IuK-Strafrecht

IuK-Strafrecht

Geschichte der Cybercrime

Erscheinungsformen, Erklärungen und Bewertungen

IuK-Strafrecht

Teil 1

die wichtigsten Strafvorschriften

Hackerstrafrecht

© Dieter Kochheim, 12.05.12

IuK-Strafrecht, Überblick 1

strafrechtlicher Datenschutz

202a I	Ausspähen von D.
202b	Abfangen von D.
202c	Hackerparagraph
17 UWG	Geschäfts- / Betriebgeheimnis
44 BDSG	personen-bezogene D.
108b I Nr. 1 UrhG	Cracking, Zugangsschutz

Daten- und Datenverarbeitungsintegrität

303a	Datenveränderung
303b I	Computersabotage
303b II	schwere Comp.
303b IV	besonders schw. Fall der schweren Computersabotage
303a III	Vorbereitungshandl.
303b V	
303a II	Versuch
303b III	

© Dieter Kochheim, 12.05.12

IuK-Strafrecht, Überblick 2

Computerbetrug

263a	Computerbetrug
263 III	bes. schw. Fall
263 V	Bande und gewm. Handeln
263a III	Vorbereitungsh.
263 II	Versuch

Schutz des Rechtsverkehrs

269	Fälschung beweis-erheblicher Daten
267 III	bes. schw. Fall
267 IV	Bande und gewm. Handeln
269 II	Versuch
268	Fälsch. techn. Aufz.
270	Täuschung im Rechtsverkehr ...
274 I Nr. 2	Urkundenunter-drückung

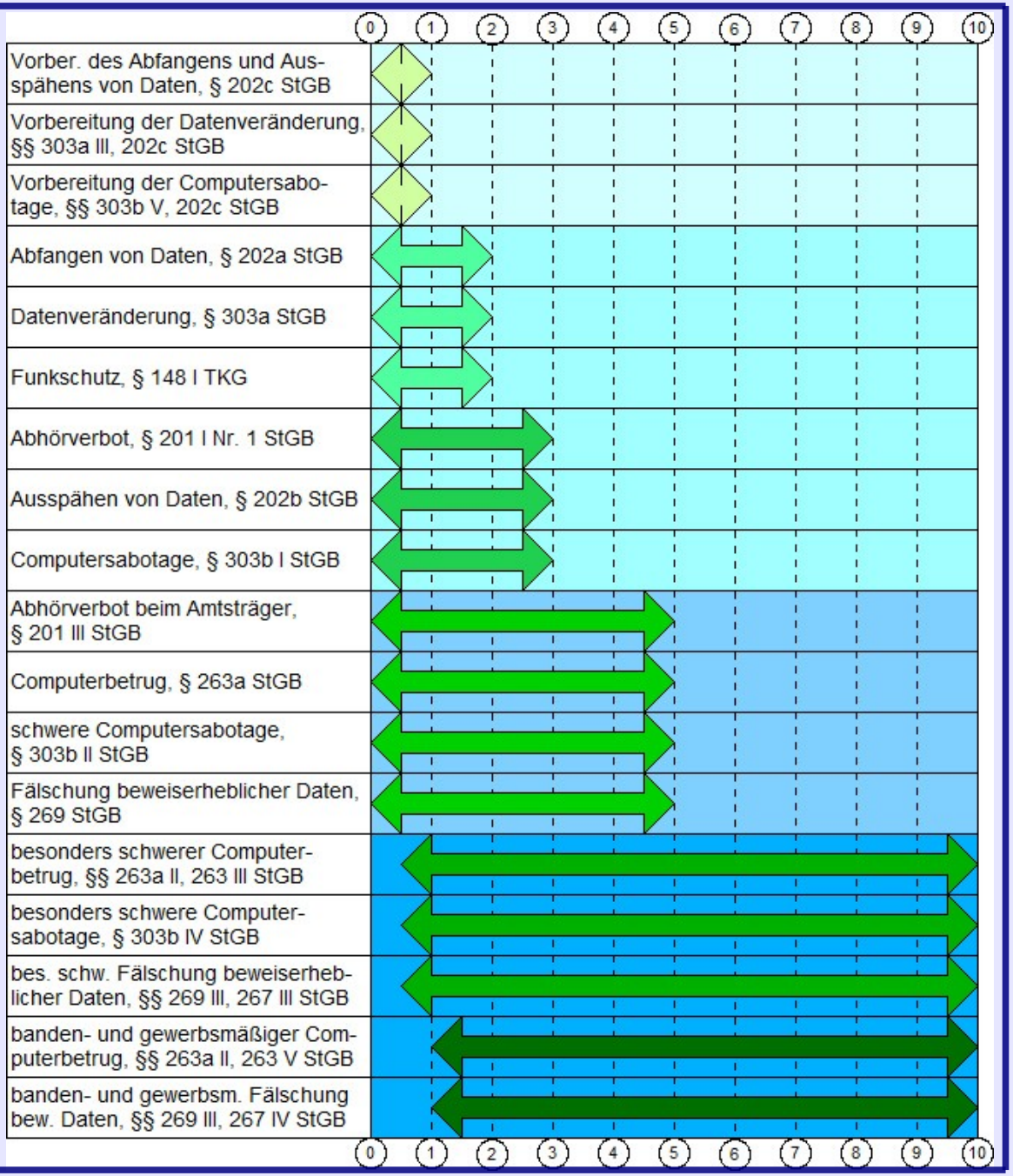
© Dieter Kochheim, 12.05.12

Schwere der Kriminalität

einfache Kriminalität

mittlere Kriminalität

schwere Kriminalität



© Dieter Kochheim, 12.05.12

im engeren und weiteren Sinne

Computer-Strafrecht **Internet-Strafrecht**	**IuK-Strafrecht**
	bezieht sich auf die einheitliche Verantwortung und Administration in einem örtlichen Netz **Local Area Network – LAN** **auch: WLAN**
im engeren Sinne	**unmittelbarer Missbrauch der Informations- und Kommunikationstechnik** **Hacking, Malware, Botnetze**
im weiteren Sinne („besondere Kenntnisse“)	**Nutzung der Technik als Hilfsmittel** **Beleidigung, Erpressung, Betrug**

© Dieter Kochheim, 12.05.12

Datendefinition

202a II Datendefinition

Daten ... sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

gespeicherte Daten - Ausspähen
übermittelte Daten - Abfangen

Dateneingabe fehlt

Datenveränderung
Computersabotage

Hackerstrafrecht (2007):
Der Gesetzgeber hatte vor allem das Eindringen, Ausspähen und Sabotieren von technischen Anlagen vor Augen

© Dieter Kochheim, 12.05.12

Ausspähen und Abfangen von Daten

202a I Ausspähen von Daten

Wer *unbefugt* sich ... Zugang zu Daten, die *nicht für ihn bestimmt* und die gegen unberechtigten Zugang *besonders gesichert* sind, unter *Überwindung der Zugangssicherung* verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

202b Abfangen von Daten

Wer *unbefugt* sich ... unter Anwendung von *technischen Mitteln nicht für ihn bestimmte* Daten ... aus einer *nichtöffentlichen Datenübermittlung* oder aus der elektromagnetischen *Abstrahlung* einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

© Dieter Kochheim, 12.05.12

Systematik

Verletzung des persönlichen Lebens- und Geheimbereiches

201 Grundtatbestand

verbotener *Technikeinsatz*:
- Aufnahme auf Tonträger
- Abspielgerät
- Abhörgerät

inhaltlicher Schutz:
nichtöffentlich gesprochene Worte

Funkschutz

148 I Nr. 1 TKG

Abhör- und Weitergabeverbot betr. *Meldung*
Inhalte der Kommunikation

unvollständiger Schutz:
Amateurfunk ist nicht geschützt

weite Teile der Frequenzbänder für WLAN und Bluetooth liegen im Amateurfunkbereich

© Dieter Kochheim, 12.05.12

Daten und Geheimnisse

Besonderer Schutz der Telekommunikationsdaten – 206

Art 10 GG TK-Geheimnis

auch wegen der Verkehrsdaten

3 Nr. 30 TKG
… die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden

… umfasst die TK insgesamt
... Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung)
... Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten)
… auf der Übertragungsstrecke oder am Endgerät
… auch die Umstände der Telekommunikation …
BVerfG, Urt. 27.02.2008 – 1 BvR 370/07

… endet sobald die Nachricht beim Empfänger angekommen und der Übertragungsvorgang beendet ist.
BVerfG, B. 13.11.2010 – 2 BvR 1124, Rn 13

© Dieter Kochheim, 12.05.12

strafrechtlicher Datenschutz

- Geheimnisse als solche werden nicht gefordert
- nichtöffentliche Daten
- mit einem Aussagegehalt, der über punktuelle Aspekte des persönlichen Lebensbereiches hinaus geht
- nicht für den Späher bestimmt
- beim Ausspähen: besondere Sicherung

  BGH, B. 14.01.2010 – 4 StR 93/09, S. 4 (Skimming)
- das entfällt beim Abfangen
- TK-Geheimnis und
  Schutz der Integrität informationstechnischer Systeme:
  Umfasst auch Verkehrsdaten, wenn sie nicht für den Späher bestimmt und nicht öffentlich sind

© Dieter Kochheim, 12.05.12

öffentliche Daten vom Browser

Webbrowser übermitteln regelmäßig Angaben über

- Art und Version des Browsers
- das Betriebssystem
- die Ländereinstellungen
- den Zugangsprovider

Diese Angaben sind öffentlich und unterliegen nicht dem strafrechtlichen Datenschutz

obwohl sie mehr als punktuelle Auskünfte über den Anwender geben

mögliche Rückschlüsse

- Aktualität
- regelmäßige Updates
- Herkunft / Region des Anwenders
- seine Kenntnisse (Linux)

Social Engineering

© Dieter Kochheim, 12.05.12

Schutz bei der Übertragung

Fischer (aA Graf):
Verschlüsselung ist nicht zwingend

Verkehrsdaten sind nur für den Zugangsprovider und die Netzbetreiber bestimmt

nicht für die Allgemeinheit

Kochheim:
Frage nach dem Ereignishorizont bei

- **Webservern**
- **Routern**
- **Mailservern**

Oberfläche ist öffentlich
Konfiguration ist geheim

© Dieter Kochheim, 12.05.12

Hackerparagraph

202c Hackerparagraph

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

Dual Use

Tatobjekt des § 202c Abs. 1 Nr. 2 StGB kann nur ein Programm sein, dessen Zweck die Begehung einer Straftat nach § 202a StGB ... oder § 202b StGB ... ist. Danach muss das Programm mit der Absicht entwickelt oder modifiziert worden sein, es zur Begehung der genannten Straftaten einzusetzen. Diese Absicht muss sich ferner objektiv manifestiert haben.

BVerfG, B. 18.05.2009 – 2 BVR 2233/07, Rn 61

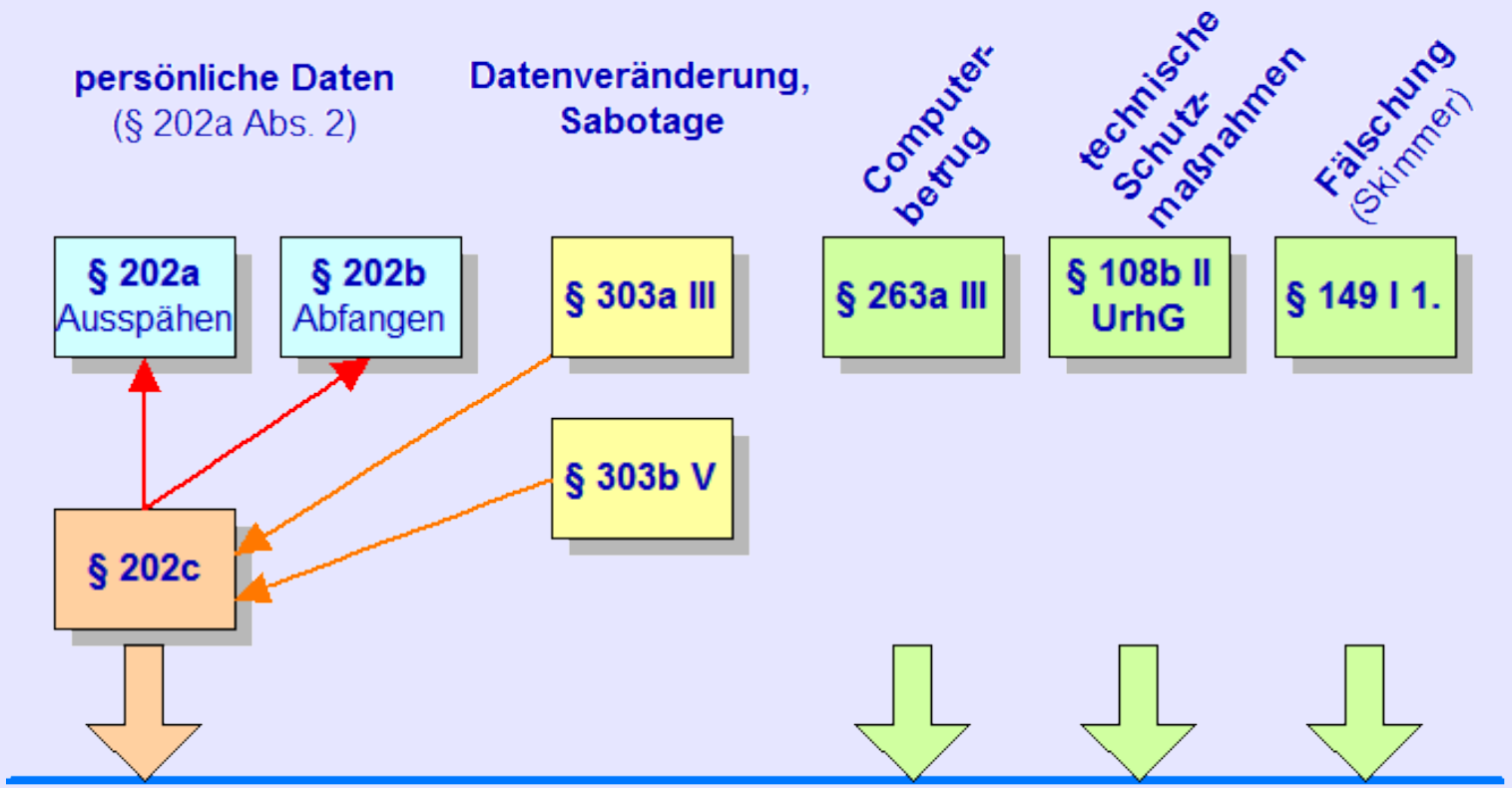
© Dieter Kochheim, 12.05.12

strafbare Vorbereitungshandlungen

Skimmer	**152a V, 152b V i.V.m. 149 I Nr. 1**
Computerbetrug	**263a III** ▸ **nur wegen Computerprogramme** ▸ **kein Hardwareverbot** ▸ **unklar: „Werktiefe“**
Computersabotage	**303a III, 303b V i.V.m. 202c**

© Dieter Kochheim, 12.05.12

strafbare Vorbereitungshandlungen



© Dieter Kochheim, 12.05.12

Exkurs: Datenhehlerei

Datenhehlerei als solche ist nicht strafbar

begrenzter Schutz durch

202c I Nr. 1	**Passwörter, Zugangscodes**
17 UWG	**Betriebs- / Geschäftsgeheimnisse**
44 BDSG	**personenbezogene Daten** **▸ Strafantrag des Datenschutzbeauftragten** **▸ kein öffentliches Interesse** **▸ Freiheitsstrafe bis 2 Jahre**
108b I Nr. 1 UrhG	**Umgehungsschutz – Cracking**

© Dieter Kochheim, 12.05.12

Datenveränderung

Datenveränderung – 303a I

Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

systematischer Hintergrund:

Sachbeschädigung

- **gibt es eine Schwelle?**
- **gilt der Schutz auch für wiederherstellbare Daten?**

© Dieter Kochheim, 12.05.12

Computersabotage

Computersabotage – 303b

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 oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,
wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

neue Fassung seit 2007

Schutz auch für private IT,

- **wenn sie von wesentlicher Bedeutung und**
- **die Störung erheblich ist**
- **Bagatelltechnik ist ausgeschlosen**

Hilfsargumentation:
Wo beginnt der Integritätsschutz?

© Dieter Kochheim, 12.05.12

… von wesentlicher Bedeutung

Die Leistungsfähigkeit derartiger Rechner ist ebenso gestiegen wie die Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien. Heutige Personalcomputer können für eine Vielzahl unterschiedlicher Zwecke genutzt werden, etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät. Dementsprechend ist die Bedeutung von Personalcomputern für die Persönlichkeitsentfaltung erheblich gestiegen.

Systeme, die lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen verarbeiten, zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik, vermitteln noch keinen Integritätsschutz.

BVerfG, Ur. 27.02.2008 – 1 BvR 370/07 …, Rn 172, 202 (Onlinedurchsuchung)

© Dieter Kochheim, 12.05.12

… erhebliche Störung

… nicht nur

- bagatellhafte,
- leicht behebbare und
- vorübergehende Störungen

nicht nur Schutz der Daten, sondern auch der Rechenabläufe

© Dieter Kochheim, 12.05.12

Eingabe und Übermittlung

303b I Nr. 2 Vorverlagerung:

… Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, *eingibt* oder *übermittelt*

Nachteil

ist jede nachteilige Folge oder Beeinträchtigung rechtmäßiger Interessen

- **auch ohne dass der Nachteil eintritt und**
- **ohne dass ein Vermögensschaden eintritt**

ausdrücklich: verteilte Angriffe Distributed Denial of Service – DDoS

Auch: Anlieferung von Malware

- **Pharming**
- **Anlagen zu E-Mails**

© Dieter Kochheim, 12.05.12

schwere Computersabotage

schwere Computersabotage - 303b II

Handelt es sich um eine Datenverarbeitung, die für einen *fremden Betrieb*, *ein fremdes Unternehmen* oder *eine Behörde* von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

auch:

- Freiberufler
- karikative und kulturelle Einrichtungen

© Dieter Kochheim, 12.05.12

besonders schwere Fälle

besonders schwere Fälle der schweren Computersabotage - 303b IV

- Vermögensverlust großen Ausmaßes
- gewerbs- oder bandenmäßige Begehung
- Versorgung der Bevölkerung, Sicherheit der Bundesrepublik

Regelgrenze: 50.000 €
beim einzelnen Opfer
(dann auch in der Summe)
BGH, B. 18.10.2011 – 4 StR 253/11, Rn 3

© Dieter Kochheim, 12.05.12

flankierende Regeln

Vorbereitungsstadium

303a III, 303b V i.V.m. 202c

- **Passwörter, Sicherungscodes**
- **Computerprogramme**

Strafantrag

303c

- **303a I, II**
- **303b I bis III**

kein Strafantrag bei den besonders schweren Fällen und wegen der Vorbereitungshandlungen

© Dieter Kochheim, 12.05.12

Hackerstrafrecht

Grundzüge des Hackerstrafrechts – 202a I, 202b, 202c, 303a, 303b

- Schutz fremder, nicht für den Angreifer bestimmter Daten und Datenverarbeitungen

- Schutz normaler Computertechnik
- geringe Schwelle bei der wesentlichen Bedeutung

- niederschwelliger Zugangsschutz
- Schutz gegen den Einsatz irregulärer Technik (bes. Abfangen)

Strafmaß:

Abfangen, Daten verändern	bis 2 Jahre Freiheitsstrafe
Ausspähen, Computersabotage	bis 3 Jahre Freiheitsstrafe
schwere Computersabotage	bis 5 Jahre Freiheitsstrafe
besonders schwere Fälle der schweren Computersabotage	6 Monate bis 3 Jahre Freiheitsstrafe

© Dieter Kochheim, 12.05.12

Malware

Teil 2

Malware

473.480 unterschiedliche botinfizierte Computer wurden in 2010 ausfindig gemacht - jeder fünfte europäische Bot-Computer steht hierzulande. Im Durchschnitt waren pro Tag 1.946 Bots aktiv. Damit ist Deutschland der bevorzugte „Logistikstandort“ für alle, die Viren, Phishing-Mails oder Spam verbreiten.

… klettert Deutschland auf den zweiten Platz bei Phishing-Aktivitäten (2009: Platz 6) und der Verbreitung von Trojanern (2009: Platz 5).

... ist dies auf die gute Internetinfrastruktur und die im Schnitt höhere Belastbarkeit deutscher Bankkonten zurückzuführen.

© Dieter Kochheim, 12.05.12

Malware

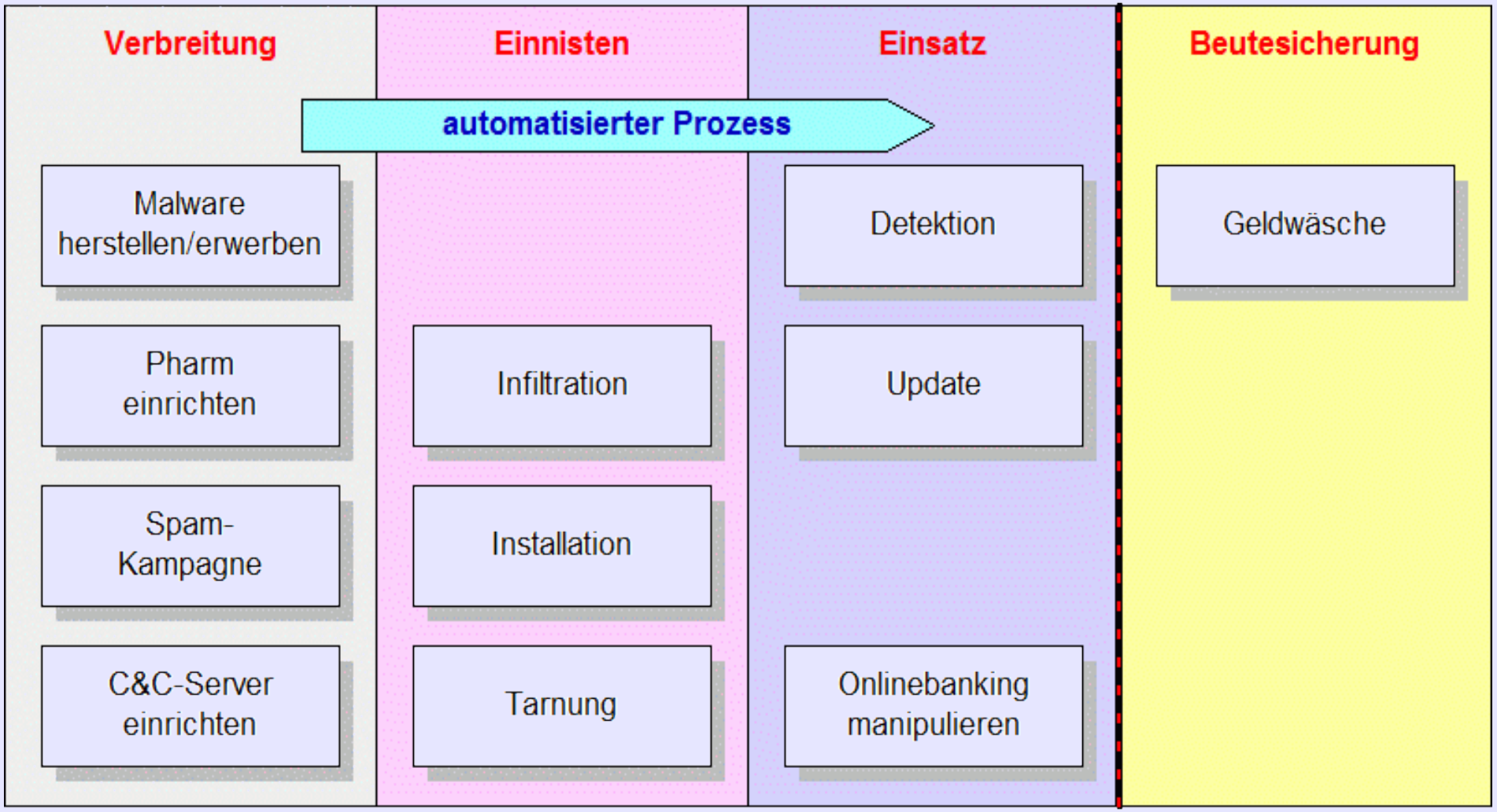
Überblick

▸ Virus	bindet sich in eine bestehende Datei ein und wird mit ihr zusammen ausgeführt
▸ Wurm	selbständiges Programm, das als Anhang zu einer anderen Datei transportiert und von aktiven Prozessen ausgeführt wird
▸ Trojaner	in einer nützlichen Anwendung versteckte Schadfunktion
▸ Kommando-string	kurze Folge von Befehlen, die den Browser zum Download der Malware veranlassen

