Manipulationen am Türöffner einer Bank

Eine andere Variante ist die Manipulation des Kartenlesers am Türöffner des Bankinstitutes. Die Täter tauschen hierzu den originalen Kartenleser gegen einen manipulierten Kartenleser aus, der äußerlich nicht erkennbar ist.

Ihre PIN-Eingabe wird dann (wie schon beschrieben) mittels einer Mikrokamera oder einem Foto-Handy am Geldausgabeautomaten aufgezeichnet.

Verhaltenstipps

- Gehen Sie bitte sorgsam mit Ihren Zahlungskarten um und bewahren Sie die PIN stets getrennt von der Karte auf.
- Sofern Sie im Besitz von mehreren Zahlungskarten sind, sollten Sie den Türöffner eines Bankinstitutes nicht mit der Karte nutzen, mit der Sie anschließend Geld abheben möchten.
- Geben Sie Ihre PIN niemals an einem Türöffner eines Bankinstitutes ein. Kein Geldinstitut verlangt für den Zugang zum Geldausgabeautomaten die Eingabe der PIN. Der Kartenleser hat immer nur die Funktion des Türöffners. Verständigen Sie in solchen Fällen die Polizei und das Geldinstitut.
- Achten Sie darauf, dass die Eingabe Ihrer PIN durch Personen nicht beobachtet werden kann. Sorgen Sie für einen ausreichenden Sicherheitsabstand zum nächsten Kunden.
- Geben Sie niemals mehrfach Ihre PIN ein, wenn Sie von einer Ihnen unbekannten Person aufgefordert werden.
- Einen wirkungsvollen Schutz gegen „Skimming“ können Sie erreichen, wenn Sie während der PIN-Eingabe mit der anderen Hand oder einem Gegenstand (z. B. Geldbörse, Blatt Papier) als Sichtschutz das Tastaturfeld vollständig abdecken. Das erschwert das „Ausspähen“ per Kamera oder Foto-Handy erheblich.

- Nutzen Sie keinen Geldausgabeautomaten, an dem Ihnen etwas ungewöhnlich erscheint, z. B. angebrachte Leisten oder Verblendungen, abstehende und lockere Teile, Spuren von Klebern rund um den Kartenschlitz.
- Bei Verdacht auf Manipulation sollten Sie die Geräte nicht nutzen. Verständigen Sie die Polizei, um mögliche Spuren sichern zu können.

Weitere Maßnahmen

- Kontrollieren Sie regelmäßig Ihre Kontoauszüge und wenden Sie sich bei Auffälligkeiten sofort an Ihre Bank.

- Bei dem Verdacht der Ausspähung Ihrer Kartendaten lassen Sie bitte umgehend die Karte über Ihre Bank bzw. den bundesweiten Sperrnotruf unter 116 116 sperren und erstatten Sie Anzeige bei der Polizei.

Weitere Infos finden Sie im Internet unter:

www.kartensicherheit.de

www.polizei-beratung.de/vorbeugung

Impressum

Herausgeber:

Landeskriminalamt Sachsen
Neuländer Straße 60
01129 Dresden

www.polizei.sachsen.de
E-Mail: praevention.lka@polizei.sachsen.de

Polizeidirektion Dresden
Schießgasse 7
01067 Dresden

„Kein Zugang für elektronisch signierte sowie für elektronisch verschlüsselte Dokumente“

Fotos: Quelle Landeskriminalamt Sachsen und Bundeskriminalamt

Mit freundlicher Unterstützung:

Ostsächsische Sparkasse Dresden

POLIZEI Sachsen

Skimming

Manipulationen von Geldausgabeautomaten

Wie Ihr Konto „geplündert” wird ...

Was ist „Skimming“?

Der englische Begriff „Skimming“ bedeutet „Abschöpfen“ oder „Absahnen” und steht für eine Methode, illegal elektronische Daten von Zahlungskarten (ec-Karte und Kreditkarte) „auszuspähen“. Bundesweit ist bei diesen Straftaten in den letzten Jahren ein Anstieg zu verzeichnen. Nach polizeilichen Erkenntnissen handelt es sich überwiegend um organisiert vorgehende ausländische Tätergruppen.

Mit den auf diese kriminelle Art erlangten Daten werden Kopien der Geldkarten gefertigt. Damit können die Täter ausschließlich im Ausland Geld von Ihrem Konto abheben.

Vorgehensweise der Täter

Um in den Besitz der Daten auf dem Magnetstreifen zu kommen, installieren die Täter vor dem originalen Karteneinschubschacht zusätzlich ein manipuliertes Aufsatzkartenlesegerät oder vor dem originalen Kartenschacht am Geldausgabeautomaten eine vollständige Frontplatte.

originale Frontplatte

manipulierte Frontplatte

Diese manipulierten Kartenleser sind optisch dem Modell des Geldausgabeautomaten angepasst (gleiche Farbe, gleiche Aufkleber) und so hergestellt, dass Ihre eingeschobene Bankkarte durch das illegale Lesegerät zum originalen Kartenleser weitertransportiert wird.

So werden die Kontodaten durch das manipulierte Aufsatzkartenlesegerät ausgelesen und gespeichert, ohne dass die Bedienung des Geldausgabeautomaten beeinträchtigt wird und Sie als Kunde misstrauisch werden. Das Geldabheben am Geldausgabeautomaten verläuft für Sie störungsfrei.

Um an Ihre PIN zu gelangen, wird Ihre Eingabe mit einer Kamera oder einem Foto-Handy „ausgespäht“ und aufgezeichnet.

Es gibt hierbei verschiedene Örtlichkeiten, die (Mini-) Kamera oder das Foto-Handy zu installieren:

- Oberhalb der PIN-Tastatur wird eine speziell für den Geldausgabeautomaten-Typ passende Verblendung oder Leiste (Kameraleiste) angebracht. Die (Mini-) Kamera bzw. das Foto-Handy ist dann in der Lage, über einen längeren Zeitraum alle PIN-Eingaben an der Tastatur aufzuzeichnen.

- seitlich in einem manipulierten Prospekthalter

- an der Decke versteckt in einer Rauchmelderattrappe

Weitere Möglichkeiten zum Ausspähen der PIN bestehen durch:

- den Aufsatz einer täuschend echt wirkenden Tastatur-Attrappe

- ein Aufsatzkartenlesegerät mit integrierter Kamera