



Bundeskriminalamt

ZAHLUNGSKARTEN- KRIMINALITÄT

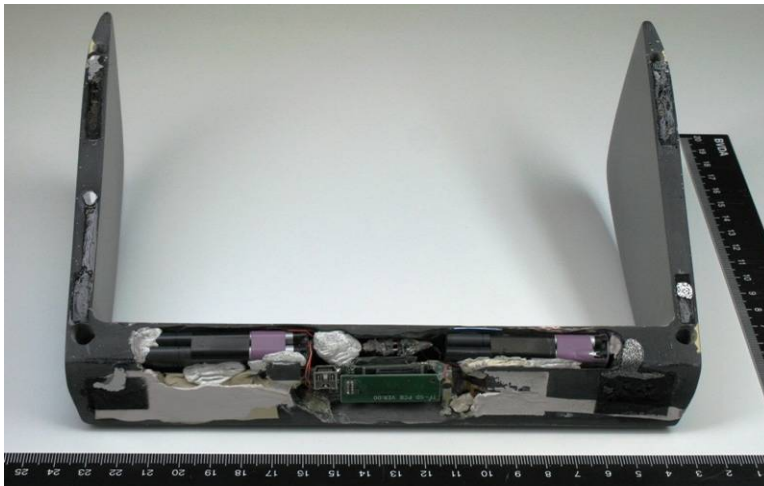
Bundeslagebild 2010



Die Modi Operandi zur Erlangung der PIN/Geheimzahl sind nach wie vor die Gleichen: Häufig installieren die Täter versteckte (Mini-)Kameras oberhalb der PIN-Tastatur. Dazu wird eine speziell für den jeweiligen Geldautomaten-Typ passende Verblendung oder Leiste mit einer Aufnahmeeinheit ausgestattet, die über einen längeren Zeitraum alle PIN-Eingaben an der Tastatur aufzeichnet.



Manipulierter Sichtschutz mit Öffnung für die Kamera



Rückseite des manipulierten Sichtschutzes mit eingebauter Elektronik

Alternativ werden Tastaturattrappen eingesetzt, die identisch aussehen und unmittelbar auf der Originaltastatur angebracht werden. Die durch den Kunden eingegebene PIN wird gespeichert, während gleichzeitig die Originaltastatur und damit der Geldautomat störungsfrei bedient wird.

Auch werden weiterhin Kameras an der Decke in Rauchmelderattrappen installiert.



Täter beim Anbringen eines mit einer Kamera präparierten Rauchmelders

Nachdem im Jahr 2009 der Abgriff der Magnetstreifendaten noch in rund 13 % der Fälle³ an Türöffnern von Bankfoyers erfolgte, spielte dieser Modus Operandi im abgelaufenen Jahr keine nennenswerte Rolle mehr: Nur noch in ca. 2 % der Fälle ist der Datenabgriff durch Türöffnermanipulationen erfolgt. Diese rückläufige Entwicklung begründet sich durch den Abbau bzw. die sicherheitstechnische Aufrüstung der Türöffner bei bundesweit sowie lokal vertretenen Geldinstituten.

2.2.2 Manipulation von POS⁴-Terminals

Im Jahr 2010 wurden mehrere Fälle registriert, in denen Täter versucht hatten, Kartendaten und PIN durch die Manipulation von POS-Terminals zu erlangen. Aus unterschiedlichen Gründen ist die Datenerlangung in allen Fällen jedoch im Versuchsstadium geblieben, so dass es in 2010 keine erfolgreichen POS-Terminal-Manipulationen gab.

2.2.3 Manipulation von Tankautomaten

In 2010 wurden erstmals in Deutschland Manipulationen an Tankautomaten (ohne Personal) festgestellt. Es handelte sich hierbei um zwei Fälle in Nordrhein-Westfalen und einen in Baden-Württemberg, bei

³ Gesamtzahl der Angriffe auf Geldautomaten

⁴ Point of Sale-Terminals = Kassenterminals

2.4 Einsatz gefälschter Debitkarten mit deutschen Kartendaten

Der Einsatzschwerpunkt gefälschter Debitkarten (sog. „white plastics“) mit deutschen Kartendaten lag im ersten Halbjahr 2010 in Europa, vor allem in Großbritannien, Italien, den Niederlanden, Bulgarien und Russland.

Einsatz gefälschter Debitkarten mit deutschen Kartendaten in Europa



Im zweiten Halbjahr 2010 erfolgten die missbräuchlichen Karteneinsätze zunehmend im außereuropäischen Bereich, in den sog. „Nicht-Chip-Ländern“. Grund dafür ist, dass ab 2011 Transaktionen europäischer Debitkarten im SEPA-Raum chip-basiert abgerechnet werden. Da viele Banken im Hinblick auf diese Umstellung die Geräte bereits sukzessive umgerüstet haben, wichen Täter im zweiten Halbjahr 2010 zunehmend in Nicht-Chip-Länder aus. Diese erst teilweise vorgezogene Umstellung erschwert die Einsatzmöglichkeiten von „white plastics“ (mit Magnetstreifen) bzw. macht diese unmöglich. In diesem Zusammenhang waren insbesondere die Staaten Südafrika, Kenia, die USA, Kanada sowie die Dominikanische Republik von Bedeutung.



Bundeskriminalamt



65173 Wiesbaden

info@bka.de

www.bka.de