Das Zusammenführen der einzelnen Dienste in einem System

ermöglicht Firmen den Aufbau einer ganzheitlichen, konsolidierten Zugriffssicherheit bei gleichzeitiger Reduktion der Komplexität. Demnach vereinfachen intelligente Systeme die Log-in-Prozedur der User – bei gesteigerter Sicherheit.

ESSO – ein Passwort reicht

Einen wichtigen Beitrag zur Vereinfachung der Verwaltung von Benutzerdaten und Zugriffsrechten leisten ESSO-Lösungen. Sie ermöglichen den Nutzern über ein starkes Passwort einen konsolidierten Zugang zu allen individuell freigegebenen Applikationen und Ressourcen. Hat sich der User einmal authentifiziert, wird er automatisch bei allen ihm freigegebenen Anwendungen angemeldet. Dieser SSO-Prozess lässt sich auch im Offlinebetrieb anwenden.

Moderne ESSO-Appliances lassen sich sowohl bei Grossfirmen als auch bei KMUs einfach implementieren, ohne in den Code bestehender Systeme eingreifen oder Konnektoren erstellen zu müssen. Vielmehr werden die unterschiedlichen Authentisierungsmechanismen der einzelnen Applikationen vom System «erlernt». Dabei wird die ESSO-Plattform mit den vorhandenen Domains und anderen LDAP User Directories synchronisiert. Alsdann erstellt sie auf Basis der vorhandenen Passworteigenschaften für alle Anwendungen XML-Profile. Diese werden mit den entsprechenden Regeln in der ESSO-Appliance gespeichert und bei jeder neuen Benutzerauthentisierung überprüft. Von Bedeutung ist ferner, dass ESSO-Lösungen die automatisierte Implementierung von Passwortrichtlinien ermöglichen. Dabei erstellt das System im Hintergrund eindeutige und sichere Passwörter, die die Einhaltung von Richtlinien garantieren. Auch komplexe Passwörter lassen sich durch einen Zufallsgenerator erstellen. Diese sind dem jeweiligen Benutzer unbekannt und können folglich nicht an Unbefugte weitergegeben werden. Auch turnusmässige Passwortänderungen lassen sich automatisieren.

> «Zu einer weiteren Erhöhung der Sicherheit bei gleichbleibend einfacher Handhabung trägt die Einbindung einer Multi-Faktor-Authentifizierung bei.»

Dank Enterprise Single Sign-On gehört die Verwendung unzähliger Identitäten (Benutzernamen, Passwörter, Pin-Codes usw.) der Vergangenheit an. Ein starkes Passwort reicht für den konsolidierten, hoch gesicherten Zugang zu den individuell freigegebenen Applikationen und Ressourcen. Bildquelle: istockphoto.com

Starke Authentisierung

Zu einer weiteren Erhöhung der Sicherheit bei gleichbleibend einfacher Handhabung trägt die Einbindung einer sogenannten Multi-Faktor-Authentifizierung bei. Dabei werden zur Anmeldung neben Benutzername und Kennwort auch zusätzliche Hardwarekomponenten eingesetzt. So zum Beispiel Smartcards, aktive und passive RFIDs sowie Fingerprint-Sensoren. Häufig verwendet werden bisher namentlich ID- beziehungsweise OTP-Token, die jeweils nur für eine begrenzte Zeit gültige Zahlenkombinationen generieren. Die jeweiligen Hardwarekomponenten lassen sich sowohl einzeln als auch in Kombination nutzen. Welche Multi-Faktor-Authentifizierungen pro Applikation, User und PC unterstützt werden sollen, lässt sich durch den Administrator mittels Policies definieren.

Physical/Logical – der integrale Ansatz

Unter der Bezeichnung Physical/Logical wird die Integration der physischen Zugangskontrollsysteme für Gebäude und Netzwerke in ein unternehmensweites Sicherheitsmanagementsystem verstanden. Dadurch wird es beispielsweise möglich, einem Benutzer nur dann Zugriff auf die Netzwerkressourcen im Büro zu gewähren, wenn er das Gebäude auch tatsächlich betreten hat. Ebenso lässt sich der Zugriff via VPN unterbinden, wenn sich die entsprechende Person im Gebäude befindet. Des Weiteren können sämtliche Zugangsberechtigungen einer Person auf Knopfdruck gesperrt werden – sowohl der Zugriff auf Applikationen und Daten als auch der Zutritt zu Gebäuden und Firmenarealen.

Die Verknüpfung physikalischer und logischer Kriterien gewährt eine bisher nicht erreichte, für die Sicherheit relevanten Konvergenz von physikalischen Gegebenheiten und IT-Verzeichnissen. Dies führt gegenüber heutigen Lösungen zu einer wesentlich feinmaschigeren Authentifizierungsschicht und hilft, bisher unberücksichtigte Schlupflöcher zu schliessen. ■