Gefälschte Kreditkarten: Von Ermittlern des Landeskriminalamts Wien 2013 sichergestellt.

Missbrauch von Zahlungskarten

Bei der Jahrestagung zum Thema Kreditkartenbetrug am 30. und 31. Oktober 2013 in Bad Radkersburg tauschten Emittler und Sicherheitsexperten von Kreditkartenunternehmen Wissen und Erfahrungen aus.

Nach einem Anstieg der Zahl von Betrugsdelikten mit Kreditkarten in Wien und Niederösterreich im ersten Halbjahr 2013 begannen Polizistinnen und Polizisten der LKA-Außenstelle Wien-Mitte mit Ermittlungen und Überwachungsmaßmaßnahmen.

Anfang April konnte ein Betrüger in Vösendorf bei einem Betrugsversuch festgenommen werden. Es folgten Einvernahmen, weitere Ermittlungen und Observationen – bis die Polizisten auf den Stützpunkt der kriminellen Organisation stießen. Dort entdeckten sie eine Fälscherwerkstatt mit verschiedenen Geräten zur Herstellung von Kreditkarten und Ausweisen. 129 falsche Kreditkarten, 48 falsche Ausweise und 91 falsche Kontoeröffnungsunterlagen wurden beschlagnahmt und zwei weitere Bandenmitglieder festgenommen. Auf den Datenspeichern von Laptops befanden sich Tausende Datensätze aus Phishing-Attacken. Sichergestellt wurden auch Hacker-Programme. Der Reisepass eines Festgenommenen war eine der besten Fälschungen der letzten Jahre. ID-Karten wurden einfach immer wieder mit neuen mit Personendaten bedruckten Folien versehen, um den Aufwand für neue Identitäten möglichst gering zu halten. Der Haupttäter stammt aus Rumänien, die Fälscherwerkstatt befand sich in Österreich und Mittäter ergaunerten mit den gefälschten Dokumenten und Kreditkarten hohe Geldbeträge in den USA und in anderen Ländern.

Die Bande hatte seit 2011 in Europa unzählige Betrugshandlungen mit gefälschten Kreditkarten sowie andere Delikte begangen. Die Kartendaten beschafften sie sich über Skimming, Phishing-Attacken und gefakte Internetseiten. Die Ermittlungen erfolgten in Kooperation mit dem US-Secret-Service-Office in Frankfurt, der US-Bundeskriminalpolizei FBI, dem ungarischen Ermittlungsbüro für Zahlungsmittelfälschung und Europol.

Internationale Krimnalität. Dieser Fall zeigte die internationale Dimension von Kartenbetrugsdelikten auf. Er war einer jener Fälle, die bei der 17. Informationsveranstaltung für Polizeibeamte zum Thema „Kreditkartenbetrug“ am 30. und 31. Oktober 2013 in Bad Radkersburg besprochen wurden. Ermittler des Bundeskriminalamts und der Landeskriminalämter sowie Experten von fünf Kreditkartenorganisationen nahmen an der Veranstaltung teil. Bei diesem Erfahrungsaustausch wurden auch aktuelle Deliktsformen mit Zahlungskarten erörtert.

FOTO: WERNER SABITZER

Kreditkartenbetrug beginnt mit dem Missbrauch der eigenen Kreditkarte, indem ohne Deckung eingekauft wird, und geht über Fälle, in denen die Karte an einen „guten Freund" weitergegeben wird, der aber außer der erlaubten Abhebung weitere Abhebungen oder Bestellungen durchführt. Bei der nächsten Stufe wird die Karte von Angehörigen oder Bekannten entfremdet und missbräuchlich verwendet. „Nicht wenige Karteninhaber verwahren mit der Karte auch die dazugehörende PIN und machen es Taschendieben leicht", warnte Dr. Stefan Strahwald von der Staatsanwaltschaft Graz. Weitere Methoden sind der Diebstahl von Karten aus dem Postkasten, Online-Geschäfte mit ergaunerten Kreditkartendaten sowie Phishing und Skimming.

Card-not-present-Fraud. Phishing ist nach wie vor weit verbreitet. Während die Zahl der Skimming-Delikte im heurigen Jahr deutlich zurückgegangen ist, entwickeln sich Straftaten im Zusammenhang mit Card-not-present-Transaktionen („Distanzzahlungen") zu einem immer größer werdenden Problem. Bei dieser Zahlungsart wird die Kreditkarte nicht vorgelegt, sondern der Kunde teilt seine Kartendaten (Kartennummer, Ablaufdatum, Kartenprüfnummer/CVC2) telefonisch oder über Online-Eingaben dem Geschäftspartner

Ali Basas (PayLife): Mitorganisator der Tagung für Polizeibeamte zum Thema „Kreditkartenbetrug".