© Dieter Kochheim, 12.05.12

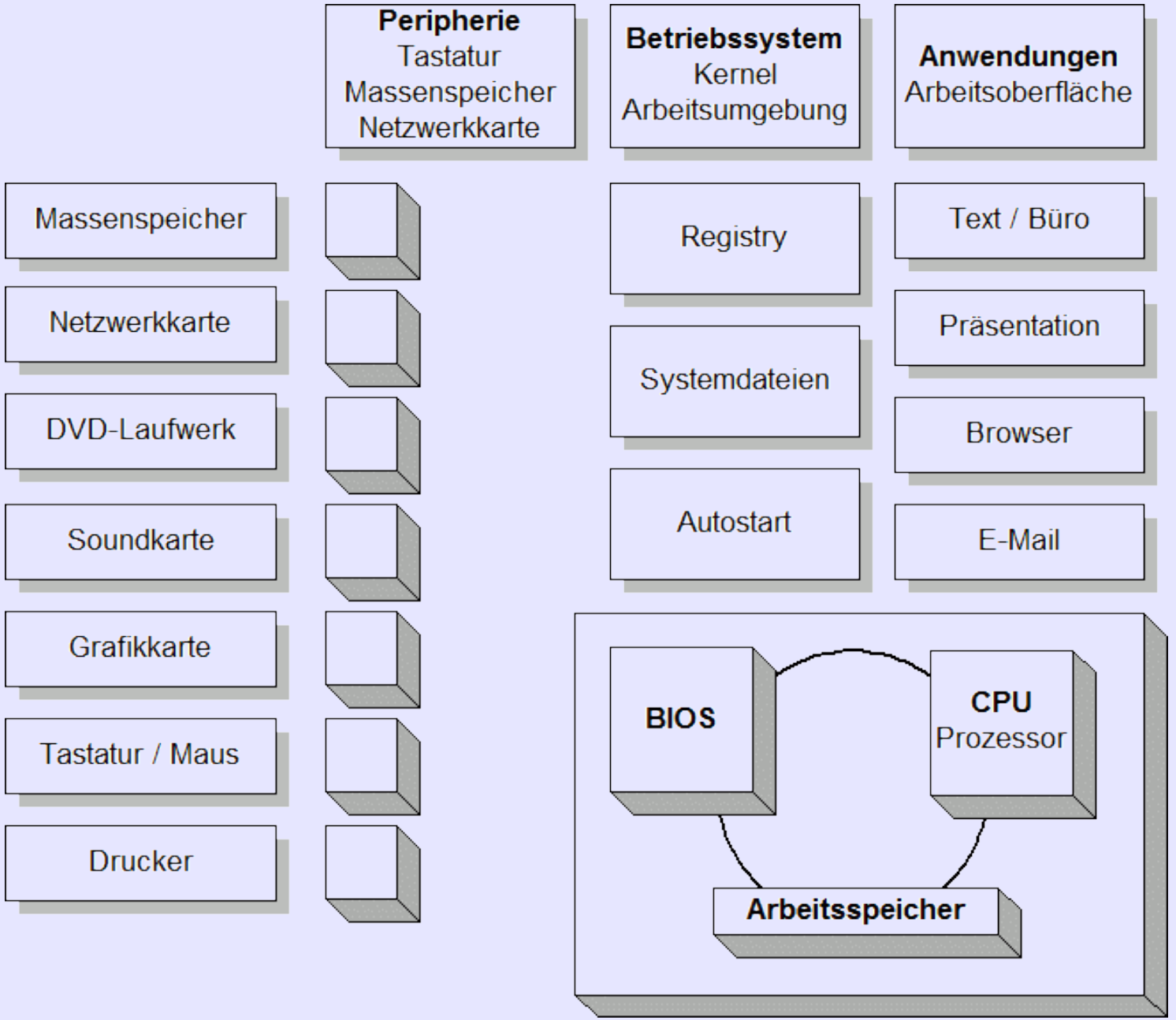
automatische Malware

Tatphasen beim Einsatz von Onlinebanking-Trojanern



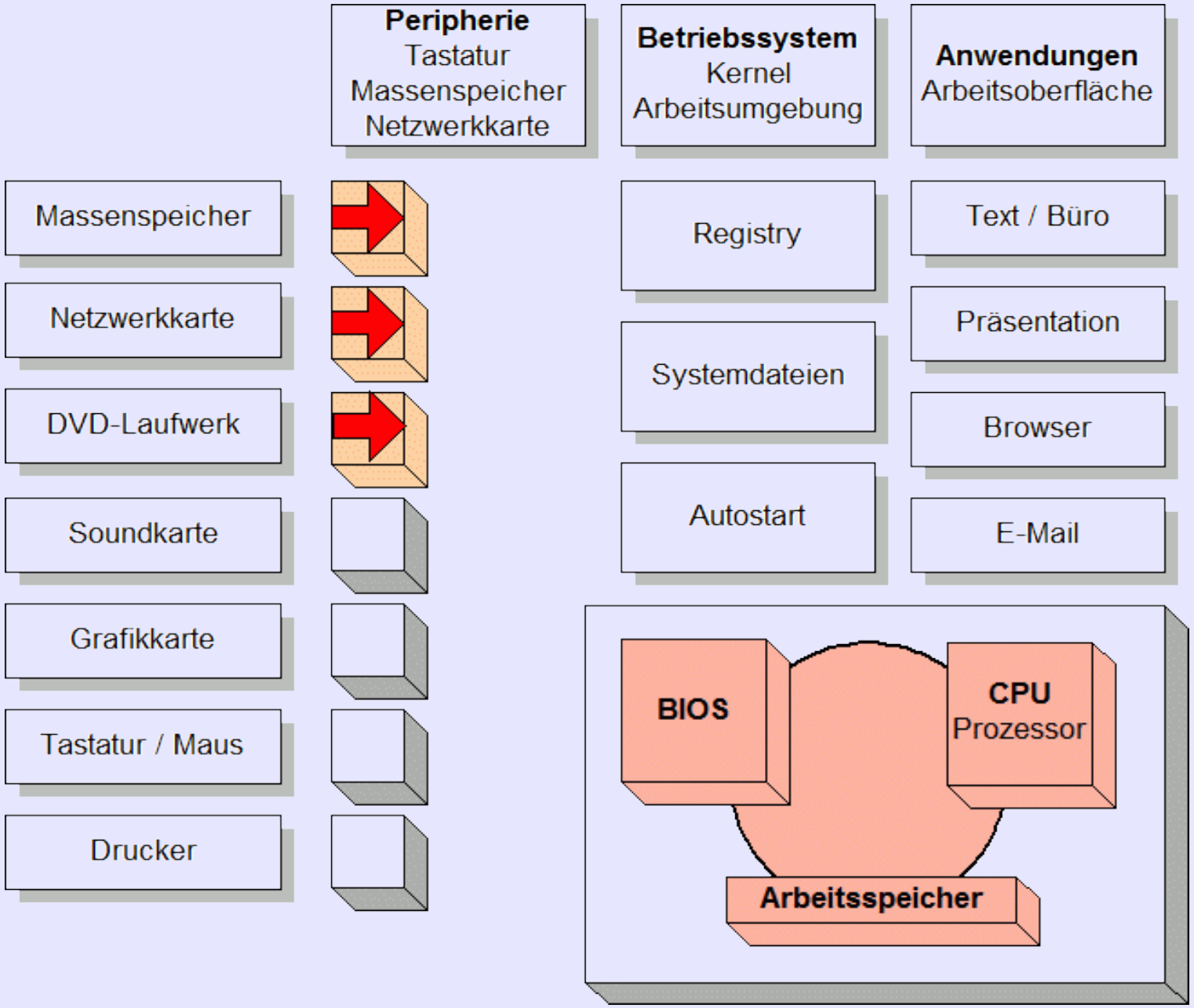
© Dieter Kochheim, 12.05.12

das Innere eines PCs



© Dieter Kochheim, 12.05.12

Anlieferung



© Dieter Kochheim, 12.05.12

Anlieferung

Übermittlung **i.S.v. 303b I Nr. 2 setzt die Übergabe der Malware an einen aktiven Prozess voraus. Dazu müssen Schwachstellen im angegriffenen System überwunden werden.**
Die vom Browser veröffentlichten Daten reichen in aller Regel aus.
Die Anlieferung selber ist noch im Versuchsstadium angesiedelt.
Die Tat ist frühestens mit der Injektion vollendet.

Anhänge zu E-Mails	**Word, Excel, PDF, Shockwave**
verteilte Datenträger	**CD, USB-Sticks, Festplatten**
Pharming	**präparierte Webseiten, Drive-By-Download**
manipulierte Hosttabellen	**DNS-Poisoning, Server-Poisoning**

© Dieter Kochheim, 12.05.12

Anlieferung. Aktive Prozesse

Spam-Nachrichten

+ aktiver Trojaner im Anhang
- noch nicht geladene Anhänge
- Link zu präparierter Webseite
+ automatischer Kommandostring
- manueller Kommandostring
+ - aktive Elemente (Bilder, Video, Animationen, Sound)

präparierte Webseiten

+ iFrames
+ Java- u.a. Routinen
+ automat. Kommandostring
- manueller Kommandostring
+ - aktive Elemente …
+ - Fake-Buttons
- unbedachte Eingaben
  bei Erfolg: 202c I Nr. 1
  Passwörter, Sicherungscodes
  nicht: 202a I
  Dateneingabe

© Dieter Kochheim, 12.05.12

Exkurs: DNS Changer

Botnetz mit 2 Mio. Zombies 2007 - 2011

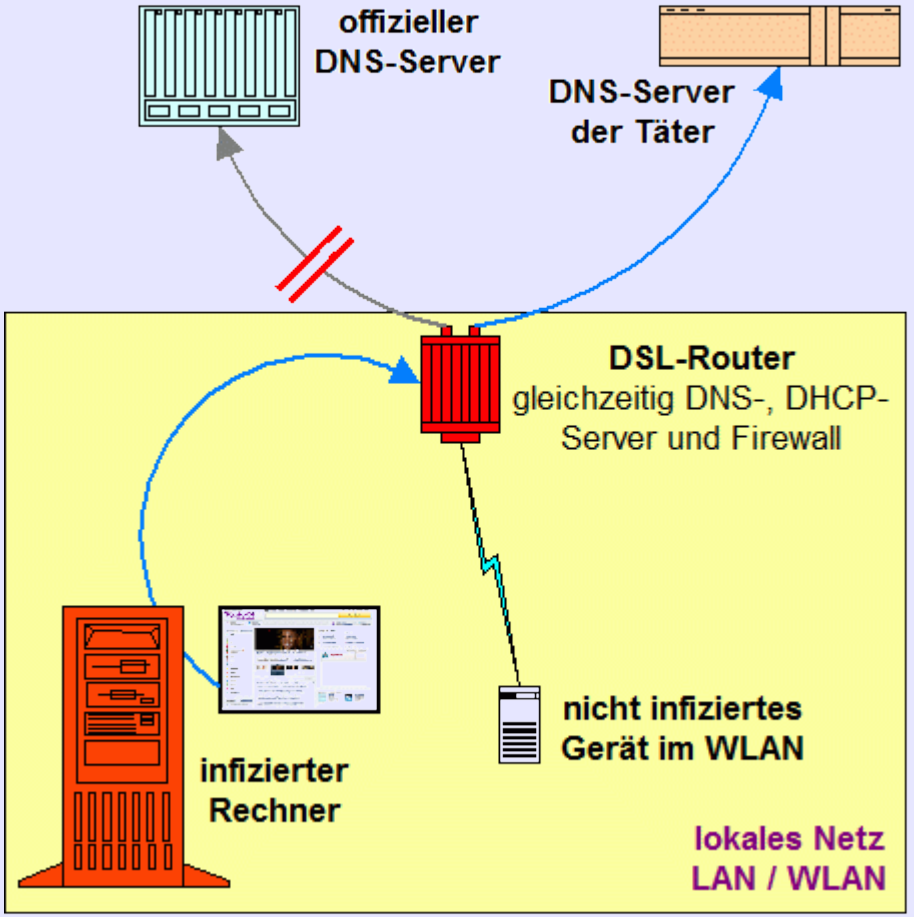
Umleitung auf präparierte Webseiten

Scheinfirmen für Werbeaufträge

14 Mio. US-$ Beute

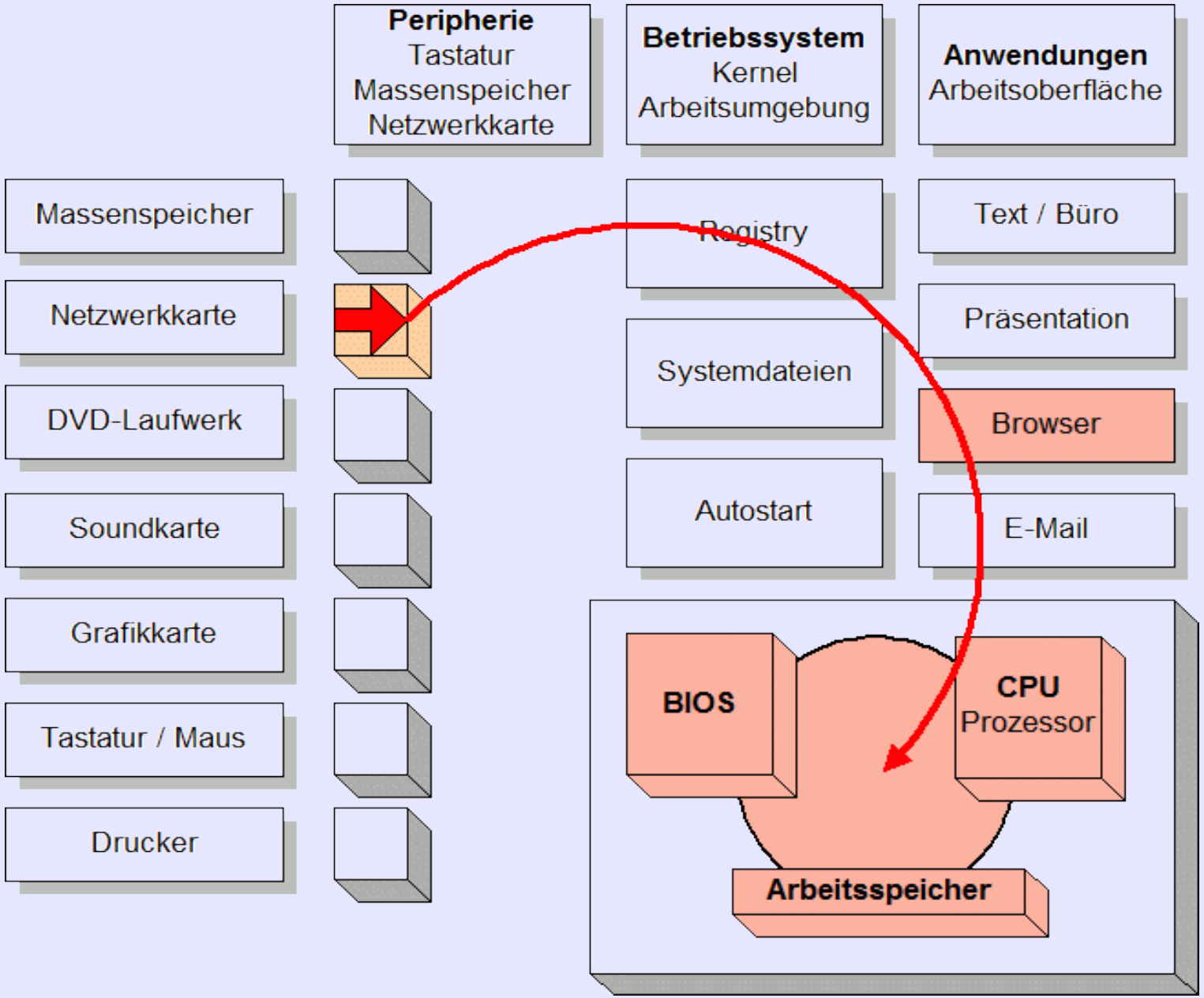
6 Verdächtige in Estland verhaftet und angeklagt

FBI nimmt DNSChanger-Botnetz hoch, c't 25/2011 S. 41



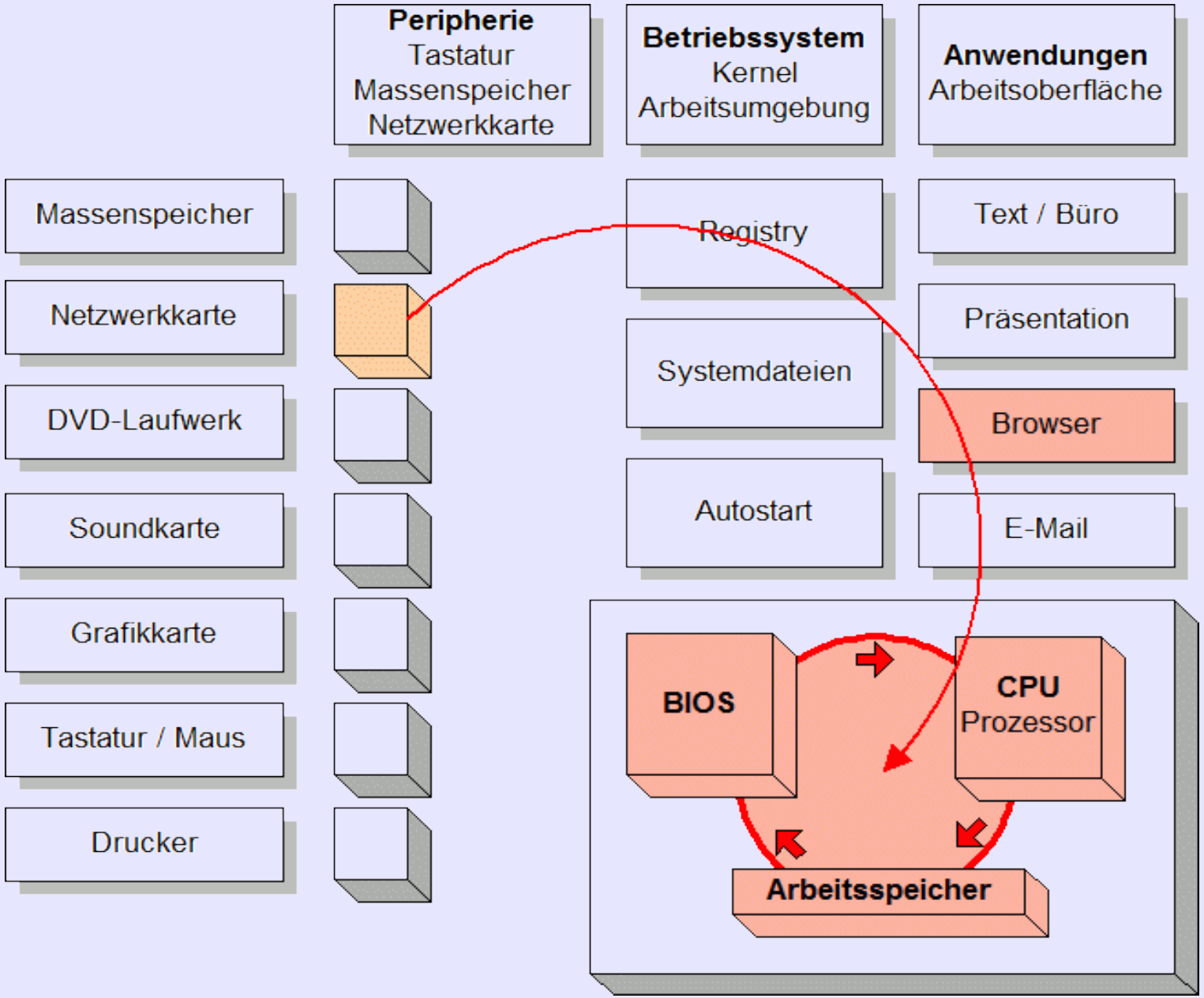
© Dieter Kochheim, 12.05.12

Injektion



© Dieter Kochheim, 12.05.12

Infektion



© Dieter Kochheim, 12.05.12

Infektion. Einnisten

Mit der *Infektion* wird massiv auf den Prozess der Datenverarbeitung eingewirkt. Das Ausmaß richtet sich nach der Malware im Einzelfall.

Die dabei veränderten Daten sind in aller Regel wieder herstellbar, so dass noch von Bagatell-schäden ausgegangen werden muss.

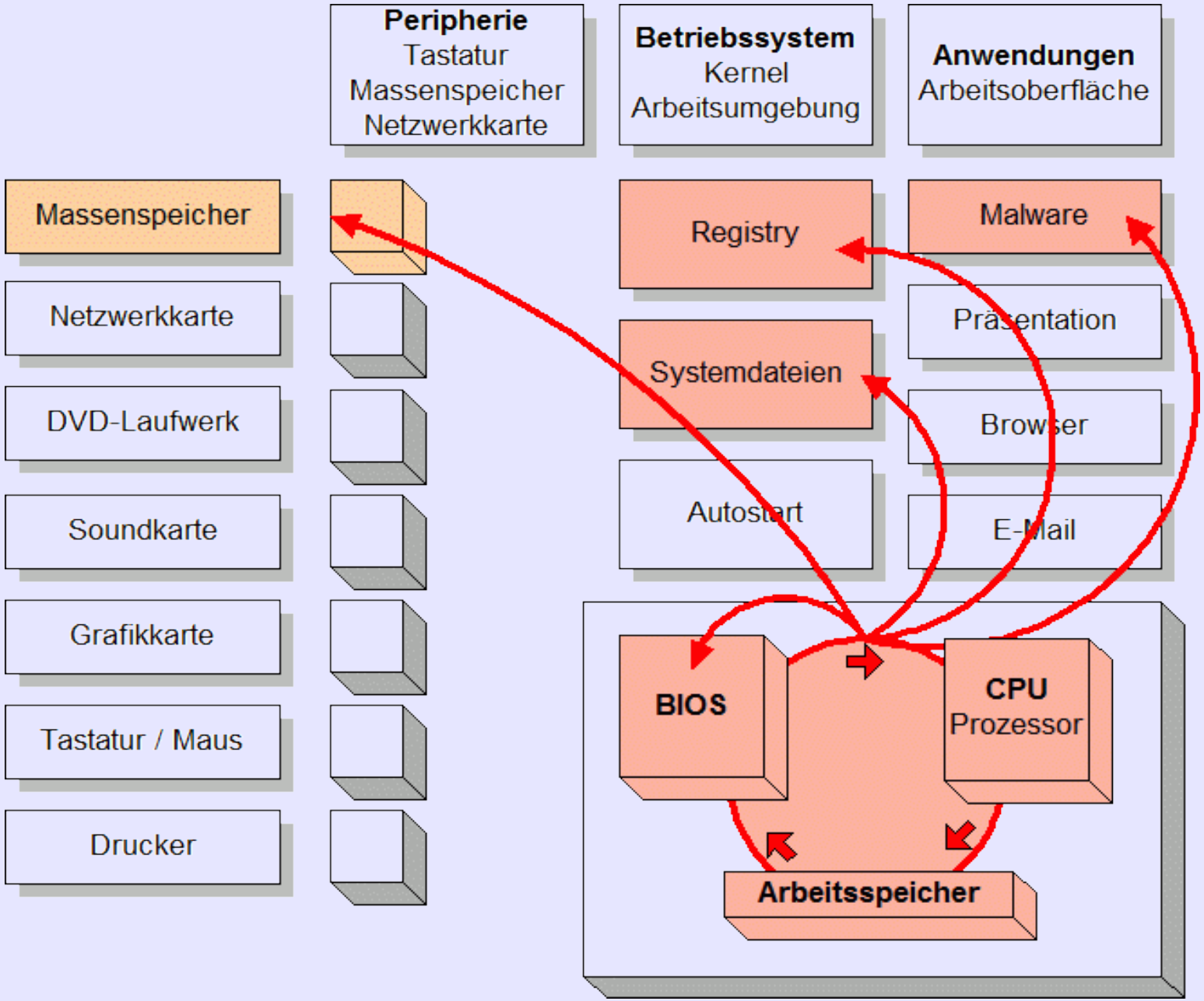
Beim *Einnisten* werden die Systemeinstellungen massiv verändert, die Malware eingerichtet, vorhandene Dateien verändert und zusätzliche installiert. Dabei wird meistens auch der vorhandene Virenscanner abgeschaltet.

Dazu müssen Schwachstellen im System überwunden werden (Exploits).

Spätestens mit dem Einnisten ist die Computersabotage vollendet.

