Plattform zur Betrugsbekämpfung

Funktechnologie und neue Verfahren machen drahtloses Bezahlen komfortabler, eröffnen aber Angriffsflächen. Das Bundeskriminalamt ist Partner einer Plattform zur Betrugsbekämpfung und -prävention.

Drahtloses Bezahlen ist heute mit Bankomat- und Kreditkarten sowie mit Smartphones möglich, die mit der *NFC*-Technologie ausgestattet sind *(NFC* steht für *Near-Field-Communication)*. Das Symbol für drahtloses Bezahlen auf der Karte sind vier Funkwellen, die von unten nach oben größer werden. Beim kontaktlosen Zahlen tauscht der Chip Daten des Nutzers mit einem Kartenterminal aus. Übermittelt werden die Kartennummer, das Verfallsdatum, der Betrag und ein von einem Sicherheitsmodul auf dem Chip erzeugtes Kryptogramm. Kunden müssen die Karte oder das Smartphone kurz an das Kartenlesegerät halten und können Einkäufe bis 25 Euro in der Regel ohne PIN-Eingabe und Unterschrift bezahlen. Kontaktlose Bezahldienste stellen für Kunden und Händler komfortablere und schnellere Verfahren dar.

Drahtlose Bezahlverfahren sind bequem, können aber Angriffsflächen für Kriminelle bieten.

Gefahren. Die Anzahl der Anbieter für drahtloses Bezahlen nimmt zu. Handelsketten, Banken, Mobilfunkunternehmen, Logistiker entwickeln eigene Verfahren. Neue Technologien bedeuten neue Angriffsflächen für Kriminelle. Wenn diese neuen Systeme nicht genau und hochsicher gebaut werden, dann könnten die Daten einer Bezahl- oder Kreditkarte mit *NFC*-Technologie z. B. mit Schnüffelsoftware auf einem Smartphone des Täters gescannt werden, ohne dass der Kartenbesitzer es merkt. Nähert sich der Kriminelle dem Kartenbesitzer auf wenige Zentimeter, kann er mit seinem Handy die Kartennummer und das Ablaufdatum scannen, teilweise sogar den Vor- und Nachnamen. Mit diesen Daten könnte er bei Online-Shops einkaufen, die die zusätzlichen Sicherheitskriterien nicht verlangen. Das sind in der Regel die dreistellige Prüfnummer auf der Kartenrückseite oder das 3-D-Secure-Verfahren – ein erneutes Kennwort. Bisher sind solche Betrugsfälle in Österreich nicht bekannt.

Betrugsbekämpfung. Um Betrug mit diesen neuen Bezahltechnologien zu verhindern oder zu bekämpfen, wurde mit dem KIRAS-Forschungsprojekt *3B3M* – einer Initiative des Bundesministeriums für Verkehr, Innovation und Techologie – eine gemeinsame Plattform zwischen Finanzinstituten und dem Bundeskriminalamt (BK) geschaffen. „Das Potenzial des Angriffs auf die Bezahlmittel der Bürgerinnen und Bürger wächst vor allem durch die Vielfalt an mobilen Geräten und unterschiedlichen Bezahlformen, die mit diesen Geräten getätigt werden können“, sagt DI Florian Fankhauser, Sicherheitsspezialist des Projektpartners *RISE GmbH*. „Diese Plattform bildet einen gemeinsamen Erfahrungs-Pool über Betrugsfälle bei modernen Bezahlmethoden sowie bei Phishing-Mails, Malware oder der betrügerischen Verwendung von Kreditkartendaten im Internet. Es werden alle neuen Kanäle am Endgerät umfasst sowie die unterschiedlichen Verfahren von der *NFC*-Technologie mit Karte und Handy, über QR-Code-Zahlungen, Bluetooth-Übertragungstechnik, virtuelle Geschenksmünzen, Bitcoin-Transaktionen bis hin zu Altverfahren via SMS“, erläutert der Sicherheitsspezialist.

