Authentifizierungslösung mit RFID und mobilen Technologien

SINGLE-SIGN-ON-ANWENDUNGEN FÜR DIE NEUE ARBEITSWELT

Ob in Unternehmen, Organisationen oder Behörden: Die Pandemie hat das Arbeitsleben nachhaltig verändert. Bei der Wahl des Arbeitsorts können Mitarbeiter heute häufig flexibel entscheiden. Doch egal, ob Büro oder Homeoffice: Daten und Netzwerke müssen immer und überall vor unbefugtem Zugang geschützt werden. Single-Sign-on/PC-Logon-Systeme, welche die Middleware mit RFID (Radio-Frequency Identification) oder smartphonefähigen Technologien zur Benutzerauthentifizierung kombinieren, können hierzu einen wichtigen Beitrag leisten.

Die Vorteile des flexiblen, ortsunabhängigen Arbeitens wollen viele Beschäftigte auch in Zukunft für sich nutzen. Einer Umfrage zufolge möchten 75 Prozent der Teilnehmer auch in Zukunft verstärkt mobil arbeiten [1]. Unternehmen, Organisation, aber auch Behörden können im Wettbewerb um die besten Köpfe ihre Chance ergreifen, indem sie ein attraktives Arbeitsumfeld schaffen. Einfache, komfortable Prozesse, die im Büro ebenso reibungslos ablaufen wie beim mobilen Arbeiten, sind für Mitarbeiter ein klarer Pluspunkt. Dabei müssen Zugänge zu Daten, vernetzten Geräten und Softwaresystemen jederzeit bestmöglich geschützt sein.

Um Prozesse zu vereinfachen und die Komplexität für Mitarbeiter zu reduzieren, sind Single-Sign-on (SSO)/PC-Logon-Systeme ein probates Mittel. Eine einmalige Authentifizierung erlaubt Mitarbeitern Zugriff auf alle Dienste, Netzwerke und Dateien, für die sie autorisiert sind. Die Vorteile liegen auf der Hand: Die Einmalanmeldung spart dem Mitarbeiter Zeit und steigert so die Produktivität. Die Authentifizierung bei SSO-/PC-Logon-Systemen erfolgt jedoch häufig noch über Passwörter – mit den bekannten Problemen. Anwender verwenden beispielsweise oft besonders leicht zu merkende Passwörter, die sich einfach erraten oder kompromit-

Egal ob Büro oder Homeoffice: Um Daten und Netzwerke vor unbefugtem Zugang zu schützen, können Single-Sign-on/PC-Logon-Systeme in Verbindung mit RFID- oder smartphonefähigen Technologien kombinieren, einen wichtigen Beitrag leisten. (Quelle: ELATEC)

tieren lassen. Zwar sind die Anforderungen an ein sicheres, sogenanntes „nicht kompromittierbares" Passwort in der ISO-Norm 27001 für Informationssicherheitsmanagementsysteme klar festgelegt. Diese sind jedoch so umfassend und komplex, dass sich bei Nutzern schnell eine gewisse Passwortmüdigkeit einstellen kann. Die häufige Folge: Eine Behelfslösung, bei der die Passwörter auf einem Zettel notiert und für alle gut sichtbar an den Computer geklebt werden. Die Folgen kompromittierter oder geteilter Passwörter können jedoch gravierend sein und reichen vom Diebstahl geistigen Eigentums über die Schädigung des Arbeitgeberimages bis hin zu Bußgeldern aufgrund von Datenschutzverstößen.

GESPANN FÜR KOMFORTABLE AUTHENTIFIZIERUNG: SSO MIT RFID UND MOBILEN TECHNOLOGIEN

Am Markt sind Alternativen zur Authentifizierung mittels Passwort verfügbar. Eine sichere und besonders komfortable Möglichkeit für Nutzerauthentifizierung und Zugangskontrollen bietet eine SSO-Lösung, die PC-Logon-Middleware mit RFID oder smartphonebasierten Bluetooth Low Energy-(BLE-) oder Near Field Communication-(NFC-)Systemen kombiniert.

