

6. Konferenz kartensicherheit.de – 30. September 2010

Skimming – Erlangung und Verwendung

**Rechtliche und tatsächliche Probleme
bei der Strafverfolgung
einer professionellen und organisierten Form
der Cybercrime**



Vita

...

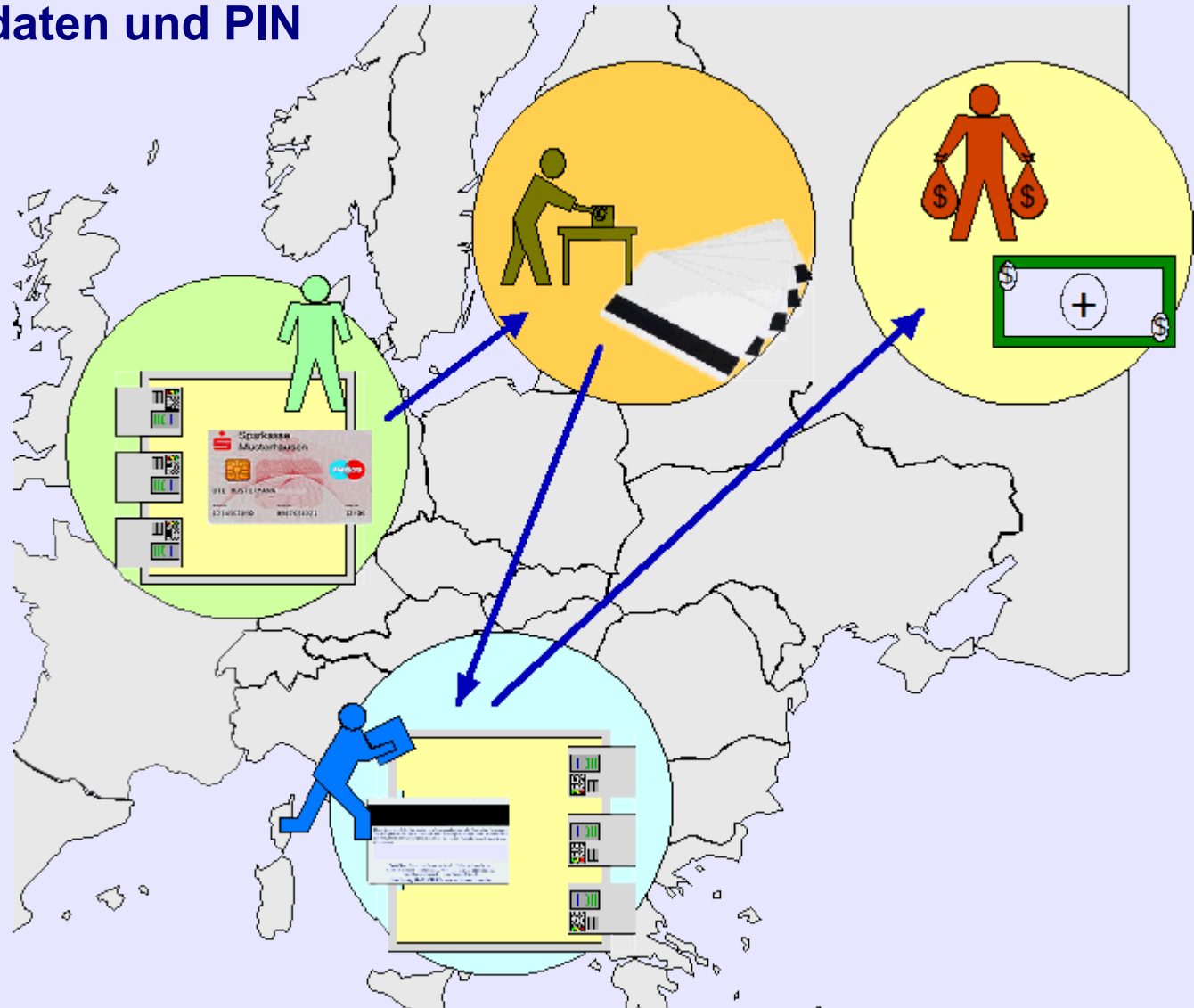
Seit April 2007: Webseite **Cyberfahnder.de**





mehrgliedrige Tatausführung

- ▶ Ausspähen von Kartendaten und PIN
- ▶ Fälschung von Zahlungskarten
- ▶ Missbrauch von Zahlungskarten
- ▶ Beutesicherung



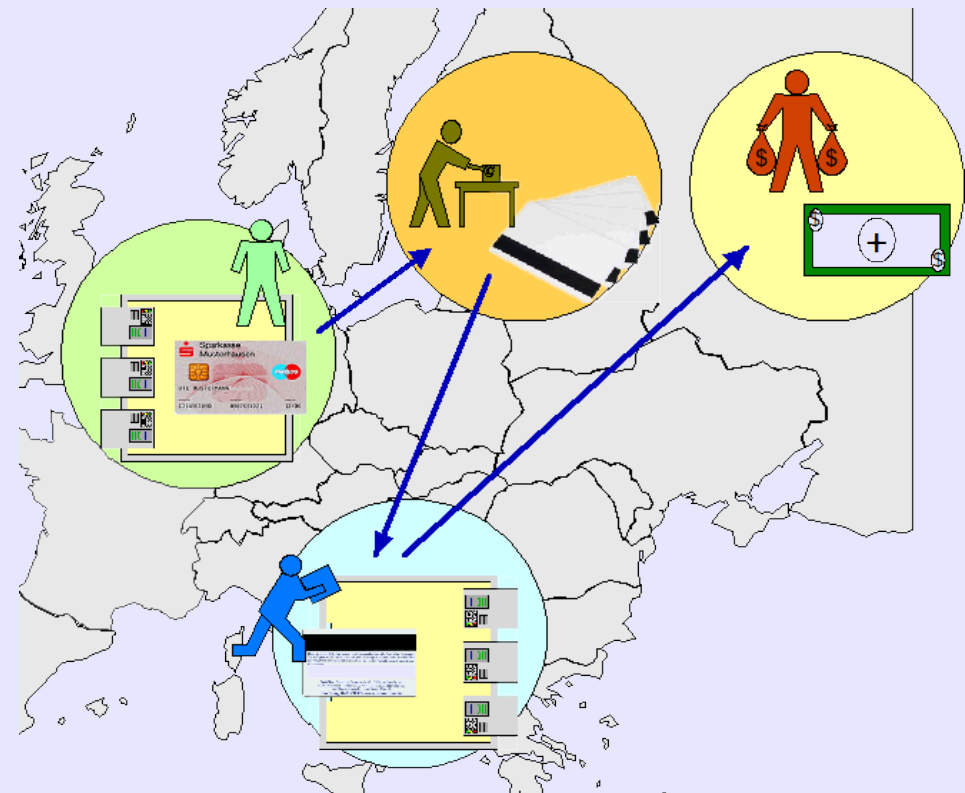


mehrgliedrige Tatausführung

- ▶ Ausspähen von Kartendaten und PIN
- ▶ Fälschung von Zahlungskarten
- ▶ Missbrauch von Zahlungskarten
- ▶ Beutesicherung

Skimming im engeren Sinne

Cashing





Zahlen für 2009

▶ Geldautomaten	59.394		
▶ Angriffe gegen GAA	809		
▶ ... Türzugangskontrollen	155	= 1,62 %	
▶ POS-Terminals	3		
▶ Zahlungskarten	125.801.300		
▶ Cashing-Fälle	17.072	= 0,014 %	
▶ Bargeld Inland	156.785.000.000		
▶ Bargeld Ausland	8.377.000.000		
▶ Gebühren (1 %)	84.000.000	~ 1,00 %	
▶ Cashing-Schaden	40.000.000	= 0,48 %	
▶ Phishing-Schaden	10.000.000		
		▶ Dumps pro Angriff	18
		▶ Schaden pro Dump (€)	2.350

