Risiken beim Einsatz von RFID-Identmedien? Der BHE klärt auf!

Berichte über Sicherheitslücken bei RFID-Karten beziehen sich häufig auf veraltete Technologien, die durch modernere, sicherere Standards ersetzt wurden. Frühere Karten enthielten unverschlüsselte und leicht auslesbare Daten, wodurch sie anfällig für Kopierversuche und Missbrauch waren.

Aktuelle Entwicklungen in der RFID-Technologie setzen auf Verschlüsselungsalgorithmen und authentifizierte Kommunikationsprotokolle. Hauptsächliche Sicherheitsprobleme entstehen jedoch oft durch nachlässigen Umgang mit den Datenträgern, etwa Diebstahl, Weitergabe oder Beschädigung. Moderne RFID-Systeme bieten in der Regel ein hohes Maß an Sicherheit, wenn sie richtig implementiert und verwaltet werden. Im Folgenden wird auf diese Thematik näher eingegangen.

Verschlüsselnde Kartentechnologien sind seit Jahren Standard

Berührungslose Kartentechnologien haben sich zur Zutrittssteuerung nachhaltig durchgesetzt. Die Hersteller sind sich der sicherheitstechnischen Relevanz sehr wohl bewusst. Daher erhöhen seit Jahren am Markt übliche, verschlüsselnde Kryptoverfahren die Sicherheit der Gesamtsysteme erheblich. Diese Verfahren orientieren sich an eigens dafür erstellten Normen wie der ISO/IEC 14443 1-4.

Um die Forderung nach Schutz gegen Fernkopieren und Abhören zu erfüllen, werden hierbei auf der Luftstrecke (z. B. zwischen Karte und Zutrittsleser) verschlüsselte Technologien (Übertragungsprotokolle) eingesetzt. Dieser „Kopierschutz“ für Karte oder Transponder verhindert ein Duplizieren von Berechtigungen und macht ein Mitlesen der über die Luftstrecke zwischen Karte und Beschlag ausgetauschten Daten unmöglich.

Da diese technischen Features schnelle und sichere Schreib-/Leseverfahren zwischen Karte und Lesesystem bzw. mechatronischem Schließsystem vorsieht, wurde die zuvor übliche 125-kHz-Kartentechnologie durch die 13,56-MHz-Technik abgelöst. Heute bieten Karten und Transponder, z. B. des Typs Mifare DESFire EV3 oder Legic Advant, eine 128-Bit-AES-Verschlüsselung auf der Luftstrecke zwischen Karte und Beschlag.

Diese verschlüsselnden Kartentechnologien sind seit Jahren Stand der Technik und werden mittlerweile standardmäßig für die Zutrittssteuerung eingesetzt. Die Leser dieses Artikels sind daher gut beraten, solchen Berichten über offensichtlich veraltete Installationen, die als vermeintliches Beispiel für eine angeblich generell unsichere Technologie herangezogen werden, keinen Glauben zu schenken.

Einflussfaktoren zur Sicherheit von RFID-Mitarbeiterausweisen

Physische Ausweise können leicht verloren gehen oder gestohlen werden und das Klonen von 125-KHz-RFID-Daten stellt eine zusätzliche Bedrohung dar. Daher sind Risikominderungsmaßnahmen unerlässlich. Dazu zählen mehrfache und zusätzliche biometrische Authentifizierung sowie ein effektives Zugriffsmanagement. Bei Verlust sollte eine sofortige Sperrung möglich sein. Mitarbeiter sollten regelmäßig zu Risiken und zur sicheren Aufbewahrung geschult werden. Regelmäßige Sicherheitsüberprüfungen sind wichtig.

Digitale Mitarbeiterausweise auf dem Smartphone

Der digitale Mitarbeiterausweis auf dem Smartphone ermöglicht eine einfache und sichere Verwaltung von Identität und Berechtigungen. Mitarbeiter können sich über eine App, Over-the-Air (OTA) und digitale Wallets ausweisen und benötigen dafür ein NFC-fähiges Smartphone. NFC (Near Field Communication) erlaubt sichere Datenübertragungen über bis zu 5 cm und arbeitet mit einer Frequenz von 13,56 MHz, entsprechend dem ISO-Standard 14443A.

Die Technologie nutzt biometrische Authentifizierung (z. B. Fingerabdruck oder Gesichtserkennung) und Verschlüsselung, um die Daten zu schützen und unbefugten Zugriff zu verhindern.

Die Verwendung digitaler Ausweise fördert Ressourcen- und Umweltfreundlichkeit, da Kosten und Aufwand für traditionelle Identifikationsmedien entfallen. Dieses Konzept verbindet Bequemlichkeit mit Sicherheit, stellt jedoch Herausforderungen in der Cybersecurity dar.

Eine effektive Implementierung und Infrastruktur im Unternehmen sind entscheidend, um die Vorteile zu maximieren und die Sicherheit zu gewährleisten.

Vergleich von RFID-Karten und mechanischen Schlüsseln

Eine RFID-Karte bietet für Betreiber und Nutzer eine Vielzahl von Vorteilen gegenüber einem mechanischen Schlüssel. Sie kann z. B. jederzeit unkompliziert aus dem Zutritts- oder Schließsystem gelöscht werden, sollte z. B. ein gekündigter Mitarbeiter, Besucher oder Hotelgast versehentlich vergessen haben, seine Karte abzugeben.

Gleichzeitig lassen sich mit RFID-Karten sogenannte Multiapplikationen, z. B. für Zeit und Zutritt sowie zur Absicherung von Templates (biometrische Merkmale), betreiben.

BHE; 03/2026

BHE Bundesverband Sicherheitstechnik e.V., Feldstraße 28, 66904 Brücken, Tel.: 06386 9214-0, Fax: 06386 9214-99, info@bhe.de, www.bhe.de