Skimming

Erscheinungsformen und Strafbarkeit

Cyberfahnder

1. Bargeldloser Zahlungsverkehr und das Ausspähen von Daten [1]

Namen gebend für das Skimming ist der Einsatz von Kartenlesegeräten – Skimmer – zum Ausspähen der Kartendaten auf dem Magnetstreifen von Zahlungskarten. Dazu werden entweder an den Kartenlesegeräten an der Eingangstür der betreffenden Bank oder an den Geldautomaten selber Aufsatz- oder Einsatzgeräte angebracht, die so hergerichtet sind, dass sie die Daten auf den Magnetstreifen nicht nur auslesen, sondern entweder auf ein zusätzliches Speichermedium schreiben oder per Funksignale an ein Aufnahmegerät der Täter senden.

Das Skimming beschränkt sich jedoch nicht auf das Ausspähen von Daten, sondern zielt auch auf die Persönlichen Identifikationsnummern - PIN, die die Bankkunden zur Autorisierung ihrer Verfügungen in die Geldautomaten eingeben. Dazu werden meistens Kameras oder Tastaturaufsätze verwendet, mit denen die Tasteneingaben ausgespäht oder unmittelbar bei den Tastendrucken protokolliert werden.

1.1 Missbrauch gefälschter Zahlungskarten

Das Ziel der Skimming-Täter beschränkt sich jedoch in aller Regel nicht darauf, Kartendaten und PINn auszuforschen (zusammen bilden sie den sogenannten Dump), sondern mit den Kartendaten Dubletten herzustellen und im Ausland an Geldautomaten zu missbrauchen.

Nötig ist der Einsatz der Dubletten im Ausland, weil die üblichen Zahlungskarten über mehrere Sicherheitsmerkmale verfügen. Auf den Magnetstreifen befinden sich drei Spuren mit den Identifikationsmerkmalen des Bankkunden. Dazu gehört auch der LRC-Sicherungscode, der gleichzeitig auf zwei Spuren abgelegt ist, aber nur eine einfache Plausibilitätsprüfung ermöglicht und nicht als Codierung im Sinne von § 152b Abs. 4 Nr. 2 StGB anzusehen ist. Hinzu kommt das modulierte Merkmal - MM, das in den Kartenkörper eingebettet ist und das bei der Herstellung von Dubletten nicht nachgemacht werden kann. Geldautomaten im Ausland prüfen das MM in aller Regel nicht.

1.2 Sicherheitsmerkmale und Autorisierung mit Zahlungsgarantie

Die PIN wird auf den Magnetstreifen, entgegen einer früheren Praxis, nicht mehr gespeichert. Auch die Autorisierung des Bankkunden erfolgt nicht mehr vom Geldautomaten selber. Vielmehr werden die Kartendaten und

Inhalt

[1] Wegen weiterer Einzelheiten und Beispiele wird auf die Webseite cyberfahnder.de verwiesen.
Erstfassung dieses Textes vom 15.04.2009, Update vom 16.05.2009.

die PIN im Online-Datenverkehr an die Bank gesendet, die die Karte herausgegeben hat – das aber nur, wenn sie regional nahe angesiedelt ist, oder an eine Clearingstelle von einem Bankenverbund. Die Landesbanken sind zum Beispiel die Clearingstellen für die ihr angeschlossenen Sparkassen, die Firma MasterCard International mit ihren nationalen Niederlassungen für den Maestro-Verbund und die seit 2006 von der First Data Deutschland GmbH übernommene GZS Gesellschaft für Zahlungssysteme mbH betreut (jetzt) mehr als 1.200 Kreditinstitute und andere Herausgeber von Identifikationskarten. Die Dumps von im Ausland eingesetzten Zahlungskarten werden immer von einer Clearingstelle geprüft, die keinen direkten Zugriff auf das Konto des berechtigten Karteninhabers nimmt. Stellt sie anhand von Sperrlisten und den Daten von den ihr ange-schlossenen Banken fest, dass es sich um berechtigte Kartendaten handelt, autorisiert die Clearingstelle die Verfügung und haftet für den Anweisungs- oder Auszahlungsbetrag (Zahlungsgarantie durch Autorisierung).