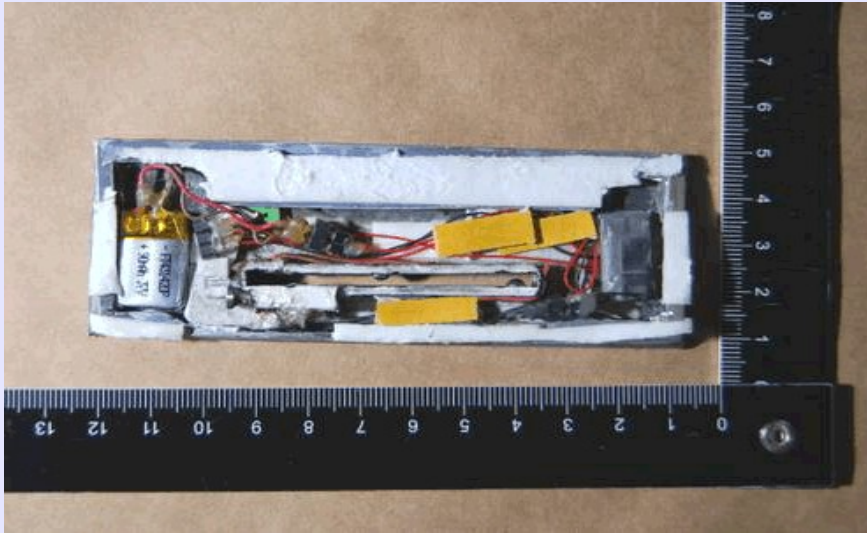
Quellen:

Deutsche Bundesbank 8/2010

EKS 3/2010 (Spiegel online)

BKA 5/2010 (PKS)

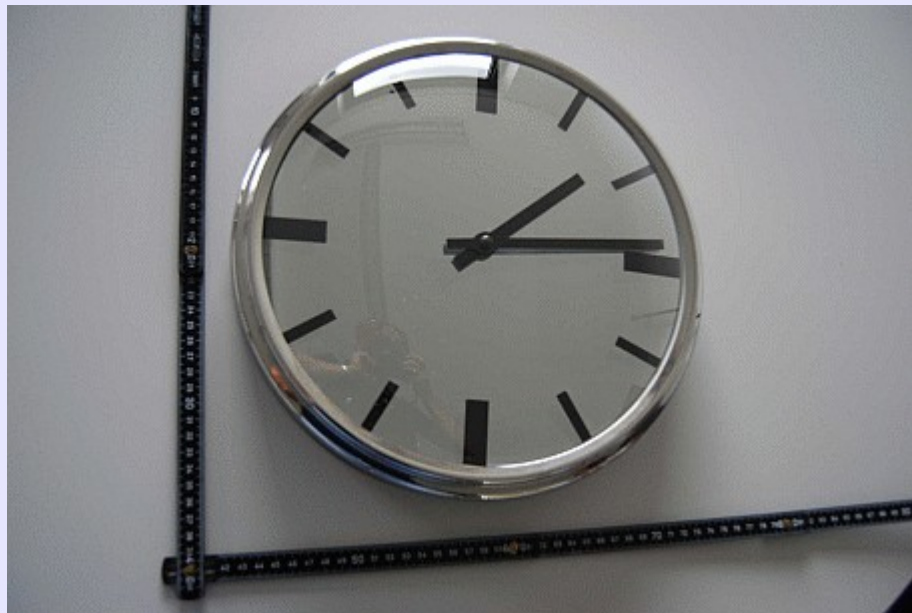
eigene Berechnungen



- ▶ **Kartenlesegeräte (Skimmer)**
 - ▶ Aufsätze (nachgeformte Bauteile)
 - ▶ Einsätze im Einzugschacht
 - ▶ Türzugangskontrolle

- ▶ **Kameras**
 - ▶ Blenden oberhalb der Tastatur
 - ▶ Propagandahalter
 - ▶ Rauchmelder u.a.
 - ▶ Sichtschutz um Tastatur

- ▶ **Tastaturaufsätze**
- ▶ **komplette Fassaden (Front Covering)**
- ▶ **mobile Geldautomaten**
- ▶ **Hacking**



Das Skimming im engeren Sinne stellt hohe Anforderungen an die handwerklichen Fähigkeiten und Erfahrungen der Täter. Sie konzentrieren sich auf bestimmte Typen von Geldautomaten und müssen ihre Geräte häufig an die Gegebenheiten vor Ort anpassen.



Ich habe meine Tante im Krankenhaus besucht. Sie hat es ja schwer an den Beinen und kann nur hier in Deutschland richtig behandelt werden. Irgendwann bin ich dann runter vor die Tür, um eine Zigarette zu rauchen. Plötzlich stand so ein Typ im grünen Kittel neben mir, rauchte hastig auch 'ne Zigarette und sprach davon, dass er üblen Stress habe. Die OP würde kein Ende nehmen und der nächste Patient läge bereits im anderen OP.

Dann schaute er mich direkt an und sagte, Mensch, ich könne ihm helfen, das sei ganz einfach. Ich müsse nur ein Skalpell nehmen, den Bauch aufschneiden, den Blinddarm rausnehmen und dann würde mir die OP-Schwester dabei helfen, alles wieder zuzunähen.

Das habe ich dann gemacht, ich bin ja Kumpel, und der Typ hat mir nachher 50 Euro gegeben.



Der US-amerikanische Automatenhersteller Diebold hat ein Sicherheits-Update für seine Opteva-Geldautomaten an seine Kunden verteilt, die Windows als Betriebssystem einsetzen. Der Hersteller reagiert damit auf Vorfälle in Russland, wo bereits im Januar eine nicht genannte Zahl von Geldautomaten entdeckt wurden, die mit einem speziellen Trojanischen Pferd verseucht waren.

**Quelle:
Russische Geldautomaten mit Trojaner infiziert,
tecchannel 19.03.2009**



Ende 2008 wurde ein Angriff auf den Finanzdienstleister RBS World Pay bekannt, der für Unternehmen die Auszahlung von Lohngeldern vornimmt. Dabei hatten die Eindringlinge laut RBS die Daten von 100 Karten ausspioniert.

Die Kriminellen haben das Geld am 8. November 2008 von 130 Geldautomaten in 49 Städten weltweit, darunter Atlanta, Chicago, New York, Montreal, Moskau und Hongkong im 30-Minuten-Takt abgehoben. Das besondere an dem Coup: Normalerweise ist die Summe der Auszahlungen am Automaten pro Tag begrenzt. Vermutlich hatten die Hacker bei dem Einbruch in das Netz von RBS aber nicht nur die Daten gestohlen, sondern auch die Limits manipuliert.

Quelle:
Kriminelle stehlen 9 Millionen Dollar in weltweitem Coup, Heise online 06.02.2009

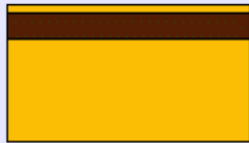


- ▶ ***Cashing***
- ▶ **Sicherheitsmerkmale**
- ▶ **Zahlungskarten**
- ▶ **Zahlungskarten mit Garantiefunktion**
 - ▶ **Autorisierung**
 - ▶ **Genehmigungscode „0“**
- ▶ **Computerbetrug**
- ▶ **Schadenseintritt**
- ▶ **Handlungsort**





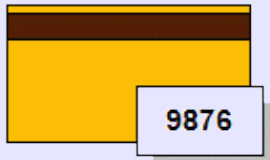
Cashing



Fälschung von **Zahlungskarten** mit Garantiefunktion
sich verschaffen von gefälschten Zahlungskarten mit Garantiefunktion

§ 152b Abs. 1 StGB

Freiheitsstrafe von **1 bis 10 Jahre**



Gebrauch von **Zahlungskarten** mit Garantiefunktion
Computerbetrug durch unbefugte Verwendung von Daten (vor allem: **PIN**)



§§ 152b Abs. 1, 263a Abs. 1 StGB

Freiheitsstrafe von **1 bis 10 Jahre**



§ 152a StGB

(1) Wer zur Täuschung im
Rechtsverkehr ... ,

1. inländische oder ausländische
Zahlungskarten, Schecks oder
Wechsel **nachmacht** oder **verfälscht**
oder

2. solche falschen Karten, Schecks
oder Wechsel sich oder einem
anderen **verschafft**, feilhält, einem
anderen überlässt oder **gebraucht**,

wird mit Freiheitsstrafe bis zu fünf
Jahren oder mit Geldstrafe bestraft.

