



Bundeskriminalamt

# IUK-KRIMINALITÄT Bundeslagebild 2009

- Pressefreie Kurzfassung -









## 2. DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

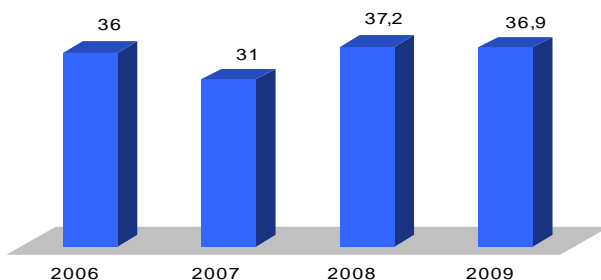
### 2.1 Polizeiliche Kriminalstatistik

Im Jahr 2009 wurden in der PKS 50.254 Fälle der IuK-Kriminalität im engeren Sinne registriert. Dies entspricht einem Anstieg von rund 33 % (12.354 Fälle) gegenüber dem Vorjahr. Wie in den Jahren zuvor stellen dabei die Fälle des "Computerbetruges" mit einem Anteil von rund 46 % (22.963 Fälle) die mit Abstand größte Fallgruppe; das Fallaufkommen in diesem Bereich ist gegenüber dem Jahr 2008 um 35 % gestiegen.

Straftaten (-Gruppen)	Jahr 2009	Jahr 2008	Veränderung -absolut-	Veränderung -in %-
Computerbetrug	22.963	17.006	5.957	35,0
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	7.205	5.244	1.961	37,4
Datenfälschung, Täuschung im Rechtsverkehr bei Datenverarbeitung	6.319	5.716	603	10,6
Datenveränderung / Computersabotage	2.276	2.207	69	3,1
Ausspähen/Abfangen von Daten	11.491	7.727	3.764	48,7
<b>IuK-Kriminalität im engeren Sinne</b>	<b>50.254</b>	<b>37.900</b>	<b>12.354</b>	<b>32,6</b>

Im Gegensatz zu den Fallzahlen zeigt sich bei den registrierten Schäden ein leichter Rückgang gegenüber dem Jahr 2008. So beläuft sich der im Jahr 2009 registrierte Schaden aller in der PKS mit Schadenssummen erfassten Delikte der IuK-Kriminalität im engeren Sinne auf 36,9 Millionen Euro und ist somit gegenüber dem Vorjahr (37,2 Mio. Euro) um rund 1 % gefallen. Die Fallzahlen der PKS alleine spiegeln jedoch nicht die tatsächliche Lage im Bereich der IuK-Kriminalität wider.

#### Schäden der IuK im engeren Sinn (in Mio. Euro)



Einzelne bzw. besonders relevante Phänomene im Bereich der IuK-Kriminalität, wie z. B. "Phishing" oder „Bot-Netze“<sup>1</sup>, werden in der PKS nicht erfasst. Da sich diese Phänomene in unterschiedliche Tathandlungen gliedern, erfolgt keine Erfassung unter einer einheitlichen PKS-Schlüsselzahl, wodurch statistische Angaben auf Basis der in der PKS erfassten Daten nicht möglich sind.

<sup>1</sup> Ein „Bot-Netz“ ist ein ferngesteuertes Netz zahlreicher, über einen Schadcode infizierter Computer, die ohne Wissen ihres Besitzers gesteuert werden.







Wie bereits im vergangenen Jahr wurden wiederum verschiedene Massenangriffe auf Webseiten registriert, in deren Verlauf die Webseiten ohne Wissen der Betreiber entsprechend mit dem Ziel manipuliert worden sind, deren Besucher zu infizieren. Darunter befanden sich auch viele renommierte Webseiten mit hohen Besucherzahlen. Der Grund für die Nutzung dieses Modus Operandi besteht darin, dass viele Internetnutzer bei ungewollt erhaltenen E-Mails zunehmend skeptisch reagieren und vorsichtiger geworden sind.

Zudem versuchen Hacker gezielt, renommierte Webseiten mit hohen Besucherzahlen anzugreifen. In der Folge bietet auch die ausschließliche Nutzung von bekannten bzw. vertrauenswürdigen Webseiten keinen ausreichenden Schutz, auch wenn viele Hersteller von Antivirenprodukten versuchen, die Bedrohung durch die Weiterentwicklung ihrer Produkte zu minimieren.

### 2.2.2 Carding

Beim sog. Carding erfolgen in aller Regel keine direkten online-Vermögensverfügungen anhand ausgespähter oder entwendeter Kreditkartendaten. Die Kreditkartendaten werden in diesen Fällen missbräuchlich dazu genutzt, um damit zunächst online Waren zu kaufen, die anschließend z. B. über eBay oder eigene (scheinbar legale) Webshops weiterverkauft werden.