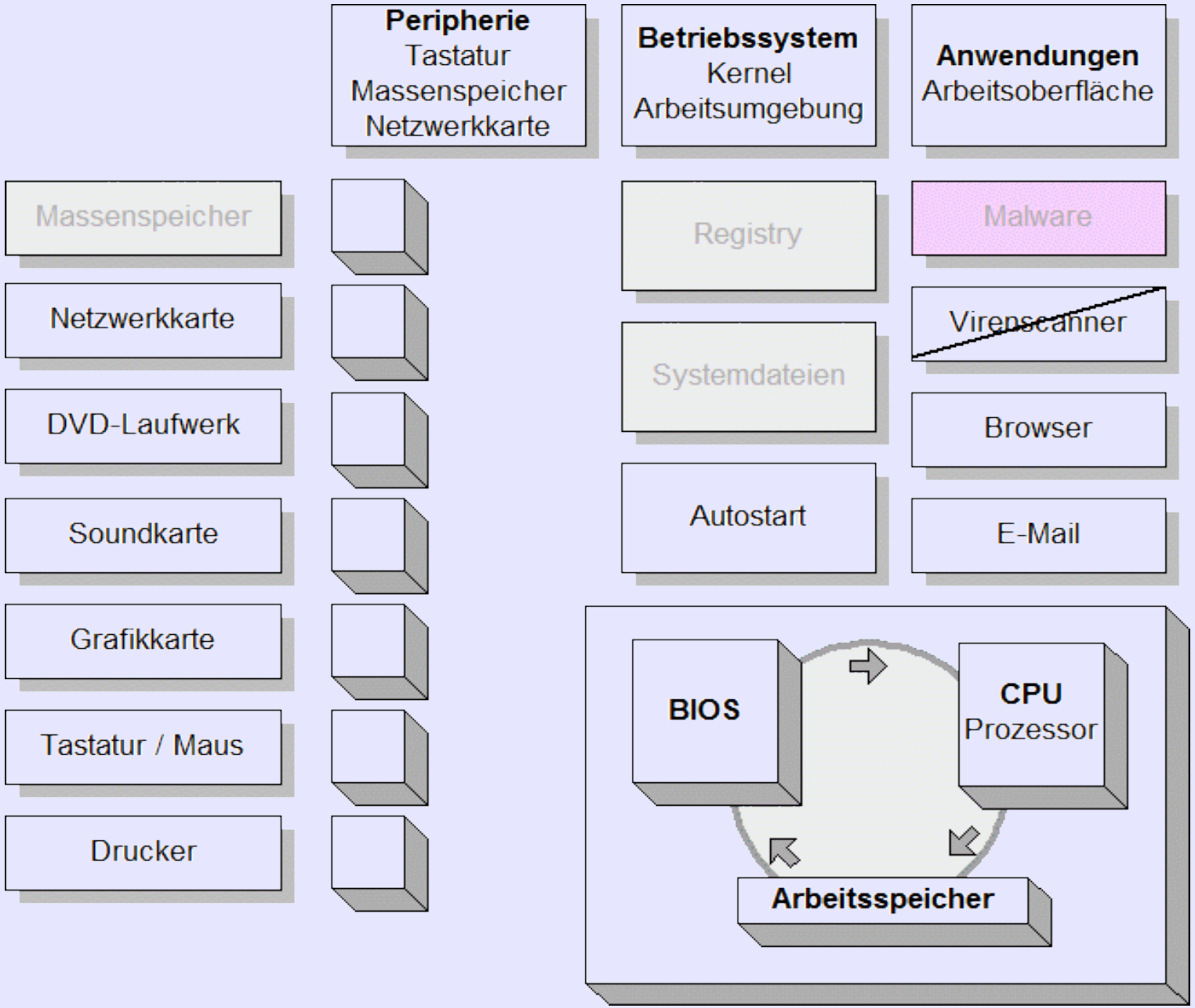
© Dieter Kochheim, 12.05.12

Einnisten



© Dieter Kochheim, 12.05.12

Tarnen



© Dieter Kochheim, 12.05.12

Tarnen

Botnetz- und Onlinebanking-Malware ist darauf ausgelegt, auf Dauer im angegriffenen System betrieben zu werden.

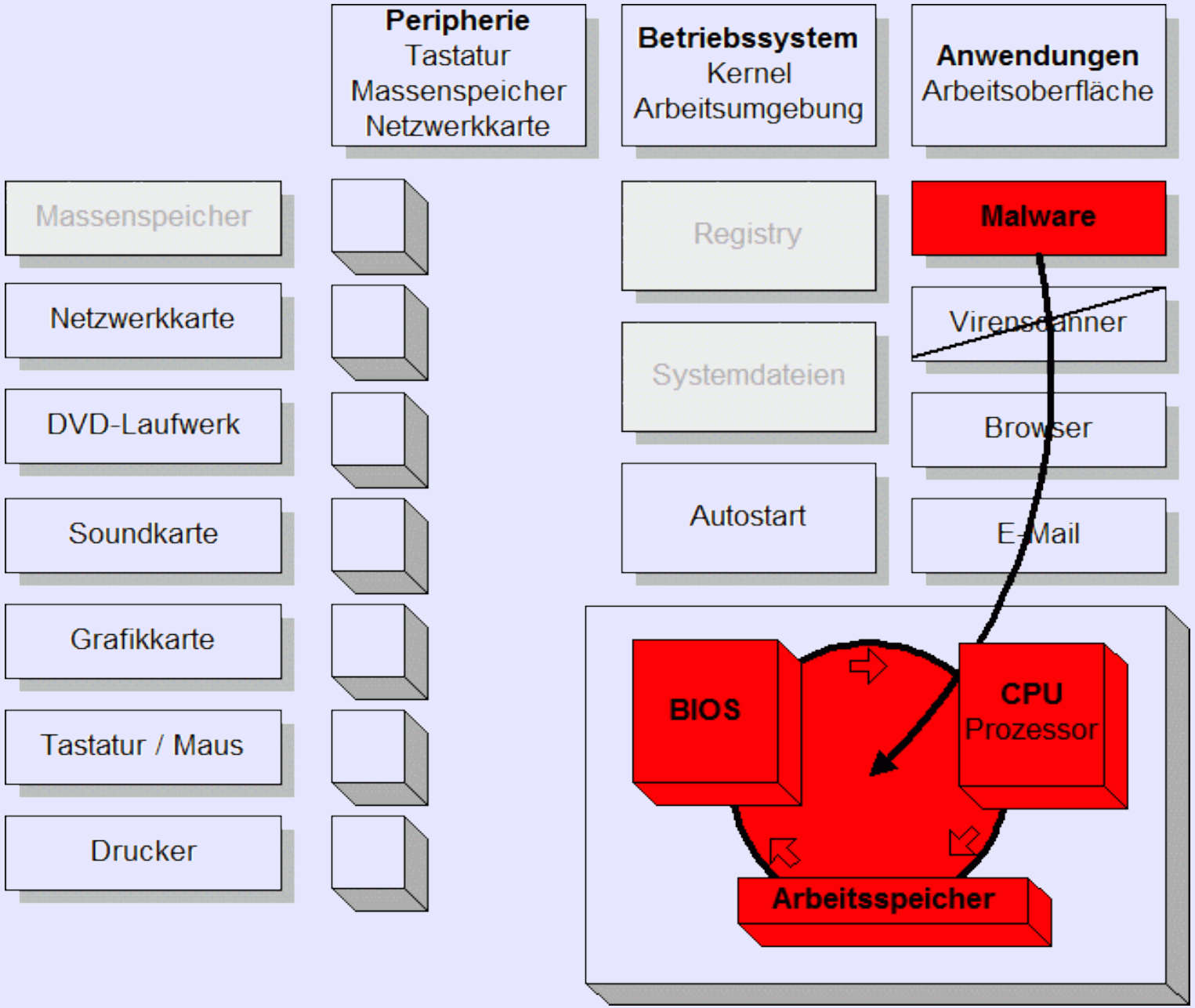
Ihre modernen Formen machen sich deshalb kaum bemerkbar und versuchen, die von ihnen verursachten Schäden klein zu halten.

Sie sind in aller Regel Update-fähig und werden von einer zentralen Instanz mit Updates und Anweisungen versorgt (Command & Controll-Server – C&C; Flux-Server).

Um sie vor Entdeckung zu schützen, kommen besondere Tarnmechanismen zum Einsatz (Rootkits).
Sie bewirken zum Beispiel, dass Laufzeitbibliotheken ausgewechselt und wesentliche Programmfunktionen verschlüsselt werden (gegen heuristische Erkennung).

© Dieter Kochheim, 12.05.12

Malware-Aktion



© Dieter Kochheim, 12.05.12

Ausführungsfunktionen

Die Ausführungsfunktionen hängen von der Aufgabe der Malware ab.

- **Ausspähen des Systems nach Zugangsdaten zu Konten und Programmen (Accounts, Codes, PIN).**
  Verkauf als Drop.
- **Protokollierung der eingegebenen Daten (Keylogger).**
- **Einrichtung einer Backdoor (Spionage).**
- **Bereitstellung als Zombie (DDoS, Spam, Kapazität).**
- **Manipulation des Onlinebanking**

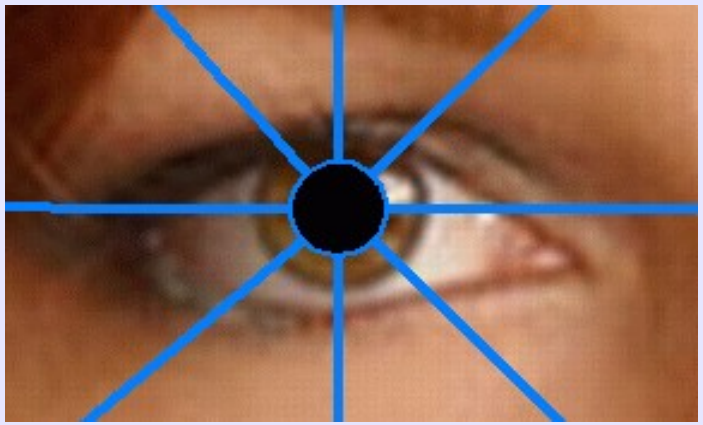
© Dieter Kochheim, 12.05.12

kriminelle Erscheinungsformen

Teil 3

kriminelle Erscheinungsformen

- Spamming
- Botnetze
- Onlinebanking-Malware
- Skimming

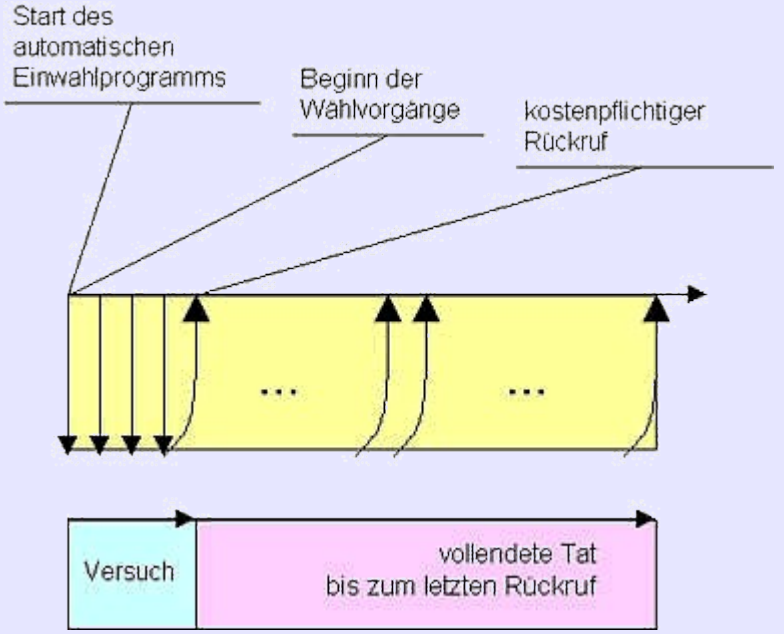


© Dieter Kochheim, 12.05.12

Rückruftrick

2002

- **mehrere Rufnummern aus der frei tarifierbaren Nummern-gasse 190 – 0.**
- **Rechner und Telefonanlage verbunden**
- **Programmstart: ausgewählter Nummernkreis des D 1-Netzes wird angewählt und die Verbindung sofort unterbrochen**
- **„Anruf in Abwesenheit“**
- **bei Rückruf: Freizeichen vom Tonband**



- **Vielzahl von Betroffenen**
- **ein Betrug in Tateinheit**

© Dieter Kochheim, 12.05.12

Dialer

Dialer

- Einwahlhilfe zum Internet
- frühe Form der Malware
- versteckte Funktionen
- täuschende Angaben
- Formenwechsel nach der Installation

je nach Funktionsweise:
263, 263a
269 wegen der Zugangsdaten

Mehrwertdienste Premium Rate

der Zugangsprovider stellt nicht nur eine TK-Verbindung her, sondern darüber hinaus wird eine weitere Dienstleistung erbracht, die gegenüber dem Anrufer gemeinsam mit der Telekommunikationsdienst-leistung abgerechnet wird.

Gesetz von 2003:

- 0190-Nummerkreis abgeschafft
- 0900-eingeführt und gedeckelt
- Datenbanken für Dialer und Mehrwertdienstenummern
- Verbot der Durchsetzung

© Dieter Kochheim, 12.05.12

Spamming

Spam: Massenhaft versandte, unerwünschte E-Mails

- **Werbung**
- **Verleitung zu unbedarften Eingaben in Formularfeldern**
- **Verleitung zum Aufruf unbekannter Webseiten**
- **Transportmittel für Malware (Anhänge)**

Kosten sind gedeckt, wenn 0,1 % der Spam-Mails erfolgreich sind

Urform des Phishings (Eingabefelder für Kontodaten)

© Dieter Kochheim, 12.05.12

Strafbarkeit des Spammings

Manipulationen in Spam-Mails

- **falsche Angaben über den Absender im Header**
  erster (unterster) Received-Eintrag
  kann von Versender eingestellt werden
  Netzadressen, über die die E-Mail „gelaufen“ ist
- **täuschende E-Mail-Adressen**
  volks-banken.de

meine-liebe-bank.de/zugang@www.abzocker.ru

© Dieter Kochheim, 12.05.12

Header

```
Return-Path: <bounce68hnu@rr.use.cc>
Received: from mailin33.aul.t-online.de (mailin33.aul.t-online.de [172.20.27.61])
        by mhead106 (Cyrus v2.3.15-fun-3.2.12.0-1) with LMTPA;
        Sat, 03 Dec 2011 12:09:19 +0100
X-Sieve: CMU Sieve 2.3
Received: from mi-ob.rzone.de ([2a01:238:20a:202:51f0::2044]) by
2003:2:2:10:fee::33
...
Received: from b8.rzf.lan (tt.use.cc [192.168.98.108])
    by pmta01.rzf.lan (Haraka/1.0.2) with ESMTP id A2E18C08-07C7-
...
Date: Sat, 3 Dec 2011 12:04:02 +0100
To: dieter@kochheim.de
From: MDM-Muenzen <gedenkmuenze@muenzen.de.cc>
Reply-to: gedenkmuenze@muenzen.de.cc
Subject: =?utf-8?Q?Tausch-
Aktion:_10_Euro_Gedenkm=C3=BCnzen_f=C3=BCr_nur_je_10_?=
 =?utf-8?Q?Euro?=
Message-ID: <6fb8af0f668ecefab98f81aea97f2d2c@tt.use.cc>
...
```


© Dieter Kochheim, 12.05.12

Traceroute

Traceroute to 192.168.98.108

Hop	T1	T2	T3	Best	Graph	IP	Hostname	Dist	TTL	Ctry	Time
1	1	3	*	0.9 ms		70.86.70.33 AS21844 THEPLANET-AS	21.46.5646.static.theplanet.com.		255	US	Unix: 13:33:59.391
2	1	0	*	0.9 ms [+0ms]		70.87.254.1 AS21844 THEPLANET-AS	po101.dsr01.dllstx5.networklayer.com.	0 miles [+0]	254	US	Unix: 13:33:59.428
3	1	1	*	1.2 ms [+0ms]		70.85.127.105 AS21844 THEPLANET-AS	po51.dsr01.dllstx3.networklayer.com.	0 miles [+0]	250	US	Unix: 13:33:59.459
4	*	*	*	99999 ms [+99999ms]		[Unknown]	[Unknown - Firewall did not respond]	0 miles [+0]			
5	*	*	*	99999 ms [+0ms]		[Unknown]	[Unknown - Firewall did not respond]	0 miles [+0]			
6	*	*	*	99999 ms [+0ms]		[Unknown]	[Unknown - Firewall did not respond]	0 miles [+0]			
7	*	*	*	99999 ms [+0ms]		[Unknown]	[Unknown - Firewall did not respond] [4 hops with no response: assuming we hit a firewall that blocks pings]	0 miles [+0]			

© Dieter Kochheim, 12.05.12

Fälschung beweiserheblicher Daten

269

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

Urkunden im Sinne des Strafrechts sind verkörperte Erklärungen, die ihrem *gedanklichen Inhalt* nach geeignet und bestimmt sind, für ein *Rechtsverhältnis* Beweis zu erbringen, und die ihren *Aussteller* erkennen lassen.

BGH, B. 23.03.2011 – 5 StR 7/10, Rn 4

© Dieter Kochheim, 12.05.12

Abbilder sind keine Urkunden

- schriftliche Lüge
- Fotokopie
- Fax

Fotokopie und Fax sind nur die bildliche Wiedergabe der im Original verkörperten Erklärung, ohne dass sie als offensichtliches Abbild selber zur Urkunde werden

BGH, B. 27.01.2010 – 5 StR 488/09, Rn 10
BGH, Ur. 11.05.1971 – 1 StR 387/70
BGH, Ur. 14.09.1993 – 5 StR 283/93

- computerbearbeitete Kollagen mit eingesetzten Paraphen

… bleiben Reproduktionen

BGH, B. 23.03.2011 – 5 StR 7/10, Rn 4

- Abbild von einem Personalausweis (Photoshop)

BGH, B. 09.03.2011 – 2 StR 428/10, Rn 3

+ gefälschte Beglaubigung auf Kopie

BGH, Ur. 14.09.1993 – 5 StR 283/93

- Absenderaufdruck auf Fax

BGH, B. 27.01.2010 – 5 StR 488/09, Rn 11

© Dieter Kochheim, 12.05.12

Reproduktionen sind keine Urkunden

Eine Reproduktion, die nicht den Anspruch erhebt, selber das Original zu sein, ist keine Urkunde im Sinne von § 267 StGB.

Dieser Grundsatz ist auch auf die Fälschung beweiserheblicher Daten anzuwenden.

BGH, B. 27.01.2010 – 5 StR 488/09, Rn 13

© Dieter Kochheim, 12.05.12

Schlüsse 1

- ältester Received-Eintrag	schriftliche Lüge vergleichbar dem Fax-Absender
+ „Postbank“ nachgemachte E-Mail mit den Gestaltungselementen des Originals	unerlaubte Verwendung von Marken, Symbolen und Grafiken 143 I MarkenG 106 I UrhG 269
+ täuschende E-Mail-Adresse: post-bank.de Verwendung kyrillischer Zeichen	269
- Phantasienamen: Volksbank AG	- 269
+ nachgemachte Webseiten mit Original-Layout (Pharming)	269

© Dieter Kochheim, 12.05.12

Schlüsse 2

+ Verwendung gefälschter oder gestohlener SSL-Zertifikate

Secure Socket Layer werden bei SHTTP-Verbindungen gegen eine „trust list“ des Zertifizierers geprüft

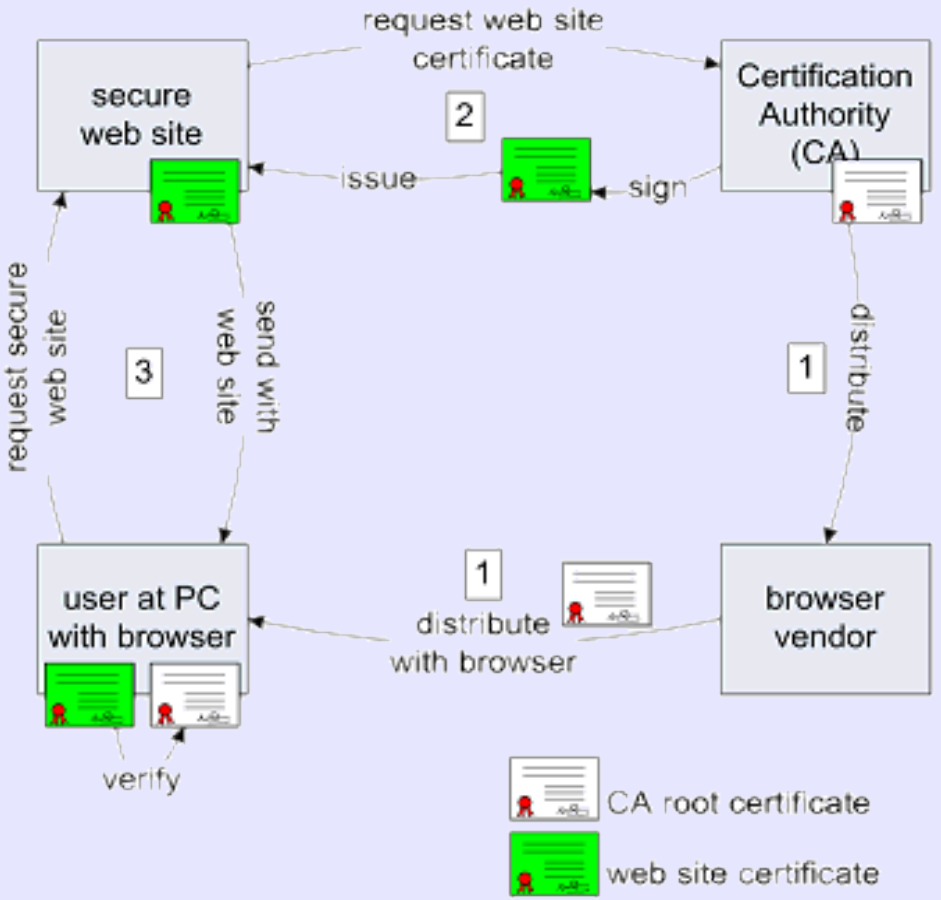
© Dieter Kochheim, 12.05.12

Secure Sockets Layer - SSL

Secure Sockets Layer – SSL
jetzt: Transport Layer Security – TLS

Webseite lässt sich von einer Zertifizierungsstelle (CA) ein web site certificate ausstellen und übergibt beim Aufruf das Zertifikat an den Browser.

Der Browser prüft gegen eine Interne Prüftabelle oder gibt es an den Browser-Hersteller weiter, der es gegen das root certificate der Certification Authority – CA – prüft.



© Dieter Kochheim, 12.05.12

Schlüsse 3

+ Spams mit Zugangsdaten zu Pharmen (oder mit Malware-Anhängen)

spricht für die Verbreitung von Malware für Botnetze oder Onlinebanking-Trojaner

269 III i.V.m. 267 III, IV

bes. schw. Fall (gewm. oder Bande)

schwere Fälschung beweiserh. Daten (gewm. und Bande)

© Dieter Kochheim, 12.05.12

Identitätsdiebstahl

Beim *Identitätsdiebstahl* geht es darum, fremde Zugangsrechte zu erlangen und zu missbrauchen. Betroffen sind alle personenbezogenen Rechte, die in der Carding-Szene und der Underground Economy gehandelt werden.

Dazu gehören Verrechnungs- und Einkaufskonten sowie die Zugangsdaten zu Paketstationen, aber auch falsche Personalpapiere, Führerscheine und Hochschuldiplome sowie vor allem Bankkonten, die zur Geldwäsche genutzt werden können (Mule-Account).

Besonders begehrt sind in den USA komplette Lebensläufe, die mit Urkunden unterlegt sind und eine aktive Sozialversicherungsnummer umfassen.

Besondere Erscheinungsformen:

- Phishing
- Skimming
- Carding

© Dieter Kochheim, 12.05.12

klassisches Phishing

bis 2007 / 2008

E-Mail mit Formularfelder für die Kontozugangsdaten	erfolgreiches „Abphishen“: 202c I Nr. 1
Eindringen in das Bankkonto	Ausspähen von Daten: 202a I Computersabotage: 303b I Nr. 2
Veränderung der Zugangsdaten	269
Kontobelastung	263a
Beutesicherung durch Finanzagent	leichtfertige Geldwäsche: 261 V
Variante: Paketagent	dto.: 261 Hehlerei / Absatzhilfe: 259

© Dieter Kochheim, 12.05.12

Password-Stealer

Malware späht die Zugangsdaten aus

Keylogger: 202a I

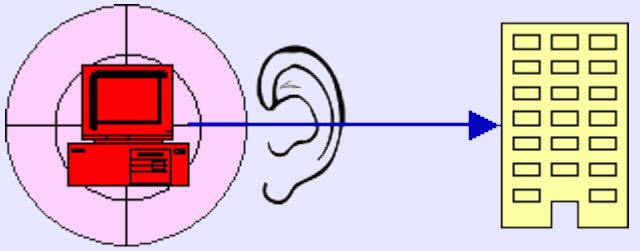
wegen der Installation: Einnisten von Malware: 303b

Ausführung wie beim „klassischen“ Phishing

© Dieter Kochheim, 12.05.12

Man-in-the-Middle

Beim Man-in-the-Middle-Angriff leitet die Malware die Kommunikation über eine Zwischenstation, an der der Angreifer den vollen Zugriff auf alle wechselseitigen Meldungen hat und sie nach seinen Vorstellungen manipulieren kann.