...

(4) Zahlungskarten im Sinne des
Absatzes 1 sind Karten,

1. die von einem **Kreditinstitut** oder
Finanzdienstleistungsinstitut
herausgegeben wurden und

2. durch **Ausgestaltung** oder
Codierung besonders gegen
Nachahmung **gesichert** sind.



BGH, Urteil vom 13.01.2010
– 2 StR 439/09, Rn. 11:

Falsch sind Zahlungskarten (mit Garantiefunktion), wenn sie fälschlicherweise den Anschein erwecken, sie seien von demjenigen ausgegeben worden, auf den die lesbaren Angaben auf der Karte oder die auf ihr unsichtbar gespeicherten Informationen als Aussteller hinweisen. Optische Wahrnehmungsmöglichkeit und digitale Maschinenlesbarkeit müssen nicht gleichzeitig gegeben sein, so dass eine "falsche" Karte **nicht die kumulative Nachahmung beider Komponenten voraussetzt.**

Es genügt, dass die Fälschung entweder nur die Urkundenfunktion zum Gegenstand hat - was etwa bei einer gefälschten Kreditkarte der Fall ist, die nur in ihrem äußeren Erscheinungsbild einer echten Kreditkarte entspricht, aber keinen funktionsfähigen Magnetstreifen oder Mikrochip enthält - oder ein Magnetstreifen bzw. ein Mikrochip zwecks ausschließlicher Verwendung an Automaten gefälscht und auf ein unbedrucktes Stück Plastik oder Pappe geklebt ist ...



optische Merkmale

- ▶ Maße (Identitätskarte)
- ▶ Druckbild, Zeichensatz (OCR-B)
- ▶ Logo und Name der Bank
- ▶ Logo des Akzeptanzverbundes
- ▶ Kontonummer
- ▶ Kartenummer
- ▶ Gültigkeit
- ▶ Unterschriftsfeld
- ▶ Magnetstreifen
- ▶ EMV-Chip
- ▶ Kartenfunktionen
- ▶ erhabener Prägedruck
- ▶ Karten-ID



§ 152b StGB

(1) Wer eine der in § 152a Abs. 1 bezeichneten Handlungen in Bezug auf **Zahlungskarten mit Garantiefunktion** oder Euroscheckvordrucke begeht, wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft.

(2) Handelt der Täter gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach Absatz 1 verbunden hat, so ist die Strafe Freiheitsstrafe nicht unter zwei Jahren.

...

(4) Zahlungskarten mit Garantiefunktion im Sinne des Absatzes 1 sind Kreditkarten, Euroscheckkarten und sonstige Karten,

1. die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer **garantierten Zahlung** zu veranlassen, und

2. durch **Ausgestaltung** oder **Codierung** besonders gegen Nachahmung **gesichert** sind.



**BGH, Urteil vom 12.05.1992
- 1 StR 133/92, Rn. 9:**

Die Garantiefunktion wird darin gesehen, „dass das die Karte ausgebende Unternehmen ... sich gegenüber Vertragsunternehmen (verpflichtet), deren Forderungen gegen den Kartenbenutzer zu bezahlen“.

Zahlungskarten mit Garantiefunktion sind

- ▶ Kredit-,
 - ▶ Eurocheck- und
 - ▶ sonstige Karten,
- die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer garantierten Zahlung zu veranlassen.**



