< Cyberversicherungen

Manipulierte Geldautomaten

Betrug durch „Skimming“ und „Cash-Trapping“

Seien Sie beim Geldabheben umsichtig

Betrüger lassen sich immer neue Methoden einfallen, um Menschen um ihr Geld zu bringen. Auch das Manipulieren von Geldautomaten gehört dazu. Durch das so genannte „Skimming“ oder „Cash-Trapping“ werden immer wieder Bankkunden geschädigt.

So gehen die Täter vor

Beim Skimming (engl. „to skim“ = abschöpfen) bringen die Täter ein eigenes Kartenlesegerät oder sogar eine ganze Frontplatte an dem Automaten an. Diese gefälschten Bauteile sind dem Original so gut nachempfunden, dass man als Kunde den Unterschied nicht bemerkt. Zusätzlich wird eine Mini-Kamera über dem Tastenfeld installiert. Hebt ein Kunde mit seiner Bankkarte Geld ab, werden die Kontodaten über den Magnetstreifen ausgelesen und entweder auf dem Kartenlesegerät gespeichert oder direkt per Funk an die Datendiebe weitergeleitet. Die installierte Kamera filmt parallel dazu die eingegebene PIN des Karteninhabers. Mit diesen Informationen stellen die Betrüger im Anschluss Kartendubletten her, mit denen sie dann im Ausland Geld vom Konto ihres Opfers abheben. Der Kartenbesitzer bemerkt den Betrug meist erst, wenn er seine Kontoauszüge prüft oder die Bank ihn wegen des überzogenen Kontos informiert. Die Betrüger manipulieren dabei nicht nur Bankautomaten – zunehmend sind auch Kontoauszugdrucker, Überweisungsterminals, Fahrkarten- oder Zapfsäulenautomaten an Tankstellen von der Skimming-Methode betroffen. Eine weitere Möglichkeit des Betrugs: Die Türöffner zu Banken werden manipuliert. Der Kunde soll seine Karte in spezielle, von den Betrügern angebrachte Aufsätze, durchziehen und seine PIN eingeben. Die Daten werden dann in dem Aufsatz gespeichert.

Das sagt die Statistik

Laut dem Bundeslagebild „Angriffe auf Geldautomaten“ 2019 des BKA gab es im Jahr 2019 einen erneuten Rückgang von Skimming-Betrugsfällen. Insgesamt erfolgten hier 244 Angriffe auf Geldautomaten zur Erlangung von Kartendaten und Geheimnummern (PIN) (2018: 449 Angriffe). Obwohl die Anzahl der Betrugsfälle im Vergleich zu den beiden Vorjahren gesunken ist, bleibt die Schadenssumme mit rund 1,4 Millionen Euro in etwa gleich. Das Phänomen des so genannten „Jackpotting“ per „Blackboxing“ wurde deutschlandweit 47 Mal registriert, was einem Anstieg um 9 Prozent entspricht. Bei dieser Vorgehensweise manipulieren Täter die Software eines Geldautomaten. Dadurch entstand eine Schadenssumme von rund 940.000 Euro – ein Anstieg um 109 Prozent.
Eine weitere Angriffsmethode ist die Sprengung von Geldautomaten. Diese wurde im Jahr 2019 349 Mal von Kriminellen angewandt, was einem Rückgang von 5,4 Prozent entspricht. Bei den Tätern handelt es sich häufig um reisende Banden aus den Niederlanden.

Cash-Trapping

Eine weitere Betrugsmethode ist das so genannte „Cash-Trapping“ („Bargeld-Fangen“). Dabei versehen die Betrüger den Geldausgabeschacht des Geldautomaten mit einer unauffälligen Blende. Innen ist diese mit einer selbstklebenden Folie bestückt. An dieser Folie bleiben die Scheine haften. So wird verhindert, dass das vom Kunden abgehobene Geld an diesen ausgezahlt bzw. dass es vom Automaten wieder eingezogen wird. Der Kunde bemerkt davon nichts. Er erhält auf dem Automaten-Display lediglich den Hinweis auf eine Automaten-Störung. Nachdem der Kunde die Bank verlassen hat, entfernen die Betrüger die angebrachte Blende und holen sich das festgeklebte Geld aus dem Ausgabeschacht.

Beim „Cash-Trapping“ bleibt das Geld im Ausgabeschacht kleben

So schützen Sie sich vor Betrug am Geldautomaten:

- Geben Sie niemals Ihre PIN in den Türöffner am Eingang der Bank ein. Keine Bank verlangt als Zugang Ihre persönliche PIN!
- Benutzen Sie, wenn möglich, zum Türöffnen und Geld abheben jeweils unterschiedliche Karten.
- Geben Sie grundsätzlich Ihre PIN nur verdeckt ein – auch wenn keine anderen Personen in der Nähe sind. Das erschwert das Ausspähen der PIN per Kamera erheblich.
- Achten Sie darauf, dass niemand Ihre PIN-Eingabe beobachtet, halten Sie Abstand zu anderen Personen und lassen Sie sich nicht von Fremden ablenken.
- Heben Sie, wenn möglich, immer am gleichen Geldautomaten Bargeld ab. Mögliche Veränderungen oder Manipulationen am Automaten fallen Ihnen dann schneller auf.
- Erfolgt der Abhebe-Vorgang an einem Automaten soweit ganz normal, das Geld wird aber nicht ausgezahlt, wenden Sie sich an einen Bankmitarbeiter oder rufen Sie die Polizei.
- Nutzen Sie keinen Geldautomaten, an denen Ihnen etwas Ungewöhnliches auffällt (z. B. nicht ganz fest sitzende Teile und Verblendungen, Klebespuren etc.)
- Informieren Sie umgehend die Polizei und die Bank, wenn Sie den Verdacht haben, dass ein Geldautomat manipuliert wurde.
- Haben Sie die Vermutung, dass Sie Opfer eines Automatenbetrugs geworden sind, sperren Sie umgehend Ihre Karte (Sperr-Notruf 116 116) und erstatten Sie Anzeige bei der Polizei.

SBa (28.08.2020)

Folgende Artikel könnten Sie auch interessieren:

- Taschendiebstahl und Geldkartenklau
- Cyber-Betrugsmasche „Jackpotting“
- Lassen Sie sich nicht austricksen!
- Fallen beim Geschenkekauf
- Bankgeschäfte und Einkaufen im Netz
- PIN-Nummer und EC-Karte getrennt aufbewahren
- Vorsicht vor Taschendieben!
- Taschen- und Trickdiebstahl

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Internet und Mobil

Hilfestellung oder Irreführung?

Kundenbewertungen im Netz

Für viele Verbraucherinnen und Verbraucher ist der Einkauf im...[mehr erfahren]

Welche menschlichen Schwächen Internetbetrüger ausnutzen

Gier und Neugier

Tricks rund um vermeintlich unschlagbare Schnäppchen, verführerisch...[mehr erfahren]

Mobile Kommunikationsmittel im Visier von Kriminellen

Vom Smartphone bis zum Tablet-PC

Smartphones sind nicht nur zum Telefonieren da. Aufgrund ihrer...[mehr erfahren]

Internetkriminelle wollen an ihre Zugangsdaten für Online-Geschäfte gelangen

Phishing – so können Sie sich schützen

„Phishing“ ist ein Kunstwort, das sich aus den englischen Begriffen...[mehr erfahren]

Wer hat Zugriff auf die Daten aus den Fahrerassistenzsystemen?

Das vernetzte Auto

Nach einem schweren Unfall ist es für Verletzte lebenswichtig, dass...[mehr erfahren]