202a I, 202b, 202c
263a, 269

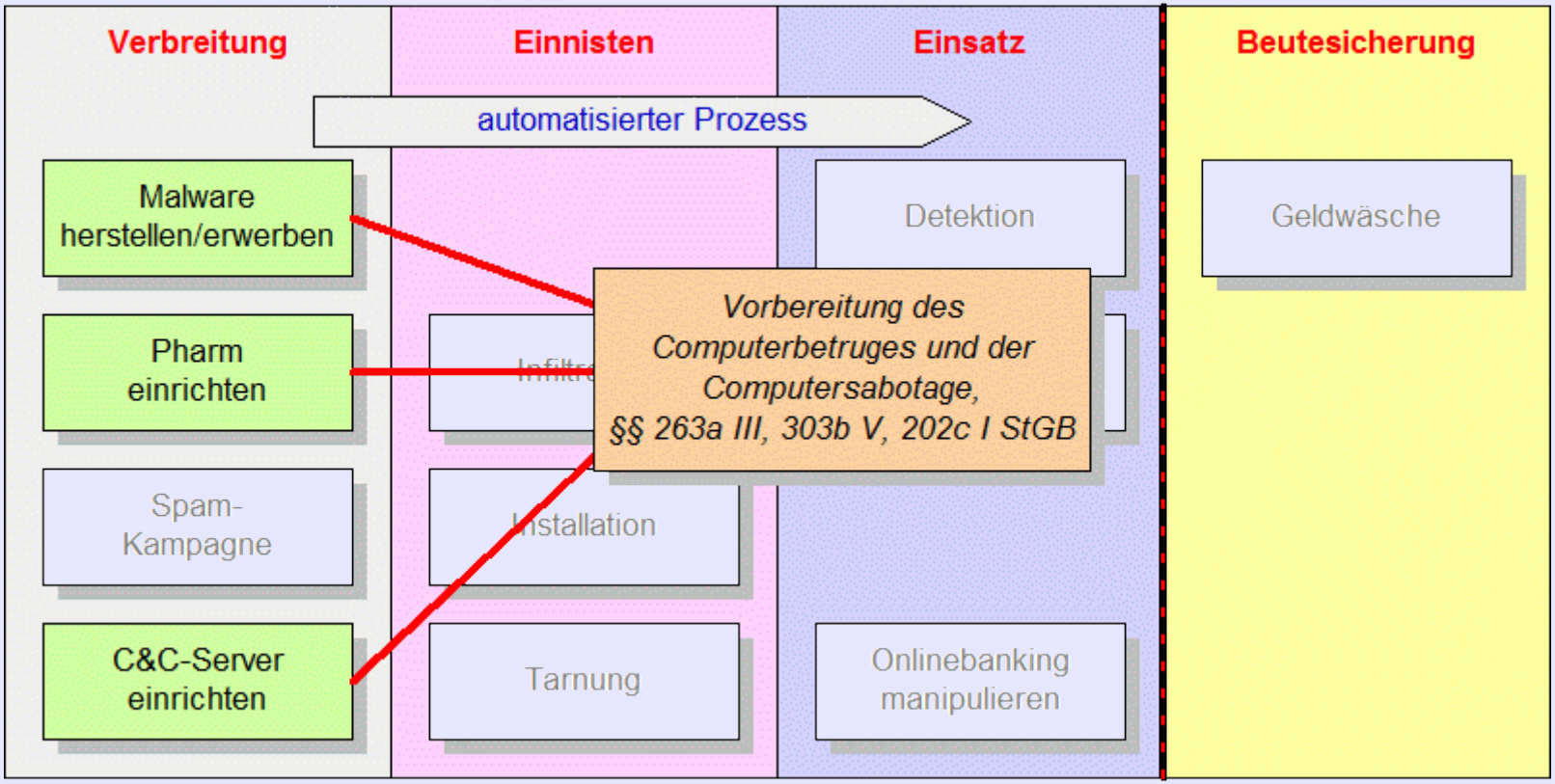
- **Veränderung von Überweisungen**
- **Vorspiegelung gefälschter Webseiten von Banken**
- **Veränderung der Hosttabelle**

heute:
vollständig automatisierter Prozess über C & C-Server

© Dieter Kochheim, 12.05.12

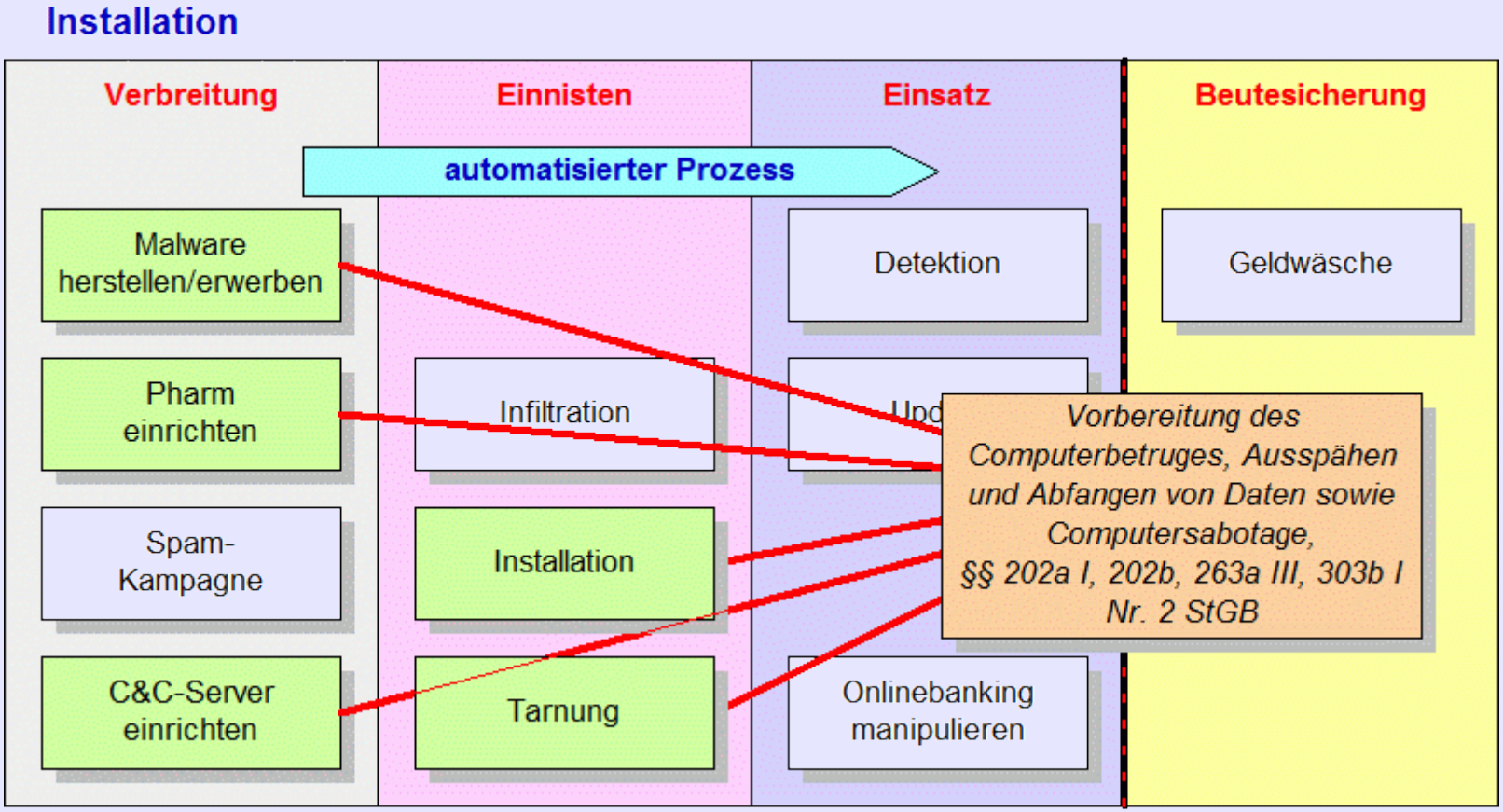
Onlinebanking-Malware

Vorbereitungsphase



© Dieter Kochheim, 12.05.12

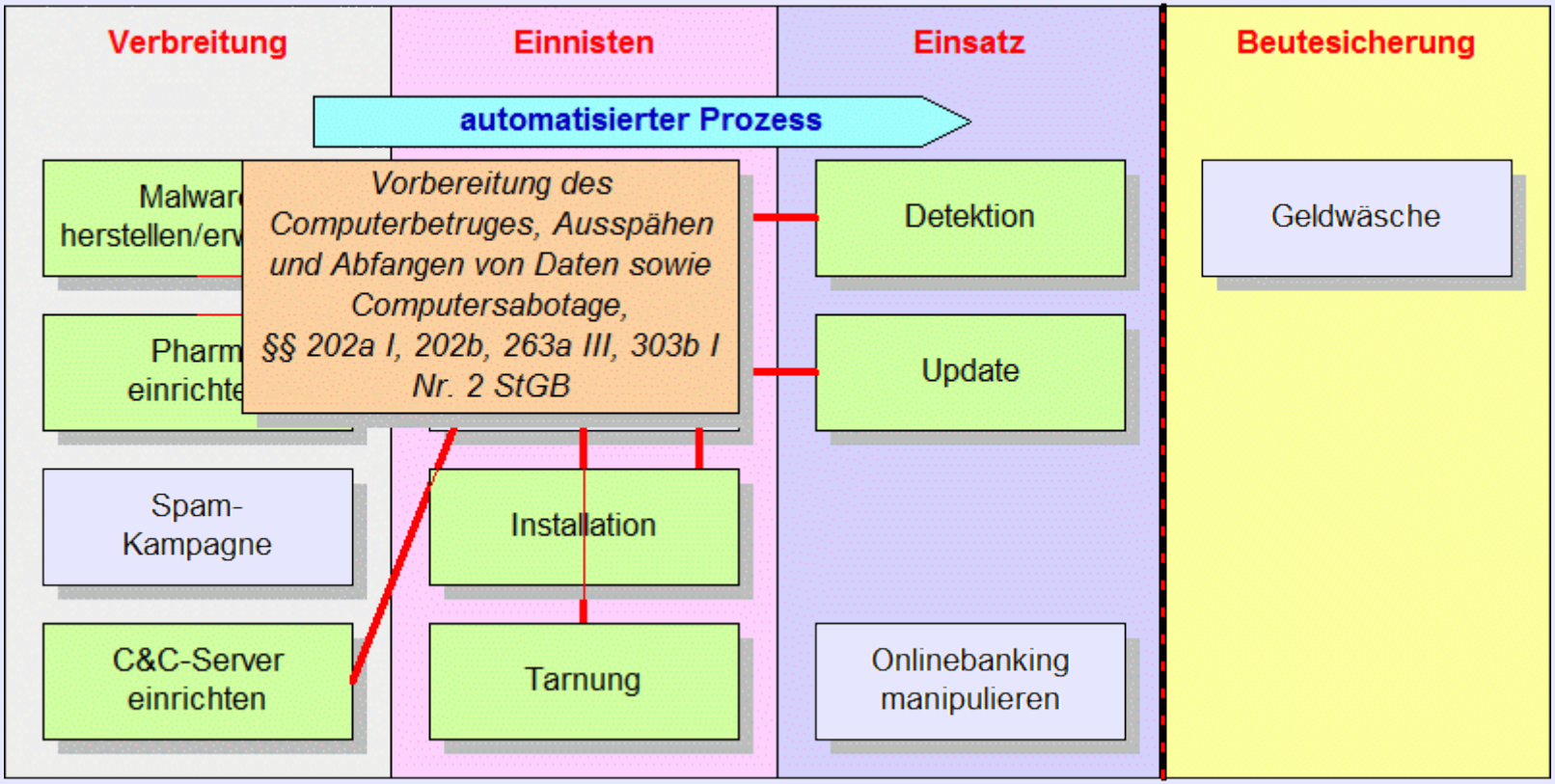
Onlinebanking-Malware



© Dieter Kochheim, 12.05.12

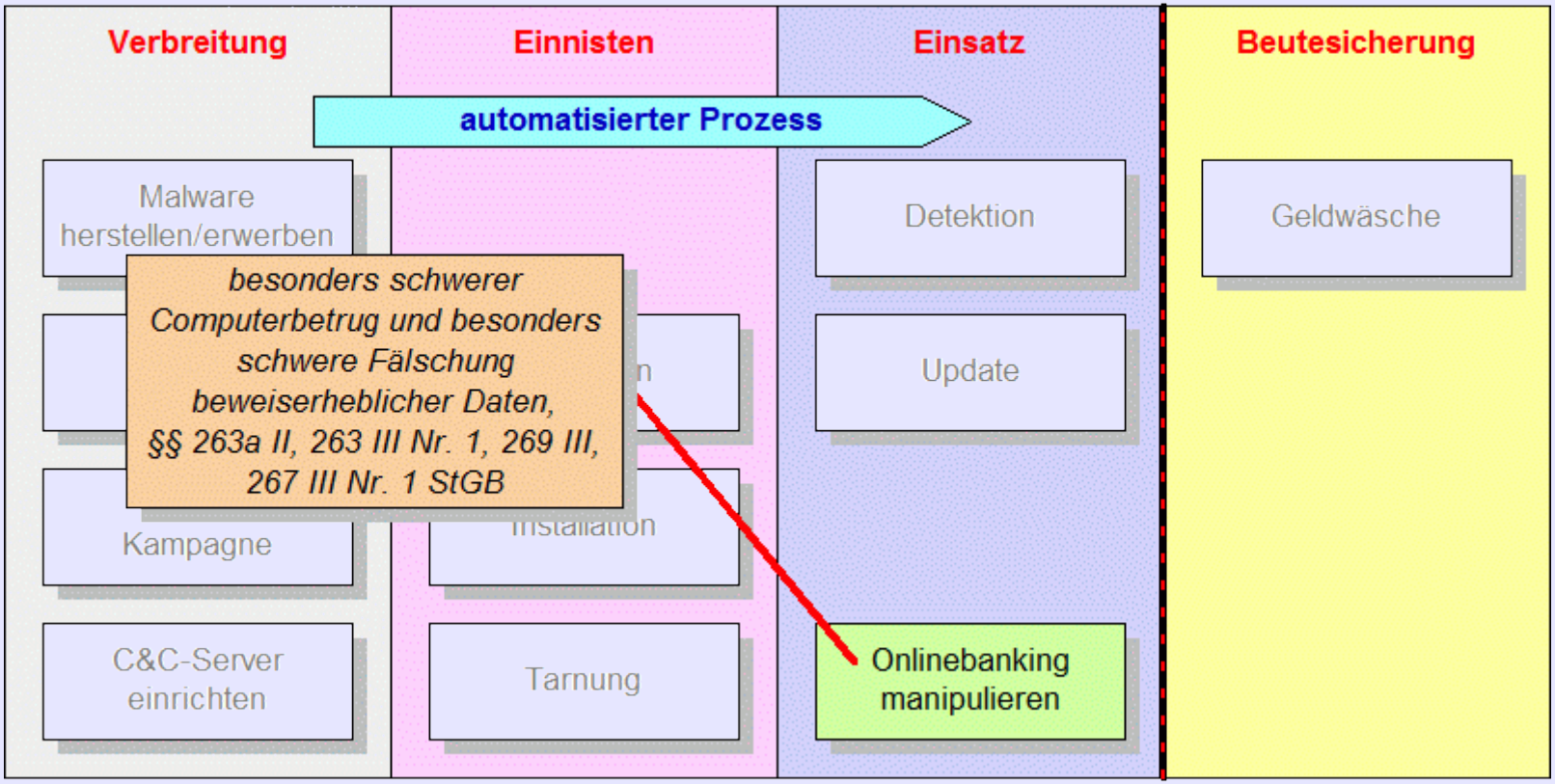
Onlinebanking-Malware

"schlafender" Einsatz



© Dieter Kochheim, 12.05.12

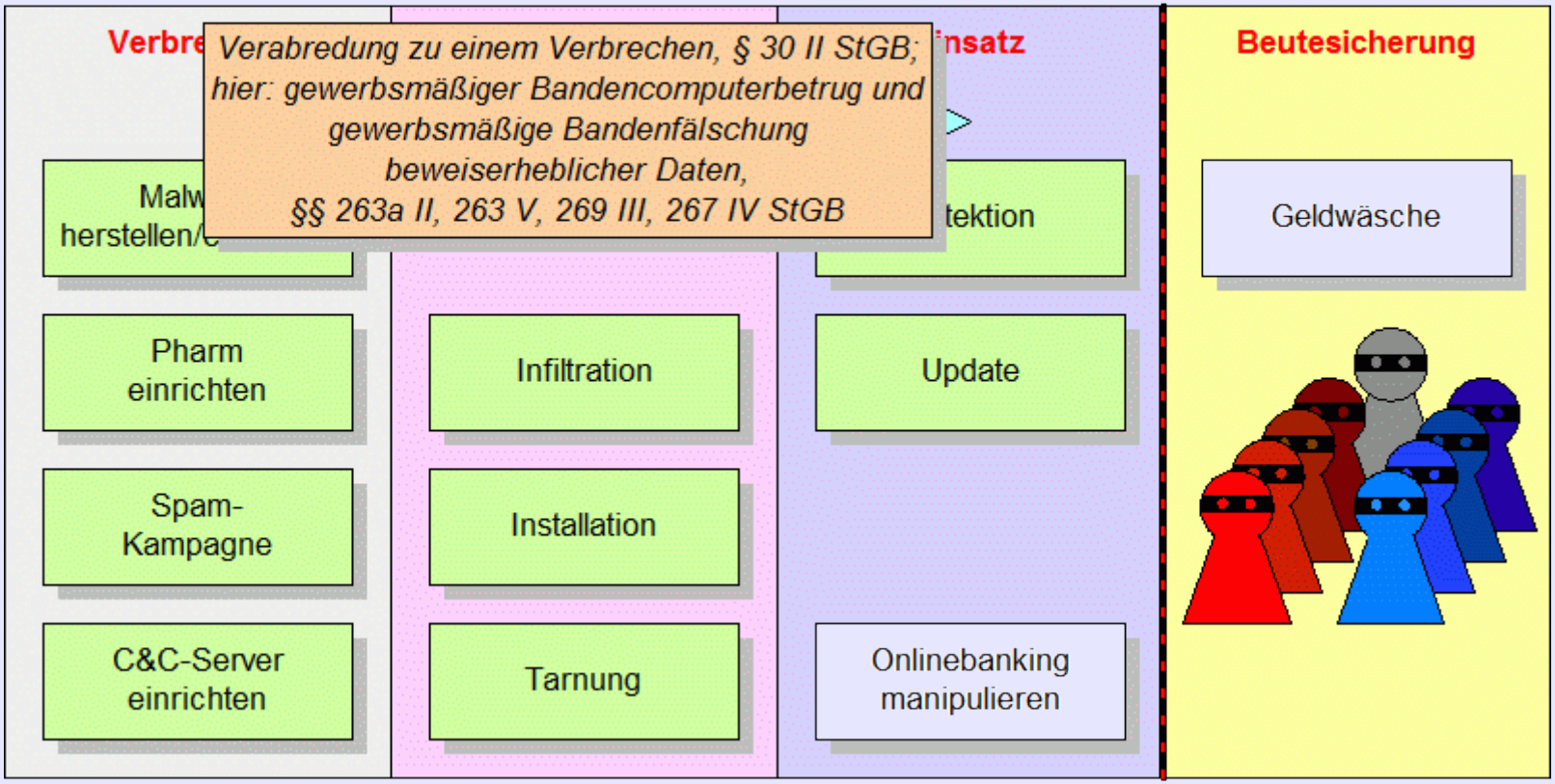
Onlinebanking-Malware



© Dieter Kochheim, 12.05.12

Onlinebanking-Malware

Verabredung zu einem Verbrechen (Bande)



© Dieter Kochheim, 12.05.12

Onlinebanking-Malware

	Anwender	Malware	C&C	Bank
1.1	A ruft die Webseite seiner Bank auf			
1.2		MW protokolliert Aufruf und Daten		
1.3				B meldet Zugangsprozedur
1.4	A gibt Kontodaten und Captcha ein			
1.5		MW meldet Kontozugang und die protokollierten Daten		
1.6		MW kappt die Verbindung und leitet auf C&C um		B meldet Übersichtsseite
2.1		MW vermittelt die Kommunikation zwischen Anwender, C&C und Bank	C&C liefert über die MW Daten für eine Überweisung	
2.2			C&C generiert Bankseite (Sicherheitshinweis) und fordert iTAN an	B fordert iTAN an
2.3	A gibt iTAN ein	MW gibt iTAN weiter		
2.4			C&C generiert eigene Bankseite ohne Überweisungsdaten	B bestätigt Überweisung

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware

3.1	A startet eigene Überweisung	▶	➤	▶	C&C generiert über die MW eine weitere Überweisung	▶
3.2		◀	◀	◀	C&C generiert mit den Daten von A Bankseite und fordert iTAN an	◀ B fordert iTAN an
3.3	A gibt iTAN ein	▶	MW gibt iTAN weiter	▶	▶	▶
3.4		◀	◀	◀	C&C bestätigt mit den Daten von A die Überweisung	◀ B bestätigt Überweisung
4.1	A beendet die Session	▶	MW gibt Logout weiter und meldet sich beim C&C ab	▶	▶	▶
4.2		◀	MW kappt die Verbindung und verhindert den Neustart für das Internet			

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware. Ablauf 1

Anwender	ruft Homebanking-Seite auf, gibt Kontonummer, PIN und Captcha ein
Malware	ruft offene Kontoinformationen ab – 202b
Bank	sendet Startseite
Malware	unterdrückt die Ausgabe zum Browser – 274 I Nr. 2
C & C	generiert neue Startseite und liefert die Daten für eine heimliche Überweisung - 269 I, II
Malware	bereitet Überweisung bei der Bank vor – 263a I, II und sendet neue Startseite an den Browser
Bank	fordert iTAN
Malware	Anforderung wird abgefangen – 274 I Nr. 2

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware. Ablauf 2

C & C	generiert neue Anforderungsseite für iTAN – 269 I
Malware	gibt neue Anforderungsseite an Browser
Anwender	gibt geforderte iTAN ein – 263
Malware	fängt iTAN ab – 202b sendet iTAN an Bank und bestätigt damit die Überweisung – 263a
Bank	sendet Bestätigungsseite
Malware	fängt Bestätigungsseite ab – 274 I Nr. 2
C & C	generiert neue Bestätigungsseite mit den Grunddaten des Anwenders – 269
Malware	sendet neue Bestätigungsseite an Browser

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware. Ablauf 3

Anwender	**startet eigene Überweisung**
Malware C & C	**…** **▸ gleicher Ablauf** **▸ weitere Überweisung mit Daten vom C & C** **▸ Bestätigungsseite mit den Daten vom Anwender (auch Summe des Kontostandes und Fakeseite für die Überweisung des Anwenders)**
C & C	**generiert Fehlerseite**
Malware	**Hosttabelle wird geändert – 303b I Fehlerseite zum Browser gemeldet**

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware. Vorschriften

Abfangen von Daten	202b
Betrug	263
Computerbetrug	263a
Fälschung beweiserh. Daten	269
Urkundenunterdrückung	274 I Nr.2
Computersabotage	303b

Urkundenunterdrückung — Vergehen (bis 5 Jahre FS)

… beweiserhebliche Daten (§ 202a Abs. 2), über die er nicht oder nicht ausschließlich verfügen darf, in der Absicht, einem anderen Nachteil zuzufügen, löscht, unterdrückt, unbrauchbar macht oder verändert ...

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware. Recht 1

von zentraler Bedeutung ist der Computerbetrug – 263a

263a, 269 und 274 I Nr. 2

202a, 202b, 303a, 303b

303a wird von 303b verdrängt
202a, 202b sind nachgeordnet

Betrug wird dadurch vollständig verdrängt – 263

Tatanteile sind gleichwertig

können ebenfalls Tateinheit bilden

Computerbetrug in Tateinheit mit Fälschung beweiserheblicher Daten, Unterdrückung beweiserheblicher Daten und mit Computersabotage

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware. Recht 2

besonders schwerer Fall des Computerbetruges	263a II i.V.m. 363 III Nr. 1
… der Fälschung beweiserheblicher Daten	269 III i.V.m. 267 III
gewerbsmäßiger Bandencomputerbetrug	263a II i.V.m. 263 V
gewerbsmäßige Bandenfälschung beweiserheblicher Daten	269 III i.V.m. 267 IV
selbständige Verbrechen	Verabredung zu einem Verbrechen – 30 II

© Dieter Kochheim, 12.05.12

Onlinebanking-Malware. Ergebnis

Wenn eine arbeitsteilige Gruppe mit mindestens 3 Tätern plant, Onlinebanking-Malware einzusetzen, um damit dauerhaft kriminelle Beute zu erzielen, besteht der Verdacht der Verabredung zu einem Verbrechen des jeweils gewerbsmäßigen Bandencomputerbetruges und der Bandenfälschung beweiserheblicher Daten.