Kreditkarte



**Zahlungsgarantie
gegenüber dem
Akzeptanten.**



**Buchung gegen
Kreditkonto.**

Debitkarte

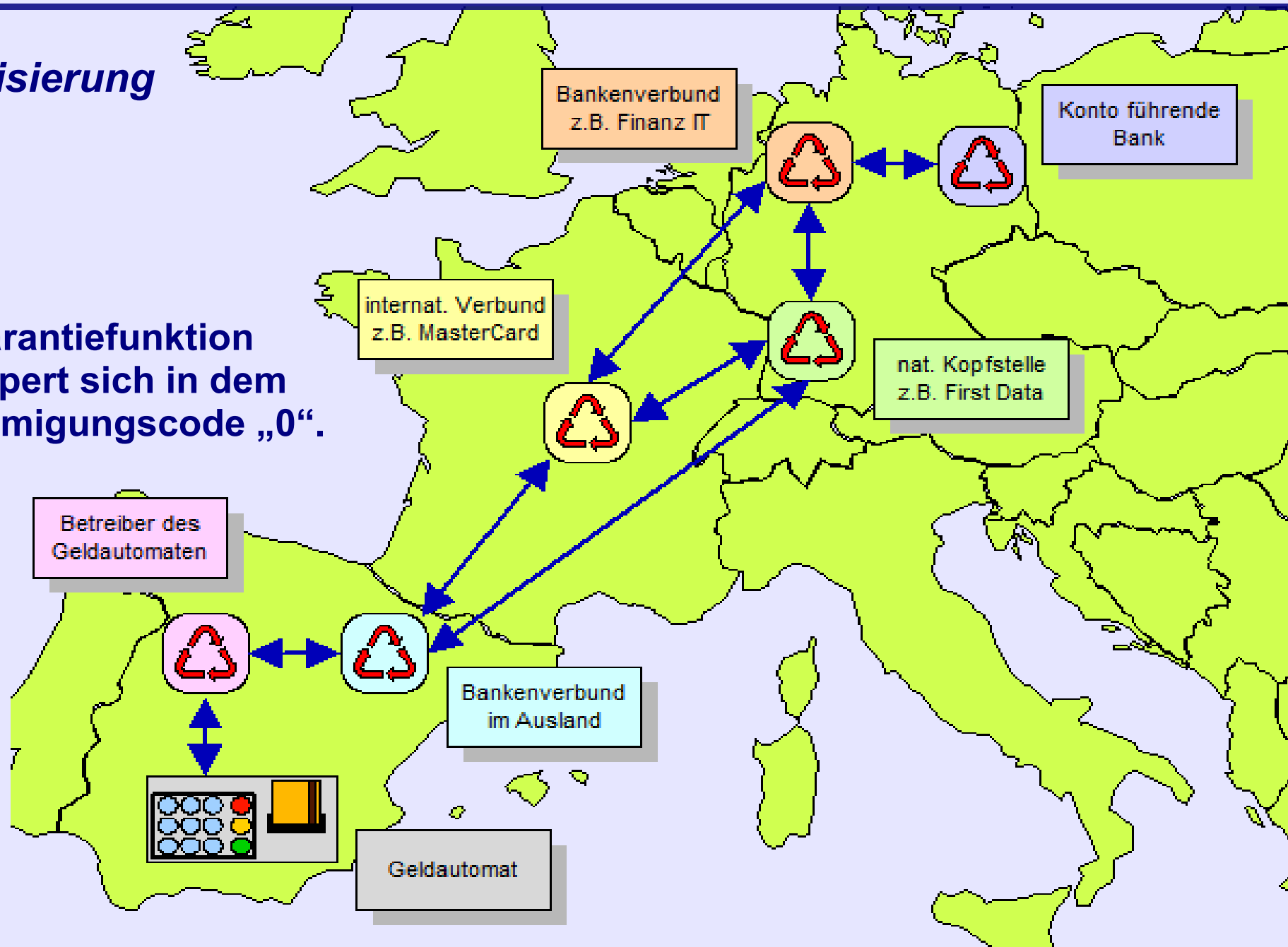


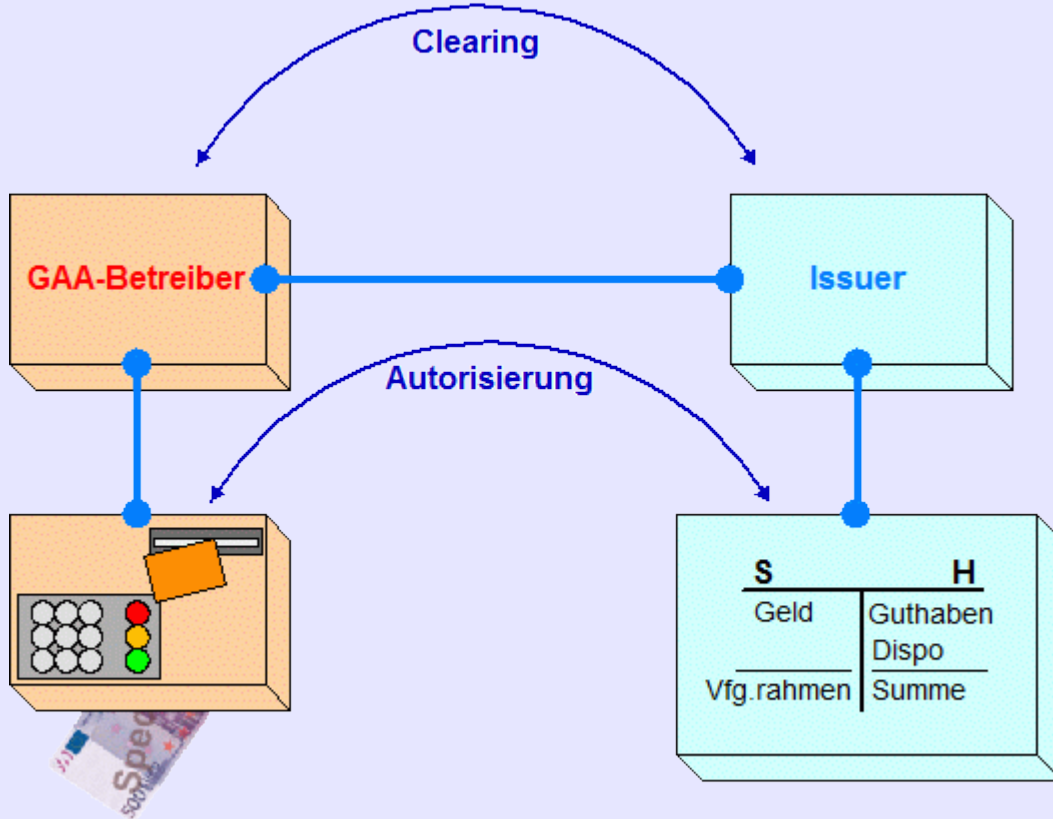
**Hat die übliche Debitkarte
eine Garantiefunktion?**



Autorisierung

Die Garantiefunktion verkörpert sich in dem Genehmigungscode „0“.





Die **Garantiefunktion** zeigt sich darin, dass das Rechenzentrum der kartenausgebenden Bank (Issuer) dem Verbundpartner, also der Betreiberin des Geldautomaten, im Autorisierungsverfahren den Genehmigungscode "0" sendet. Damit tritt es für die Auszahlung des angeforderten Geldbetrages sowie die damit verbundene Gebühr ein und stellt den Partner von allen Störungen im Innenverhältnis zwischen Kartenausgeber und Kontoinhaber frei.



§ 263a StGB

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, **durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.**



Die Missbrauchshandlung beim Skimming ist im Grunddelikt der Gebrauch falscher inländischer oder ausländischer Zahlungskarten gemäß 152a Abs. 1 Nr. 2 StGB. In Tateinheit damit steht der Computerbetrug gemäß § 263a StGB, dessen Vollendung mit der Auszahlung am Geldautomaten eintritt.

**Grundlegend:
BVerfG, Beschluss vom 18.03.2009
- 2 BvR 1350/08 (verfassungsgemäß)
BGH, Urteil vom 21.09.2000 - 4 StR 284/00
(Tateinheit)**

§ 6 StGB

Das deutsche Strafrecht gilt weiter, unabhängig vom Recht des Tatorts, für folgende Taten, die im Ausland begangen werden:

...

7. Geld- und Wertpapierfälschung (§§ 146, 151 und 152), Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks (§ 152b Abs. 1 bis 4) sowie deren Vorbereitung (§§ 149, 151, 152 und 152b Abs. 5)

...



Versuch

Strafbarkeit des Versuchs

- ▶ **§ 152a Abs. 2 StGB**
- ▶ **(§ 152b StGB) - § 23 Abs. 1 StGB**
- ▶ **§ 263a Abs. 2**
i.V.m. § 263 Abs. 2 StGB
- ▶ **besonders schwerer Fall:**
§ 263 Abs. 3 Nr. 1 StGB
- ▶ **gewerbs- und bandenmäßiges**
Handeln:
§ 263 Abs. 5 StGB

BGH, Beschluss vom 07.11.2007
- 5 StR 371/07:

Dies ist insbesondere der Fall, wenn der Täter subjektiv die Schwelle zum "jetzt geht es los" überschreitet, ... so dass sein Tun ohne Zwischenakte in die Erfüllung des Tatbestandes übergeht.



Versuch

BGH, Urteil vom 13.01.2010 – 2 StR 439/09:

Danach ist ein Versuch des ...
Nachmachens von Zahlungskarten
mit Garantiefunktion ... erst dann
gegeben, wenn der Täter vorsätzlich
und in der tatbestandsmäßigen
Absicht **mit der
Fälschungshandlung selbst** - also
dem Herstellen der falschen Karte ...
- beginnt.

*BGH, Beschluss vom 14.09.2010
- 5 StR 336/10, Rn. 4:*

Zum Versuch des Nachmachens
setzt daher ... noch nicht an, wer die
aufgezeichneten Datensätze **noch
nicht in seinen Besitz bringen** und
sie deshalb auch **nicht an seine
Mittäter**, die die Herstellung der
Kartendoubletten vornehmen sollten,
übermitteln konnte.



Vollendung

§ 152a StGB: Gebrauch

- ▶ **Einstecken der falschen Karte**
- ▶ **Eingabe der PIN**

§ 263a StGB: Vermögensverfügung

- ▶ **Eingabe des Geldbetrages**
- ▶ **„Bestätigen“**
- ▶ **Entnahme des Geldes**



Schaden

- ▶ **Betreiber des Geldautomaten**
- ▶ **Kartenaussteller**
- ▶ **Kunde**

Der aus dem Guthaben des Kunden und dem Überziehungskredit bestehende Verfügungsrahmen wird unmittelbar durch die Autorisierung verringert und spätestens beim Clearing, also dem Forderungsausgleich zwischen den beteiligten Banken und ihren Verbänden, endgültig manifestiert.

*BGH, Beschluss vom 18.02.2009
- 1 StR 731/08:*

Der mit der Vermögensverfügung unmittelbar eingetretene Vermögensschaden ist durch das Verlustrisiko zum Zeitpunkt der Vermögensverfügung bestimmt. Dies stellt hinsichtlich des Straftatbestands einen endgültigen Schaden dar und nicht nur eine (schadensgleiche) Vermögensgefährdung. Die Höhe des Vermögensnachteils zum Zeitpunkt der Verfügung ist nach wirtschaftlichen Maßstäben zu bewerten.

