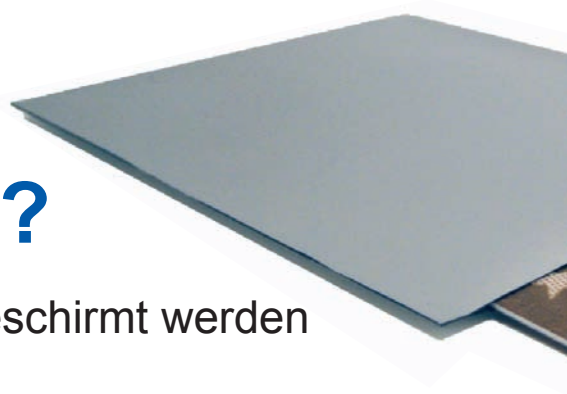
RFID-Keycards – eine Sicherheitslücke?



Sicherheitsausweise müssen sorgfältig abgeschirmt werden

Nicht nur im neuen Personalausweis, auch bei der Zugangskontrolle spielen RFID-Chips eine wichtige Rolle. Die kontaktlose Identifikation kann aber auch Probleme durch Überreichweiten verursachen oder zum Einfallstor für Hacker werden. Experten raten zu regelmäßiger Revision und sorgfältiger Abschirmung.

Sicherheitspersonal kann unversehens selbst zum Sicherheitsrisiko werden. Diese Erfahrung machte man in der geschlossenen Abteilung einer Klinik in Süddeutschland. Immer wieder lösten Wachleute versehentlich den Öffnungsmechanismus von Türen aus, sozusagen „im Vorbeigehen“. Die Ursache: ein Sicherheitsausweis, den sie an der Kleidung trugen. Der darauf befindliche RFID-Chip hatte unbemerkt Kontakt zum Lesegerät aufgenommen.

Negativbeispiele

Eine schlechte Figur machte auch das RFID-basierende Sicherheitssystem des Hamburger Flughafens, das vom berühmt-berüchtigten Chaos Computer Club (CCC) unter die Lupe genommen wurde. Ein einfaches RFID-Lesegerät, das auch die Signale eines RFID-Chips emulieren konnte, hatte bereits ausgereicht, um die Sicherungen schachmatt zu setzen. Mit so wenig Widerstand hatten die Chaos’ler nicht gerechnet: Wir waren schlicht schockiert, überhaupt keine Hürden zu finden, die wir hätten überwinden müssen“, wunderte sich CCC-Mitglied Karsten Nohl.

Identifikation per Mikrochip

RFID steht für Radio Frequency Identification. RFID-Sicherheitsausweise beinhalten im Wesentlichen einen Mikrochip mit einem Sicherheits-Code und eine kleine Spule, die als Antenne fungiert. RFID arbeitet in aller Regel passiv, kommt also ohne eigene Stromversorgung aus. Ausgelesen werden die Chips mit einem elektromagnetischen Wechselfeld. Durch das pulsierende Magnetfeld wird in der Spule eine Spannung induziert, die als Stromversorgung für den Chip dient.

Die Hersteller der RFID-Tags haben viel Zeit und Energie darauf verwandt, das Auslesen auch unter schwierigen Bedingungen problemlos zu ermöglichen. Denn erfunden wurde das System eigentlich für den Logistik-Bereich. Aber auch aus der Zugangskontrolle ist RFID nicht mehr wegzudenken. Die Ausweise funktionieren problemlos über Jahre hinweg.

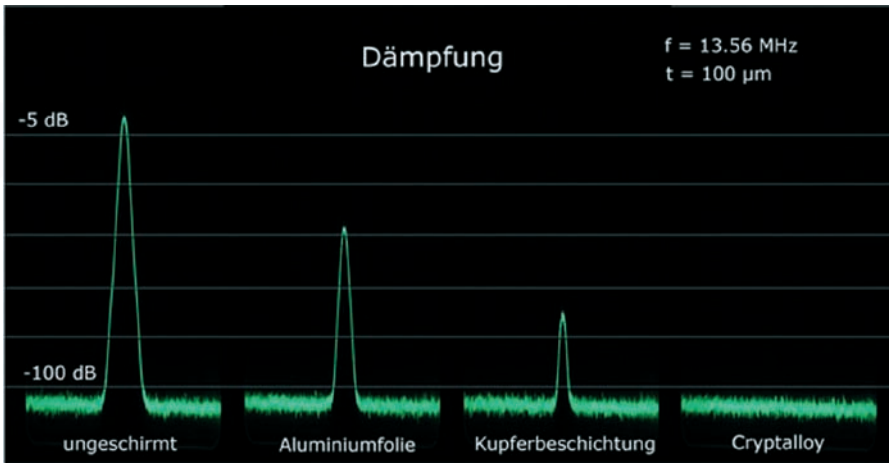
Gerade die kontaktlose Übertragung macht Datenschützern und Sicherheitsexperten allerdings Kopfzerbrechen. „Die Reichweite von RFID-Sicherheit-Chips kann stark variieren“, weiß Stefan Horvath, Managing Director bei Kryptronic. Sein Unternehmen befasst sich schon seit vielen Jahren mit dem Thema RFID-Abschirmung. Umgebungsparameter wie Luftfeuchtigkeit, oder sogar eine Oberbekleidung aus Kunstfaser, können die

Speziallegierungen wirken auch, wenn sie das Objekt nicht komplett umschließen.