Vorbereitungsstadium:
- Malware herstellen
- Pharmen einrichten
- Malware verbreiten
- Malware pflegen
- Arbeitsvorgänge überwachen

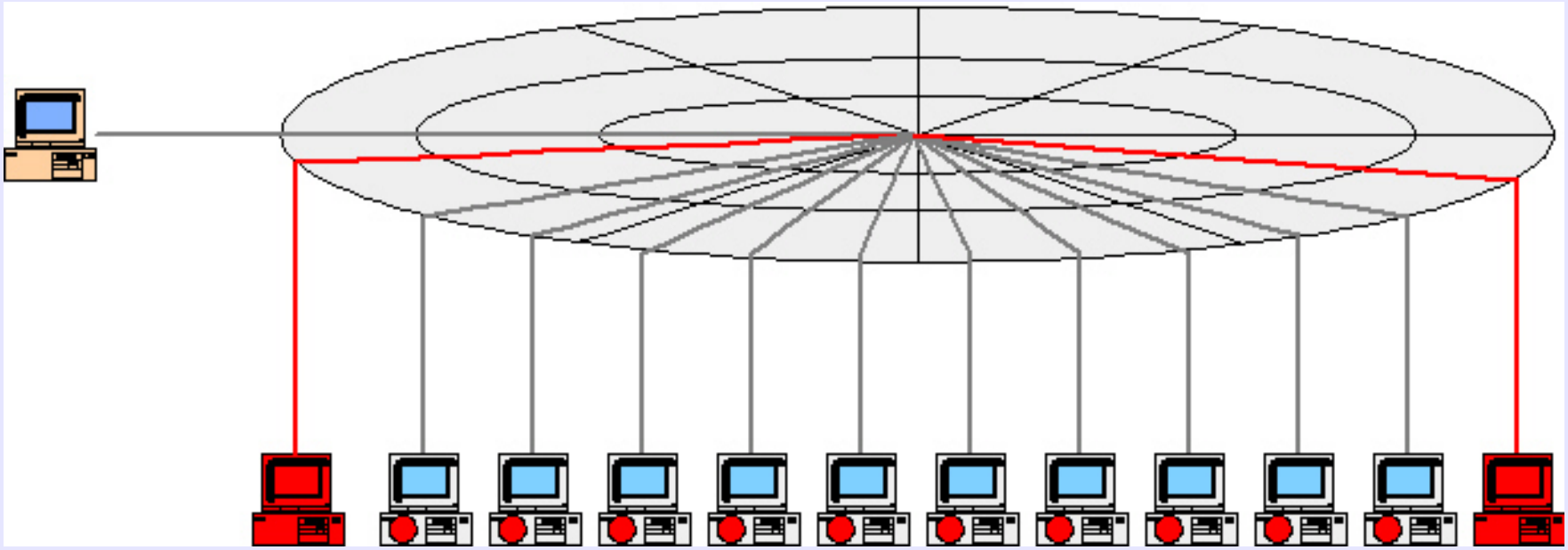
Versuch:
- beim Aufruf der Bankseite

Vollendung:
- Anlieferung erster Fakeseite
- Eingabe der iTAN bei der Bank

Beendigung:
- Manipulation der Hosttabelle
- Gutschrift der Beute

© Dieter Kochheim, 12.05.12

Botnetze



Infiltration einer Vielzahl von Computern mit Malware (Botware), um sie als verbundenes Netz zu verschiedenen kriminellen Aktionen zu missbrauchen (Zombies)

- **Zombies**
- **C & C-Server**
- **Fluxserver**

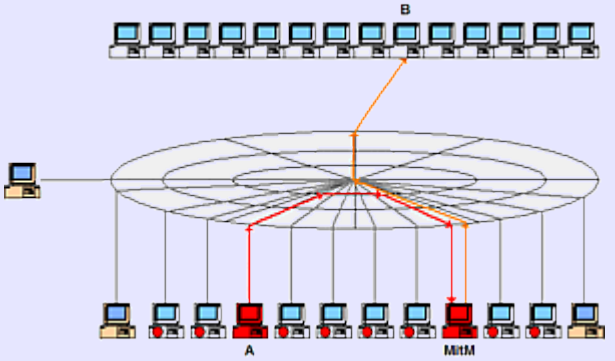
- **peer-to-peer-Technik: gegenseitiges Update der Zombies**

© Dieter Kochheim, 12.05.12

Botnetze

Einsätze am einzelnen Gerät:

- Ausspähen des einzelnen Zombies
- Nutzung als Konsole
- Nutzung als Fluxserver
- Nutzung als Fileserver (Speicher)



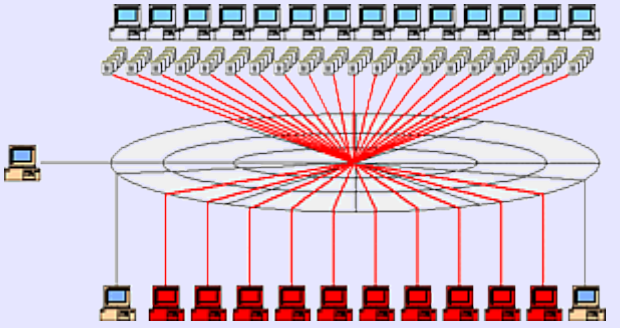
Einsätze im Verbund:

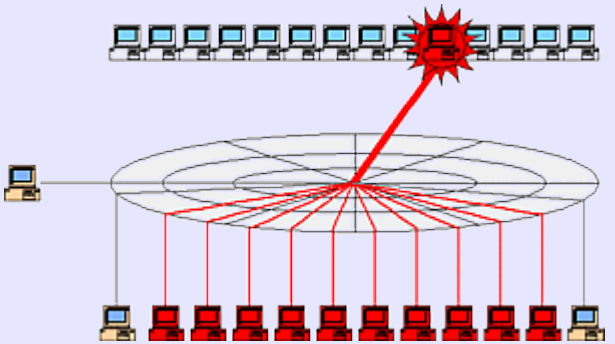
- Versand von Spam-Mails
- Versand von Malware-Anhängen
- Distributed Denial of Service – DDoS
- Einsatz als Rechnerverbund

  Zugangskennungen

  – Brute Force, Cracking

  Verrechnungseinheiten – BitCoin

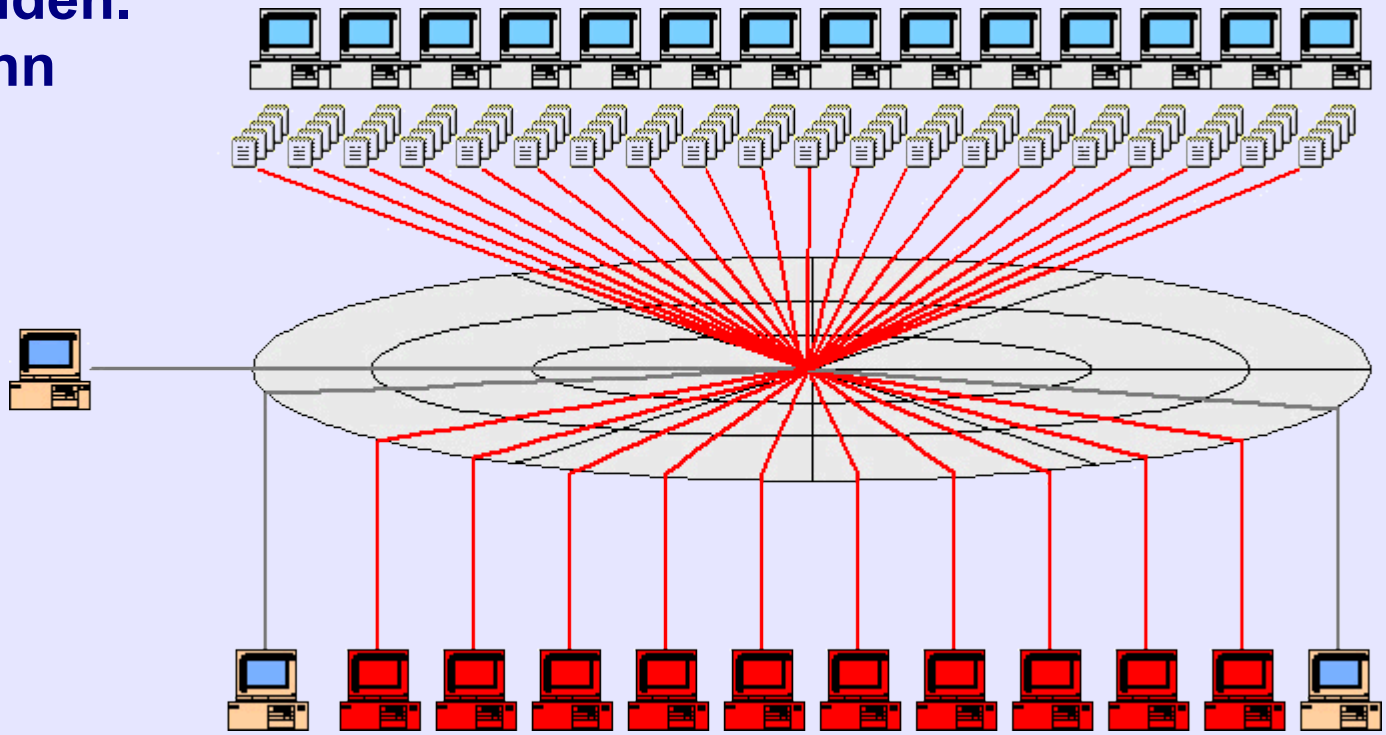




© Dieter Kochheim, 12.05.12

Botnetze

Mit einem eher kleinen Botnetz von rund 20.000 Zombie-Rechnern benötigt ein Botnetz-Betreiber für die Ausführung eines Auftrags mit 1.000.000 Mails bei ... 2 Mails pro Sekunde und aktivem Bot gerade mal 25 Sekunden. Rein rechnerisch kann er für den Versand also bis zu 115.200 US-Dollar pro Stunde verdienen.



© Dieter Kochheim, 12.05.12

Botnetze

Strafbarkeit wie beim Einsatz von Malware:

▸ bes. schw. Fall der schweren Computersabotage	303b IV	6 M – 10 J
gewerbsm. *oder* Bande	303b IV Nr. 2	
Vermögensverlust großen Ausmaßes	303b IV Nr. 1	

… nach der Art des Einsatzes:

▸ Erpressung bei DDoS	253 I	GS – 5 J
bes. schw. Fall (gew. oder B.)	253 IV	1 J – 15 J
▸ Computersabotage (Anhänge)	303b IV	6 M – 10 J
▸ Computerbetrug (Konsole)	263a I	GS – 5 J
schwerer Computerbetrug	263a II, 263 V	1 J – 10 J

© Dieter Kochheim, 12.05.12

globale Botnetze

Es gibt rund 2 Dutzend große globale Botnetze

- Paget: Für den Betrieb bedarf es wahrscheinlich 2 Vollzeit-Programmierer
- hinzu kommen wahrscheinlich 2 Leute für die kaufmännische Betreuung und die Beutesicherung
- DNS Changer: 6 Täter, die über einen Zeitraum von 4 Jahren zusammengearbeitet haben.
- auf Dauer angelegte Zusammenarbeit
- gewerbsmäßiges Handeln
- Bandenabrede
- kriminelle Vereinigung

© Dieter Kochheim, 12.05.12

kriminelle Vereinigung

kriminelle Vereinigung – 129

- Gründung, Mitgliedschaft — Freiheitsstrafe bis 5 Jahre
- Hinterleute 129 IV — Freiheitsstrafe bis 10 Jahre
- Rädelsführer 129 IV

- Unterstützer — „wesentliche Förderung“

Klammerwirkung führt zu einer einheitlichen *materiellen* Tat

Tatmehrheit richtet sich nach der einzelnen Unterstützungshandlung

BGH, B. vom 19.04.2011 - 3 StR 230/10 (Internetradio)

Staatsschutzdelikt nach 74a I Nr. 4. GVG

© Dieter Kochheim, 12.05.12

betrügerische Webshops

Handel mit begehrten Waren (Elektronik)

Vorkassebetrug

- Tarnung der Identität
- Tarnung des Standortes
  bullet proof Services
  Schurkenprovider
- Geldwäsche

© Dieter Kochheim, 12.05.12

Abofallen

Werbung mit komfortablem und schnellem Download

Kochrezepte, Schülerhilfe Musteraufsätze

- **versteckte AGB**
- **irreführende Buttons**
- **unauffälliger Text**

Offertenbetrug

BGH, Ur. vom 26.04.2001 – 4 StR 439/00

- **Forderung der Abogebühren (Versuch des Betruges)**

Göttinger Abofalle

LG Göttingen, Ur. vom 17.08.2009 - 8 KIs 1/09

10 Taten des gewerbsmäßigen Betruges (10 Spam-Aktionen)
2 Täter, 1 Gehilfe, keine Bande
1.000 Opfer
mindestens 130.000 € Beute
Freiheitsstrafen bis zu 1 J 6 M

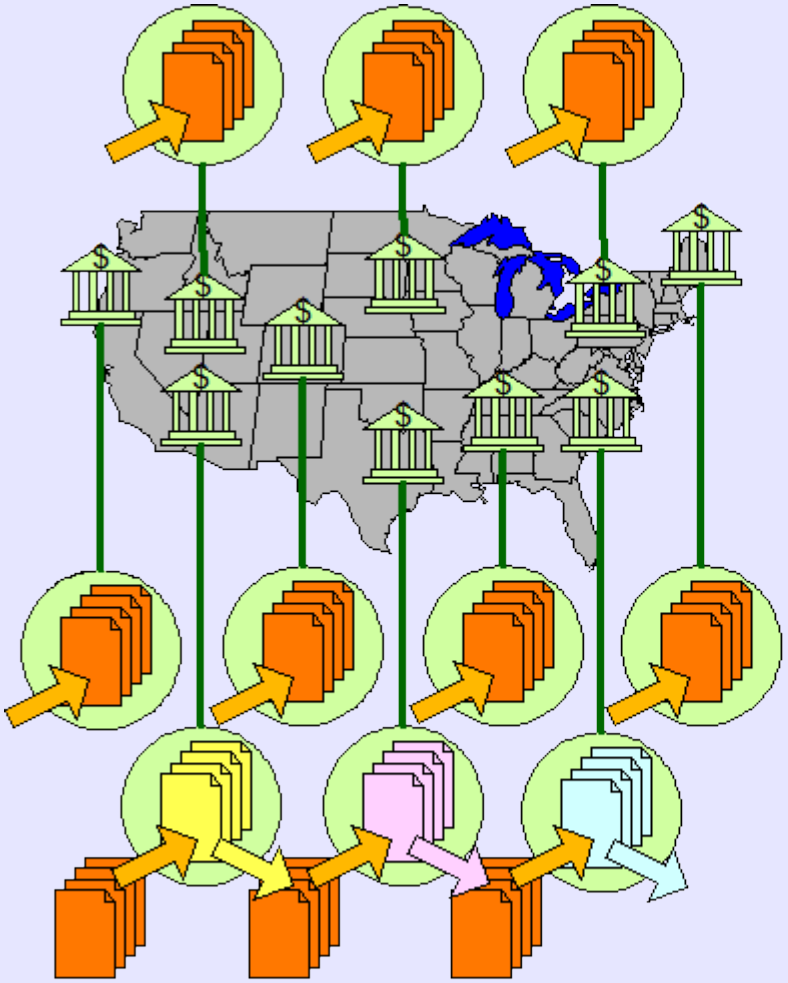
- **gezieltes Spear-Phishing anhand rechtswidrig erlangter Kundendaten**
- **automatisches Inkasso mit den Daten aus der Datenbank**
- **keine Auseinandersetzung mit 17 II Nr. 1., 2. UWG: eigennütziges Verschaffen und Verwertung fremder Geschäftsgeheimnisse**

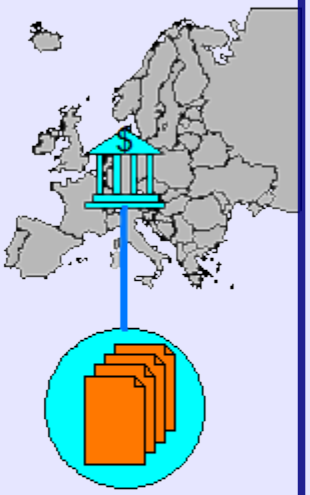
© Dieter Kochheim, 12.05.12

Kursmanipulation

… mit Penny-Stocks

- kein stoffgleicher Vermögenszuwachs
- keine eigennützige Geldwäsche
  261 IX S. 2





© Dieter Kochheim, 12.05.12

weitere Erscheinuungsformen

was fehlt noch?

- **Skimming**
- **Carding-Boards**
- **Koordinatoren**
- **Operating Groups**
- **Schurkenprovider**

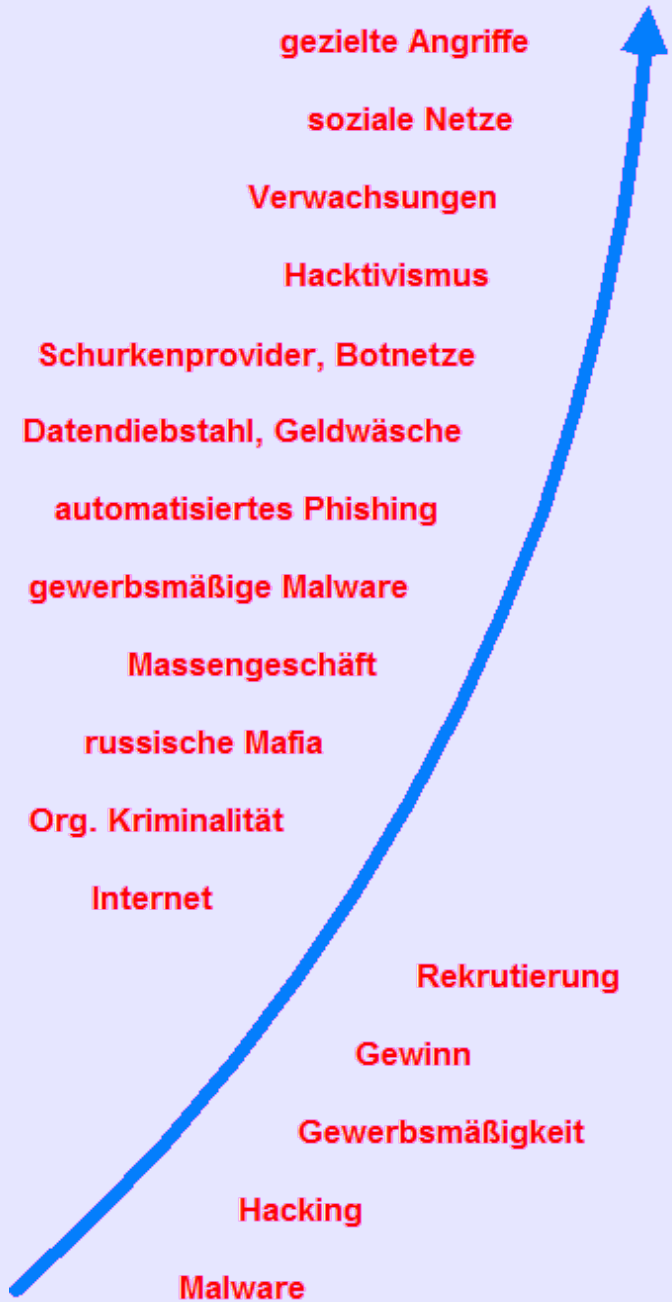
© Dieter Kochheim, 12.05.12

Teil 4

Zeitgeschichte der Cybercrime

© Dieter Kochheim, 12.05.12

Zeitgeschichte der Cybercrime



gezielte Angriffe
soziale Netze
Verwachsungen
Hacktivismus
Schurkenprovider, Botnetze
Datendiebstahl, Geldwäsche
automatisiertes Phishing
gewerbsmäßige Malware
Massengeschäft
russische Mafia
Org. Kriminalität
Internet
Rekrutierung
Gewinn
Gewerbsmäßigkeit
Hacking
Malware

2010: Aurora, Night Dragon, Stuxnet, WikiLeaks, Anonymous, Reaktionen
2009: Twitter-Wurm, PirateBay
2008: DDoS (Litauen, Georgien), Online-Phishing, RBS WorldPay
2007: Pharming, Estland, Malware-Baukästen
2006: RBN, Gozi-Botnet, DarkMarket
2005: TJX-Hack, Finanzagenten
2004: Homebanking-Trojaner, Sasser, TeamEvil, Phishing, Musik-Download
2003: Hackerschulen, Trojaner-Verkauf
2002: Glückspiel, Sportwetten
2001: CarderPlanet
2000: Skimming, Defacement
1998: Virus-Fabriken, Grabbing, Filesharing
1997: Green Army, Dialer
1996: Pornographie, Phishing
1990: Hackerfabriken
1985: KGB-Hack
1982: Viren

© Dieter Kochheim, 12.05.12

Neuzeit bis 2000

1982	Malware	Viren und Varianten
1985	Hacking	KGB-Hack *(Kuckucksei)*
1990	Gewerbsmäßigkeit	Hackerfabriken in Bulgarien
1996	Gewinnstreben	Pornographie *(USA)* Phishing *(Osteuropa)*
1997	Rekrutierung	Green Army *(Hackerszene in China)* Dialer *(Einwahlhilfen, Mehrwertdienste)*
1998	Internet	Virusfabriken in Russland Grabbing *(Diebstahl von Internetadressen)* Filesharing *(direkter Datentausch)*
2000	Organisierte Kriminalität	Skimming Defacement *(Verunstaltung, Propaganda)*

© Dieter Kochheim, 12.05.12

Hackerschulen, Virusfabriken

Paget:

In Russland begann der Hacking-Boom 1998 infolge der Finanzkrise.
Eine Armee von jungen, gut ausgebildeten Programmierern hatte plötzlich keine Arbeit mehr und sie sahen sich einem Umfeld von Korruption, wirtschaftlichem Niedergang und beginnender Internetkriminalität ausgesetzt. Auch hier entstanden wie in Bulgarien „Virus-Fabriken“.

© Dieter Kochheim, 12.05.12

Carding

2001 russische Mafia CarderPlanet

Paget:

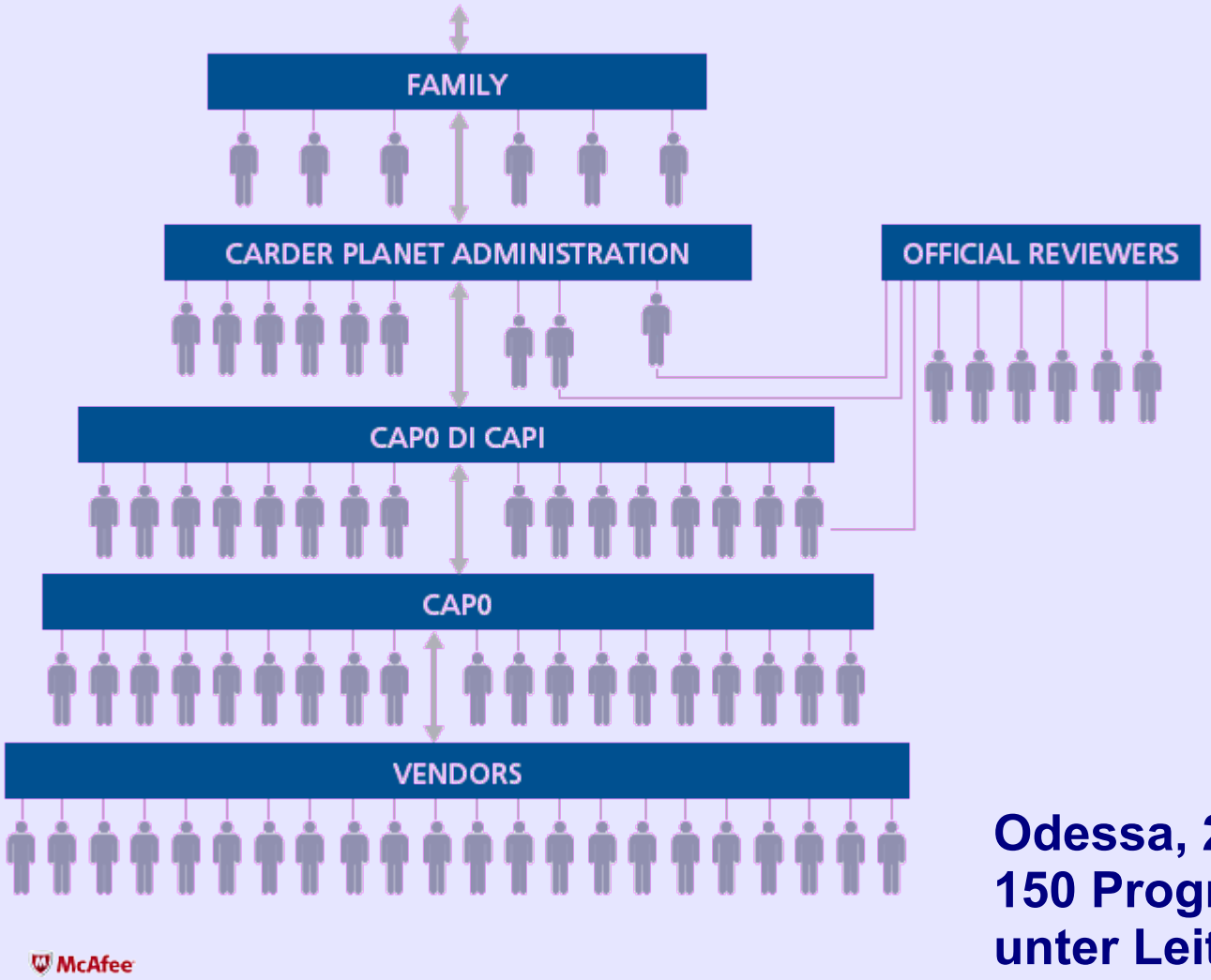
Im Mai 2001 trafen sich in Odessa 150 Cyber-Kriminelle und gründeten CarderPlanet. Sein sichtbarer Teil ist ein Forum (CardersPlanet), in dem Zahlungskartendaten von Hackern aus den USA und Großbritannien gehandelt wurden. Diese Daten wurden verkauft oder auf Kommission überlassen, um mit ihnen Internetgeschäfte abzuwickeln oder Zahlungskarten zu fälschen.