Umgang im Vorbereitungsstadium



Skimmer

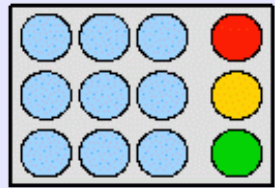
Programme oder **ähnliche Vorrichtungen**, die zur Fälschung von Zahlungskarten geeignet sind



§§ 149 Abs. 1, 152a Abs. 5, 152b Abs. 5 StGB

Geldstrafe oder Freiheitsstrafe bis 5 Jahre

für alle Geräte, die zum Ausspähen der PIN bestimmt sind, gilt, dass sie nicht zum Fälschen von Zahlungskarten dienen, sondern zu dem **Computerbetrug**, der mit dem abschließenden **Cashing** begangen wird



Tastaturaufsatz

Programme, deren Zweck der Computerbetrug ist, das umfasst auch die individuelle Steuerung für die Aufnahme (Tastendruck, Bilder) und deren Speicherung

§ 263a Abs. 3 StGB

Geldstrafe oder Freiheitsstrafe bis 3 Jahre

der Umgang mit den **Geräten** als solche (Hardware) unterliegt keiner Strafbarkeit

keine Strafbarkeit im Vorbereitungsstadium in Bezug auf **Geräte**



Kamera



Dual Use

die **unveränderten Steuerungen** von Mobiltelefonen mit Kamerafunktion und von handelsüblichen Digitalkameras sind als solche nicht strafbar (Dual Use)

keine Strafbarkeit im Vorbereitungsstadium in Bezug auf **handelsübliche Programme**



§ 149 StGB

(1) Wer eine **Fälschung** von Geld oder Wertzeichen vorbereitet, indem er

1. Platten, Formen, Drucksätze, Druckstöcke, Negative, Matrizen, **Computerprogramme oder ähnliche Vorrichtungen**, die ihrer Art nach zur Begehung der Tat geeignet sind,

...

herstellt, sich oder einem anderen **verschafft**, feilhält, **verwahrt** oder einem anderen überläßt, wird, wenn er eine Geldfälschung vorbereitet, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe ... bestraft.

§ 152a Abs. 5 StGB (Wertzeichen)

§ 152b Abs. 5 StGB (Geld)

▶ Verweise auf § 149 StGB

▶ Computerprogramme oder ähnliche Vorrichtungen

▶ geeignet zum Fälschen von Zahlungskarten

▶ Kartenlesegeräte

▶ nicht Kameras

▶ nicht Tastaturaufsätze



§ 202c StGB

(1) Wer eine Straftat nach § 202a oder § 202b **vorbereitet**, indem er

1. **Passwörter** oder sonstige **Sicherungs-codes**, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. **Computerprogramme**, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen **verschafft**, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Vorbereitung des

▶ Ausspähen von Daten (§ 202a StGB)

▶ Abfangen von Daten (§ 202b StGB)



§ 202a StGB

(2) Daten im Sinne des Absatzes 1 sind nur solche, die **elektronisch**, **magnetisch** oder sonst nicht unmittelbar wahrnehmbar **gespeichert** sind oder **übermittelt** werden.

Tastatureingaben

- ▶ kein Ausspähen gespeicherter Daten
- ▶ kein Abfangen „fließender“ Daten
- ▶ sondern manuelle Dateneingabe



Die Daten auf den Magnetstreifen sind nicht durch besondere Sicherungsvorkehrungen geschützt.

Ausspähen der Daten auf dem Magnetstreifen:

- ▶ **früher: ja**
BGH, Urteil vom 10.05.2005 – 3 StR 425/04

- ▶ **jetzt: nein**
BGH, Beschluss vom 06.07.2010
- 4 StR 555/09



§ 263a StGB

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er **Computerprogramme**, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen **verschafft**, feilhält, **verwahrt** oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Tastaturaufsätze und Kameras

- ▶ nicht der Umgang mit dem Gerät als solches ist strafbar
- ▶ sondern nur der Umgang mit einem Computerprogramm
- ▶ Steuerung zum Aufnehmen und Speichern



Allein die Eignung eines Computerprogrammes zur Begehung von Computerstraftaten genügt zur Erfüllung des objektiven Tatbestands des § 202c Abs. 1 Nr. 2 StGB nicht aus.

Das ist übertragbar auf § 263a StGB.

Dual Use ist strafneutral

**BVerfG, Beschluss vom 18.05.2009
- 2 BvR 2233/07, 1151/08, 1524/08**

- ▶ handelsübliche Digitalkamera**
- ▶ Mobiltelefon mit Kamerafunktion**
 - ▶ sind keine Computerprogramme**
 - ▶ auch nicht, wenn zusätzliche Akkus verbaut werden**
 - ▶ sondern nur dann, wenn die Steuerung verändert wird**



§ 303b StGB

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
 2. Daten (§ 202a Abs. 2) in der **Absicht, einem anderen Nachteil zuzufügen**, eingibt oder übermittelt
- ...
- wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

...

(5) Für die **Vorbereitung** einer Straftat nach Absatz 1 **gilt § 202c entsprechend**.

§ 202c Abs. 1 Nr. 1 StGB:

... **Passwörter** oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen ...

▶ PIN

- ▶ Das Ausspähen von PIN mit Dual Use-Geräten ist jedenfalls dann strafbar, wenn mehrere PIN ausgespäht wurden

Auspähen - Skimming im engeren Sinne



Skimmer

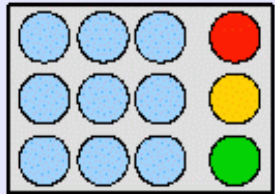
Programme oder **ähnliche Vorrichtungen**, die zur Fälschung von Zahlungskarten geeignet sind



§ 149 Abs. 1, §§ 152a Abs. 5, 152b Abs. 5 StGB



Geldstrafe oder Freiheitsstrafe bis **5 Jahre**



Tastaturaufsatz

Programme, deren Zweck der Computerbetrug ist



§ 263a Abs. 3 StGB



Geldstrafe oder Freiheitsstrafe bis **3 Jahre**

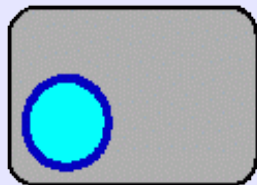
mit dem abschließenden Cashing ist auch eine Computersabotage gemäß § 303b Abs. 1 Nr. 2 StGB verbunden, weil dabei Daten in der Absicht eingegeben werden, einen anderen zu schädigen

das führt gemäß § 303b Abs. 5 StGB zur Strafbarkeit im Vorbereitungsstadium nach Maßgabe von § 202c StGB

danach sind die nachweislich aufgezeichneten PIN **Passwörter** im Sinne von § 202c Abs. 1 Nr. 1 StGB, die sich die Täter verschafft haben

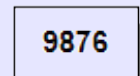


Kamera



Dual Use

nachweislich ausgespähte **PIN** (= Passwörter)



§ 303b Abs.5 i.V.m. § 202c Abs. 1 StGB



Geldstrafe oder Freiheitsstrafe bis **1 Jahr**



Skimming im engeren Sinne

- ▶ **Strafbarkeit wie im Vorbereitungsstadium**
- ▶ **noch kein Versuch des Fälschens**
- ▶ **ausgespähte Daten müssen erst synchronisiert und**
- ▶ **übermittelt werden**



§ 25 StGB

(2) Begehen mehrere die Straftat gemeinschaftlich, so wird jeder als Täter bestraft (Mittäter).