Sevim Sinci (Card Complete): „Bei vier Fünftel der Kartendelikte handelt es sich um Internet-Betrug."

mit. Card-not-present-Transaktionen gibt es vorwiegend beim Online-Shopping. Immer mehr Betrüger nutzen illegal erlangte Kartendaten. „Der Card-not-present-Fraud steigt weltweit stark an", sagte Chefinspektor Christoph Heichinger, stellvertretender Leiter des Büros 7.1 (Betrug, Fälschung und Wirtschaftskriminalität) im Bundeskriminalamt.

Aktuelle Herausforderungen. Mag. Thomas Von der Gathen, Prokurist bei *PayLife,* gab einen Überblick über aktuelle Herausforderungen im Kartengeschäft. Es herrsche bei den Strafverfolgungsbehörden nicht immer Einigkeit, wann ein Gerichtsbeschluss erforderlich sei, um Bilder aus einer Überwachungskamera oder andere Daten weiterzugeben. Bei Delikten im Zusammenhang mit Geldausgabeautomaten gehe der internationale Trend hin zu Lowtech-Crime; beispielsweise werde der Geldausgabeschlitz blockiert. Im Visier der Täter seien vermehrt Fahrschein- und Parkautomaten. Hier gebe es meist nur wenige Sicherungen und oft keine Videoüberwachung.

Eine wirksame Maßnahme gegen Skimming ist das Geo-Blocking. Das hat sich in anderen Ländern gezeigt. Mit dieser Funktion kann der Bargeldbezug auf bestimmte Länder beschränkt werden. Der *PayLife*-Sicherheitsexperte berichtete von einem interessanten britischen Ansatz im Bereich der Betrugsprävention. Um möglichst viele Menschen zu erreichen und aufzuklären, werden beispielsweise Informationen zum Thema Phishing über moderne Formate verbreitet, etwa über Comics in Zeitungen oder in Fernseh-„Soap-Operas", wo dieses aktuelle Thema in die Handlung eingebaut wird und somit eine Sensibilisierung für dieses Thema erreicht werden soll.

Sicherheitsmaßnahmen. Die großen Kreditkartenorganisationen versuchen, mit Monitoringsystemen, Betrugsanalysen und Präventionsmaßnahmen Kriminalität einzudämmen.