Carding = Kreditkartenbetrug

- **Bezahlen mit ausgespähten Kreditkartendaten**
- **Phishing (Onlinebanking)**
- **Skimming (Cashing)**
- **Identitätsdiebstahl im Allgemeinen**

© Dieter Kochheim, 12.05.12

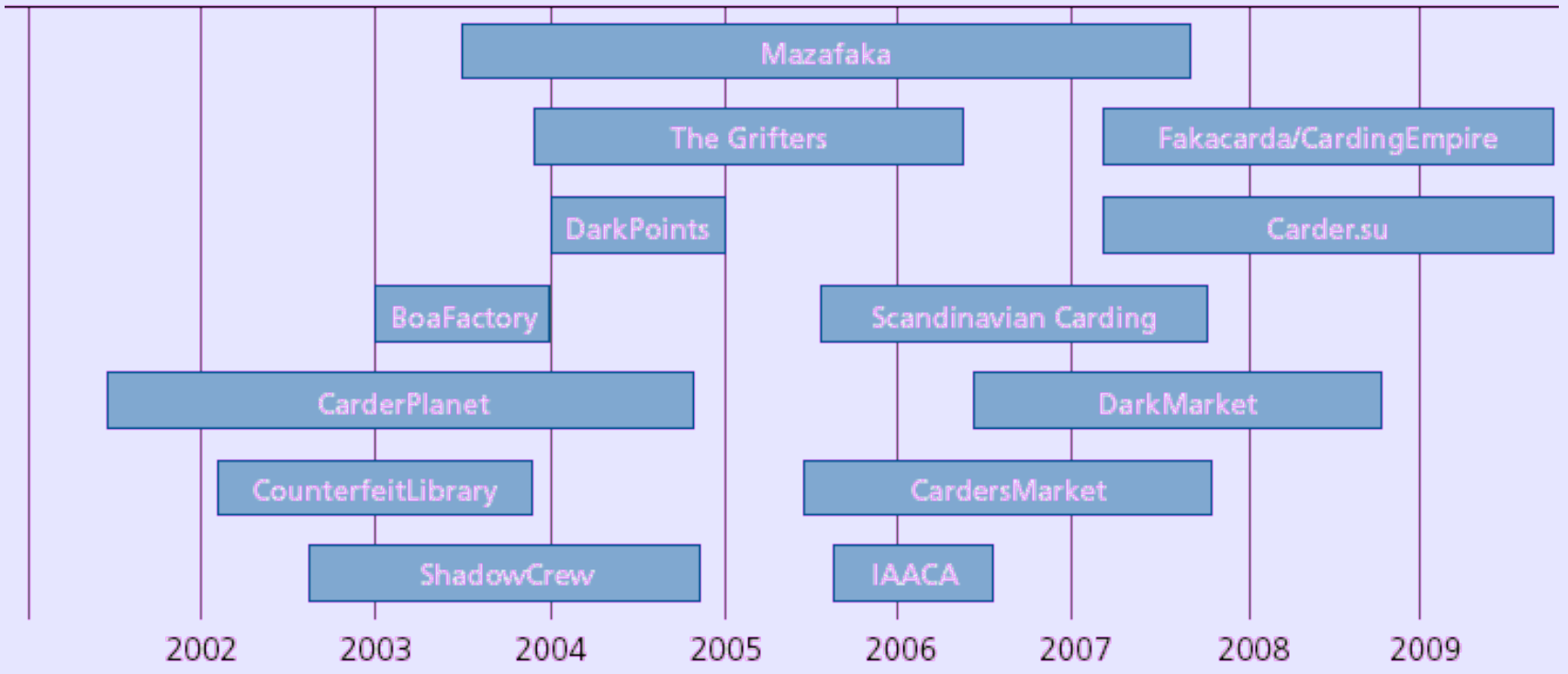
CarderPlanet



Odessa, 2001
150 Programmierer gründen unter Leitung von „Gottvater Dmitry Golubov“ das erste Carding-Board

© Dieter Kochheim, 12.05.12

Carding-Boards



McAfee

geschlossene Benutzergruppen
Gewinnbeteiligung des Veranstalters
Abschottung

Daten, Malware, Exploits, Diplome, Personalpapiere - alles

© Dieter Kochheim, 12.05.12

Carding-Boards

Carding-Boards in Deutschland:

etwa 20 Carding-Boards in Deutschland

Dumps von rivalisierenden Gruppen

Erfahrungsberichte (Benzmüller, Moritz Jäger, Paget)

Beobachtungen

vedeckte Ermittlungen

Hier finden alle ein Zuhause, die Drop Zones für die Daten ihrer Botnetze suchen, illegale Shops betreiben, Command & Control (C&C)-Server sicher unterbringen wollen und dergleichen mehr. Unter Dropzones ist in diesem Zusammenhang ein Server zu verstehen, auf dem beispielsweise die auf dem Rechner des Opfers installierte Spyware ihre gesammelten Daten ablegen kann. Das Produktportfolio reicht hier wie bei jedem seriösen Anbieter vom kleinem Webspace-Angebot, über virtuelle Server bis hin zu ganzen Serverclustern, je nach Geldbeutel und Anforderungen.

© Dieter Kochheim, 12.05.12

Carding-Boards

Carding-Boards in Deutschland:

Zugangsdaten
- Bankkonten, PayPal
- Kaufhauskonten
- Paketstationen

Fälschungsgeräte
- für Zahlungskarten
- Prägestempel für Ausweise
- Skimmer
- Papiere, Tinten

Fälschungen
- Ausweise, Pässe
- Diplome
- Fahrkarten

- Waffen
- BtM

- alles

© Dieter Kochheim, 12.05.12

Neuzeit bis 2005

2002	Massengeschäft	Glückspiel, Sportwetten *vor allem im englischsprachigen Raum*
2003	gewerbsmäßige Malware	Hackerschulen in Moskau Trojaner-Verkauf *(Osteuropa)*
2004	automatisiertes Phishing	Homebanking-Trojaner Sasser TeamEvil *(Hacktisvismus gegen Israel)* Musik-Downloads
2005	Geldwäsche Datendiebstahl	Finanzagenten TJX-Hack *94 Millionen Kundendatensätze beim Finanzdienstleister TJX (USA) gestohlen* *Vertrieb in den Dark Markets*

© Dieter Kochheim, 12.05.12

Pornographie, Glückspiel

Paget:

Mehrere Mitglieder der Gambino-Familie gestanden 2005, von 1996 bis 2002 auf ihren kostenlosen Pornoseiten als Altersnachweis von den Besuchern ihre Kreditkartendaten verlangt zu haben.

Durch deren Missbrauch hätten sie mehr als 750 Millionen US-$ erbeutet.

Paget:

2007 gestand Nicholas "Nicky the Hat" Cimino, seit 2002 einen kriminellen Umsatz von monatlich rund 1 Million US-$ erzielt zu haben.

In Kanada verdiente die Mafia zwischen 2005 und 2006 binnen 18 Monaten 26 Mio. Dollar mit betwsc.com, einer illegalen Seite für Sportwetten. Der Server befand sich in Belize und später in der indianischen Reservation of Kahnawake, westlich von Montreal in Québec. Die wichtigste Person hinter der Betrug soll einen persönlichen Gewinn von 17 Mio. C-$ erzielt haben.

© Dieter Kochheim, 12.05.12

TJX-Hack

Paget:

TJX: Zwischen 2005 und 2007 wurden von 94 Mio. Kunden dieses Unternehmens aus Nordamerika und Großbritannien die Kreditkarten-Nummern gestohlen. Im August 2008 wurden elf Personen verhaftet, darunter drei US-Bürger, ein estnischer, zwei chinesische, ein weißrussischer Täter und drei Ukrainer. Nach Medienberichten waren sie Teil eines internationalen Hacker-Netzwerks, das in das Funknetzwerk (Wi-Fi) und in die Daten der leitenden Angestellten eingedrungen war.

© Dieter Kochheim, 12.05.12

Neuzeit bis 2006

2006 **Schurkenprovider** *(Rogue Provider)*

Russian Business Network *(St. Petersburg)*

Bullet-Proof-Dienste

- technische Verschleierung
- DNS-Protection
- Aliasnamen, Scheinfirmen
- keine Auskünfte an Dritte

- stabile Anbindung an das Internet
- technische Infrastruktur
- soziokulturelle Einbindung

© Dieter Kochheim, 12.05.12

Schurkenprovider

Balduan (2008):

Die Rogue Provider werben mit „bullet proof hosting“, also versprechen im Prinzip, dass sie Ermittlungen von Strafverfolgern nicht übermäßig unterstützen und dass sie auf Missbrauch-Beschwerden nicht reagieren.

Das ... Geschäftsmodell des RNB war simpel und dreist: Je mehr eine Domain in den Fokus der Öffentlichkeit geriet, je mehr Beschwerden an die E-Mail-Adresse für Missbrauch geschickt wurden, desto mehr Geld verlangten die Russen von ihren Kunden.

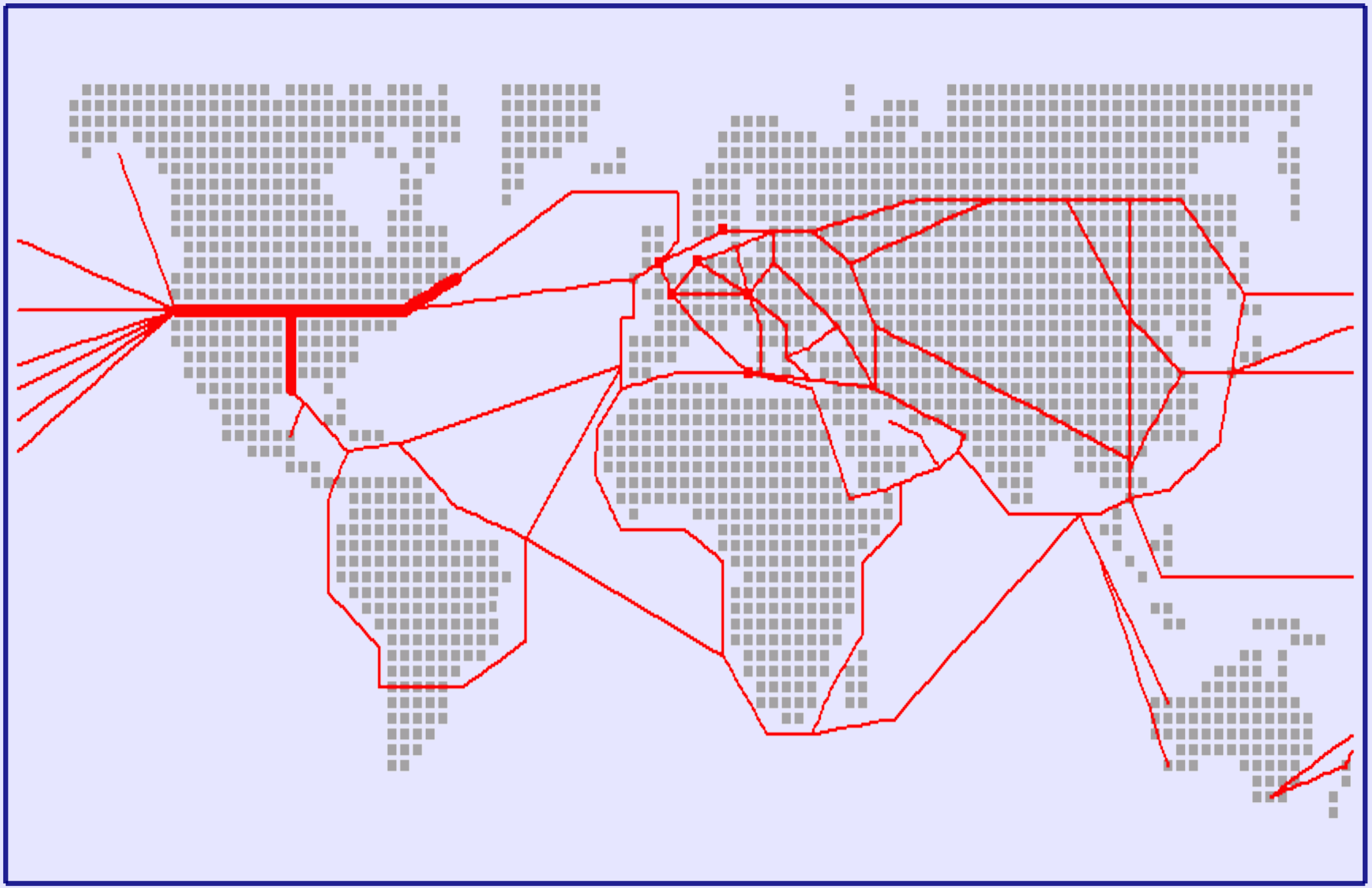
Paget: … etwa 600 $ im Monat.

Schurkenprovider:

- vollwertiger Internetprovider
  Autonomes System - AS
- Bullet Proof Hosting
  „sichere“ Speicherplätze für Boards, Daten, „Drops“, Pharmen, Malware.
- DNS-Protection
  Verschleierung der Domaininhaber
- Beschwerderesistenz
- Scheinfirmen
- Geldverkehrsabwicklung
- gesellschaftliche Einbindung

© Dieter Kochheim, 12.05.12

„Internetz“



© Dieter Kochheim, 12.05.12

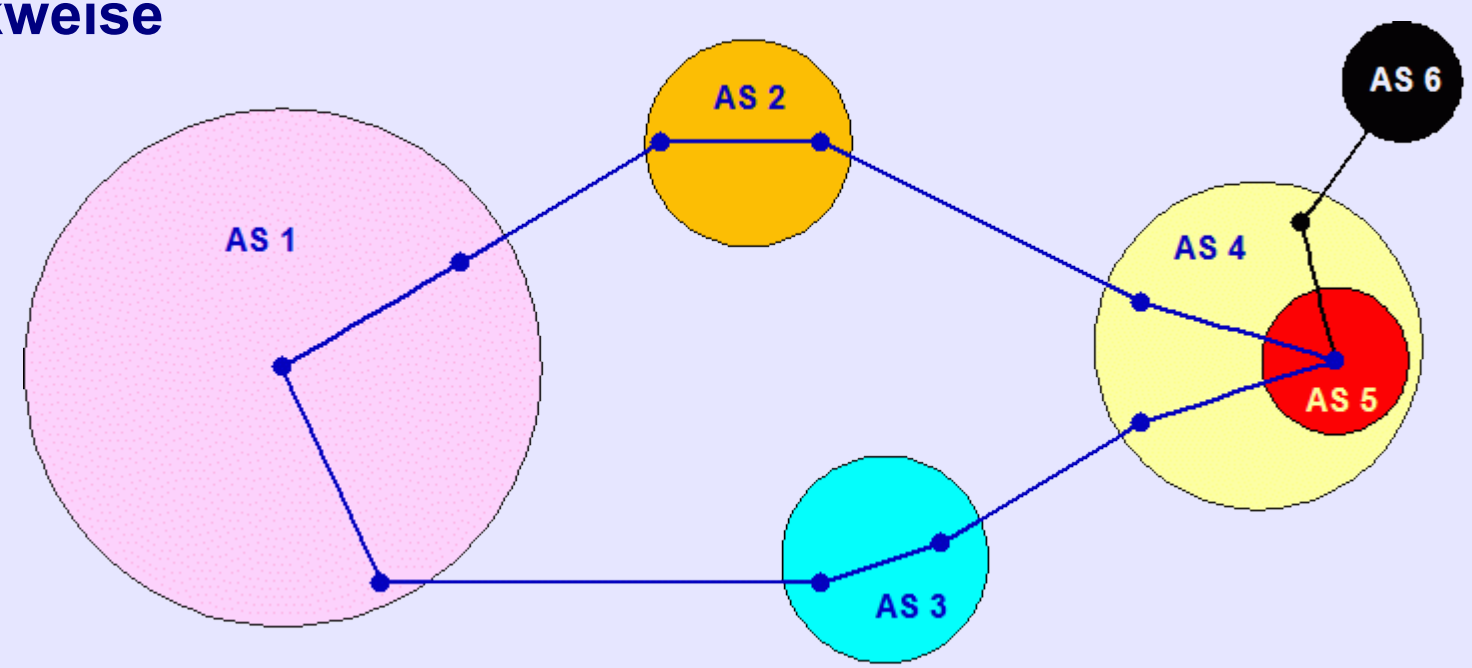
Autonome Systeme

Border Gateway Protocoll – BGP

Autonome Systeme
Verbindung zu mindestens 2 anderen AS

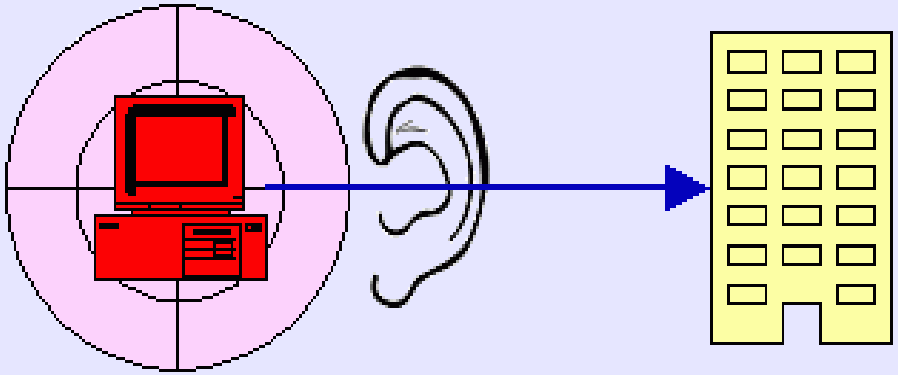
Vertrauen
keine Kontrolle

AS-Nummern von
- **ICANN, blockweise**
- **RIPE, einzeln**



© Dieter Kochheim, 12.05.12

Identitätsdiebstahl



alle persönlichen Daten, die einen Wert auf dem Schwarzmarkt haben

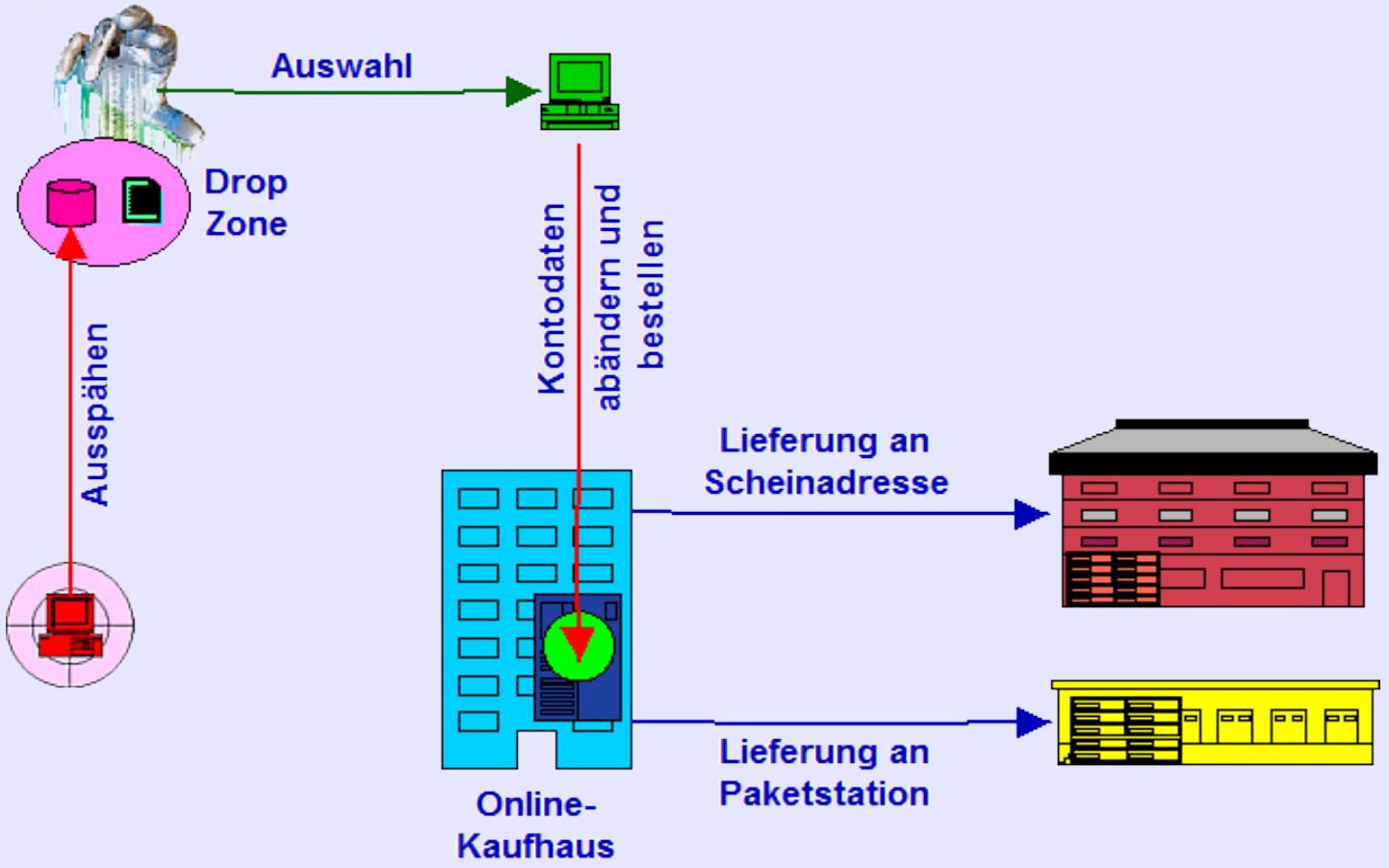
- Onlinebanking (Phishing)
- Handelskonten (Kaufhäuser, Amazon, eBay, PayPal)
- Sozialversicherung (USA)
- Personalpapiere

Phishing

- E-Mail-Formulare
  zur Eingabe der Kontodaten, PIN, TAN
- Spyware
  Trojaner mit Keylogger und Suchfunktionen
  DropZone
- Online-Phishing
  Man-in-the-Middle

© Dieter Kochheim, 12.05.12

Beutesicherung



- Finanzagenten
- Warenagenten
- Fake-Bankkonten
- Bezahlsysteme

© Dieter Kochheim, 12.05.12

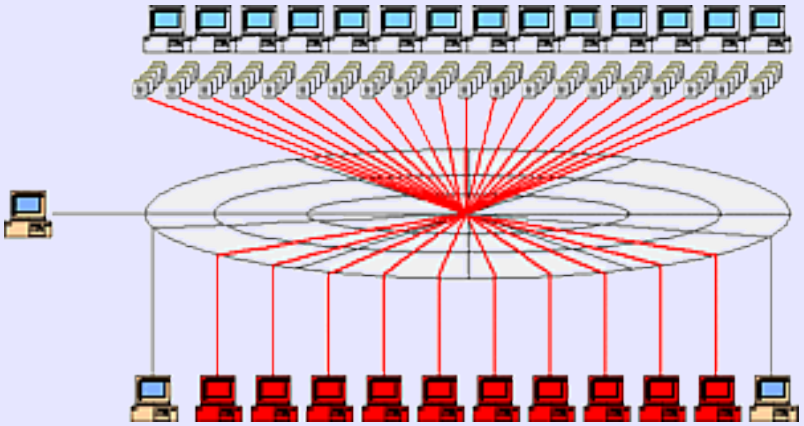
Neuzeit bis 2006

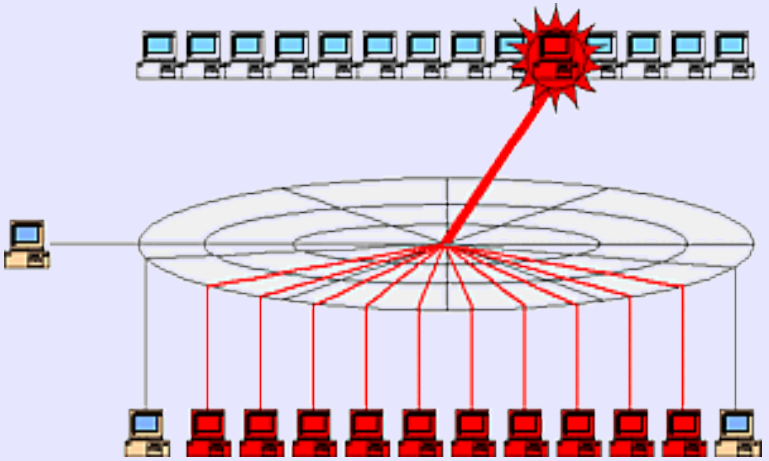
2006 Botnetze

Gozi-Botnet

Fernsteuerung einer Vielzahl von Zombies
- Malware, Exploits, Rootkits
- Fernwartung, Filesharing

- Spam, Malwareverbreitung
- verteilte Angriffe *(DDoS)*
- Auspähen
- Kontrolle *(CC-Server, Webserver)*





© Dieter Kochheim, 12.05.12

2006 kriminelles Projektmanagement

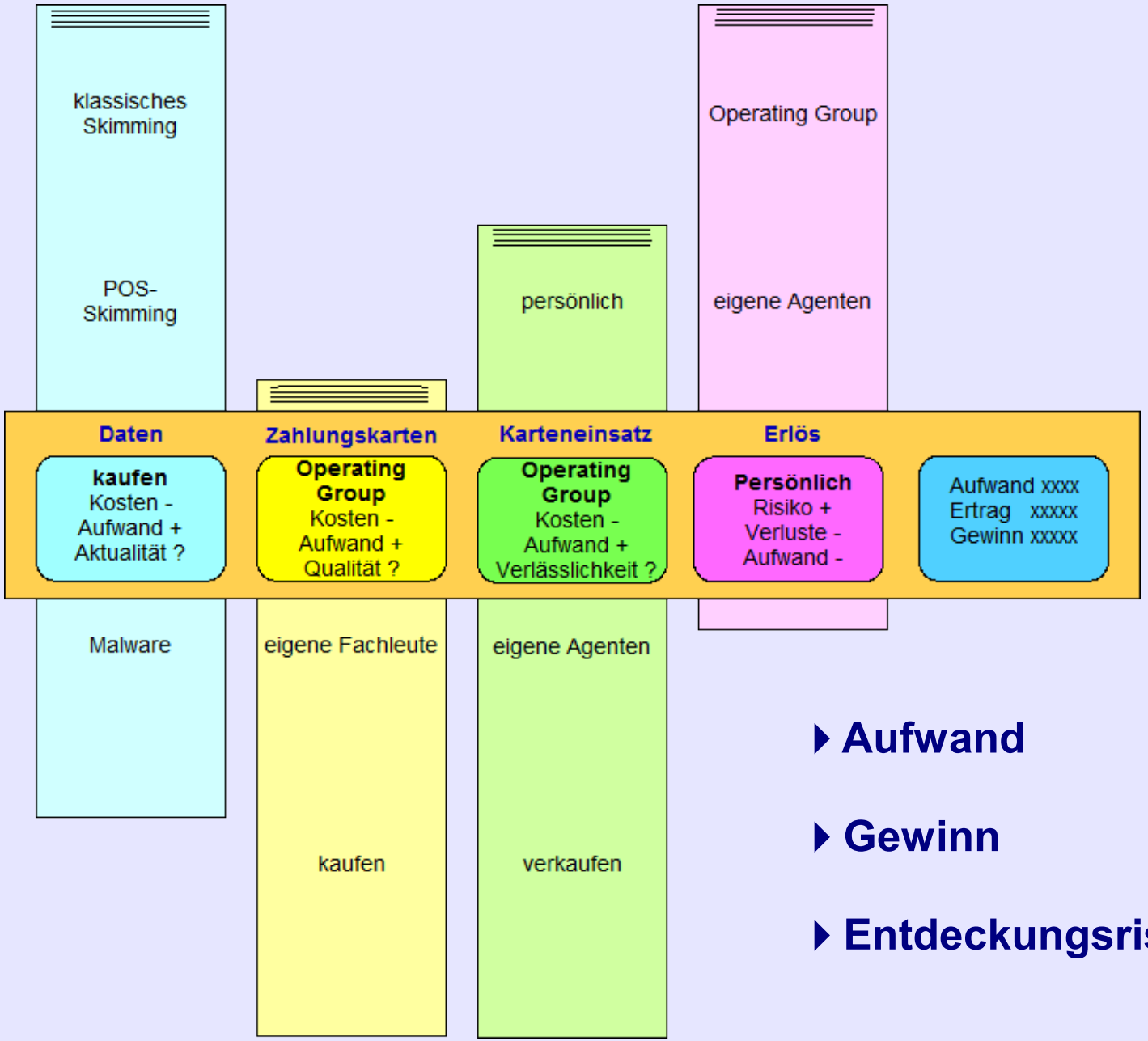
Koordinatoren

Balduan

Die zentrale Figur jedoch ist ... ein „Independent Business Man“ – eine Person, die Kontakte zur Unterwelt pflegt und zwischen Bot-Herdern, Hackern, Malware-Schreibern und Spammern koordiniert. ... mithilfe der Botnetz-Infrastruktur kann der Koordinator Unternehmen mit verteilten Massenangriffen auf ihre Webseiten drohen und so Schutzgeld erpressen, Spam-Wellen mit Werbung für überteuerte Produkte oder Aktien lostreten oder tausendfach persönliche Informationen wie Bankzugangsdaten ergaunern.