→AUTOR

***Ralf Siebler** ist Fachjournalist und Spezialist für Sicherheitstechnik, München.*
Tel.: +49 89 30726216
E-Mail: rs@siebler-kreativ.de
www.cryptalloy.de

Nur physikalische Absicherung schützt sensible Daten wirklich zuverlässig.



RFID-Abschirmeigenschaften verschiedener Materialien: Nur Speziallegierungen sind wirklich sicher. Bilder: Kryptronic/Cryptalloy

Übertragungseigenschaften beeinflussen. Das führt oft zu unvorhersehbaren Überreichweiten.

Kontaktlos ausspioniert

Ein weiteres Problem: RFID-Sicherheitsausweise können ausspioniert werden, ohne dass der Besitzer dies mitbekommt. Die Lesegeräte sind frei erhältlich. Da es sich bei RFID um ein rein passives System handelt, ist ein Leseversuch nur mit einem speziellen Detektor festzustellen.

Vier oder fünf Jahre alte RFID-Ausweise sind keine Seltenheit, und gerade ältere Systeme sind oft unsicher. Bereits im Dezember 2009 hatten CCC-Hacker demonstriert, wie einfach Funkchipkarten des Schweizer Herstellers Legic zu knacken sind. Dabei habe sich herausgestellt, dass die Daten auf dem Chipsystem der „Prime"-Produktreihe unverschlüsselt gespeichert würden, gab der CCC an.

Auch der immer noch weit verbreitete RFID-Chip „Mifare Classic" gilt als unsicher. Er speichert die Daten zwar verschlüsselt, verwendet aber dafür ein sehr leicht zu knackendes System.

Ist ein Zugangskontrollsystem auf RFID-Basis im Einsatz, sollte es in regelmäßigen Abständen einer Sicherheits-Revision unterzogen werden. Dabei sollte man nach einer standardisierten Checkliste vorgehen. Die systematische Prüfung ist natürlich auch bei der Neuanschaffung dringend anzuraten. Denn auf Anfrage wird natürlich jeder Hersteller versichern, sein Produkt sei sicher.

Physikalische Abschirmung

Die eingangs geschilderten Beispiele zeigen, dass RFID-Chips schnell zum Sicherheits-Problem werden können. Daher gilt grundsätzlich: RFID-Ausweise müssen mit geeigneten Abschirmmaterialien gegen verdeckte Leseversuche gesichert sein. Das gilt besonders nach dem Verlassen des gesicherten Perimeters. Soll ein besonders sicherheitsrelevanter Bereich abgesichert werden oder besteht die Gefahr einer Überreichweite, muss die RFID-Keycard ständig in einer Abschirmvorrichtung verbleiben. Sie darf nur unmittelbar vor der Authentisierung entnommen werden.

RFID-Chips abzuschirmen, ist allerdings leichter gesagt als getan. Einfache Aluminiumfolie oder zinkbeschichtete Billig-Abschirmungen können das Auslesen oft nicht verhindern. Gerade der unsichere EM41XXX-Chip sendet zum Beispiel auf einer Trägerfrequenz von 125 kHz, die viele No-Name-Abschirmungen mühelos durchdringt. Auch von improvisierten Schutzmaßmaßnahmen raten Experten dringend ab. Denn zum Beispiel Aluminiumfolie muss den Chip komplett umschließen. Kleine Lücken können hier schon zum Sicherheitsrisiko werden. RFID-Sicherheitsausweise müssen aber vielfach offen an der Kleidung getragen werden.

Wirkliche sicher sind nur Abschirmungen aus einer eigens für diesen Zweck entwickelten Speziallegierung, zum Beispiel Cryptalloy. Folien aus Cryptalloy wirken nicht nur durch die Abschirmung, sondern auch durch eine Frequenzverzerrung des Lesesignals. Diese Beschichtungen schützen also vor Leseversuchen, auch wenn sie die Karte nicht vollständig umschließen. Das ermöglicht auch Ausweishüllen, die auf einer Seite durchsichtig sind. □

↓ INFOS IM DETAIL

Schrittweise Revision von RFID-Sicherheitssystemen

Wie alt ist das System?
RFID-Zugangskontrollen, die älter als drei Jahre sind, verwenden oft inzwischen geknacktes Verschlüsselungssystem – oder gar keines.

Welcher Chip ist auf der Karte?
Ausgetauscht werden sollten in jedem Fall Karten, die noch mit einem Mifare Classic Chip arbeiten. Sicher sind nur die neueren Versionen des Mifare-Chips. Ebenfalls unsicher, aber weit verbreitet: Chips der Serie EM41XXX mit unverschlüsseltem Speicher.

Welche Verschlüsselung wird verwendet?
Viele herstellerspezifische Algorithmen erweisen sich als angreifbar. Die Verschlüsselung muss mit standardisierten und anerkannten Verfahren geschehen, zum Beispiel AES.

Sind die Ausweise abgeschirmt?
RFID-Ausweise müssen mit Spezialfolien gegen nicht autorisierte Leseversuche geschützt werden.

Artikel als PDF
www.sicherheit.info
Webcode: 1118707