



Skimming

Präventionshinweise gegen das
Ausspähen von EC-Kartendaten an Geldautomaten

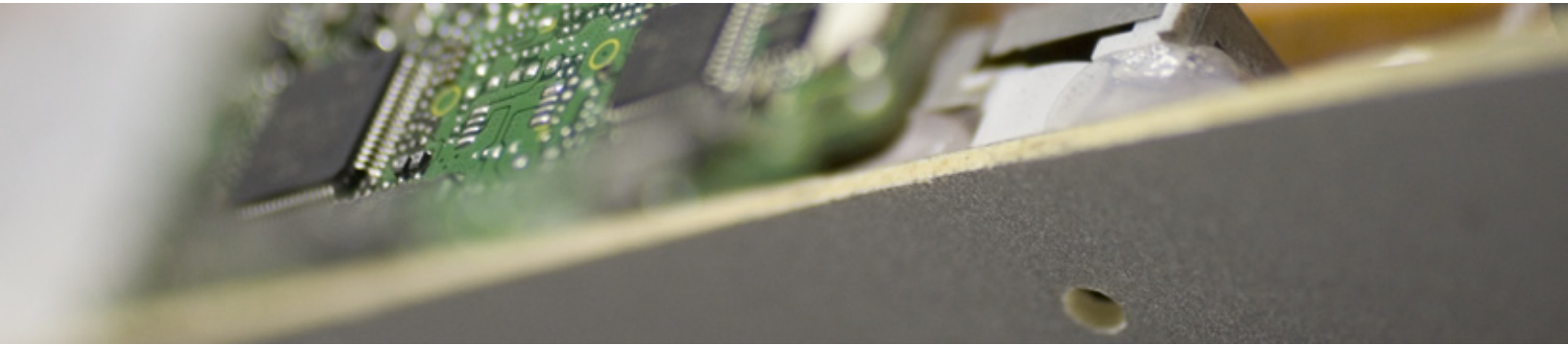


Foto LKA NRW: Versteckt eingebaute Minikamera

Skimming

ist ein englischer Begriff für das Ausspähen von EC-Kartendaten. Nach deutlichem Anstieg der Fallzahlen (allein 50% von 2006 auf 2007) in den letzten Jahren ist 2008 in Nordrhein-Westfalen erstmals ein leichter Rückgang festzustellen. Die gemeldeten Fallzahlen fielen von 191 Fällen im Jahr 2007 auf 172 Fällen in 2008. Dieser Trend wird sich aber nach Einschätzung der Polizei nicht fortsetzen. Im Jahr 2008 wurden der Polizei bundesweit 809 Fälle (2007: 459 Fälle, Anstieg der Fallzahlen um 77%) von manipulierten Geldausgabeautomaten gemeldet.

Erkenntnisse

Nach den bisherigen Erkenntnissen handelt es sich überwiegend um organisiert vorgehende ausländische Tätergruppen, die mit den ausgespähten Daten Geld vom Konto des Opfers abheben. Mit den ausgespähten Daten fertigen die Täter eine Kopie der EC-Karte, mit der sie dann im Ausland Bargeld abheben. Eine Geldabhebung in Deutschland ist aufgrund einer Prüfung durch die Geldausgabeautomaten nicht möglich.



Foto LKA NRW: manipulierter Kartenleser

Für die Herstellung einer EC-Kartenkopie benötigen die Täter die Daten des Magnetstreifens der EC-Karte und die PIN (vierstellige Geheimnummer). Um in den Besitz der Daten auf dem Magnetstreifen zu kommen, bringen die Täter zusätzlich einen manipulierten Kartenleser vor dem Original des Geldausgabeautomaten an. Diese Kartenleser sind optisch dem jeweiligen Modell des Geldautomaten angepasst und so gebaut, dass die eingeschobene

EC-Karte zum originalen Kartenleser weiter transportiert wird. So können die Daten des Magnetstreifens ausgelesen werden, ohne dass die Bedienung des Geldautomaten beeinträchtigt und der Kunde misstrauisch wird.