ZAHLUNGSKARTENKRIMINALITÄT

Deliktsformen

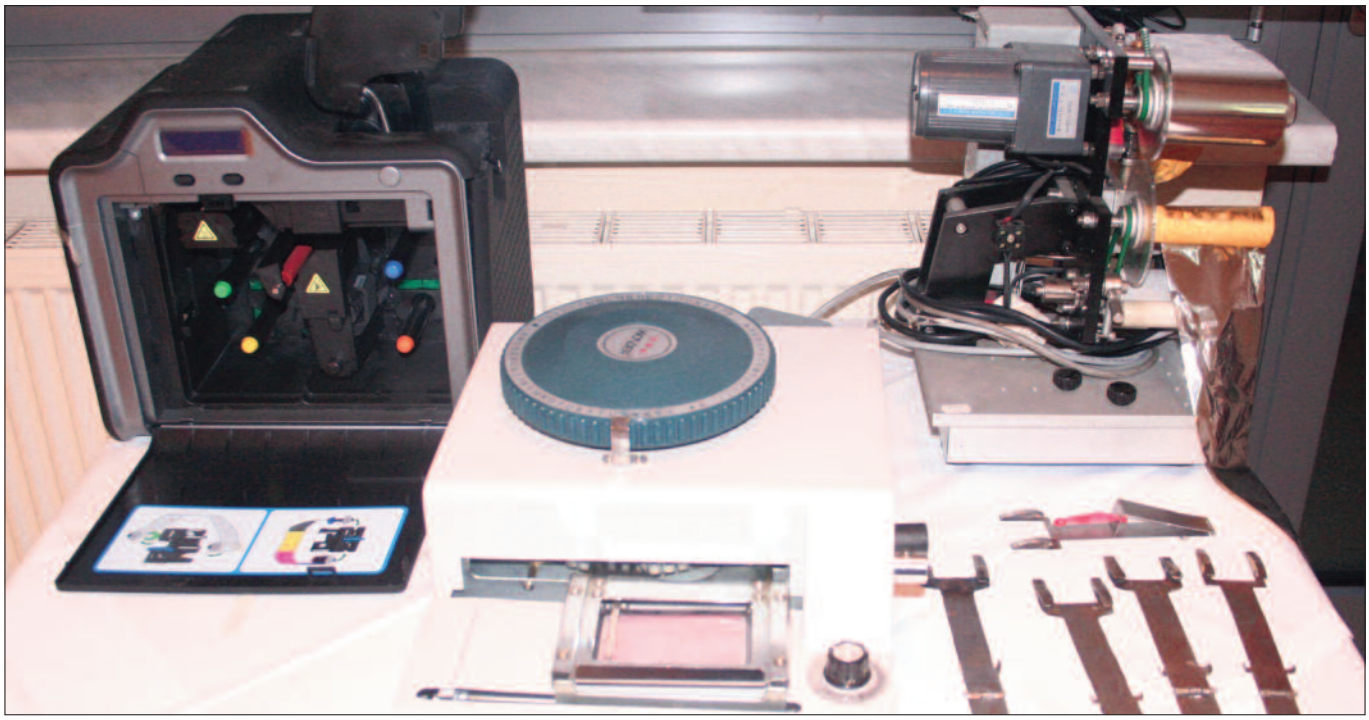
Phishing ist das Ausspähen vertraulicher Daten von Internet-Nutzern. Die Betrüger versenden E-Mails mit gefälschten Absenderadressen (z. B. Bankinstitute), um Zugangsdaten für das Internet-Banking oder Kontoinformationen von Online-Auktionsanbietern zu erlangen. Beispielsweise wird in einer E-Mail eines vermeintlichen Bankinstituts das Opfer aufgefordert, auf einer Homepage Zugangscodes einzugeben, um angeblich Sicherheitsmängel herauszufinden. Durch die Eingabe der Daten gelangen die Täter in den Besitz der Informationen für Online-Transaktionen. Eine andere Form ist die Installation eines Trojaners am PC. Nimmt das Opfer eine Transaktion vor, protokolliert der Trojaner die Zahlungsinformationen und übermittelt sie an den Täter.

Vishing steht für „Voice Phishing" und ist die Bezeichnung für Phishing über Internettelefonie *(Voice over Internet Protocol – VoIP)*. Potenzielle Opfer werden zum Beispiel durch einen Anrufer, der sich als Bankangestellter ausgibt, oder über eine Bandansage darauf hingewiesen, dass etwa seine Kreditkarte missbraucht worden sei, er solle deshalb seine Kreditkartendaten bekannt geben. Die Betrüger erfahren so alle wichtigen Daten des Opfers: Name, Adresse, Geburtsdatum und Kreditkartennummer, mit der sie dann Artikel bezahlen oder sich Geld auf ihre Konten überweisen lassen.

SIM-Swap-Betrug. Bei dieser Deliktsform erschleichen sich Kriminelle mit falschen Angaben eine Kopie der SIM-Karte eines Kunden und missbrauchen die Daten, um sich zu bereichern.

Skimming (engl.: abschöpfen, absahnen) ist eine kriminelle Handlung, bei der die Daten von Bankomat- und Kreditkarten ausgespäht werden. Die Täter bringen beispielsweise in den Karteneinschiebeschacht eines Geldausgabeautomaten ein elektronisches Gerät an. Schiebt der Bankkunde die Karte hinein, werden die Daten ausgelesen; gleichzeitig wird mit einer kleinen Kamera die Eingabe der PIN in die Tastatur aufgezeichnet. Die Täter speichern die ausgespähten Kartendaten auf Blankokarten *(White Cards)* und heben damit bei Bankomaten Geld ab. Das Skimming bei Kreditkarten ist einfacher. Bezahlt ein Kunde in einem Geschäft, Restaurant oder in einer Tankstelle mit der Kreditkarte und händigt die Karte aus, werden von Kriminellen die Daten mit einem Lesegerät ausgelesen und damit Duplikate hergestellt.

Fotos: Werner Sabitzer



Groß angelegter Kreditkartenbetrug: Sichergestellte Geräte zur Herstellung von Zahlungskarten und ID-Karten.

