Polizei Baden-Württemberg

Vortrag zur Internetkriminalität

am Donnerstag, 27.11.2008,
an der Hochschule Albstadt-Sigmaringen

Erster Kriminalhauptkommissar
Karl-Otto Gerstenecker
Polizeidirektion Balingen

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIDIREKTION BALINGEN

DEFINITIONEN IUK-KRIMINALITÄT

- Die IuK-Technik wird zur Planung, Vorbereitung oder Ausführung der Tat eingesetzt.
- **INTERNETKRIMINALITÄT (IUK-KRIMINALITÄT IM WEITEREN SINNE)**
- Straftaten, die mit dem Tatmittel Internet begangen werden (z. B. Waren- und Warenkreditbetrug,
- Verstoß gg. UrheberrechtsG, Verbreitung pornografischer Schriften.

COMPUTERKRIMINALITÄT (IUK-KRIMINALITÄT IM ENGEREN SINNE)

- Straftaten, bei denen die EDV in den Tatbestandsmerkmalen der Strafnorm genannt ist.

- Der Computerkriminalität werden in der PKS folgende Delikte zugeordnet:
- - Betrug mittels rechtswidrig erlangter Debitkarten mit PIN (§ 263a StGB)
- - Computerbetrug (§ 263a StGB)
- - Betrug mit Zugangsberechtigung zu Computerdiensten (§ 263 StGB)
- - Fälschung beweiserheblicher Daten (§ 269 StGB)
- - Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269,270 StGB)
- - Datenveränderung, Computersabotage (§§ 303a+b StGB)
- - Ausspähen von Daten (§ 202a StGB)
- - Abfangen von Daten (§ 202b StGB)
- - Vorbereitung des Ausspähens und Abfangen von Daten (§ 202c StGB)
- - Softwarepiraterie, privat und gewerbsmäßig (UrhG)

- **Computer-/Internetkriminalität mit allgemeinen Tatbeständen abgleichen**
- **Computer/Internet als Tatmittel = i.d.R. allgemeine Straftaten (z.B. Betrug, Erpressung, Kinderpornographie)**
- **Computer/Internet als Angriffspunkt = i.d.R engere IuK-Delikte (z.B. Computerbetrug, Ausspähen von Daten, Zerstören von Daten)**

PKS-BAROMETER IUK-KRIMINALITÄT BW2006-07

	2006	2007	%
Computerbetrug (§ 263a StGB)	3.034	2.436	-19,7
Fälschung beweiserheblicher Daten (§ 269 StGB)/Täuschung im Rechtsverkehr (§ 270 StGB)	154	405	163,0
Datenveränderung (§ 303a StGB)/ Computersabotage (§303b StGB)	139	197	41,7
Ausspähen von Daten (§ 202a StGB)	280	522	86,4
Computerkriminalität	6.833	6.549	-4,2

Straftatbestände

- § 263a StGB: Computerbetrug

- § 269 StGB: Fälschung technischer Aufzeichnungen

- § 201 a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

- - § 202a StGB: Ausspähen von Daten
- - § 202b StGB: Abfangen von Daten

- - §202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

- - § 303a StGB: Datenveränderung

- - § 303b StGB: Computersabotage

- **§ 263a [1] Computerbetrug**
- (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.
- (2) § 263 Abs. 2 bis 7 gilt entsprechend.
- (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.
- (4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

Computerbetrug § 263a StGB

- **Angriff auf Datenverarbeitungsprogramm mit Vermögensschaden als Folge**
- **Tatalternativen**
  Einwirkung auf Programm/Ablauf
  „Missbräuchliche“ Verwendung von Daten
- **Abs. 3 Vorbereitung mit Programmen**

- **§ 269 Fälschung beweiserheblicher Daten**
- (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.

Fälschung beweiserh. Daten § 269 StGB

- **Abgrenzung zu 267 StGB**
- **Daten im Medium nicht sichtbar dauerhaft abnehmbar verkörpert**
- **Ausdruck als solcher 267 StGB**
- **Beweiserhebliche Daten**
- **Daten dazu bestimmt, keine nachträgliche Beweiskraft wie 267 StGB**
- **Speichern verändern gebrauchen**
- **Wahrnehmung = echte oder verfälschte Urkunden (Identitätstäuschung Ersteller)**
- **„elektronisches Urkundsdelikt“**

- **§ 201a [1] Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen**
- (1) Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
- (2) Ebenso wird bestraft, wer eine durch eine Tat nach Absatz 1 hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht.