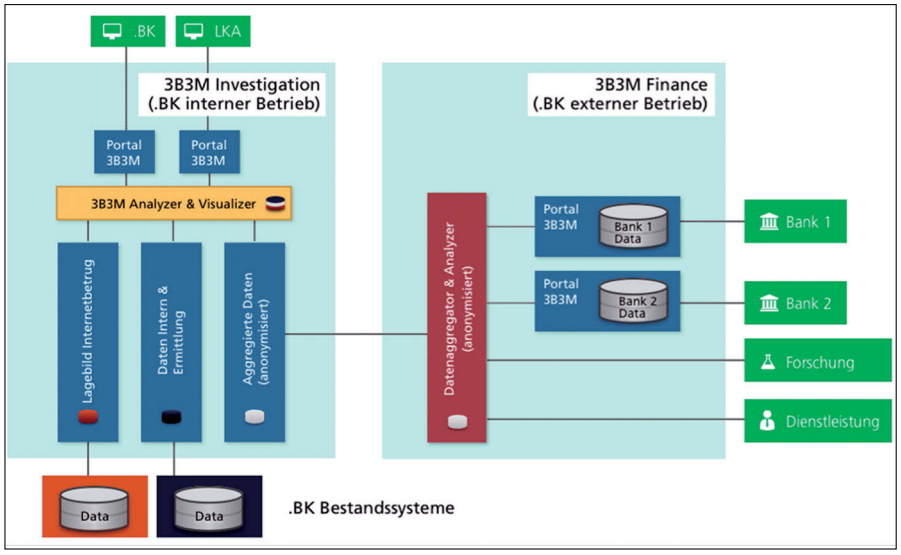
Die Plattform soll auch der besseren Bekämpfung der „Money-Mules“ (Finanzagenten) dienen. Das sind Personen, die per E-Mail von Betrügern für die Tätigkeit als Unterstützer geködert werden. Sie müssen Bankkonten eröffnen, auf denen betrügerisch lukrierte Geldbeträge überwiesen werden. Auch Ransomware-Fälle (Erpresser-Trojaner) oder Dating-Scam-Fälle sollen erfasst werden.

„Je rascher auf einen Angriff reagiert wird, desto geringer fällt der Schaden aus und der Angriffsort Österreich wird für die Täter letztlich uninteressant. Dieses Vorgehen ist dem Bundeskriminalamt bei der Betrugsbekämpfung im Umfeld von Manipulationen von Bankomaten gut gelungen“, sagt Fankhauser.

Die Betrugsbekämpfungs-Plattform des BKs besteht aus zwei Zonen mit scharf getrennten rechtlichen und technischen Territorien: *3B3M Finance* und *3B3M Investigation*. Im Modul *3B3M Finance* können Finanzinstitute ihre Daten über Betrugssachverhalte erfassen und in einem nur ihnen zugänglichen Datencontainer sicher ablegen. Dies betrifft beispielsweise Phishing, Malware, betrügerische Verwendung von Kreditkartendaten im Internet oder Kontoeröffnungen zur Verschleierung von Finanzströmen.

Diese Informationen werden in anonymisierter Form dem vom BK verwalteten Modul *3B3M Investigation* übermittelt. Dieses im Bundeskriminalamt angesiedelte zweite Modul ermöglicht

FOTO: WAVEBREAKMEDIAMICRO/FOTOLIA



***3B3M*-Plattform: Informationskanal vom Bundeskriminalamt zu den Banken.**

den BK-Ermittlern die Zusammenschau: Trends und Muster rasch zu erkennen. Umgekehrt können die BK-Mitarbeiter Informationen, die sie von Europol oder Interpol erhalten haben, an die *Zone-Finance* den Finanzinstitutionen zur Verfügung stellen, sodass diese in ihrem Umfeld rechtzeitig präventive Maßnahmen setzen können. Diese Vorgangsweise ist aufgrund des Spannungsverhältnisses zwischen Schutz der Privatsphäre und Bankgeheimnis, Kundendiskretion und effektiver polizeilicher Verfolgungsarbeit eine grundsätzliche Notwendigkeit.

Digitale Anzeige. Zukünftig sollen mit Hilfe der Plattform auch Anzeigen gegen Straftäter erstattet werden können und zusätzliche Daten zur Ermittlung und Verfolgung von Straftaten für die Gerichte aufbereitet werden. Der bisher oft sehr lange Zyklus aus Erkennung, Verfolgung und Ermittlung der Straftaten sowie der Hilfe zur Erstellung einer profunden Anklage der Täter wird den modernen Erfordernissen angepasst.