- ▶ **der Skimmer muss sich die Tatvollendung durch den Casher zurechnen lassen, wenn sie in einer arbeitsteiligen Täterstruktur aufgrund eines gemeinsamen Tatplanes zusammen arbeiten**
- ▶ **der Skimmer ist dann Mittäter und wird wie der Casher bestraft**
- ▶ **wenn das Cashing erfolgreich war**

**BGH, Beschluss vom 13.01.2010
- 5 StR 506/09, Rn. 5:**

Mittäterschaft liegt ... dann vor, wenn ein Tatbeteiligter nicht bloß fremdes Tun fördern will, sondern seinen Beitrag als Teil der Tätigkeit des anderen und umgekehrt dessen Tun als Ergänzung seines eigenen Tatanteils will. ... Wesentliche Anhaltspunkte hierfür können gefunden werden im Grad des eigenen Interesses am Erfolg der Tat, im Umfang der Tatbeteiligung und in der Tatherrschaft oder wenigstens im Willen zur Tatherrschaft, so dass Durchführung und Ausgang der Tat maßgeblich von seinem Willen abhängen.



Beteiligungsmodell

täterschaftliche Verabredung:

„Wir wollen Kartendaten ausspähen und anschließend zum Cashing einsetzen.“

- ▶ der Vorsatz umfasst die eigenhändige Tatausführung

mittäterschaftliche Verabredung:

„Wir wollen Geld damit verdienen, dass wir wiederholt Kundendaten ausspähen, um diese an unsere Leute weiter zu geben, die damit das Cashing betreiben.“

- ▶ arbeitsteilige Mittäterabrede

- ▶ gewerbsmäßiges Handeln
- ▶ Handeln als Bande
- ▶ Verabredung zu einem Verbrechen

Verabredung mit Absatzabsicht:

„Wir wollen Geld damit verdienen, dass wir wiederholt Kundendaten ausspähen, um diese an noch unbestimmte Interessenten zu verkaufen.“

- ▶ „Datenhändler“

- ▶ Beihilfe zum Cashing
- ▶ keine Verbrechensabrede, weil das Verbrechen im Cashing besteht



BGH, Beschluss vom 01.09.2009
- 3 StR 601/08, Rn. 5:

Gewerbsmäßig handelt, wer sich durch wiederholte Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang und einiger Dauer verschaffen will. Liegt diese Absicht vor, ist bereits die erste Tat als gewerbsmäßig begangen einzustufen, auch wenn es entgegen den ursprünglichen Intentionen des Täters zu weiteren Taten nicht kommt. ... Erforderlich ist dabei stets, dass sich seine Wiederholungsabsicht auf dasjenige Delikt bezieht, dessen Tatbestand durch das Merkmal der Gewerbsmäßigkeit qualifiziert ist.

BGH, Urteil vom 03.12.2009
- 3 StR 277/09, S.18:

Eine **Bande** ist danach gekennzeichnet durch den Zusammenschluss von mindestens drei Personen, die sich mit dem Willen verbunden haben, künftig für eine gewisse Dauer mehrere selbstständige, im Einzelnen noch ungewisse Straftaten zu begehen; ein gefestigter Bandenwille und ein Tätigwerden in einem übergeordneten Bandeninteresse sind demgegenüber nicht mehr erforderlich. ... Die Mitgliedschaft in einer Bande ist ... kein strafbegründendes, sondern ein strafschärfendes Merkmal.



Deliktische Einheit

▶ Fälschung mehrerer Karten

BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn. 13

BGH, Beschluss vom 23.06.2010 – 2 StR 243/10, Rn. 3.

▶ Fälschen und Gebrauch

BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn. 17

BGH, Beschluss vom 26.01.2005 - 2 StR 516/04

BGH, Beschluss vom 07.03.2008 - 2 StR 44/08

▶ Ausspähen

▶ Cashing

BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 8.



Subjektive Faktoren

- ▶ **Fälschung (§ 149 StGB)**
- ▶ **Ausspähen**
- ▶ **Cashing**
- ▶ **arbeitsteilige Zusammenarbeit**
- ▶ **Gewerbsmäßigkeit**
- ▶ **Bande**
- ▶ **sonst Ordnungswidrigkeit nach § 127 OWiG**



Leitbild des Gesetzgebers

- ▶ Fälschung oder Gebrauch nur eines „Stück“ Geldes (§ 146 StGB)
- ▶ ... **einer** Zahlungskarte mit Garantiefunktion
- ▶ das umfasst auch die Verfälschung nur **eines** Magnetstreifens einer Zahlungskarte
- ▶ Verbrechen, 1 bis 15 Jahre Freiheitsstrafe
- ▶ Gleichstellung in § 152b Abs. 1 StGB, 1 bis 10 Jahre
- ▶ BGH, Urteil vom 21.09.2000 - 4 StR 284/00
- ▶ aber: minder schwerer Fall bei geringer Stückzahl
BGH, Urteil vom 21.09.2000
- 4 StR 284/00, Rn. 12.

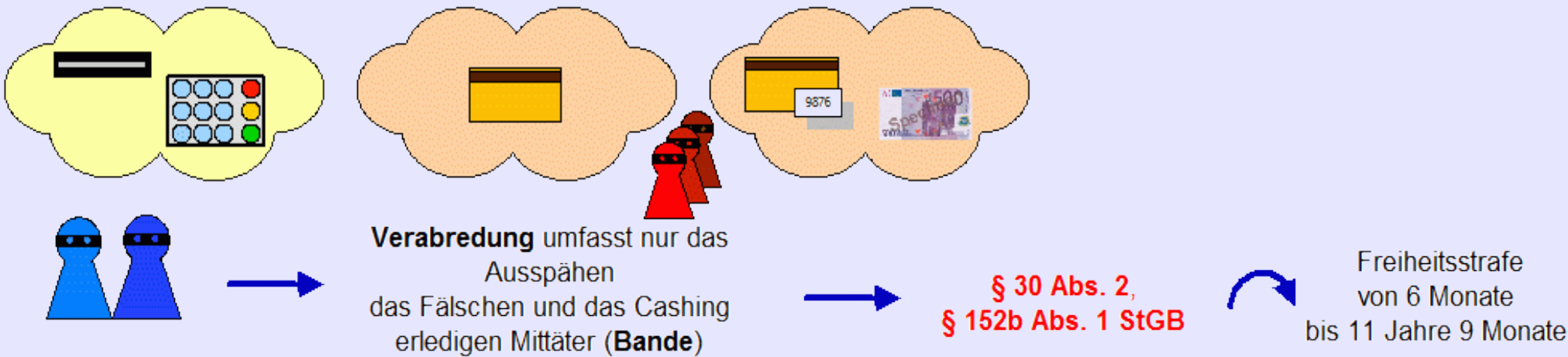
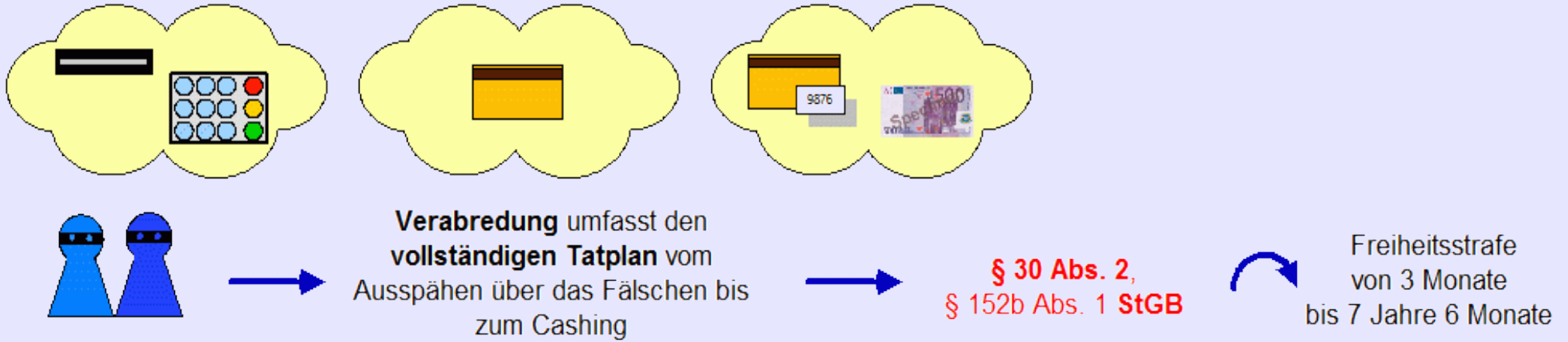