- (3) Wer eine befugt hergestellte Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, wissentlich unbefugt einem Dritten zugänglich macht und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
- (4) 1Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. 2§ 74a ist anzuwenden.

- **§ 202a [1] Ausspähen von Daten**
- (1) Wer unbefugt sich oder einem anderen 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.
- (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.
- [1] § 202a Abs. 1 neu gef. mWv 11. 8. 2007 durch G v. 7. 8. 2007 (BGBl. I S. 1786).

- **§ 202b [1] Abfangen von Daten**
- Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) 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.
- [1] § 202b eingef. mWv 11. 8. 2007 durch G v. 7. 8. 2007 (BGBl. I S. 1786).

- **§ 202c [1] Vorbereiten des Ausspähens und Abfangens von Daten**
- (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.
- (2) § 149 Abs. 2 und 3 gilt entsprechend.

Strafrecht: §§ 202a,b,c

- **Unbefugter Datenzugriff**
- **§ 202a Definition Daten**
- **§ 202a Erlangen von Daten unter Überwindung von Zugangssicherung**
- **§ 202b Abfangen von Daten mit technischen Mitteln (subsidiäre Vorschrift)**
- **§ 202c Strafbare Vorbereitungshandlung für 202a/b**
- **Erstellen von Programmen**
- **Verschaffen von Zugangsberechtigungen**

- **§ 303a [1] Datenveränderung**
- (1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
- (2) Der Versuch ist strafbar.
- (3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

Strafrecht: § 303a,b StGB

- **§ 303a Rechtswidrige Einwirkung auf Daten**
- **Löschen/Verändern/Unbrauchbarmachen/ Unterdrücken**
- **Motivation bzw. Erfolg spielen keine Rolle**
- **Vorbereitungshandlung strafbar**

- **§ 303b [1] Computersabotage**
- (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 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.
- (2) 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.
- (3) Der Versuch ist strafbar.

- (4) 1In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. 2Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
- *1.* einen Vermögensverlust großen Ausmaßes herbeiführt,
- *2.* gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
- *3.* durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.
- (5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.
- [1] § 303b Abs. 1 neu gef., Abs. 2 eingef., bish. Abs. 2 wird Abs. 3, Abs. 4 und 5 angef. mWv 11. 8. 2007 durch G v. 7. 8. 2007 (BGBl. I S. 1786).

Strafrecht: § 303b StGB

- **§ 303b Rechtswidrige Einwirkung auf Datenverarbeitung von wesentlicher Bedeutung**
- **Qualifizierung zu 303a**
- **Strafschärfung bei**
- **„Fremdschaden“, Vermögensschaden, Folgen für Bevölkerung oder Sicherheit BRD**
- **Banden- / Gewerbsmäßig**
- **Vorbereitungshandlung strafbar**

- **§ 106 UrhRGes [1] Unerlaubte Verwertung urheberrechtlich geschützter Werke** (1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Urheberrecht §§ 106 ff UrhG

- **nicht notwendiges Antragsdelikt**
- **Umgehung Kopierschutz § 95a, 108b UrhG**
- **Quelle zweifelhaft § 96 UrhG**
- **erweiterte Einziehung § 110 UrhG**

Urheberrecht §§ 106 ff UrhG

- **nicht notwendiges Antragsdelikt**
- **Umgehung Kopierschutz § 95a, 108b UrhG**
- **Quelle zweifelhaft § 96 UrhG**
- **erweiterte Einziehung § 110 UrhG**

- **Internet-Seiten zur Ermittlung**
- **von Seiteninhaber und IP-Adressen:**

- **www. denic.de (deutsche Seiten)**
- **www.nic.at (Österreich) oder www. nic.ch (Schweiz)**
- **www. checkdomain.com**
- **www.ripe.net**
- **www.ikz-jena.de/cgi-bin/whois**
- **www.allwhois.com**
- **www.whois.eu**
- **www.eurid.eu**
- **www.schwarzl.at**
- **www.arin.net (USA)**
- **www.geektools.com**

- **Wie lese ich eine IP-Adresse aus einem E-Mail-Header aus?**
- **Was ist ein E-Mail-Header?**
- Der Header einer e-Mail enthält Informationen über den Absender und den Weg der Nachricht. Diese Informationen sind für eine Analyse der eigentlichen Herkunft einer Nachricht unabdingbar.

