ESSO vereinfacht Passwort-management

Eine Vielzahl von Zugangscodes gehören zur gängigen «Ausrüstung» fast aller Mitarbeitenden. Entsprechend schwierig präsentiert sich die Verwaltung auch hinsichtlich der Sicherheit. «Echtes» Single Sign-On schafft Abhilfe. Urs Fink

Urs Fink
ist Produkt Manager IAM bei der Boll Engineering AG
uf@boll.ch

Das Handling der eigenen Identität hat in fast allen Unternehmen eine hohe Komplexitätsstufe erreicht. Der Zugriff auf Applikationen, Daten und IT-Systeme setzt den Einsatz unterschiedlichster Zugangscodes voraus. Und es liegt in der Natur der Sache, dass der Zugriff auf kritische Applikationen mit sogenannten «starken Passwörtern» gesichert wird. Dabei sind oft eine Mindestzeichenzahl, die Kombination aus Gross- und Kleinbuchstaben, ändernde Zahlen, Sonderzeichen etc. gefordert. In aller Regel sind die Benutzenden auch aufgefordert, das Passwort in kurzen Kadenzen zu wechseln. Zwar sind starke Passwörter im Vergleich zu einfachen Zugangscodes nur schwer «knackbar» und gewähren eine vordergründig höhere Log-in-Sicherheit. Andererseits erschweren sie das Leben der jeweiligen User. Namentlich dann, wenn es gilt, mehrere Zugangscodes in Erinnerung zu behalten. Die entsprechenden Probleme und «Workarounds» sind hinlänglich bekannt. So werden einerseits Passwörter schriftlich notiert – was die notwendige Sicherheit regelrecht unterminiert und je nach Branche gar gesetzliche Richtlinien missachtet. Andererseits werden die persönlichen Identifikationscodes schlichtweg vergessen, was dazu führt, dass gewünschte Anwendungen nicht genutzt werden können und dass der Helpdesk belastet wird. Keine Frage: Die zunehmende Zahl der zu verwaltenden Accounts und Passwörter ist für viele Personen und Firmen zur Belastung geworden.

Zugriff auf alle Anwendungen – mit einem Passwort

Dieser Problematik Abhilfe verschaffen moderne «Enterprise Single Sign-On»-Lösungen (ESSO), die die Verwaltung von Benutzerdaten und Zugriffsrechten massiv vereinfachen. ESSO ermöglicht den Benutzenden einen konsolidierten Zugang zu unterschiedlichsten Applikationen und Ressourcen – mittels lediglich einer Log-in-Prozedur. Dazu authentifi-

Dank ESSO (Enterprise Single Sign-On) entfällt für die User die Notwendigkeit, mit einer unübersichtlichen Anzahl Identitäten (Benutzernamen, Passwörter, Pin-Codes etc.) zu operieren. Stattdessen verschafft ESSO einen konsolidierten, hoch gesicherten Zugang zu den individuell freigegebenen Applikationen. Bildquelle: Boll

ziert sich ein Anwender einmalig an geeigneter Stelle (zum Beispiel beim Log-in am PC, an einem Thin-Client oder an einer Workstation) und wird dann bei allen weiteren Anwendungen wie Terminal-Applikationen, Webbrowser- oder ASP-Lösungen automatisch angemeldet. Alle dem jeweiligen User freigegebenen Applikationen stehen ihm – ohne nochmalige Eingabe von Log-in-Daten – zur Verfügung. Dieser Single-Sign-On-Prozess stellt für Benutzerinnen und Benutzer eine wesentliche Erleichterung dar und reduziert aufgrund der zentralen Verwaltung der User-Accounts den Administrationsaufwand für das Passwortmanagement.

Beachtenswert ist die Möglichkeit, auch im Offlinebetrieb von den ESSO-Möglichkeiten zu profitieren. Dazu werden die entsprechenden Zugangsdaten für eine vordefinierte Zeit im Notebook gespeichert. Von Bedeutung ist dies beispielsweise für Aussendienstmitarbeitende, die vor Ort bei ihren Kunden – ohne Remote-Zugriff auf das Firmennetzwerk – einen gesicherten Zugriff auf die lokale Applikation sowie auf die im Notebook gespeicherten Kundendaten benötigen.

Vorzüge einer integralen ESSO-Lösung

- Vereinfacht das Passworthandling der User
- Erhöht die Sicherheit von Daten, Applikationen und Systemen
- Reduziert die Aufwendungen für das Passwortmanagement
- Limitiert die Helpdesk-Aufwendungen
- Garantiert die Einhaltung von gesetzlichen Richtlinien und Regeln hinsichtlich der Verwendung starker Passwörter
- Verschafft einen detaillierten Einblick in die Zugangsaktivitäten der User zu den einzelnen Applikationen und Systemen

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 benötigt. So zum Beispiel Smart Cards, aktive und passive Proximity Cards (RFID) sowie Fingerprint-Sensoren. Häufig eingesetzt werden bisher namentlich ID- beziehungsweise OTP-Token (On Time Password), 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.

Starke Passwörter und Passwortänderungen

Moderne ESSO-Lösungen unterstützen die automatisierte Implementierung komplexer, anwendungsspezifischer Passwortregeln. Dazu erstellen sie ohne Zutun der User gemäss vorgegebenen Richtlinien automatisch einzigartige, starke Passwörter, wobei auch sich zyklisch ändernde Passwörter unterstützt sind. Dank dieser Funktion sind Administratoren und Sicherheitsverantwortliche in der Lage, auf Basis der primären Benutzerauthentisierung starke Passwortrichtlinien durchzusetzen, ohne zusätzliche Schulung oder Belastung der Nutzenden zu verursachen.

ESSO-Lösungen zeichnen sich in der Regel auch durch weitreichende Monitoring- und Reporting-Funktionen aus. Diese ermöglichen Unternehmen, die Passwortereignisse zu überwachen, zu protokollieren und in einer zentralen Datenbank abzulegen. Sie versetzen Administratoren in die Lage, die Zugangsdaten für jeden Benutzer sowie für jede Anwendung und Arbeitsstation an einer zentralen Stelle zu überwachen. Entsprechende Reports tragen dazu bei, dass die Einhaltung von Richtlinien anwendungsübergreifend geprüft und dokumentiert werden kann.