Cyberfahnder-Newsletter 2 vom 12.12.2009

Schwerpunkt: Skimming

Das Arbeitspapier Skimming (**Download** [1]) wurde um weitere Rechtsprechungsnachweise ergänzt. Eingefügt wurde ein Abschnitt über den Beginn und die Vollendung des strafbaren Handelns beim Skimming [2] und ein neues Kapitel, das die ersten kriminalistischen Erfahrungen mit dieser Form der Kriminalität beschreibt und bewertet [3].

Skimming

Das Skimming ist geprägt von einem komplexen Tatplan, der von dem Ausspähen von Kartendaten und Persönlichen Identifikationsnummern – PIN – über die Herstellung gefälschter Kredit- oder Zahlungskarten bis zum Missbrauch der Dubletten an anderen Geldautomaten reicht. In der Öffentlichkeit treten die Täter beim Skimming im engeren Sinne auf, also dem Ausspähen der Kundendaten an Geldautomaten, und beim Cashing, dem abschließenden Missbrauch mit dem Ziel, Beute zu machen.

Die bislang gemachten Erfahrungen zeigen, dass in aller Regel arbeitsteilige und gut organisierte Tätergruppen im Einsatz sind.

Ausgespäht werden vor Allem die Kundendaten im Zusammenhang mit Debitkarten aus den Finanzverbunden elecronic cash – EC – und Maestro. Bei ihnen handelt es sich um Zahlungskarten mit Garantiefunktion. Aufgrund der in Deutschland geltenden Sicherheitsbestimmungen können diese im Inland ausgespähten Daten nur an Geldautomaten im Ausland missbraucht werden. Das liegt daran, dass sich die Täter auf das Auslesen der Daten auf dem Magnetstreifen der Karten beschränken und die Geldautomaten im Inland die besonderen Merkmale [4] im Kartenkörper und die Daten aus dem EMV-Chip prüfen. Diese Sicherheitsmerkmale verhindern eine erfolgreiche Fälschung.

[1] Aktueller Stand: 09.12.2009
[2] **6.4 Anfang und Ende**, S. 17.
[3] **E. kriminalistische Erfahrungen**, S. 22. Das Kapitel basiert auf dem Aufsatz: CF, Geltung von Beweisen und Erfahrungen, 29.11.2009
[4] Maschinenlesbares Merkmal – MM.

Autorisierung und Genehmigung

Zu Zahlungskarten mit Garantiefunktion werden Debitkarten durch das im Hintergrund ablaufende Autorisierungsverfahren. Es besteht darin, dass die in einen ausländischen Geldautomaten eingegebenen Daten per Datenfernübertragung bis zu dem Datenverarbeitungszentrum der kartenausgebenden Bank übermittelt und dort die Berechtigung der Transaktion geprüft werden. Die Prüfung umfasst die Kontodeckung, den Überziehungskredit, das Tages- und Wochenlimit und andere Beschränkungen (z.B. Auslandsverfügung). An den Geldautomaten zurückgemeldet wird ein Genehmigungscode, ohne den die Auszahlung verweigert würde.

Mit dem Genehmigungscode verbunden ist eine Auszahlungsgarantie der kartenausgebenden Bank, die sich auch darin äußert, dass der Auszahlungsbetrag und die Gebühr zunächst gegen ein bankinternes Konto gebucht werden. Nach der Auszahlung erfolgt wegen der gegenseitigen Forderungen zwischen den Bankverbunden und -instituten ein Clearingverfahren, worauf das Konto des Bankkunden mit dem Auszahlungsbetrag und der Gebühr belastet wird.

Strafbarkeit

Der erfolgreiche Missbrauch der Kundendaten stellt sich als der Gebrauch gefälschter Zahlungskarten mit Garantiefunktion gemäß den §§ 152a, 152b Strafgesetzbuch in Tateinheit mit Computerbetrug gemäß § 263a Strafgesetzbuch dar. Der strafbare Versuch dieser Tat beginnt mit der Installation der Geräte zum Ausspähen der Kartendaten und PIN.

Aus der „erfolgreichen“ Auszahlung im Ausland lassen sich mehrere Rückschlüsse ziehen:

► Die Originalkarte nimmt am grenzüberschreitenden bargeldlosen Zahlungsverkehr teil.

► Die Bank, die die Originalkarte ausgegeben hat, hat die Kontoverfügung genehmigt.

► Die Genehmigung weist die Originalkarte als Zahlungskarte mit Garantiefunktion aus.

Tatvarianten

Neben dem Ausspähen der Kundendaten an Geldautomaten ist auch das POS-Skimming verbreitet [5]. Dazu werden die Kartenlesegeräte im Einzelhandel, in Tankstellen, Hotels oder sonstwo so manipuliert, dass sie die eingegebenen Kartendaten und PIN für die Täter speichern.

Laut einzelner Meldungen sind Kundendaten auch schon bei Finanzdienstleistern gestohlen oder von manipulierten Geldautomaten für die Täter gespeichert worden.

Denkbar ist es, dass sich Tätergruppen auf das Ausspähen spezialisieren und die dabei gewonnen Daten an Andere verkaufen, ohne selber das Cashing zu betreiben. Dagegen spricht die Erfahrung, dass die Zeit zwischen Skimming und Cashing immer kürzer zu werden scheint. Das spricht für eine ganz enge Zusammenarbeit aller an der Tat Beteiligten und gegen einen Zwischenschritt, in dem der Verkauf der ausgespähten Daten abgewickelt wird.

Weitere Informationen

Die Argumente im Einzelnen finden Sie hier:

Kochheim, Skimming, 09.12.2009 (PDF)

CF, Zwischenbilanz: Skimming, 14.11.2009

Impressum

[5] POS: Point of Sale.