2. arbeitsteiliges Vorgehen

Der Tatplan beim Skimming umfasst bei einer groben Unterteilung drei Arbeitsschritte:

1) Ausspähen von PINn und Kartendaten

2) Fälschung von Zahlungskarten

3) Missbrauch der gefälschten Zahlungskarten

Vor dem Arbeitsschritt 1) ist die Herstellung der teilweise handwerklich anspruchsvollen Skimming-Hardware angesiedelt und nach dem Arbeitsschritt 3) die Beuteverteilung, wenn es sich um eine arbeitsteilig aufgestellte Gruppe von Tätern handelt.

2.1 Missbrauch von Zahlungskarten

Der Arbeitsschritt 3) [2] stellt nach Maßgabe des deutschen Strafrechts einen Gebrauch gefälschter Zahlungskarten gemäß § 152a Abs. 1 Nr. 2 StGB dar. Die Kombination von Kartendaten und PIN sowie die Verwendung eines MM belegen, dass die Originalkarten über Codierungen im Sinne von § 152b Abs. 4 Nr. 2 StGB verfügen. Der erfolgreiche Einsatz im Ausland belegt zudem, dass eine Zahlungsgarantie von einer Clearingstelle erklärt wurde, weil im grenzüberschreitenden Zahlungsverkehr kein Direktzugriff auf das Konto des berechtigten Karteninhabers erfolgt (§ 152b Abs. 4 Nr. 1 StGB). Daraus folgt, dass bereits im Einzelfall der Verbre-chenstatbestand des § 152b Abs. 1 StGB einschlägig ist. Handelt der Einzeltäter mehrfach, ist gewerbsmäßiges Handeln nahe liegend. Handeln mehr als zwei Täter – auch in verschiedener Besetzung – serienmäßig, dann kommt auch eine bandenmäßige Begehung in Betracht. In beiden Fällen der Gewerbs- oder Bandenmäßigkeit greift der Verbrechenstatbestand des § 152b Abs. 2 StGB, der mit einem Strafrahmen von 2 Jahren bis 15 Jahre Freiheitsstrafe droht.

Die Fälschung von Zahlungskarten mit Garantiefunktion (§ 152b StGB) und ihre Vorbereitung ist gemäß § 6 Nr. 7 StGB auch als Auslandstat verfolgbar.

Der Arbeitsschritt 3) stellt zudem einen Computerbetrug gemäß § 263a Abs. 1 StGB in der Begehensform der unbefugten Verwendung von Daten und die fälschliche Beeinflussung einer Datenverarbeitung im Zusammenhang mit beweiserheblichen Daten gemäß §§ 270 i.V.m. 269 Abs. 1 StGB dar, weil die Täter unter einer fremden Identität auftreten. Beide

[2] Die Täter werden gelegentlich als „Casher“ bezeichnet.

Strafnormen verfügen über Qualifizierungstatbestände, die bei gewerbs- und bandenmäßiger Begehung die Verfolgung als Verbrechen androhen (§ 263 Abs. 5 StGB; §§ 269 Abs. 3 i.V.m. 267 Abs. 4 StGB). Ihre Verfolgung als Auslandstat sieht § 6 StGB jedoch nicht vor und diese Tatbestände treten, wie die Urkundenfälschung, hinter § 152b StGB zurück.

2.2 Herstellung gefälschter Zahlungskarten

Die Herstellung von Falsifikaten (Arbeitsschritt 2) [3] ist das Nachmachen in- oder ausländischer Zahlungskarten mit Garantiefunktion gemäß §§ 152b, 152a Abs. 1 Nr. 1 StGB. Darauf, ob die Täter die Garantiefunktion auch nutzen wollen, kommt es bei Totalfälschungen von Kredit- und Zahlungskarten nicht an, wenn das Original über eine Garantiefunktion verfügt [4].

