# Skimming vereiteln mit Hilfe künstlicher Intelligenz und Analytics

## Wie Banken ihre Kunden vor Geld-automaten-Betrug schützen können

**Berichte über Skimming, das Stehlen von Karten- und PIN-Informationen während der Geld-automatenbenutzung mit dem Ziel, damit gefälschte Karten zu erstellen und Geld abzuheben, verunsichern Bankkunden und erschüttern deren Vertrauen in ihr Geldinstitut. Wir zeigen in diesem Artikel auf, wie Skimming-Attacken erkannt und vereitelt werden können, um Bank-kunden vor Betrug zu schützen.**

BUSINESS.
DATA.
TECHNOLOGY.

CINTELLIC
CONSULTING GROUP

Berichte über Skimming, das Stehlen von Karten- und PIN-Informationen während der Geldautomatenbenutzung mit dem Ziel, damit gefälschte Karten zu erstellen und Geld abzuheben, verunsichern Bankkunden und erschüttern deren Vertrauen in ihr Geldinstitut. Was man weiß: Am Wochenende und mit der Nutzungshäufigkeit von Geldautomaten steigt die Wahrscheinlichkeit, Opfer einer Skimming-Attacke zu werden. Skimming-Geräte, beispielsweise Kameras und Karten-Lesegeräte, werden meist morgens früh oder abends spät montiert. Sie bleiben meist nicht länger als 24 Stunden am Gerät, werden aber wiederholt montiert. Leider helfen Hardware-Lösungen zur Erkennung von Skimming-Geräten nur bedingt, da die Täter kreativ sind und immer neue, aufwändigere Methoden finden, um an das Geld der Bankkunden zu kommen.

Ein beliebtes Einfallstor für Kriminelle sind z.B. Karten kostenloser Sparkonten, die ähnlich wie Girokonten genutzt werden können. Tragen Karten die relevanten Informationen auf einem Magnetstreifen, so laden sie damit geradezu zum Identitätsdiebstahl ein. Auch die Gewohnheiten der Besitzer begünstigen Betrug: Viele Kunden prüfen ihren Kontostand nicht regelmäßig.

## Die Lösung: Eine schnelle Erkennung manipulierter Geldautomaten auf Basis täglicher Transaktionsdaten.

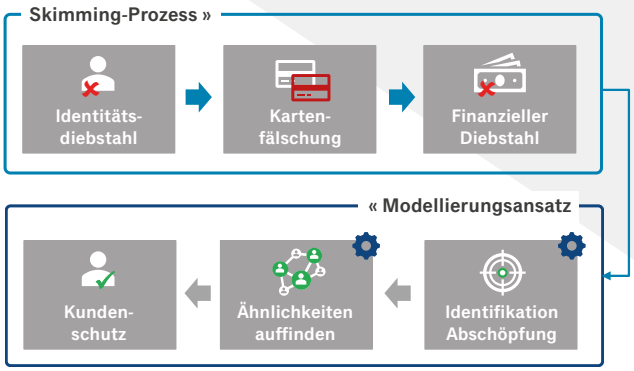


*Abbildung 1: Ex-Post Analyse - Erkennung von Skimming-Attacken ausgehend von Abschöpfungstransaktionen*

Skimming-Aktivitäten werden erst entdeckt, wenn Abschöpfungs-Transaktionen in den Transaktionsdaten erkannt werden. Der Identitätsdiebstahl geschieht bei einer normalen Bargeldabhebung des Kunden. Oft nur wenige Tage später sind dann betrügerische Bargeldabhebungen anhand auffälliger Verhaltensmuster an verdächtigen Geldautomaten identifizierbar. Der Modellierungsansatz: Im ersten Schritt werden die Abhebungen analysiert. Dann sind Ähnlichkeiten aufzufinden. Manipulierte Geldautomaten und Zeitfenster der Skimming-Attacken werden über Ähnlichkeiten in Transaktionshistorien betrogener Kunden erkannt. Schließlich kann man den Kunden vor weiterem Betrug schützen, indem alle Karten gesperrt werden, die am manipulierten Geldautomaten im identifizierten Zeitfenster genutzt wurden.

Zur täglichen Verarbeitung der Transaktionsdaten wird eine Data Science Pipeline benötigt. Transaktionsdaten werden zur Modellberechnung angereichert. Features, die für das Entlarven von Skimming-Aktivitäten herangezogen werden können, sind dann beispielsweise der Saldo aller Abhebungen, kumulierte Bargeldabhebungen für den aktuellen Monat oder Transaktionen von demselben Konto innerhalb kurzer Zeiträume.

## Modellierung mit klassischen Methoden

Um reguläre von betrügerischen Transaktionen am Geldautomaten unterscheiden zu können, kann man sich klassischer Methoden bedienen. Diese haben jedoch ihre Grenzen: Da sich Kunden nicht immer nachvollziehbar verhalten, sind z.B. Modelle zur Ausreißer-Erkennung nicht wirksam. Die Anzahl an False/Positives ist eine große Herausforderung. Features fokussieren zudem oft auf Fehler, welche die Betrüger gewöhnlich machen. Sobald diese ihr Verhalten ändern, verlieren die Modelle an Präzision. Nicht zuletzt sind Verhaltensmuster über Kundengruppen hinweg sowie Verknüpfungen zwischen verschiedenen Geldautomaten nur schwer abbildbar.