§ 30 StGB

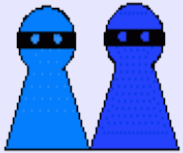
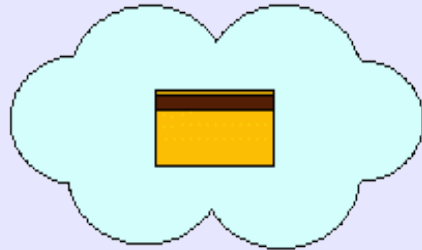
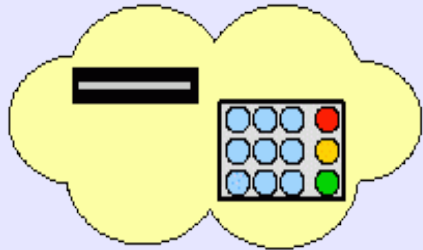
(1) Wer einen anderen zu bestimmen versucht, ein Verbrechen zu begehen oder zu ihm anzustiften, wird nach den Vorschriften über den Versuch des Verbrechens bestraft. Jedoch ist die Strafe nach § 49 Abs. 1 zu mildern. § 23 Abs. 3 gilt entsprechend.

(2) Ebenso wird bestraft, wer sich bereit erklärt, wer das Erbieten eines anderen annimmt oder **wer mit einem anderen verabredet, ein Verbrechen zu begehen oder zu ihm anzustiften.**

Verabredung zu einem Verbrechen



Verabredung zu einem Verbrechen



Verabredung umfasst nur das
Ausspähen
die Daten sollen an interessierte
Casher verkauft werden



keine Strafbarkeit wegen § 30 StGB bei
den Gehilfen des Verbrechens



Beihilfe zu
§ 152b Abs. 1 StGB



Freiheitsstrafe
von 3 Monate
bis 7 Jahre 6 Monate



Strafverfolgung

- ▶ **Zufall**
- ▶ **Festnahme beim Skimming**
- ▶ **Anfangsverdacht:**
 - ▶ **Umgang mit Kartenlesegeräten**
 - ▶ **Verbrechensabrede**
 - ▶ **Gewerbsmäßigkeit**
 - ▶ **ggf. Bande**
- ▶ **Fingerspuren**
- ▶ **DNA-Spuren**
- ▶ **Kameraüberwachung**
- ▶ **Journal aus dem GAA (POC)**
- ▶ **Testkarten**
- ▶ **Daten von den betroffenen Kunden**
- ▶ **Zeugen**
- ▶ **gleiche Bauarten**

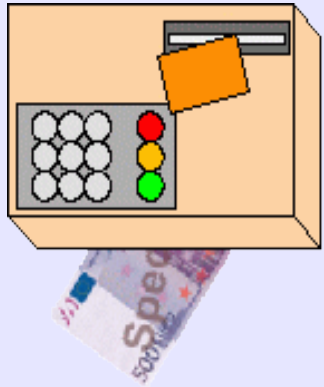
Kriminalistische Erfahrungen

- ▶ **bevorzugte Zeiten**
- ▶ **häufig Dreier-Gruppen**
- ▶ **bevorzugte nationale Herkunft**
- ▶ **häufig Abstimmung per Handy**
- ▶ **Unterkunft bei Landsleuten oder in preisgünstigen Hotels**
- ▶ **große Fahrstrecken mit geliehenen Fahrzeugen und Mietwagen**
- ▶ **häufig direkte An- und Abreise**



Cashing-Daten

- ▶ **zusammengefasste Daten reichen für den Tatnachweis**
- ▶ **die Vernehmung aller Geschädigten ist nicht nötig**
- ▶ **auch die Daten vom gescheitertem Cashing sind nötig (Gebrauch und versuchter Computerbetrug)**



16.08.10; 01:23	400,00 - 0 -
16.08.10; 01:24	400,00 - 0 -
16.08.10; 01:26	400,00 - 51 -
16.08.10; 01:27	200,00 - 51 -
16.08.10; 01:28	100,00 - 0 -
16.08.10; 01:29	50,00 - 0 -
16.08.10; 01:30	50,00 - 51 -

Auswertung von Cashing-Daten

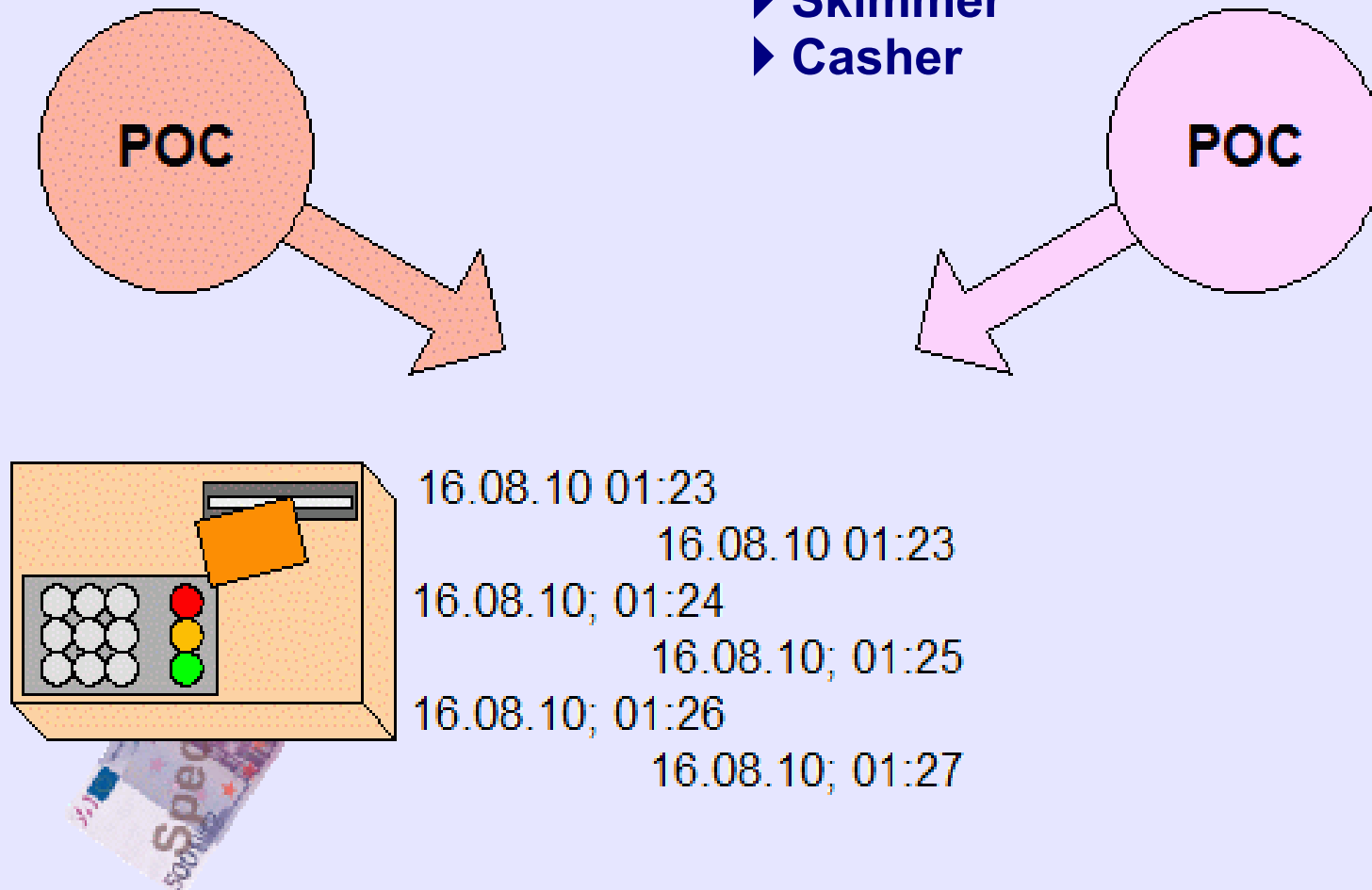
- ▶ **Zeitabstand zwischen Skimming und Cashing**
- ▶ **Orte des Cashings**
- ▶ **Professionalität**
- ▶ **Gruppenstruktur**