2.3 Ausspähen von Kartendaten

Wegen des Arbeitsschrittes 1) [5] muss danach unterschieden werden, ob die Kartendaten oder die PINn ausgespäht werden.

Zunächst zu den Kartendaten:

§ 152b Abs. 5 StGB nimmt Bezug auf die Vorbereitungstaten des § 149 StGB [6]. Danach sind der Umgang [7] mit „Computerprogrammen“ und „ähnlichen Vorrichtungen“ gemäß § 149 Abs. 1 Nr. 1 StGB mit Strafe bedroht, wenn sie zur Begehung der Tat geeignet sind.

Wegen der Kartenlesegeräte hat der BGH noch zur alten Rechtslage entschieden, dass sie keine „ähnlichen Vorrichtungen“ seien [8]. In seiner jüngsten Entscheidung in diesem Zusammenhang hat er diese Frage nicht erörtert [9], obwohl der GBA ausführlich dazu Stellung genommen hatte und das Sich-Verschaffen von für das Skimming präpa-rierten Kartenlesegeräte als strafbare Vorbereitungshandlung ansieht [10], weil das Ausspähen der Kartendaten eine notwendige Voraussetzung für die beabsichtigte Fälschung von Zahlungskarten ist. Die Kommentarliteratur teilt überwiegend die vom GBA vertretene Ansicht [11].

Wenn die Handlungsformen des § 149 StGB die Vorbereitungshandlungen umfassen, dann stellt das erste Ausspähen der Daten von einer Zahlungskarten mit einem präparierten Kartenlesegerät den Eintritt in den Versuch der Fälschung von Zahlungskarten mit Garantiefunktion dar (§§ 152b, 23 Abs. 1 StGB) [12]. Gleichzeitig ist damit auch das Ausspähen von Daten gemäß § 202a StGB verbunden, wobei das versuchte Verbrechen das Vergehen verdrängt.

Die Strafbarkeit im Vorbereitungsstadium gemäß § 149 Abs. 1 Nr. 1 StGB betrifft sowohl die Hersteller von präparierten Kartenlesege-

---

3 Die Täter werden gelegentlich als „Carder“ bezeichnet.

4 BGH, Beschluss vom 17.06.2008 – 1 StR 229/08

5 Die Täter werden gelegentlich, wie das Lesegerät selber, als „Skimmer“ bezeichnet.

6 § 149 StGB in der seit dem 30.08.2003 geltenden Fassung, durch die die „Computerprogramme“ in Abs. 1 Nr. 1 und die vollständige Nr. 3 eingefügt worden sind.

7 „Umgang“ wird hier zur Vermeidung der Wiedergabe verschiedener Tatbestandsvarianten analog § 1 Abs. 3 WaffG verwendet.

8 BGH, Urteil vom 16.12.2003 – 1 StR 297/2003, S. 10

9 BGH, Beschluss vom 09.09.2008 – 1 StR 414/08

10 Nicht veröffentlichte Stellungnahme.

11 Statt vieler: Fischer, § 149 StGB Rn. 3, am Ende.

12 Mit dem Wissen, dass den Angeklagten in dem Verfahren beim BGH – 1 StR 414/08 – mehrere erfolgreiche Ausspähungen von Daten mit anschließendem Missbrauch und ein fehlgeschlagenes Ausspähen vorgeworfen wurde, kann geschlossen werden, dass der BGH das genauso sieht. Er hat den Tenor des angefochtenen Urteils dahin gehend abgeändert, dass die Angeklagten auch des Versuchs der banden- und gewerbsmäßigen Fälschung von Zahlungskarten mit Garantiefunktion schuldig sind.

räte wie auch die Skimmer (Ausspäher) von dem Moment an, wenn sie sich die Geräte beschaffen.