Hierbei wird ein Lesegerät an den Computer oder die Workstation angeschlossen beziehungsweise in diese integriert und mit der PC-Logon-Middleware verbunden. Statt zur Anmeldung ein Passwort einzugeben, hält der Nutzer lediglich seine ID-Karte oder sein Smartphone mit digitalem Berechtigungsnachweis an das Lesegerät, um Zugriff auf Netzwerke, Dienste und Dateien zu erhalten.

Beide Optionen sind für die Nutzer einfach zu handhaben: RFID-Karten werden bereits häufig für die Identifizierung von Mitarbeitern und die Zutrittskontrolle zu Gebäuden eingesetzt. Dieselben Karten können so auch für die sichere Authentifizierung im Rahmen von SSO-/PC-Logon-Systemen verwendet werden. Das ständig griffbereite Smartphone eignet sich ebenfalls optimal für den Zugang zu Unternehmensnetzwerken und Ressourcen. Ob Karte oder Smartphone: Eine solche SSO-/PC-Logon-Lösung funktioniert im Büro genauso zuverlässig wie beim mobilen Arbeiten am Laptop. Die einfache Authentifizierung spart Zeit bei der Anmeldung, lässt die Passwortmüdigkeit der Nutzer außen vor und erhöht so die Sicherheit. Ein weiterer positiver Effekt: Es ist jederzeit nachvollziehbar, wer wann auf welche Daten zugegriffen hat.

Doch nicht nur die Nutzer profitieren von einer Umstellung auf ein solches SSO-/PC-Logon-System. Vor allem Unternehmen entstehen dadurch erhebliche Vorteile, indem

- sich der Zeitaufwand für den IT-Support reduziert, der durch vergessene Passwörter entsteht
- das System zur Umsetzung der ISO 27001 beiträgt
- sich die Verwaltung der Authentifizierungssysteme zentralisieren und dadurch vereinfachen lässt
- sich die Möglichkeit bietet, alle Zugangsebenen zu Systemen zu sichern, ohne dass mehrere Anfragen durch den Anwender gestellt werden müssen
- sich Zugangskontrollinformationen für Konformitätstests mit den verschiedenen Standards zentralisieren lassen
- sie unter gewissen Voraussetzungen staatliche Förderungen für die Umstellung auf digitale Prozesse beziehungsweise die digitale Transformation beantragen können.

KRITERIEN FÜR EINE ERFOLGREICHE IMPLEMENTIERUNG

Bei der Einführung eines SSO-/PC-Logon-Systems, das RFID, NFC oder BLE für die Authentifizierung nutzt, sind drei Aspekte besonders zu beachten:

1. ***Flexibilität durch universelle Lesegeräte***

   Am internationalen Markt ist eine Vielzahl von Kartentechnologien mit jeweils eigenen Datenformaten, Kommunikationsfrequenzen und Sicherheitsfunktionen verfügbar. Für Unternehmen und Organisationen bedeutet dies, dass Mitarbeiterausweise mit unterschiedlichen Technologien im Einsatz sein können – insbesondere, wenn mehrere Standorte weltweit unterhalten werden. Die meisten Lesegeräte sind jedoch lediglich in der Lage, einige wenige Kartentechnologien zu lesen. Eine Lösung bieten Multifrequenz-Lesegeräte, die mit bis zu 60 weltweit gängigen Transpondertechnologien kompatibel und für den Einsatz in bis zu 110 Ländern zertifiziert sind. Die universellen Geräte nutzen sowohl RFID für Authentifizierung und Zugang als auch NFC oder BLE. So lassen sich auch mobile Endgeräte in das System einbinden, wodurch eine größtmögliche Flexibilität für die Nutzer gegeben ist.

   Eine moderne Authentifizierungslösung, die Multifrequenz-Leser einsetzt, erlaubt die nahtlose Integration unterschiedlicher Anwendungen in die bestehenden Systeme einer Organisation. So können mehrere Applikationen wie SSO, Zutrittskontrolle oder Zeiterfassung integriert werden. Das stellt eine einheitliche und zeitsparende Verwaltung sowie hohen Anwenderkomfort sicher.

