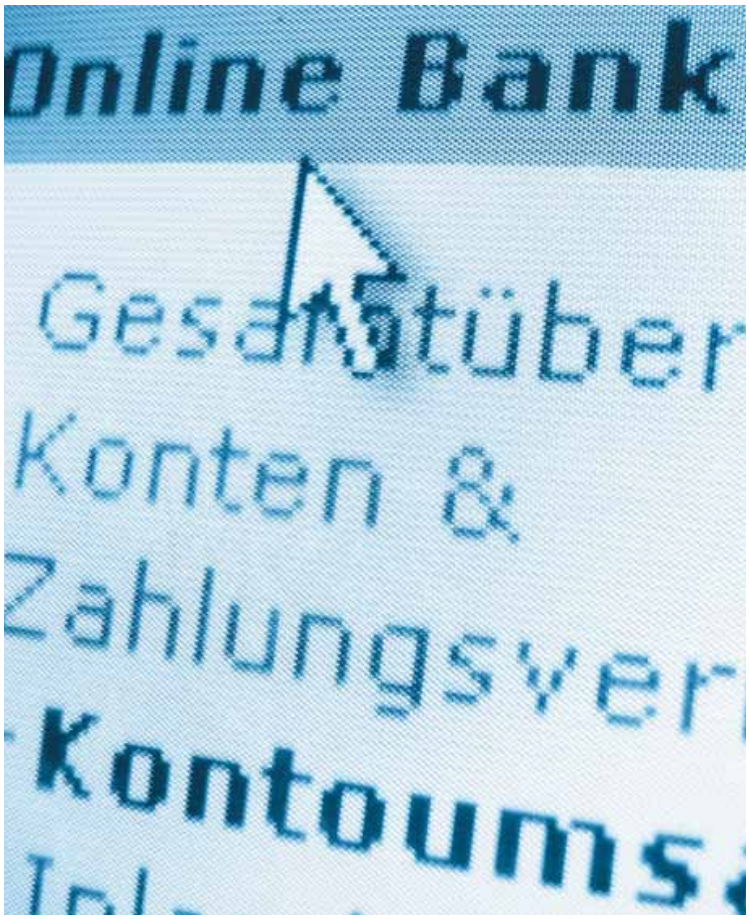
INFORM unterstützt Banken im Kampf gegen Skimming



Intelligente Betrugserkennungssoftware verhindert illegale Abbuchungen mit ausgespähten Kartendaten

Wer an einem Geldautomaten oder einem Bezahlterminal mit Hilfe seiner Kredit oder EC-Karte Geld abhebt oder bargeldlos bezahlt, muss vermehrt damit rechnen, dass seine geheimen Kartendaten durch Manipulationen ausgespäht und für illegale Abbuchungen genutzt werden. Um ihre Kunden vor einem derartigen Betrug zu schützen, setzen Banken zunehmend Betrugserkennungssoftware ein, die Abbuchungen mit illegal erworbenen Kartendaten durch intelligente Echtzeit- Anlayseverfahren verhindert.

„Eine solche Software kann zwar das Ausspähen der geheimen Kartendaten nicht verhindern. Allerdings sind Banken durch derartige IT-Systeme in der Lage, Abbuchungen zu unterbinden, die auf Grundlage illegal erworbener Daten vorgenommen werden“, so Dr. Andreas Meyer, Geschäftsbereichsleiter Risk & Fraud bei INFORM. Dazu überprüft das System in Echtzeit alle Transaktionen an den Geldautomaten und ermittelt für jede einzelne Abbuchung Indizien für einen möglichen Betrug. „Hierzu werden unter anderem die Transaktionen mit dem üblichen Verbraucherverhalten des Kontoinhabers verglichen. Auffällig hohe Abbuchungen oder ein für den Kunden ungewöhnlicher Standort des Geldautomaten, etwa im Ausland, sind nur zwei von zahlreichen solcher Kriterien“, erklärt Meyer. Weichen zu viele der überprüften Kriterien von dem normalen Verhalten des Kontoinhabers ab, schlägt die Software Alarm und blockiert die gesamte Transaktion. „Durch Echtzeit-Analyse des Einsatzortes der Debit und Kreditkarten ist eine gute Betrugserkennungssoftware außerdem in der Lage, manipulierte Geldautomaten oder Bezahlterminals zu identifizieren. Dies gibt der Bank die Möglichkeit, alle dort in einem bestimmten Zeitraum eingesetzten Karten präventiv zu sperren.“ Bei der Betrugserkennung arbeitet ein solches System wie ein menschlicher Experte und stuft das Risiko einer Transaktion unter Berücksichtigung von belastenden und entlastenden Merkmalen ein. „Hierzu haben sich vor allem Verfahren der Fuzzy Logic bewährt, die in Verbindung mit der maschinellen Effizienz von Computern die menschliche Entscheidungskompetenz bei weitem übertreffen“, so Meyer weiter.

Das illegale Ausspähen von Kartendaten an Geldautomaten und Bezahlterminals tritt europaweit immer häufiger auf. In Deutschland sind die Fallzahlen laut Bundeskriminalamt (BKA) im Jahr 2010 massiv angestiegen. Bei der Manipulation der Geldautomaten gehen die Betrüger immer trickreicher vor. Versteckt installierte MiniKameras und eine manipulierte Karteneinschubtechnik sind für die Kunden kaum wahrnehmbar. Mit Hilfe der so erschlichenen Daten sind die Betrüger in der Lage, größere Abbuchungen von Konten der Bankkunden vorzunehmen.

Zukünftig wird der Schutz vor Skimming-Attacken daher noch stärker in den Fokus von Banken und Ermittlungsbehörden rücken. Diese Einschätzung bestätige auch BKA Präsident Jörg Ziercke unlängst in einem Interview: „Die Fallzahlen belegen, dass Geldautomaten in steigendem Maße ein lohnendes Angriffsziel krimineller Gruppierungen sind. Sie verdeutlichen, dass wir zusammen mit der Wirtschaft unsere Präventionsbemühungen weiter verstärken müssen.“ Auch für Andreas Meyer ist dieser Schritt unumgänglich:„Die Nachfrage nach Softwaresystemen zur Betrugserkennung im Zahlungsverkehr wird künftig weiter steigen. Mit RiskShield bieten wir eine im Bankensektor seit vielen Jahren etablierte Software. Das Portfolio unserer Software geht dabei weit über den Schutz bei Skimming-Attacken hinaus. Vielmehr schützt RiskShield auch vor Missbrauch beim Internet-Banking durch Pishing-Techniken sowie beim bargeldlosen Zahlungsverkehr im Handel. Das System ist mittlerweile bei Banken auf der ganzen Welt im Einsatz und überwacht heute über 145 Millionen Kredit und Debitkarten.“ Darüber hinaus arbeitet INFORM beständig an der Weiterentwicklung seiner Software. „So erproben wir gerade für den Bereich Skimming in Zusammenarbeit mit einer niederländischen Großbank eine erweiterte Version von RiskShield.“

Der beste Schutz vor Skimming-Attacken ist allerdings, bereits das Ausspähen der Kartendaten zu verhindern. Das weiß auch Andreas Meyer „Hier wird sich in nächster Zeit auf Seiten der Banken viel tun. Darüber hinaus kann man den Verbrauchern nur raten, wachsam zu sein, wenn sie an einem Automaten Geld abheben. Zumindest das Aufzeichnen der PIN-Nummer durch eine Mini-Kamera lässt sich leicht verhindern, indem man die Eingabe der Geheimzahl mit einer Hand verdeckt.“