2.4 Ausspähen von Persönlichen Identifikationsnummern

Die PINn werden nicht für die Fälschung von Zahlungskarten als solche benötigt, sondern erst bei ihrem Missbrauch, um ihre Codierung (§ 152b Abs. 4 Nr. 2 StGB) zu überwinden.

Wenn sich die weite Auslegung von „Computerprogrammen“ und „ähnlichen Vorrichtungen“ durchsetzt, dann dürften die PINn „andere Bestandteile“ sein, „die der Sicherung gegen Fälschungen dienen“ (§ 149 Abs. 1 Nr. 3 StGB). Sie verschaffen sich die Täter durch das Ausspähen mit Kameras oder Tastaturaufsätzen. In der Rechtsprechung und Literatur gibt es dazu noch keine Hinweise.

Die dazu verwendeten Geräte, Tastaturaufsätze und Kameras, dürften hingegen nicht zu den „ähnlichen Vorrichtungen“ nach Nr. 1 zählen, weil sie mit dem Fälschungsvorgang selber nicht in Verbindung stehen.

Das Ausspähen der PINn ist kein Ausspähen von Daten im Sinne von § 202a Abs. 1 StGB, weil nach der Legaldefinition in § 202a Abs. 2 StGB Daten in diesem Sinne nur solche sind, die im Wege der Datenverarbeitung gespeichert oder übermittelt werden. Das ist zwar bei den Kartendaten der Fall, weil sie auf dem Magnetstreifen der Zahlungskarte gespeichert sind, nicht aber bei der PIN, die von dem Bankkunden manuell eingegeben werden muss.

Ebenso wenig kommt § 202c Abs. 1 Nr. 1 StGB in direkter Anwendung in Betracht, weil sich hier der Umgang mit Passwörtern darauf beschränkt, das Ausspähen von Daten vorzubereiten, nicht aber deren Einsatz zu anderen Straftaten.

2.4.1 Ausspähen von PINn mit Tastaturaufsätzen

Der abschließende Missbrauch von Zahlungskarten beinhaltet jedoch auch einen Computerbetrug in der Begehensform der unbefugten Verwendung von Daten (§ 263a Abs. 1 StGB), wobei mit den Kartendaten und den PINn der automatisierte Autorisierungsprozess beeinflusst wird. Die Vorbereitung des Computerbetruges durch den Umgang mit Computerprogrammen, deren Zweck die Begehung der Tat ist, wird von § 263a Abs. 3 StGB einer vorverlagerten Strafbarkeit unterworfen. Solche Computerprogramme kommen jedenfalls in Tastaturaufsätzen zum Einsatz, weil sie dazu dienen, die eingegebenen Tastendrucke auf einem Speichermedium zu speichern oder per Funk zu übermitteln. Daraus folgt, dass die Installation der Software in Tastaturaufsätzen bereits zur Strafbarkeit führt.

Das erfolgreiche Ausspähen einer PIN mit einem Tastaturaufsatz stellt deshalb den Beginn des Versuchs eines Computerbetruges gemäß §§ 263a Abs. 2, 263 Abs. 2 StGB dar, weil bereits der Umgang mit dieser Technik als strafbare Vorbereitungshandlung vorgesehen ist.

2.4.2 Ausspähen von PINn mit Kameras

Das gilt jedoch nicht für Kameras, mit denen die Tastatureingaben *beobachtet*, aber nicht automatisch aufgezeichnet werden.

