Merkblatt

SKS stärkt die Konsumenten

Bern, 19. Januar 2017

Achtung digitale Taschendiebe: So schützen Sie Ihre Kreditkartendaten

Kreditkartendaten können über die Kontaktlos-Funktion der Karte relativ einfach ausspioniert und missbraucht werden. Wenn ein Betrüger durch Absaugen der RFID-Daten in den Besitz vertraulicher Informationen kommt, kann er sich für sein Opfer ausgeben, in dessen Namen Zahlungen und Bestellungen tätigen sowie sich Zugriffe erschleichen, die ihm nicht zustehen. Wie kann man dies vermeiden?

Kreditkarte, Biometrischer Pass, Swiss Pass und Personalausweise haben eins gemeinsam – sie sind alle mit einem sogenannten RFID-Chip ausgestattet.

Wie funktioniert RFID?

RFID steht für „Radio Frequency Identification“, also Identifizierung mithilfe elektromagnetischer Wellen. Mit der RFID-Technologie können Objekte und Lebewesen mithilfe von Radiowellen lokalisiert und identifiziert werden. Dazu braucht es das Zusammenspiel eines Datenträgers (Transponder genannt) und eines Lesegerätes mit Antenne. Wenn der Transponder in die Reichweite dieser Antenne gelangt, kann man Informationen berührungslos vom Speicher des Transponders lesen oder auch Daten darauf speichern. Kontaktloses Zahlen wird durch eine Spezialisierung der RFID-Technik möglich, der sogenannten „Near-Field-Communication“, kurz NFC. Diese wurde speziell für kurze Distanzen (max. 10cm) entwickelt.

Karten und Ausweise, welche mit dieser Technologie ausgestattet wurden (bei den meisten neuen Kreditkarten erkennbar am WLAN-Symbol neben dem Chip), bergen allerdings ein nicht zu unterschätzendes Sicherheitsrisiko.

Kontaktlose Kreditkarten sparen uns Zeit an der Kasse – aber sicher sind sie nicht

Ein Diebstahl ist schnell passiert

Denn wer auf Kreditkartendaten abgesehen hat, braucht dafür keinen grossen Auwand zu betreiben: Kartenscanner gibt es auf Ebay für wenige Franken zu kaufen, bei Android-Handys muss nur die NFC-Funktion in den Einstellungen freigeschaltet und teilweise noch ein App heruntergeladen werden.[1] Die Herausforderung für Datendiebe besteht einzig darin, nah genug (dh. einige Zentimeter entfernt) an ihr Opfer zu gelangen, damit die Daten vom Gerät ausgelesen werden können. Da ein solcher Kontakt im öffentlichen Verkehr oder in einer Kassenschlange nicht unüblich ist, raten Experten zu prä-

[1] http://bit.ly/2eY4BlA (Watson)

ventiven Massnahmen. Denn mit den erbeuteten Daten können die Kriminellen beispielsweise bei Anbietern online einkaufen, welche die dreistellige Sicherheitsnummer auf der Karte nicht verlangen (beispielsweise bei Amazon) und so einen finanziellen Schaden verursachen.

Schutz durch Hülle, Alu oder Einschnitt

Weil die Banken den Funkchip der Kreditkarten nicht ausschalten können, müssen Benutzer selbst aktiv werden: So gibt es im Handel (beispielsweise bei Swicure) diverse **Sicherheitsetuis oder -portemonnaies** zu kaufen, welche die NFC abschirmen. Auch die SKS bietet für wenig Geld eine **Karten-Schutzhülle (zur Bestellung)** an. Hier können Sie sie bestellen: Solche Schutzhüllen können auch gegen das Problem helfen, dass eine Kontaktloskarte nicht erkannt wird, weil eine andere Karte ihr „dazwischenfunkt". Die umhüllten Karten wären dann aber nicht mehr kontaktlos nutzbar.

Um sich gegen Kreditkartenbetrug durch NFC-Datenklau zu schützen, gibt es auch noch eine ganz billige Lösung: Sie wickeln die Karte einfach in ein Stück **Alufolie** ein, bevor Sie sie ins Portemonnaie stecken.

Eine weitere Möglichkeit, das Senden der Informationen zu unterdrücken, ist die Unterbrechung der Antenne durch einen **kleinen Schnitt in die Karte**. Aber Vorsicht, bei dieser Variante besteht ein gewisses Risiko, dass andere Funktionen der Karte durch den Eingriff beschädigt werden. Diese Variante empfiehlt sich ausschliesslich dann, wenn Sie die Karte nie für die kontaktlose Bezahlung verwenden möchten. Sie ist nicht rückgängig zu machen, ausser Sie bestellen eine neue Karte. Sehen Sie hier, wie es gemacht wird.

Bei der PostFinance-Card (aber *nicht* bei der Postfinance-Kreditkarte) können Sie die **Funktion** am Postomaten **deaktivieren**, wenn Sie sie nicht brauchen. Oder Sie loggen sich im PostFinance-Portal ein und betätigen den Link auf dieser Seite.

Was tun im schlimmsten Fall?

Die Herausforderung bei Kreditkarten ist, dass oft erst mit der nächsten Abrechnung offensichtlich wird, wenn jemand an die Daten gelangt ist. Wer Unregelmässigkeiten entdeckt, sollte sich deshalb *sofort* an die Bank oder den Kartenhersteller wenden. Denn der finanzielle Schaden wird grundsätzlich von den Kreditkartenfirmen getragen, sofern vom Nutzer die Sorgfaltspflicht (Überprüfung der Monatsabrechung, Geheimhaltung des PIN-Codes inklusive Abdecken des PIN-Codes beim Eingeben) eingehalten wurde. Betrügerische Aktivitäten müssen bis 30 Tagen nach Rechnungsdatum gemeldet sowie die Karte gesperrt werden.

Hat Ihnen dieses Merkblatt geholfen?
Um unser Angebot ausbauen und unterhalten zu können, sind wir auf Ihre Unterstützung angewiesen.
Gönnerschaft / Förderschaft / SMS-Sofortspende / Postkonto: 30-24251-3.
Gönner und Förderer beraten wir kostenlos.
Herzlichen Dank!