© Dieter Kochheim, 12.05.12

Kalkulation



- **Aufwand**
- **Gewinn**
- **Entdeckungsrisiko**

© Dieter Kochheim, 12.05.12

Operation Groups

2006 **kriminelles Projektmanagement**

Operation Groups

Balduan

Die Zwischenhändler bezeichnet Balduan als Operation Groups. Sie haben ihre Kontakte und Leute, auf die sie bei jedem Auftrag zurück greifen können. Sie und besonders ihre leitenden Unternehmer erleichtern das Geschäft für alle Beteiligten. Die Spezialisten müssen sich nicht um ihre Vermarktung kümmern und die Auftraggeber nicht darum, den richtigen Spezialisten oder Zulieferer zu finden.

Die Cybercrime organisiert sich dadurch arbeitsteilig und marktmäßig - um Straftaten zu ermöglichen und durchzuführen.

© Dieter Kochheim, 12.05.12

Organisierte Internetverbrecher

McAfee
Zweite große europäische Studie über das Organisierte Verbrechen und das Internet (2006)

Die Täter der Internetkriminalität reichen heute von Anfängern mit nur eingeschränkten Programmiererkenntnissen, die ihre Angriffe nur mit vorgefertigten Skripts durchführen können, bis hin zu gut ausgebildeten professionell arbeitenden Kriminellen, die über die aktuellen Ressourcen verfügen.

Wie in den meisten Gemeinschaften erfolgreicher Krimineller sitzen tief im Inneren einige streng abgeschirmte Köpfe, die sich auf die Mehrung ihrer Gewinne mit beliebigen Mitteln konzentrieren. Sie umgeben sich mit den menschlichen und technischen Ressourcen, die dies ermöglichen.

© Dieter Kochheim, 12.05.12

McAfee
Zweite große europäische Studie über das Organisierte Verbrechen und das Internet (2006)

- Innovatoren; Gefahr: gering.
- ruhmgierige Amateure und Nachahmer, Gefahr: Mittel.
- Insider; Gefahr: hoch.
- Organisierte Internetverbrecher; Gefahr: hoch.

© Dieter Kochheim, 12.05.12

Neuzeit bis 2009

2007	Hacktivismus	verteilter Angriff gegen Estland Pharming Malware-Baukästen
2008	Verwachsungen	verteilte Angriffe gegen Litauen und Georgien Online-Phishing RBS WorldPay
2009	soziale Netze	Twitter-Wurm PirateBay

© Dieter Kochheim, 12.05.12

RBS World Pay

Heise:

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

© Dieter Kochheim, 12.05.12

Neuzeit bis jetzt

2010 **gezielte Angriffe**

Eskalation

Industriespionage
- **Aurora *(Ausspähen, Google)***
- **Night Dragon *(Petrochemie, VPN-Tunnel)***

Sabotage mit Malware
- **Stuxnet**
  (iranische Atomanlagen, industrielle Steuerungen)

alternative Wirtschaft
- **WikiLeaks, Whistleblowing**
  (Afghanistan, Irak, Depeschen; DoS)

2011 **Shady Rat**

Hacktivismus
- **Anonymous *(DoS gegen Amazon, professionelles Hacking)***

Internet-Wirtschaft
- **gewerbliche Exploithändler**
- **IT-Söldner *(HBGary Federal)***

© Dieter Kochheim, 12.05.12

Teil 5

Kalter Cyberwar

© Dieter Kochheim, 12.05.12

Aurora

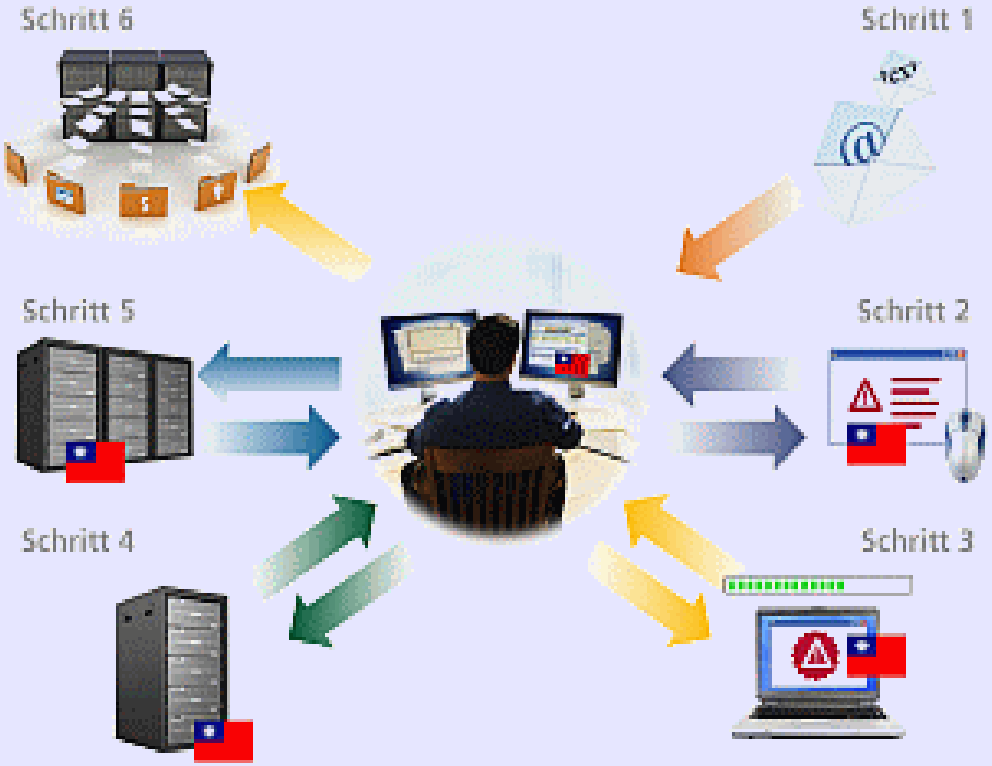
Aurora:

Gezielter Angriff chinesischer Herkunft gegen Google und rund 30 weitere Unternehmen Anfang 2010.

Ziel: vertrauliche Unternehmens-informationen, Industriespionage

Weg: gestufter Angriff

- **E-Mail**
- **Link zu infizierter Website**
- **Starter injiziert Exploit in Browser**
- **Download von Malware, die als Grafik getarnt ist**
- **Verbindung mit einem Botnetz in Taiwan**
- **Datenzugriff**
- **Ausbreitung im lokalen Netz**



Besonderheiten:

- **Zero-Day-Exploit**
- **detaillierte Kenntnisse über die IT-Infrastruktur der angegriffenen Unternehmen**

Quelle: McAfee

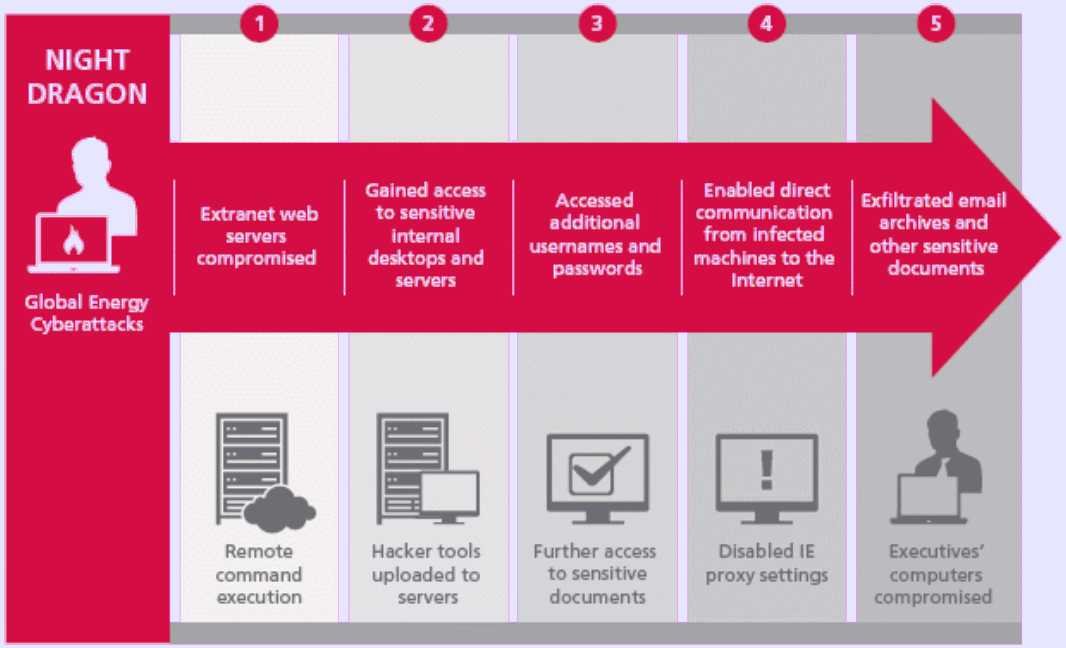
© Dieter Kochheim, 12.05.12

Night Dragon

Night Dragon:

Gezielter Angriff chinesischer Herkunft gegen Energie- und Ölverarbeitende Unternehmen seit Herbst 2009.

Ziel: Informationen über Reserven, Fördermengen, Strategien.



Weg: gestufter Angriff

- SQL-Injection gegen Webserver
- Infiltration des Active Directory
- Abschalten des Proxyservers
- Abschalten der Sicherheitsein-stellungen im Browser
- Fernzugriff aus China mit Command & Control - Server
- Durchgriff auf mobile Endgeräte durch VPN-Tunnel

Besonderheiten:

- besondere Kenntnisse über die IT-Infrastruktur der angegriffenen Unternehmen
- Infiltration gesicherter Netzverbindungen

Quelle: McAfee

© Dieter Kochheim, 12.05.12

Stuxnet

Stuxnet:

gezielte Sabotage der iranischen Atomanreicherungsanlage in Natanz

mindestens zwei Programmierer-teams seit 2007

keine Programmierer aus der Malware-Szene (Israel, USA)

Infiltration per USB-Sticks bei Mitarbeitern von Firmen, die am Bau der Atomanlagen beteiligt sind (seit Sommer 2009)

erfolgreiche Verzögerung und Behinderung der Fertigstellung

© Dieter Kochheim, 12.05.12

Stuxnet

Stuxnet:

- autonome Malware
- keine Anbindung ans Internet
- mehrere Schwachstellen, die bis zum Sommer 2010 unbekannt waren – Zero-Day-Exploits
- bislang unbekannte Rootkits
- gezielte Sabotage von mindestens zwei Industrieanlagensteuerungen von Siemens („Sprengköpfe“)
- Einkaufskosten allein für Exploits und Rootkits: sechsstellig
- Gesamtkosten: siebenstellig

Der Quellcode fand reges Interesse bei den Entwicklern von Malware und bei IT-Söldnern

© Dieter Kochheim, 12.05.12

Shady Rat

Shady Rat:

- C & C-Server seit 2006
- Spear-Phishing
- Backdoors zu weltweit 72 Unternehmen und Organisationen
- ausgespähte Daten in Peta-Bite-Größe
- reine Spionage
- wahrscheinlich chinesiche Herkunft

Kilobyte	normales Dokument
Megabite	PDF-Datei, E-Book
Gigabyte	Festplatten, Video
Terabyte	sehr große Festplatte
Petabyte	Speicher von Sony

© Dieter Kochheim, 12.05.12

WikiLeaks

WikiLeaks:

gegründet 2006
Whistleblowing-Plattform für regimekritische Dokumente aus China und anderen totalitären Staaten.

bis 2009:
vor Allem Einzeldokumente

Berico, HBGary Federal, Palantir

WikiLeaks ist keine Einzelperson und keine einzelne Organisation, sondern ein Netzwerk aus Personen und Organisationen, die nur deshalb zusammenarbeiten, um nicht nachverfolgbar massenhaft vertrauliche Dokumente zu veröffentlichen.

John Young

Wikileaks ist eine Geschäftsorganisation, die vorgibt, eine gemeinnützige Organisation zu sein.

© Dieter Kochheim, 12.05.12

WikiLeaks

2010 – Schlag auf Schlag

- Video aus der Kamera des Bordgeschützes eines Hubschraubers: Beschuss von irakischen Zivilisten und Journalisten
- Afghanistan-Krieg
- Irak-Krieg
- diplomatische Depeschen
- Guantanamo-Protokolle (April 2011)

© Dieter Kochheim, 12.05.12

Reaktionen auf WikiLeaks

Reaktionen auf WikiLeaks:

- CIA, März 2008:
  unterminieren, zerstören
- November 2010
  - Amazon, Sperrung Hostspeicher
  - DDoS gegen WikiLeaks
- Dezember 2010
  - Sperre gegen wikileak.org
  - mehr als 1.000 Mirrors
  - Kontensperren
  - Anonymous:
    DDoS gegen Amazon und Banken
- Januar 2011:
  - HBGary Federal:
    Analyse Anonymous-Anhänger
  - Palantir u.a.
    aggressive Strategie gegen WikiLeaks
- Februar 2011:
  - Anonymous hackt
    HB Gary Federal

© Dieter Kochheim, 12.05.12

Anonymous

kopfloses Kollektiv

besteht aus kleinen stabilen Gruppen und Einzelpersonen

2008: Aktionen gegen Scientology

2010: DDoS gegen Org. Amerikanischen Filmproduzenten – MPAA – und AiPlex Software

Operation Payback

Nachrichtenportal Crowdleaks (zunächst: Leakspin)

Hack gegen HBGary Federal

2011: Unterstützung des Aufstandes in Ägypten

OPSony, OPRecon

Payback, die neue Dimension:

Ein radikaler Teil der Internetgemeinde fordert die Einhaltung von Spielregeln ein! Unternehmen wie Amazon und große Finanzdienstleister können sich nicht mehr wie gewohnt selbstgerecht zurücklehnen, sich auf mehr oder weniger berechtigte AGB-Verstöße berufen, die ihnen so lange nicht aufgefallen sind, wie sie noch in Ruhe Geld verdienen konnten, oder gefahrlos politischem Druck aus dem Mainstream nachgeben. Die Angriffe von Anonymous machen sie zum Angriffsobjekt alternativen Wohlverhaltens. Das ist schmerzhaft!

© Dieter Kochheim, 12.05.12

Gegendruck

Manfred Messmer

Kein Staat, kein Unternehmen, keine Rechtsordnung kann akzeptieren, dass ein anarchistischer Schwarm von ein paar Tausend Usern sich auf willkürlich ausgewählte Unternehmen, staatliche und private Organisationen stürzt und deren Webseite – das heißt heutzutage deren Geschäftstätigkeit – für Stunden oder gar Tage lahmlegt.

© Dieter Kochheim, 12.05.12

Exploit-Handel

Exploit-Händler

- HP Tipping Point
- iDefense (Verisign)
- Vupen

Luigi, das kostet Dich etwas!

Das französische Unternehmen Vupen erstellt potenziellen Kunden eine Sicherheitsanalyse. Wenn der Kunde aber nicht zahlt, dann erhält er keine weiteren Informationen über die gefundenen Schwachstellen oder ihre Abwehr.

In der Branche wird ein bisschen von Erpressung gemunkelt.

Quelle: c't

© Dieter Kochheim, 12.05.12

IT-Söldner

Empfehlungen von Palantir, HBGary Federal und Berico:

- Gießen Sie heißes Öl zwischen die befeindeten Gruppen.
- Desinformation. Erstellen Sie Nachrichten über die Aktionen, um sie zu sabotieren oder die gegnerische Organisation zu diskreditieren. Nutzen Sie gefälschte Unterlagen und beschweren Sie sich dann über die Fehler.
- Zeigen Sie die Mängel in der Sicherheit der Infrastruktur.
- Schreiben Sie entlarvende Geschichten. Wenn Sie Glauben finden, dass der Gegner unsicher ist, dann ist er fertig.
- Cyber-Angriffe gegen die Infrastruktur zur anonymen Einsendung von Dokumenten. Dies würde das Projekt töten. …
- Medien-Kampagnen, um die radikale und rücksichtslose Natur der Wikileaks-Aktivitäten offenzulegen. Anhaltender Druck.
- Tut nichts gegen die Fanatiker, aber sät Bedenken und Zweifel unter den Gemäßigten.
- Sucht nach Lecks. Verwenden Sie soziale Medienprofile und identifizieren Sie riskantes Verhalten Ihrer Mitarbeiter.

© Dieter Kochheim, 12.05.12

professionelles Hacking

HBGary Federal

Informationsüberwachung des Datenverkehrs in Firmennetzen

Eindringen in fremde Datennetze (Exploits, Rootkits, Spionage)

Infiltration sozialer Netze mit künstlichen Persönlichkeiten

Auswertung von sozialen Netzen

Personifizierung von Anonymous-Anhängern

Anonymous-Hack

professioneller Angriff

Social Engineering

Veröffentlichung der Recherchen von Aaron Barr und der Firmen-Mails

© Dieter Kochheim, 12.05.12

graue Bezahlsysteme

Geldtransfer
- Western Union
- MoneyGram
- MoneyBookers

Verrechnungssysteme
- eGold, eSilver, ePlatinium
- WebMoney
- MoneyBookers
- Neteller

Bezugsscheine
- PaysafeCard
- ukash

Kreditkarten auf Guthabenbasis
- Wechselstuben
- vereinzelt keine Identitätsprüfung
- Beute aus dem Geldautomaten an der nächsten Ecke

eigene Bank gründen

Konto unter Alias

© Dieter Kochheim, 12.05.12

Gegenwehr

2007: Israelischer Luftangriff auf in Syrien vermutete Atomanlagen
begleitet von einem Totalausfall der syrischen Radarabwehr

2009: McCollo abgeschaltet
Spam-Aufkommen deutlich verringert

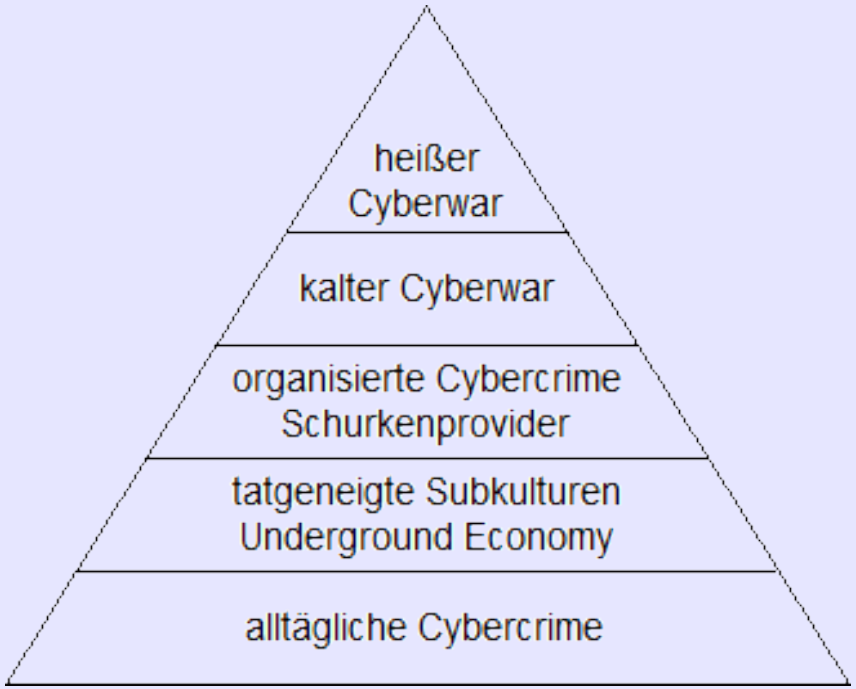
2011: Rustock-Botnetz abgeschaltet
auf Initiative von Microsoft

2011: Cyber-Abwehrzentrum unter Leitung des BSI

2011: Cybergenom-Projekt der DARPA
digitaler Fingerabdruck Trojaner in jedem elektronischen Bauteil Hardware Trojanische Pferde - HTH

© Dieter Kochheim, 12.05.12

Entwicklungsmodell Cybercrime-Cyberwar

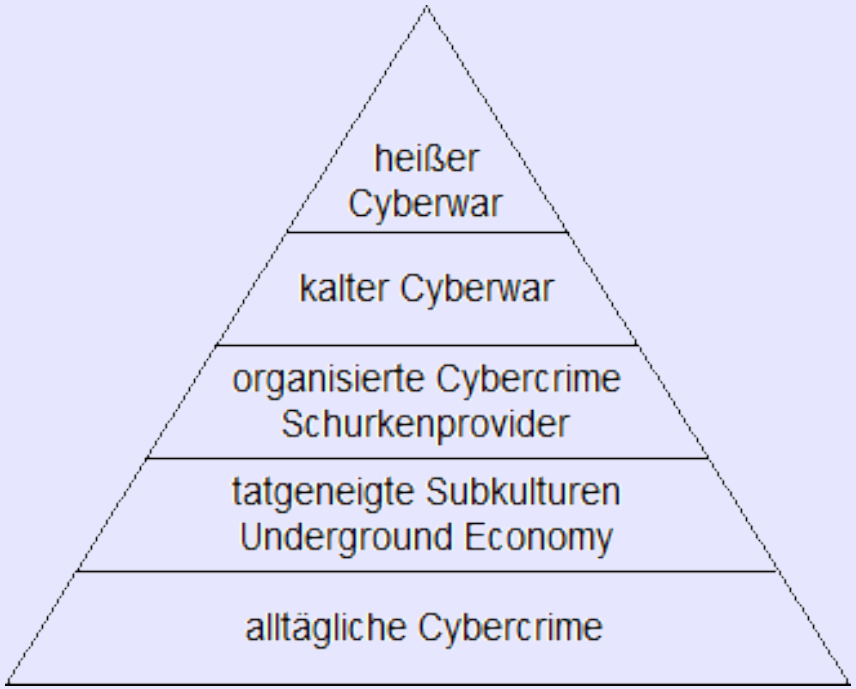


Myriam Dunn Cavelty

Aber das Verunstalten von Webseiten ist kein Cyberwar. DDoS-Attacken, auch wenn Banken betroffen sind, sind kein Cyberwar. Das Ausspionieren von Regierungsgeheimnissen oder der Klau von Wirtschaftsgeheimnissen mithilfe von Computern ist kein Cyberwar. Elektronische Kriegsführung ist nicht Cyberwar. Das Verbreiten von halb wahrer oder nicht wahrer Information im Krieg ist kein Cyberwar. Nicht einmal die Sabotage einer Industrieanlage mithilfe von ausgeklügelter Malware ist Cyberwar.