§ 303b Abs. 1 Nr. 2 StGB betrachtet auch die Tathandlung als Computersabotage, wenn eine Datenverarbeitung von wesentlicher Be-

deutung durch sie nicht unerheblich gestört wird, weil Daten in der Absicht eingegeben werden, einem anderen Nachteil zuzufügen. Das wird anzunehmen sein, wenn nicht nur einzelne Dumps ausgespäht werden, sondern eine Vielzahl von ihnen, um sie zu missbrauchen. Gestört werden schließlich die Datenverarbeitungen der Clearingstellen und der ihnen angeschlossenen Banken, weil wegen aller missbräuchlicher Verfügungen Rück- und Umbuchungen zu erwarten sind. Die Schäden treten zunächst bei den Bankkunden und mittelbar bei den kartenausgebenden Banken ein, weil sie in aller Regel die Schäden ihrer Kunden übernehmen.

§ 303b Abs. 5 StGB verweist auf die Vorschrift des § 202c Abs. 1 StGB. Über den Umweg zur Computersabotage unterliegt somit auch der Umgang mit Passwörtern (§ 202c Abs. 1 Nr. 1 StGB) der Strafbarkeit im Vorbereitungsstadium.

2.4.3 Ausspähen beim POS-Skimming

Beim POS-Skimming (Point of Sales – POS) werden in Einkaufszentren und anderen Märkten die Eingabegeräte von den Kassen zunächst gestohlen und so manipuliert, dass sie die Kartendaten und die PIN nicht nur an die Clearingstelle übermitteln, sondern auch an die Täter. Die präparierten Geräte „splitten“ sozusagen den Datenstrom. Danach werden bei einem zweiten Einbruch die präparierten Geräte wieder installiert.

Bei dieser Ausspähmethode ist die PIN ein Bestandteil des Datenstromes, so dass sowohl § 149 Abs. 1 Nr. 1 StGB als auch § 202a Abs. 1 StGB greifen, weil das Splitten während der Übermittlung stattfindet. Das bedeutet, dass bereits die Manipulation am POS-Skimmer eine strafbare Vorbereitungshandlung zur Fälschung von Zahlungskarten mit Garantiefunktion ist. Das erste erfolgreiche Ausspähen von Zahlungskartendaten stellt den Beginn des Versuchs der Fälschung von Zahlungskarten dar.

3. Ergebnisse

Gefälschte Zahlungskarten, die erfolgreich im Ausland missbraucht wurden, weisen sich bereits dadurch als Zahlungskarten mit Garantiefunktion im Sinne von § 152b StGB aus.

Die Herstellung der Falsifikate und der Missbrauch sind Verbrechen gemäß § 152b Abs. 1 StGB, bei mehrfachen Missbräuchen in gewerbsmäßiger Begehung gemäß § 152b Abs. 2 StGB, so dass als Mindeststrafe 2 Jahre Freiheitsstrafe drohen [13]. Sie sind als Auslandstaten gemäß § 6 Nr. 7 StGB nach deutschem Strafrecht verfolgbar.

Der Umgang mit präparierten Kartenlesegeräten ist eine strafbare Vorbereitungshandlung gemäß § 149 Abs. 1 Nr. 1 StGB. Auch sie ist als Auslandsstraftat gemäß § 6 Nr. 7 StGB nach deutschem Strafrecht verfolgbar.

Vereinbaren mehrere Täter nach bereits durchgeführten ein neues Ausspähen in Bezug auf eine bestimmte Bank, so liegt darin eine Verabredung zu einem Verbrechen gemäß § 30 Abs. 2 StGB [14].

Sollen Persönliche Identifikationsnummern mit einem Tastaturaufsatz protokolliert werden, so handelt es sich bei dem installierten

[13] Das BVerfG hat die schwere Strafdrohung nicht beanstandet: Beschluss vom 18.03.2009 - 2 BvR 1350/08.

[14] Während sich an den Handlungen einer Bande auch Beihilfetäter beteiligen können (BGH, Beschluss vom 22.03.2001 - GSSt 1/00), können sich an einer Verbrechensabrede nur Mittäter beteiligen (BGH, Urteil vom 04.02.2009 - 2 StR 165/08).