Auswertung von Cashing-Daten

▶ Gruppenstrukturen

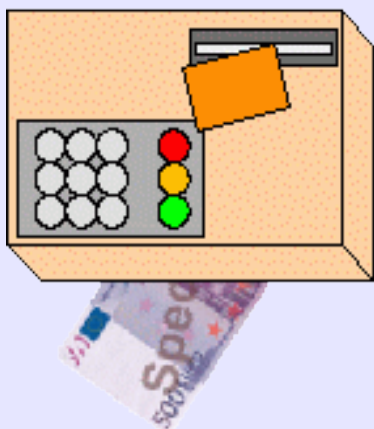
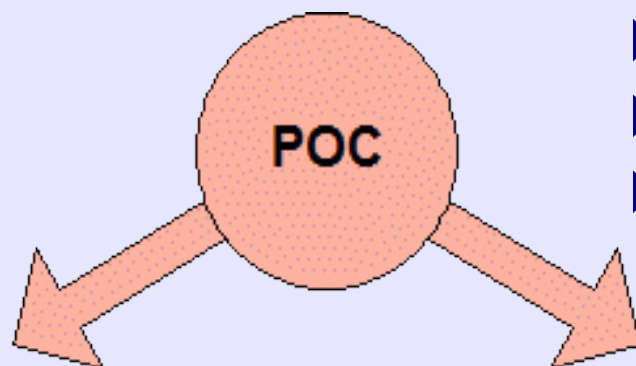
- ▶ Skimmer
- ▶ Casher





Auswertung von Cashing-Daten

- ▶ Tag, Uhrzeit (Zeitstempel)
- ▶ Ort
- ▶ Terminalnummer
- ▶ Auszahlungsbetrag
- ▶ Gebühr
- ▶ Genehmigungscode



16.08.10 01:23

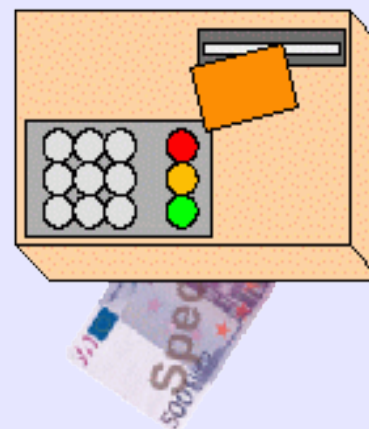
16.08.10; 01:24

16.08.10; 01:26

16.08.10 01:23

16.08.10; 01:23

16.08.10; 01:25





Strategische Strafverfolgung

- ▶ **StA Wuppertal**
Hersteller von Skimming-Geräten
und Personenumfeld
- ▶ **BKA und LKÄ**
internationale polizeiliche
Zusammenarbeit
 - ▶ **selten greifbare Ermittlungshilfe**
 - ▶ **kaum erkennbare Strafverfolgung**
in den Herkunftsländern
 - ▶ **zögerliche Rechtshilfe**
- ▶ **schwierige und ungeklärte**
Rechtsfragen auch für Polizei und
Staatsanwaltschaft
- ▶ **Zeitdruck - Haftsachen**
- ▶ **örtliche Zuständigkeitsgrenzen**
- ▶ **geschlossene Gruppen**
Sprache, Ethnie, Identität
- ▶ **keine Aufklärungsbereitschaft**
bei den Tätern
- ▶ **und in ihrem Umfeld**
(trotz § 138 Abs. 1 Nr. 4 StGB)
- ▶ **keine proaktive**
Bekämpfungsstrategie



Zusammenarbeit mit der Finanzwirtschaft

- ▶ **EKS**

- ▶ **Bank im Einzelfall**
 - ▶ **Journal**
 - ▶ **Kamerabilder**
 - ▶ **Vorsicht beim Abbau**
 - ▶ **Auskünfte über die Kunden**

- ▶ **strategische Zusammenarbeit**
 - ▶ **Alarmkette**
 - ▶ **Ansprechpartner**
 - ▶ **technische Hilfe**
 - ▶ **aktive Bekämpfung**



Maßnahmen der Finanzwirtschaft

- ▶ flächendeckender Einsatz des EMV-Chips
- ▶ Ausweitung der MM-Prüfung
 - ▶ Einzelhandel, Tankstellen
 - ▶ Ausland
- ▶ Alarmfunktionen
 - ▶ häufiger Einsatz derselben Karte
 - ▶ häufige Meldungen desselben Terminals
 - ▶ zur Nachtzeit
 - ▶ am Wochenende
 - ▶ im Ausland
 - ▶ ohne Prüfung des EMV-Chips
- ▶ Voreinstellungen
 - ▶ komfortable Einstellungen durch den Kunden nach dessen Bedarf
- ▶ iTAN für Geldauszahlungen
- ▶ Schulung von Mitarbeitern
- ▶ Verbandsarbeit bei der Internationalen Zusammenarbeit



Trends bei den Tätern

- ▶ **Arbeitsteiligkeit**
- ▶ **Spezialisierung**
 - ▶ **autonome Skimmer- und Casher-Gruppen (Operating Groups)**
- ▶ **Cashing im außereuropäischen Ausland**
- ▶ **kein Schadensausgleich**
- ▶ **Nutzung aller technischen Hilfsmittel**
- ▶ **Verschmelzung verschiedener Formen der Cybercrime**
- ▶ **IT-Standards für Geldautomaten und Rechenzentren**



Mit dem Bauch gefühlt

- ▶ **wirksame Maßnahmen**
 - ▶ **EMV-Chip**
 - ▶ **moduliertes Merkmal – MM**
 - ▶ **iTAN beim Onlinebanking**

- ▶ **zunehmende Verunsicherung bei den Kunden**
 - ▶ **Schaden ist eingetreten, auch wenn er später ausgeglichen wird**
 - ▶ **Kosten werden erhoben, ohne dass sich Wirkungen zeigen**

- ▶ **Krisenmanagement:**
 - ▶ **Öffentlichkeitsarbeit**
 - ▶ **Problembewusstsein**
 - ▶ **Verantwortung zeigen**

- ▶ **Laufereien**
- ▶ **Strafanzeige bei der Polizei**
- ▶ **gleichzeitig werden die Geldanlagen immer unattraktiver**



Dieter Kochheim
Skimming
Hintergründe und Strafrecht

Vielen Dank für Ihre Aufmerksamkeit !

Arbeitspapier Skimming bei cyberfahnder.de

The screenshot shows the Cyberfahnder website interface. At the top, there is a search bar and navigation tabs for Cybercrime, Ermittlungen, TK & Internet, Literatur, Gameback, Newsletter, Intern, and Impressum. Below the navigation, there is a main content area with several article teasers. On the left, there is a sidebar with more article teasers. On the right, there is a section for 'Meldungen' (Reports) with a list of recent reports. The website has a clean, professional layout with a blue and white color scheme.