„Wir erwarten uns mit der Plattform eine engere Zusammenarbeit mit den Finanzinstituten, um gemeinsam Betrugsfällen vorzubeugen und Straftaten effizient zu bekämpfen“, sagt Mag. Gerald Staller von der Abteilung 7 (Wirtschaftskriminalität) im Bundeskriminalamt. „Die Plattform ermöglicht einen Überblick über versuchte und vollendete Betrugshandlungen bei modernen Bezahlmethoden. Die Ressourcen können gezielter eingesetzt werden und die Kommunikation mit den Finanzinstituten wird erleichtert und verbessert. Wir arbeiten so stärker gemeinsam an einem sicheren Bezahlstandort Österreich“, erklärt Staller.

Compliance und Datenschutz. Die *3B3M-Plattform* wird auf zwei separaten Umgebungen betrieben, die miteinander über gesicherte Schnittstellen kommunizieren, basierend auf den internationalen Bank-Compliance-Regeln sowie den österreichischen und europäischen Datenschutzrichtlinien.

Die Module *Finance* und *Investigation* sind nicht nur technisch hochsicher, sie werden laufend den Regeln und Gesetzen nach den Erfahrungen in der Praxis angepasst. Jede Finanzinstitution mit Kundendaten greift ausschließlich auf den eigenen Datenbestand zu und auf die anonymen Trend- und Ereignisdaten, wie Ort, Zeit, Form und Frequenz von Angriffen. Die unterschiedlichen Datencontainer sind dabei nachweislich „blind“ für Unbefugte. Der Pilotbetrieb für das System startet ab Mai 2017 mit ausgewählten Banken, Bezahlmittelanbietern und Internethändlern.

Lagebild Cybercrime. Betrugsdelikte verlagern sich immer mehr in das Internet. Oft handelt es sich um Fälle mit geringer Schadenssumme, die von organisierten Gruppen als Massendelikt begangen werden, die einen hohen kriminellen Profit lukrieren. Spezialisten und kriminelle Gruppen bieten einander Dienste an. Es bilden sich kriminelle Gruppen, die beispielsweise Malware kaufen, logistisch verteilen und zur Verschleierung der Finanzströme „Money-Mules“ ködern.

Mit der *3B3M*-Investigationstechnik sollen zukünftig Zusammenhänge zwischen den einzelnen Fällen sowie das Organisationsmuster dahinter viel schneller erkannt werden können. Im Zusammenhang und Umfeld des Projektes *3B3M* wird auch das Lagebild Cybercrime entwickelt. Die bei der Polizei angezeigten Fälle der Betrugsformen aus dieser Klasse werden dabei geordnet. Dadurch entsteht ein schnelleres und vollständigeres Bild über die Betrugsfälle bei modernen Bezahlmethoden: Die Finanzinstitute stellen Trenddaten über die ihnen bekannt gewordenen Fälle zur Verfügung und über das Lagebild Cybercrime entstehen zusätzliche Informationen über die angezeigten Fälle, technische Spuren, Finanzströme und gleichgelagerte Fälle. Ermittlungen durch unterschiedliche Dienststellen können besser koordiniert und Ressourcen zweckmäßig eingesetzt werden.

Daten aus dem Lagebild Cybercrime und damit zusammenhängende Daten aus dem Modul *3B3M Finance* können zusammengeführt werden, um ein vollständiges Bild über eine Straftat zu erhalten. Das Lagebild Cybercrime wird in einem Probetrieb in Burgenland, Kärnten und Vorarlberg getestet.

Projektpartner. Planer und Umsetzer des *3B3M-Projektes* sind die Spezialisten DI Florian Fankhauser, Dr. Markus Gruber, Dr. Michael Schafferer, DI Werner Klein und Dr. Christian Schanes von der *Research Industrial Systems Engineering (RISE) GmbH*. In der Projektleitung sind Mag. Gerald Staller und Chefinspektor Christoph Heichinger vom Bundeskriminalamt vertreten. Als Forschungspartner fungierten die *SIX Payment Services (Austria) GmbH* mit Mag. Thomas von der Gathen, die *Erste Bank,* die TU Wien mit dem Fachbereich Rechtswissenschaften unter Prof. Dr. Markus Haslinger sowie die Karl-Franzens-Universität Graz, mit dem Institut für Soziologie.

In der Phase der Umsetzung ist unter anderem die Abteilung für Sicherheitspolitik im Innenministerium befasst und als Pilot-Partner haben sich aus dem Arbeitskreis der Wirtschaftskammer für Banken und Versicherungen unter der Leitung von Dr. Franz Rudorfer mehrere Institute als mögliche Innovatoren zum gemeinsamen Aufbau angemeldet.

Siegbert Lattacher

GRAFIK: RISE GMBH