	Verabredung	Umgang	erfolgreiches Ausspähen
Planung	§ 30 Abs. 2 StGB (6 Mo bis 11 J 9 Mo)		
Skimmer		§ 149 Abs. 1 Nr. 1 StGB (GS bis 5 J)	§§ 152a Abs. 1 Nr. 1, Abs. 2, 152b Abs. 1 StGB (3 Mo bis 7 J 6 Mo)
Tastaturaufsatz		§ 263a Abs. 3 StGB (GS bis 3 J)	§ 263a Abs. 2, § 263 Abs. 2, Abs. 3 Nr. 1 StGB (GS bis 7 J 6 Mo)
Kamera			§ 303b Abs. 1 Nr. 2, Abs. 5, § 202c Abs. 1 StGB (GS bis 1 J)
POS-Terminal		§ 149 Abs. 1 Nr. 1 StGB (GS bis 5 J)	§§ 152a Abs. 1 Nr. 1, Abs. 2, 152b Abs. 1 StGB (3 Mo bis 7 J 6 Mo)

Programm zur Speicherung der Tastatureingaben um ein Computerprogramm nach § 263a Abs. 3 StGB, mit dem der Umgang strafbar ist.

Sollen sie jedoch mit Kameras beobachtet werden, dann tritt die Strafbarkeit gemäß § 303b Abs. 1 Nr. 2 i.V.m. § 202c Abs. 1 Nr. 1 StGB erst mit dem Ausspähen der ersten PIN ein. Der Umgang mit den Kameras als solche ist nicht strafbar.

4. Strafdrohungen

Die Tabelle fasst die Tathandlungen und ihre Strafbarkeit zusammen. Unter den Strafvorschriften ist in Klammern der Strafrahmen angegeben, der den Tätern droht. Soweit eine Strafmilderung gemäß § 49 StGB in Betracht kommt, ist der Strafrahmen gemildert worden. „GS“ bedeutet „Geldstrafe“ und die Zeitangaben „J“ für „Jahre“ und „Mo“ für „Monate“ die Dauer der angedrohten Freiheitsstrafe.

Bei der „Planung“ ist das Verbrechen des Fälschens von Zahlungskarten mit Garantiefunktion gemäß § 152b Abs. 2 StGB zugrunde gelegt wurde, also entweder in gewerbs- oder bandenmäßiger Begehensweise.

5. Perspektiven

Die Ausbreitung des POS-Skimming und das zu beobachtende Verschmelzen verschiedener Formen der Cybercrime lassen erwarten, dass die Daten von Zahlungskarten künftig vermehrt bei Dienstleistern, Online-Warenhäusern und anderen Unternehmen mit den Methoden des Hackings, des Social Engineerings oder mit Malware ausgeforscht werden.

Skimming ist die Erscheinungsform der Cybercrime, die wegen ihrer Erfassung in § 152b StGB, der Erwähnung in § 6 Nr. 7 StGB als strafbare Auslandsstraftat und schließlich als schwere Straftat im Tatbestandskatalog zur TKÜ (§ 100a Abs. 2 Nr. 1.e) StPO) der schwersten Strafdrohung unterworfen ist und den Zugang zu tief greifenden Ermittlungsmaßnahmen eröffnet. Darin unterscheidet sie sich deutlich vom Phishing und anderen Formen des Identitätsdiebstahls sowie des Betruges mit den Mitteln der Informationstechnik.

Die Globalisierung der Cybercrime macht neue Formen der Strafverfolgung nach diesem Vorbild nötig. Wünschenswert wäre es, wenn der Gesetzgeber klarere Regeln für die

Cyberfahnder, Skimming, S. 7

Strafbarkeit von Überwachungstechnik und Malware schüfe und jedenfalls die arbeitsteiligen Formen der Cybercrime in § 6 StGB aufnehmen würde.

Dieter Kochheim (Cyberfahnder)