Bevorzugt wird insbesondere das sog. "Carding on Demand". Hierbei teilt ein Krimineller (der Kunde) einem anderen, der sich auf das Carden spezialisiert hat (dem Carder) mit, welche Artikel er haben möchte und wohin die Waren geliefert werden sollen.

Nachdem der Kunde dem Carder diese Information sowie abgegriffene, valide Kreditkartendetails mitgeteilt hat, beginnt das Carding. Die besondere Fähigkeit des Carders liegt darin, dass er in der Lage ist, Webshops bzw. Onlineportale zu finden, die

- ⇒ den vom Kunden gewünschten Artikel führen,
- ⇒ die vom Kunden bereitgestellte Kreditkarte akzeptieren sowie
- ⇒ eine Lieferung an die vom Kunden benannte Adresse durchführen.

Teilweise werden hierbei durch den Carder zunächst eigene, sog. "Reshipper" (Personen, die die Ware weiterleiten), eingesetzt, an welche die Ware zunächst versandt wird und die den Schlussversand an die vom Kunden benannte Adresse gewährleisten. Der Carder erhält hierbei in aller Regel zwischen 25 % und 40 % des Realpreises des gecardeten Artikels als Provision. Der Kunde verwendet die widerrechtlich erworbene Ware dann für eigene Zwecke oder veräußert diese (in der Regel) über das Internet weiter.

Über Webportale und Foren der Underground Economy findet mittlerweile ein schwunghafter Handel mit widerrechtlich erlangten Kreditkartendaten statt. Durch die ständige und massenhafte Verfügbarkeit von validen Kreditkartendaten entwickelt sich der Handel und Einsatz illegal erlangter Kreditkartendaten zu einem Massenphänomen.

### 2.2.3 Bot-Netze

Wie in den Jahren zuvor bedienten sich die Täter auch im Jahr 2009 bei der Tatausführung sogenannter "Bot-Netze", d. h. ferngesteuerter Netze zahlreicher, über einen Schadcode infizierter Computer, die ohne Wissen ihrer Besitzer gesteuert werden. Dies geschieht über sog. "Command- & Control-Server" (C&C-Server). Der physische Standort sowie die Identität der Straftäter sind dadurch nicht zu ermitteln.

Die Aufspielung des Schadcodes erfolgt analog zum Phishing. Einmal installiert, gibt diese Schadsoftware dem Täter einen nahezu vollständigen Zugriff auf den Computer des Opfers. Schätzungen gehen von weltweit mehr als 12 Millionen infizierten Computern aus, welche in verschiedenen „Bot-Netzen“ verbunden sind<sup>4</sup>. Die Anzahl der täglich in Deutschland eingesetzten, ferngesteuerten "Zombie-PC" soll bei durchschnittlich 350.000, in Spitzenzeiten bei bis zu 700.000 liegen.<sup>5</sup>

Die meisten dieser infizierten "Zombie-PC" leiten aber nicht nur die persönlichen Daten des Besitzers an die Täter weiter, sondern dienen den Straftätern auch als Werkzeug für weitere Straftaten, z. B. zum weiteren Verteilen von Schadsoftware, zum massenhaften, anonymen Versand von Spam-Mails oder zum Angriff von Webseiten.

„Bot-Netze“ und ihre Kapazitäten stellen nach wie vor eine weltweit lukrative Handelsware dar. Sogenannte "Herder" (Hirten) vermieten oder verleasen die Bots. Für Staat und Wirtschaft besonders gefährlich stellen sich sog. "DDoS-Attacken"<sup>6</sup> dar. Dabei handelt es sich um einen gezielten Angriff auf die Server z. B. eines Unternehmens. Die Server werden mit einer Flut von Anfragen bombardiert; unter Umständen ist das System dann nicht mehr in der Lage, diese Flut zu bewältigen und bricht im schlimmsten Fall zusammen. Gerade im wettbewerbsintensiven Marktsegment Internet können Nichterreichbarkeiten von Vertriebsportalen zu schwerwiegenden wirtschaftlichen Nachteilen führen. In diesem Zusammenhang sind „Bot-Netze“ auch als Infrastruktur für tradierte Kriminalitätsformen, wie z. B. Erpressungen, zu verstehen.

---

<sup>4</sup> Sicherheitsdienstleister McAfee 2009

<sup>5</sup> Sicherheitsdienstleister GData 2009

<sup>6</sup> Bei DDOS (distributed Denial of Service)-Angriffen rufen alle in einem Bot-Netz zusammengeschlossenen Zombie-PC auf Befehl des Botmasters innerhalb kürzester Abstände immer wieder z. B. eine nicht existente Seite auf den Webservern der angegriffenen Firma auf. Diese Seitenaufrufe werden so lange fortgesetzt, bis die Webserver unter der Last der Anfragen zusammenbrechen und damit ihren Service verweigern (Denial of Service), so dass die jeweilige Firmenpräsenz damit nicht mehr über das Internet erreichbar ist.