© Dieter Kochheim, 12.05.12

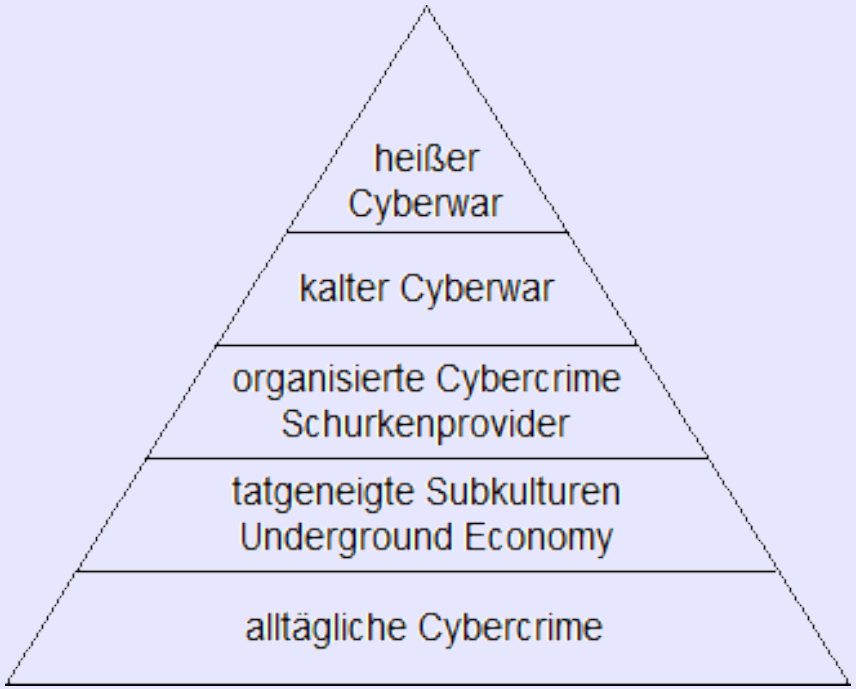
allgemeine Internetkriminalität



- Datendiebstahl *(Konten, Banking)*
  - Identitätsdiebstahl
  - Phishing
  - Finanzagenten
- „eBay“-Betrug
  - falsche Produktbeschreibungen
  - Vorauszahlungsbetrug
- Warenbetrug
  - falsche Identitäten
  - Fake-Adressen
  - Warenagenten
  - Packstationen
- Carding, Skimming
- Geldwäsche
  - „graue“ Zahlungssysteme
  - Kreditkarte auf Guthabenbasis

© Dieter Kochheim, 12.05.12

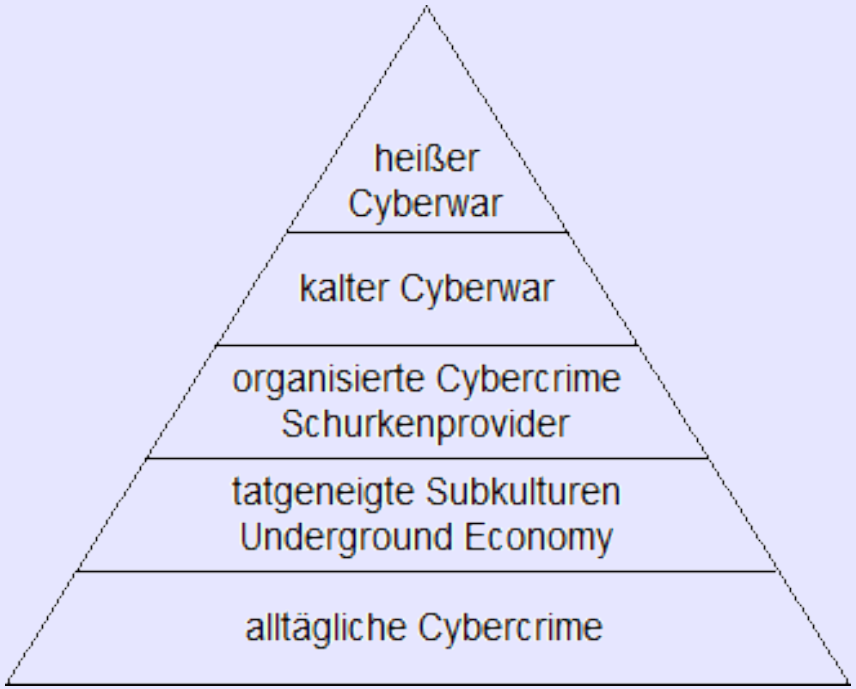
gewerbsmäßige Internetkriminalität



- **Board-Administratoren**
- **Malware-Entwickler**
  (Operating Groups)
- **Exploit-, Rootkit-Händler**
- **Projektleiter *(Koordinatoren)***
- **Webshop-, Inkassodienste**
- **„Wechselstuben“**
- **Hacktivisten**

© Dieter Kochheim, 12.05.12

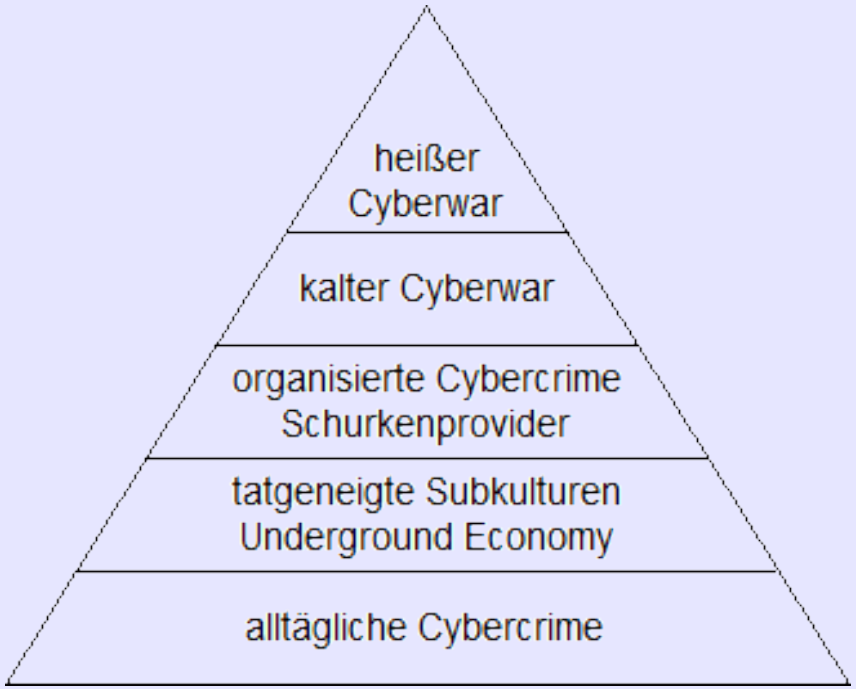
organisierte Internetkriminalität



- **Board-Betreiber**
- **Botnetz-Betreiber**
- **Schurkenprovider**

© Dieter Kochheim, 12.05.12

kalter Cyberwar



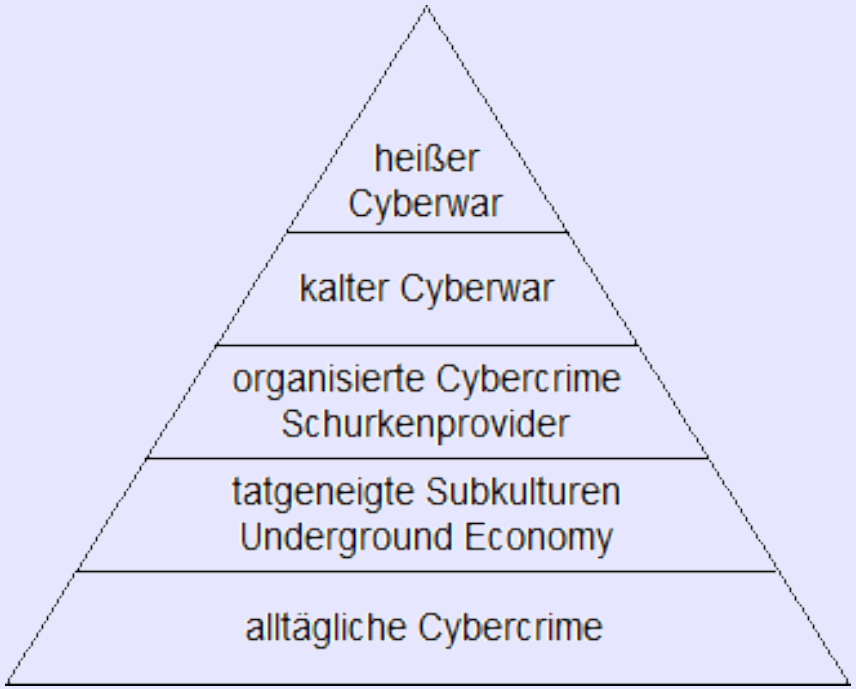
taktische Phase des Kräftemessens
Was kann ich bewirken?
Wie sind die Gegner aufgestellt?
Wie reagieren sie?

weitere „Mitspieler“

- **organisierte Kriminalität**
- **Nachrichtendienste**
- **Militär**
- **Paramilitär**
- **Terroristen**
- **Hacktivisten**
- **Wirtschaftsunternehmen**
- **Söldner**

© Dieter Kochheim, 12.05.12

heißer Cyberwar



Cyberwar ist der strategische Einsatz der Informations- und Kommunikationstechnik mit dem Ziel, Gegner und Opfer existenziell zu schädigen, also nicht nur ihre Datenverarbeitung und Netzkommunikation zu stören oder auszuschalten, sondern ihre Funktionstüchtigkeit insgesamt.

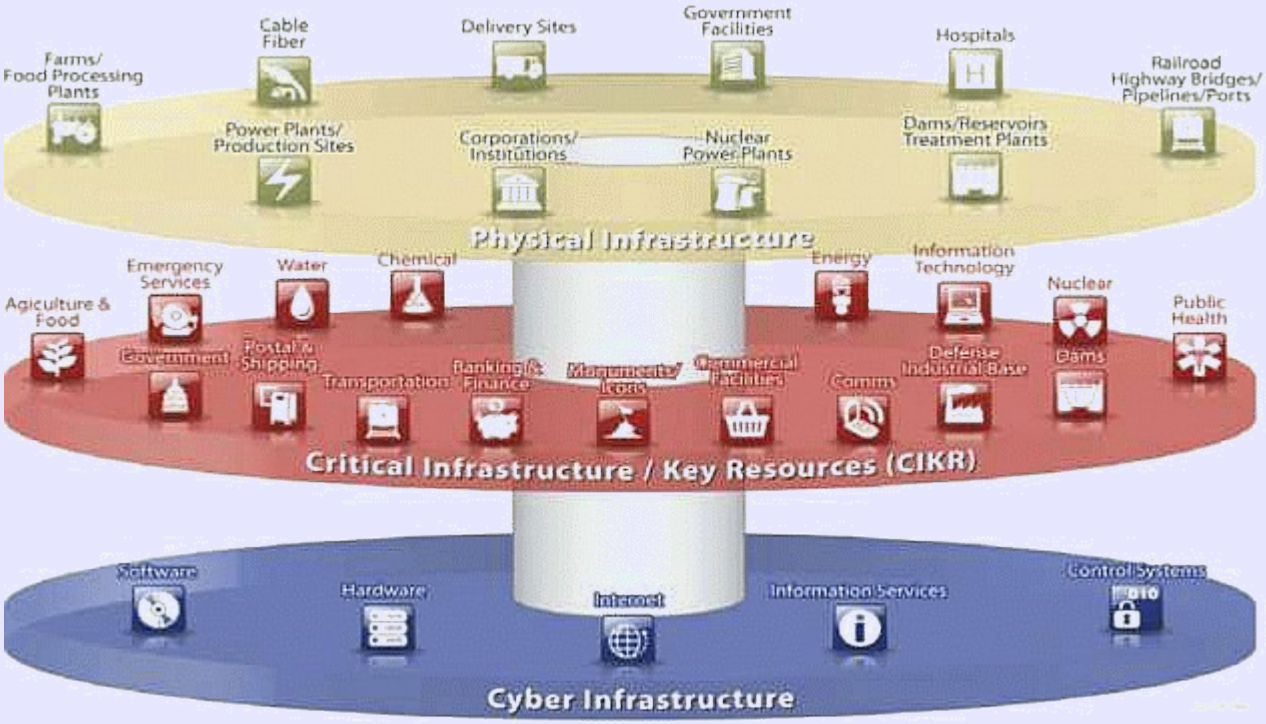
Erst in der Heißen Phase des Cyberwar dürften neben den bekannten Methoden der Cybercrime ganz verstärkt terroristische und militärische Einsätze zu erwarten sein.

© Dieter Kochheim, 12.05.12

Kritische Infrastrukturen

Kritische Infrastrukturen

- TK-Infrastruktur
- produzierendes Gewerbe
- öffentliche Grundversorgung

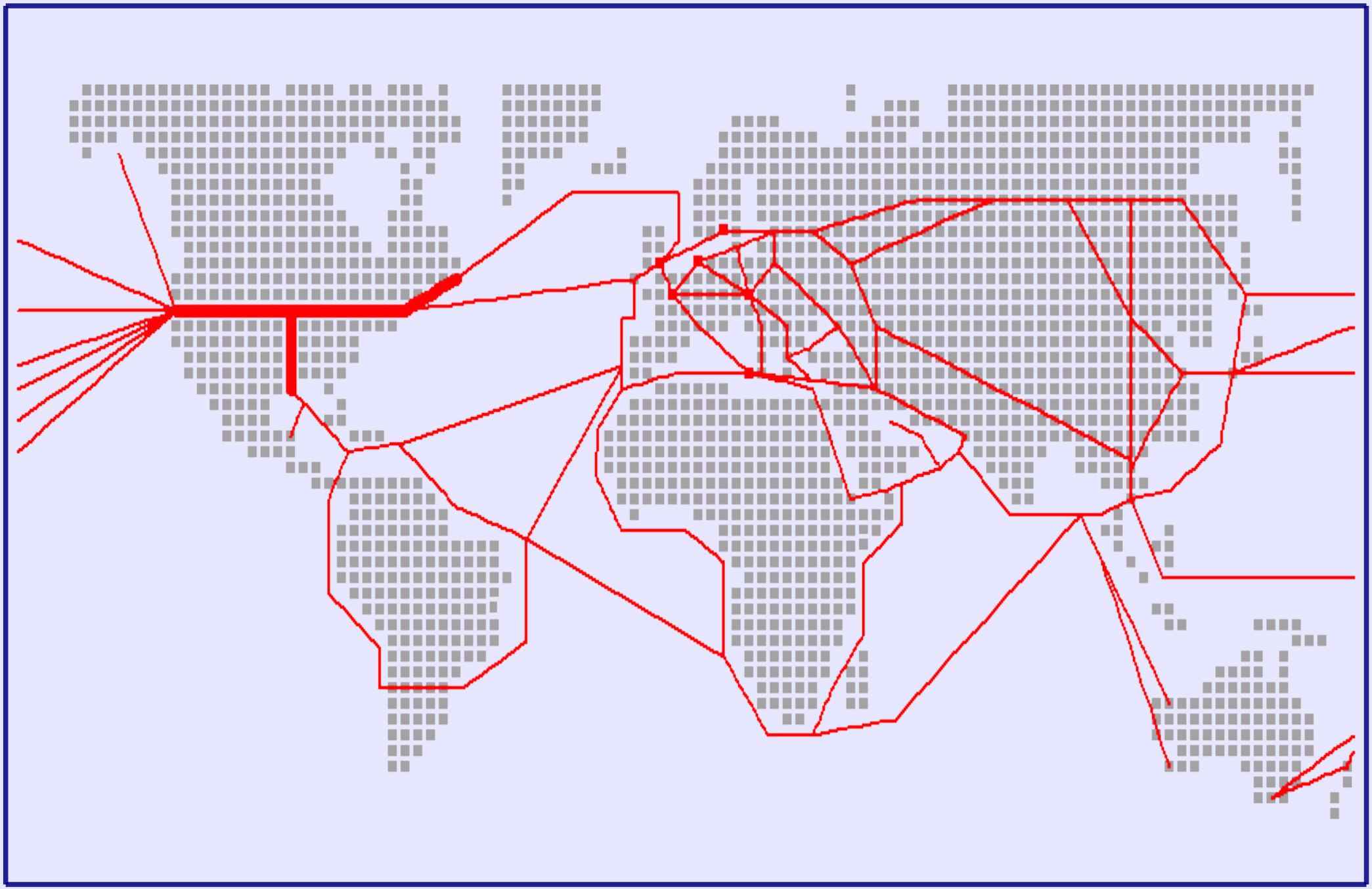


Duale Welt

- gegenseitige Durchdringung
- Abhängigkeiten

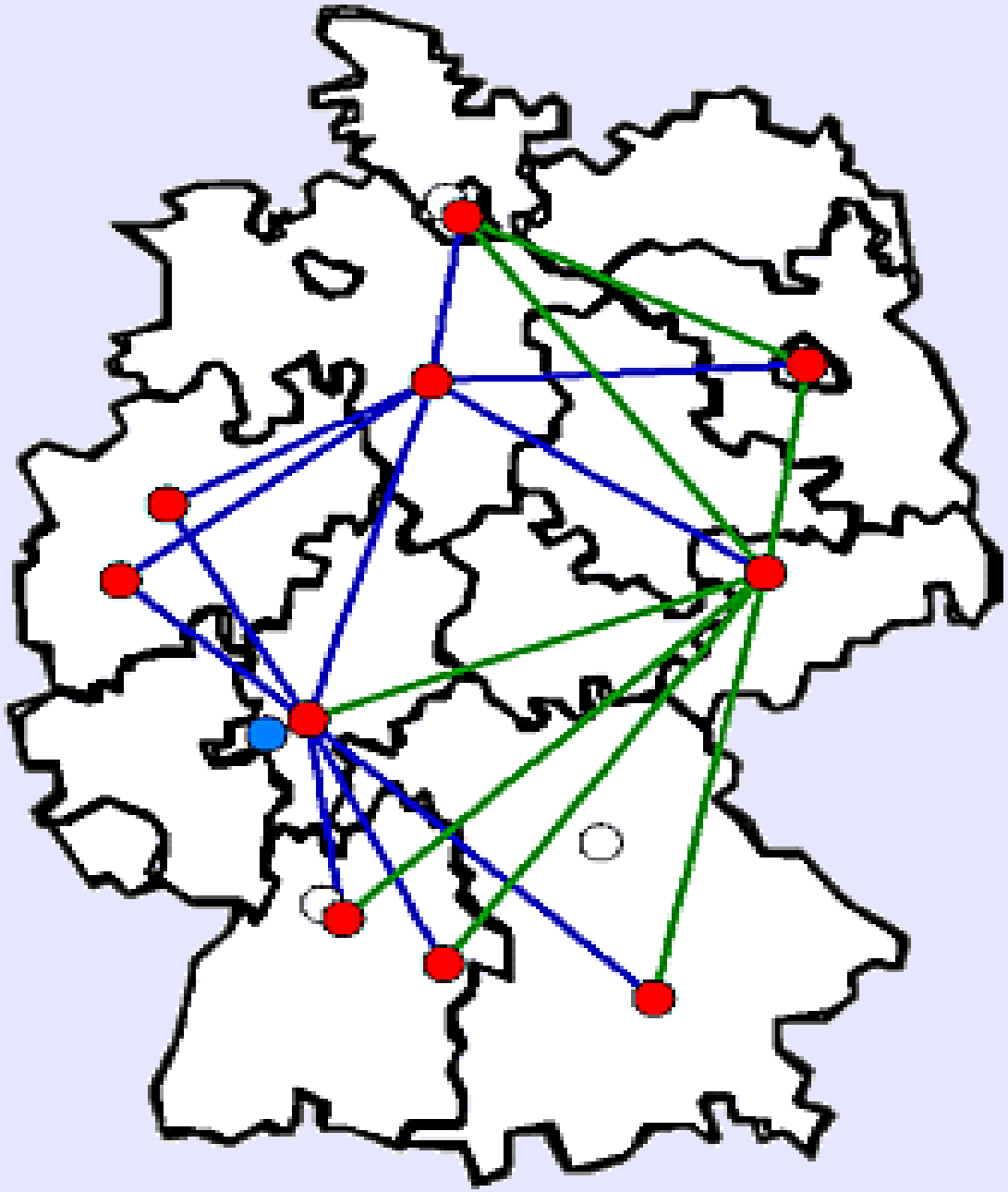
© Dieter Kochheim, 12.05.12

„Internetz“



© Dieter Kochheim, 12.05.12

Backbone der DTAG



© Dieter Kochheim, 12.05.12

Cyberwar-Debatte

James A. Lewis

Es ist nicht korrekt, alles gleich als 'Krieg' oder 'Angriff' zu bezeichnen, was im Internet an schlechten Dingen passiert.

Raoul Chiesa

Cyberwar-Aktivitäten sind gezielte Attacken auf eine andere Nation. Diese Angriffe können entweder staatlich gefördert oder durch politische und religiöse Gruppen und Ideale getrieben sein. In jedem Fall ist beim Angriff auf einen Staat die Armee für die Verteidigung zuständig.

Paul B. Kurtz

Die Grenze zwischen Internetkriminalität und Internetkrieg verschwimmt heute immer mehr, weil manche Staaten kriminelle Organisationen als nützliche Verbündete betrachten.

Sandro Gaycken

Schwache Staaten könnten Serien solcher Angriffe nutzen, um die Kräfte starker Gegner kontinuierlich zu schwächen. Es können damit gigantische Ablenkungen produziert werden. Wirtschaften können in langfristigen Operationen geschädigt werden. Es ließen sich Konflikte anheizen, andere Staaten agitieren.

© Dieter Kochheim, 12.05.12

Bedrohungen des Cyberspace

US Air Force, LeMay Center

Akteure

- **nationalstaatliche Bedrohung**

  Sabotage und Blockade von Infrastrukturen

  Spionage

  durch nationalstaatliche Einrichtungen oder beauftragte Dritte

- **transnationaler Akteure**

  grenzüberschreitende Kommunikation

  terroristische Aktionen

- **kriminelle Organisationen**

  stehlen Informationen zum eigenen Gebrauch oder um sie mit Gewinn zu verkaufen.

- **Einzelpersonen und kleine Gruppen**

  akademische Hacker, Schwachstellensucher

  Hacker mit politischen Motiven

  destruktive Hacker (Defacement)

  Malware-Programmierer

© Dieter Kochheim, 12.05.12

Bedrohungen des Cyberspace

US Air Force, LeMay Center

Methoden

- **traditionelle Bedrohungen**

  klassische militärische Konflikte, die normalerweise von anderen Staaten ausgehen

- **irreguläre Bedrohungen**

  asymmetrische Bedrohungen nutzen den Cyberspace, um mit unkonventionellen Mitteln traditionelle Vorteile zu erzielen

  Guerilla-Operationen

- **katastrophale Bedrohungen**

  Umgang mit Massenvernichtungswaffen

- **disruptive Bedrohungen**

  durch innovative und neue Technologien

- **natürliche Bedrohungen**

  Naturkatastrophen

- **unbeabsichtigte Bedrohungen**

  menschliche Fehler

  Unfälle

© Dieter Kochheim, 12.05.12

Vielen Dank für die Aufmerksamkeit!

Dieter Kochheim

cyberfahnder.de

Anhang:
Rechtspolitische Diskussionspunkte

© Dieter Kochheim, 12.05.12

Struktur der Strafverfolgung

Die Verfolgung der allgemeinen Internetkriminalität ist eine Aufgabe für alle Strafverfolger

- Aus- und Fortbildung
- Informationsaustausch
- technische und rechtliche Unterstützungsdienste

Die Verfolgung der gewerbsmäßigen Internetkriminalität ist eine Aufgabe für spezialisierte Staatsanwälte

- besondere Ausbildung
- personelle und sachliche Ressourcen
- bilden das Personal für die Aus- und Fortbildung

Die Verfolgung der organisierten Internetkriminalität ist eine Aufgabe von Schwerpunkt-Staatsanwaltschaften und Zentralstellen

- Methoden der OK-Ermittlungen
- Koordination
- internationale Zusammenarbeit

© Dieter Kochheim, 12.05.12

Strafverfahrensrecht

Der Strafverfolgung müssen effektive Instrumente zur Verfügung stehen

- Eingriffsvoraussetzungen
- Straftatenkataloge
- Entscheidungsprozesse
  - Vier-Augen-Prinzip
  - Berichtswesen

- Eingriffsermächtigungen
  - nicht offene Personalermittlungen
  - Tarnnamen für Ermittler
  - Einsatz von Privatpersonen
  - Grenzen der Tatprovokation
  - Keuschheitsprobe
- Datensammlung
- Legalitätsprinzip *(Nebentäter)*
- technische Mittel
  - Onlinedurchsuchung
  - aktive Suchprogramme
  - Datenzugriff im Ausland
- Verkehrsdaten
  - Auskünfte über Bestandsdaten
  - Zugriff auf Verkehrsdaten

© Dieter Kochheim, 12.05.12

Revision des materiellen Cyber-Strafrechts

- Strafbarkeit im Vorbereitungsstadium
- Hardware als Betrugswerkzeug
- Datenhehlerei
- klare Strukturen

© Dieter Kochheim, 12.05.12

Vernetzung

kriminalstrategische Aufgaben der Staatsanwaltschaft

- **äußerst stark von der Polizei besetzt**

diensteübergreifende Arbeitsgruppen und Informationsaustausche

- **Verwertbarkeitsprobleme**
- **operatives Cyber-Abwehrzentrum**

internationale Zusammenarbeit

- **vereinfachte Rechtshilfe**
- **Eingriffsmaßnahmen im Ausland**

© Dieter Kochheim, 12.05.12