Foto LKA NRW: manipulierter Aufsatz vor einem Kartenleser

Eine andere Variante ist die Manipulation des Kartenlesers am Türöffner der Filiale. Entweder verwenden die Täter hierzu ebenfalls Aufsatzgeräte oder bauen in die häufig nicht ausreichend gesicherten Gehäuse einen weiteren Kartenleser ein. Äußere Merkmale einer Manipulation der Türöffner sind häufig nicht erkennbar.

Um an die für eine Abhebung zwingend erforderliche PIN zu gelangen, wird diese bei der Eingabe durch den rechtmäßigen Kartennutzer am Geldautomaten von einem Täter ausgespäht, mit einem über der originalen Tastatur angebrachten Tastaturnachbau gespeichert oder mit einer (Miniatur-) Videokamera aufgezeichnet. Am häufigsten ist der Einsatz einer Videokamera, die oberhalb der Tastatur, seitlich am Geldautomaten oder an der Raumdecke angebracht ist. Eine vollflächige Abdeckung des Tastaturfeldes (z.B. mit der Hand) kann das Ausspähen der PIN-Eingabe wirkungsvoll verhindern.

Prävention

Prävention

Prävention

Prävention

Prävention

Präventionstipps

Die technischen Manipulationen sind auch für aufmerksame Kunden nur schwer zu erkennen. Die professionell arbeitenden Täter kopieren die Technik der Geldausgabeautomaten oder Türöffner täuschend echt. Das Risiko, Opfer eines Skimming-Angriffs zu werden, kann jedoch deutlich verringert werden, wenn diese Hinweise durch die Bankkunden berücksichtigt werden:

- Geben Sie Ihre PIN niemals an einem Kartenleser zur Türöffnung im Eingangsbereich zu den Geldausgabeautomaten ein. Kein Geldinstitut verlangt für den Zugang zu diesen Räumen die Eingabe der PIN. Informieren Sie in einem solchen Fall direkt Ihr Geldinstitut oder die Polizei.
- Nutzen Sie, sofern Sie über mehrere Kontokarten verfügen, stets unterschiedliche Karten für die Türöffnung und den Geldausgabeautomaten. Trotz Manipulation eines Türöffners können die Täter dann Ihre PIN nicht für Geldabhebungen nutzen.
- Sorgen Sie für einen angemessenen Sicherheitsabstand zum nächsten Kunden, damit Ihnen bei der Bargeldabhebung niemand über die Schulter sieht.
- Verdecken Sie die Sicht auf die Tastatur immer mit der freien Hand oder einem Gegenstand. Dies erschwert ein Ausspähen der PIN durch einen Täter oder eine verdeckt angebrachte Videokamera.
- Geben Sie niemals an einem Geldautomaten mehrfach die PIN ein, wenn Sie von einer Ihnen unbekannt Person dazu aufgefordert werden.
- Nutzen Sie keine Geldausgabeautomaten, an denen Ihnen etwas ungewöhnlich erscheint. Achten Sie insbesondere auf Veränderungen des Karteneinzugschachts und der Tastatur. Informieren Sie in diesem Fall sofort Ihr Geldinstitut oder die Polizei.
- Kontrollieren Sie regelmäßig Ihre Kontobewegungen und wenden Sie sich bei Auffälligkeiten sofort an Ihr Geldinstitut.
- Überlassen Sie die Karte niemals Dritten und bewahren Sie die PIN stets getrennt von der Karte auf.

Weitere Informationen

Bei Verlust oder Diebstahl der Karte sowie bei dem Verdacht einer erfolgreichen Ausspähung Ihrer Kartendaten, rufen Sie bitte umgehend die Sperrzentrale Ihres Geldinstituts oder den **bundesweiten Sperrnotruf unter 116 116** an und erstatten Sie Anzeige bei der Polizei.

Weitere Informationen erhalten Sie im Internet unter:

www.kartensicherheit.de und www.polizei-beratung.de

Herausgeber:

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Dezernat 34 - Kriminalprävention,
Zentrale Internetrecherche, ZASt Kinderpornografie

Sachgebiet 34.2

Verhaltensorientierte und technische Prävention
Telefon: (0211)939 - 3405
Telefax: (0211)939 - 3409
E-Mail: sg34.2.lka@polizei.nrw.de

Impressum:

Landeskriminalamt
Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Telefon: (0211)939 - 0
Telefax: (0211)939 - 4119
E-Mail: Landeskriminalamt@polizei.nrw.de