Bei modernen Authentifizierungslösungen hält der Nutzer lediglich seine ID-Karte oder sein Smartphone mit digitalem Berechtigungsnachweis an ein Lesegerät, um Zugriff auf Netzwerke, Dienste und Dateien zu erhalten. (Foto: ELATEC)

2. Zuverlässiger Schutz von Netzwerken und Daten

Die verwendeten Lesegeräte müssen sowohl gegen physische Manipulationen als auch gegen Hackerangriffe gerüstet sein und eine fortschrittliche Verschlüsselung für Hochsicherheitsanwendungen unterstützen. Nur dann ist ein sicherer Authentifizierungsprozess gegeben. Um eine solche Authentifizierungslösung effektiv und ganzheitlich abzusichern, reicht eine Betrachtung des Lesegeräts allein jedoch nicht aus. Es ist notwendig, das komplette System in die Sicherungskonzepte des Unternehmens einzubeziehen.

3. Mehr Sicherheit durch Remote Updates und Upgrades

Anforderungen und IT-Infrastrukturen verändern sich im Laufe der Zeit. Nur mit einem flexiblen System, das Optimierungen, Adaptionen und Upgrades vorsieht, sind Organisationen auch in Zukunft auf der sicheren Seite. Lesegeräte sollten daher über eine robuste offene Programmierschnittstelle verfügen, die sie anpassungsfähig und damit zukunftssicher macht. Damit ist es möglich, Leser so zu programmieren, dass sie wichtige Funktionen für anspruchsvolle PC-Logon-Middleware bieten und neue, möglicherweise zum Anschaffungszeitpunkt noch unbekannte Anforderungen in Zukunft zu erfüllen. Gerade bei SSO-/PC-Logon-Anwendungen ist eine zentrale Remote-Konfigurationsoption essenziell und von entscheidendem Vorteil. Sie erlaubt es, alle installierten Lesegeräte zentral und kostengünstig zu aktualisieren – und das unabhängig von ihrer Anzahl und ihrem Standort. So kann beim mobilen Arbeiten stets dieselbe Sicherheit gewährleistet werden wie am Rechner im Büro. ■

Quellen

[1] https://cmk.sueddeutsche.de/cms/articles/13084/mtssource/13078

BURHAN GÜNDÜZ,
Vice President Secure Printing EMEA & Japan bei ELATEC GmbH

So funktionieren RFID, BLE und NFC

RFID-Karten haben einen eingebetteten Chip (oder Tag), der aus zwei Hauptkomponenten besteht:

- *einer integrierten Einheit, die Informationen speichern und verarbeiten kann*
- *einer Antenne zum Senden oder Empfangen eines Signals*

Auf jeder RFID-Karte ist ein eindeutiger Datensatz – beispielsweise eine Nummer – gespeichert, der zur Identifizierung der Karte und damit auch der Person dient, die sie bei sich trägt. Befindet sich eine Karte mit einem eingebetteten RFID-Tag in der Nähe eines RFID-Lesegeräts, sendet der Reader ein Funksignal aus, um diesen Datensatz abzufragen. Das Signal aktiviert den Tag, der diese Energie dann nutzt, um dem Leser seine eindeutige ID mitzuteilen.

Sowohl NFC als auch BLE sind Technologien für den kontaktlosen Datenaustausch. Ihr Hauptunterschied zu RFID besteht darin, dass die Informationsträger (zum Beispiel Smartphones) aktive Funksender sind und eine Stromquelle benötigen.

- *NFC basiert auf hochfrequenter RFID-Technologie (13,56 MHz) und ermöglicht einen kontaktlosen Datenaustausch in der Nahfeldkommunikation (<10 cm)*
- *BLE ist eine Kurzstrecken-Funktechnologie für Entfernungen bis zu zehn Metern im Frequenzbereich von 2,4 GHz.*

Werden Smartphones für die Benutzerauthentifizierung und Zugangskontrolle verwendet, fungieren sie als Kartenemulatoren und senden eine eindeutige Benutzer-ID an das Lesegerät.