Foto: Werner Sabitzer

Barbara Lenck, Leiterin des Teams Fraud Management und Kreditkarten-Reklamationen bei der *Ersten Bank,* wies daraufhin, dass es massenhaft Phishing-Mails gebe. Der überwiegende Teil der Betrugshandlungen spiele sich im E-Commerce-Bereich ab. Die *Erste Bank* forciert zur Kartenbetrugsprävention das 3-d-Secure-Verfahren. Dabei gibt der Käufer zunächst seine Kreditkartennummer ein. Danach wird eine Verbindung zum Kartenherausgeber hergestellt und der Käufer muss seine Identität mit einem Code bestätigen. Ist die Authentisierung erfolgreich, wird die Kreditkartenzahlung ausgeführt. Bei immer mehr Kreditkartenunternehmen genügt nicht mehr die Unterschrift, sondern es ist zusätzlich die Eingabe eines Codes erforderlich.

Sevim Sinci von *Card Complete* hob hervor, dass es sich 2013 bei 81 Prozent der Kartendelikte um Internet-Betrug gehandelt habe. Der Anteil von Skimming und Fälschung habe elf Prozent betragen, Verlust/Diebstahl sieben Prozent und der Postwegverlust ein Prozent. 84 Prozent der Delikte seien mit Monitoring-Systemen erfasst worden, 16 Prozent von den Karteninhabern. Hauptbetroffene Branchen bei Kartendelikten über Internet seien Reisebüros, Fluglinien sowie Wettbüros und Spielcasinos.

Matthew Westhoff vom Frankfurter Büro des *United States Secret Services,* das neben Personenschutz für Finanzermittlungen zuständig ist, berichtete, dass es in den USA jeden Monat über zwei Milliarden Hacker-Angriffe gebe, 94 Prozent davon auf die Finanzwirtschaft. Cybercrime sei profitabler als der internationale Drogenhandel. Die Mitarbeiter der „Cyber Intelligence Section" (CIS) des Secret Services beobachten online kriminelle Netzwerke. Ziel sei es, die Kommando-Ebene auszuheben, betonte Westhoff.

Joachim Eckert, Richter am Landesgericht München und Vorsitzender einer großen Wirtschaftsstrafkammer, berichtete über Erscheinungsformen der organisierten Kreditkartenkriminalität. Eckert warnte auch vor dem lockeren Umgang mit den eigenen Daten in sozialen Netzen: „Wer seine Daten freiwillig hergibt, ist selber schuld." Mit Daten werde nicht nur betrogen, sondern Datensätze würden auch gehandelt: „Das ist wie bares Geld." In Deutschland gebe es nur in drei Bundesländern verfahrensunabhängige Internet-Kontrollen – in Bayern, Sachsen und Baden-Württemberg. „Die anderen Länder lehnen das ab", sagte Eckert. In England werde bei Kreditkartenbetrug mit geringem Schaden kein Strafverfahren mehr eingeleitet.

Dirk Zimmermann, zuständig für Sicherheit und Cybercrime-Ermittlungen bei *American Express,* berichtete über aktuelle Kreditkartenbetrugsfälle, darunter einen großen Card-not-present-Betrug bei Reiseveranstaltern. Die Ermittlungen ergaben, dass der Service-Provider, der für große Reisebüros Buchungen vornahm, von Kriminellen gehackt worden war. Die Täter benutzten gestaffelte Botnetze zum Verwischen der Spuren. „Die Reisebranche ist derzeit der absolute Fokus der Hacker, Reiseportale werden weiter stark angegriffen", warnte Zimmermann. „Die Datensicherheit ist nicht ausreichend."

Kooperation. Christoph Nissl, Leiter der *PayLife*-Sicherheitsabteilung, unterstrich, wie wichtig die nationale und internationale Zusammenarbeit in der Betrugsprävention sei.

Nikolaus Renner, Leiter des Geschäftsbereichs Risk-Management und rechtliche Angelegenheiten bei *Diners Club,* wies auf das im Jänner 2011 eingeführte SMS-Service hin: Erfolgt ein Zahlungsvorgang mit der Diners-Club-Karte, erhält der Kunde eine SMS-Nachricht mit einem Bestätigungstext: *„Bestätigung Ihrer Zahlung mit Diners Club Card End-Nr. ... Betrag ... Bei Fragen rufen Sie bitte ... Danke für Ihren Umsatz – Ihr Diners Club"*. So kann rasch auf einen eventuellen Missbrauch reagiert werden. Etwa 15 Prozent der Kunden nützen derzeit dieses Service. Hohe Schäden gebe es laut Renner im Zusammenhang mit Flugticket-Bestellungen. Hier arbeite man an einer nachhaltigen Lösung.

Werner Sabitzer