Wenn Abschöpfungstransaktionen zweifelsfrei erkannt und die betrogenen Kunden identifiziert sind, durchforstet man die Transaktionshistorien dieser Kunden, um gemeinsame „Hot Spots“ aufzuspüren: die manipulierten Geldautomaten und die Tat-Zeitfenster. Dabei gibt es zwei Aspekte, die den Fahndungserfolg zu Nichte machen können: Zum einen lassen sich viele Abschöpfungstransaktionen in kurzer Zeit an einem Geldautomaten oft auf verschiedene Skimming-Attacken zurückführen. Zweitens sind die Zeitfenster der Skimming-Attacken sehr kurz und bleiben oftmals unentdeckt. Die fehlende Evidenz erschwert die Entscheidungsfindung, da valide Ergebnisse fehlen, an denen man ein Modell trainieren könnte.

## Erkenntnisgewinn durch Embeddings

Die Nutzung von Embeddings bietet sich an, um ungewöhnliche, neue Verhaltensmuster zu erkennen. Bankkunden präferieren für gewöhnlich eine bestimmte Anzahl an Geldautomaten. Die Erfassung ähnlicher Nutzungsmuster bestimmter Geldautomaten über alle Kundenhistorien hinweg erzeugt ein Beziehungsnetzwerk zwischen den Geldautomaten. Ein Embedder reduziert dabei die Relationen eines Geldautomaten auf einen sehr viel kleiner dimensionierten Vektor reeller Zahlen. Geldautomaten, die gemeinsam häufiger in verschiedenen Kundenpfaden erscheinen, sollten eine engere Relation haben. So lassen sich Zusammenhänge erkennen und im Bestfall der Weg der Kriminellen identifizieren.

‚Word Embeddings‘ kommen aus dem Natural Language Processing und sind mächtige Modelle um latente, semantische Strukturen innerhalb einer Sprache zu erkennen. Anstatt mit Wörterfolgen wurde hier ein Embedder mittels Transaktionshistorien trainiert, um latente Verhaltensmuster erkennen zu können.

## Resultate

Damit die in der Praxis verwendeten Modelle nicht nur auf die Fehler der Betrüger abzielen, sind folgende Aspekte zu berücksichtigen:

- Die Informationen aus klassischen Scorings (Features) und Embeddings müssen verheiratet werden.
- Ein kontinuierliches Trainieren der Modelle ist in die Pipeline zu integrieren.
- Ungewöhnliches wie Urlaubsperioden oder das Verhalten von Power-Nutzern muss genau untersucht und berücksichtigt werden.
- Dem Datenmanagement kommt eine hohe Bedeutung zu.

Über ein automatisiertes Decision Support Tool für das tägliche Monitoring ist es heute möglich, spezielle Transaktionen aufzufinden, Muster zu erkennen, verdächtige Vorgänge zu identifizieren, False/Positives zu minimieren und damit Skimming-Zeitfenster nach konzentrierten Attacken zuverlässig zu erkennen. Analysten dürfen sich darüber freuen, dass die manuelle Kontrolle und Datensammlung erheblich reduziert werden kann. Abschöpfungsaktionen können auf diese Weise signifikant schneller erkannt werden – oft, bevor der Kunde selbst etwas merkt.

**von Sven Langhoff,**
**CINTELLIC Consulting Group**

# Ansprechpartner

**Dr. Jörg Reinnarth**
*Geschäftsführer*
CINTELLIC Consulting Group
joerg.reinnarth@cintellic.com

**Stephan Klöckner**
*Senior Manager*
CINTELLIC Consulting Group
stephan.kloeckner@cintellic.com

# Über CINTELLIC

**Die 2010 gegründete CINTELLIC Consulting Group ist eine auf digitales Kundenmanagement spezialisierte Unternehmensberatung, die ihre Klienten vom ersten Konzept bis zur Umsetzung in der Praxis ganzheitlich begleitet. An den Standorten in Bonn, Frankfurt am Main und München arbeiten rund 60 Mitarbeiterinnen und Mitarbeiter.**

**Zu den Klienten zählen DAX-Konzerne, führende mittelständische Unternehmen und insbesondere zahlreiche sogenannte „Hidden Champions" mit den Branchenschwerpunkten Banken und Versicherungen, Telekommunikation, IT, Medien, Unterhaltung, Handel, E-Commerce, Versorger und Logistik.**

**www.cintellic.com**

## #jointheteam

CINTELLIC befindet sich auf Wachstumskurs. Vielleicht mit Ihnen? Jetzt Stellenanzeigen entdecken und bewerben!
**https://www.cintellic.com/stellenangebote/**

Cintellic im Social Web

**Cintellic GmbH**
Remigiusstraße 16
53111 Bonn
t +49 228 92 18 20
info@cintellic.com
www.cintellic.com

CINTELLIC
CONSULTING GROUP