- **Wo finde ich die IP-Adresse im eMail-Header?**
- Sie können den e-Mail-Header auch selbst auswerten und somit erste Rückschlüsse ziehen. Bitte gehen Sie vor wie folgt:
- Beachten Sie bitte die erste Zeile im Header der eMail, die mit dem Wort **"received"** beginnt. Beachten Sie generell, dass ein e-Mail-Header **immer von unten nach oben** gelesen wird.
- Diese Headerzeile stellt den "Eingangsstempel" des Mailservers dar. Der Eingangsstempel zeigt an, von welchem Mailserver die e-Mail auf den Weg geschickt wurde und welche Zwischenstationen im Datenfluss aufgetreten sind.
- Die für Sie und die nachfolgenden Ermittlungen relevante IP-Adresse ist die Zahl, die durch 3 Punkte getrennt ist. In dem angegebenen Beispielheader wäre dies die Adresse **85.216.107.209**

- X-Account-Key:
- account2X-Mozilla-Keys:
  Return-Path: ersteinschreiter@gmx.de
- Delivery-Date: Wed, 04 Jun 2008 19:49:59 +0200
- Received-SPF: pass (mxeu2: domain of gmx.de designates 213.165.64.20 as permitted sender) client-ip=213.165.64.20; envelope-from=ersteinschreiter@gmx.de; helo=mail.gmx.net;
- Received: from mail.gmx.net (mail.gmx.net [213.165.64.20])
- by mx.kundenserver.de (node=mxeu2) with ESMTP (Nemesis) id 0MKpdM-1K3x7X3Aj1-0006XV for rmbpa3@online.de; Wed,
- 04 Jun 2008 19:49:59 +0200
- Received: (qmail 21470 invoked by uid 0); 4 Jun 2008 17:49:59 -0000
- Received: from **85.216.107.209** by www062.gmx.net with HTTP; Wed, 04 Jun 2008 19:49:58 +0200 (CEST)Content-Type: text/plain; charset="iso-8859-1"Date: Wed, 04 Jun 2008 19:49:58 +0200

- 1.0Subject: ErsteinschreiterTo: rmbpa3@online.deX-Authenticated: #48027216X-Flags: 0001X-Mailer: WWW-Mail 6100 (Global Message Exchange)X-Priority: 3X-Provags-ID: V01U2FsdGVkX1/EO/MG3bTEJzZrfYiMQXJLuBXSoIdWikGHkbCazn hgQo9KCm2PKBffahXJ7u2STLpCBrenswoVHA== Content-Transfer-Encoding: 8bitX-GMX-UID: /ud1fE8gX1V6cWS7sGNymy5/SDc4NExDX-PhishingScore: 0 tests= X-SpamScore: -5.9 tests= GMX_GENUINE_GMX_W RDNS_NONEEnvelope-To: rmbpa3@online.de

- **Received: from 85.216.107.209** by www062.gmx.net with HTTP; Wed, 04 Jun 2008 19:49:58 +0200 (CEST)Content-Type: text/plain; charset="iso-8859-1"Date: Wed, 04 Jun 2008 19:49:58 +0200From: "Karl-Heinz Rumpel" <ersteinschreiter@gmx.de>Message-ID: <20080604174958.269170@gmx.net>MIME-Version:

- X-Account-Key: account2X-Mozilla-Keys: Return-Path: <ersteinschreiter@gmx.de>Delivery-Date: Wed, 04 Jun 2008 19:49:59 +0200Received-SPF: pass (mxeu2: domain of gmx.de designates 213.165.64.20 as permitted sender) client-ip=213.165.64.20; envelope-from=ersteinschreiter@gmx.de; helo=mail.gmx.net;Received: from mail.gmx.net (mail.gmx.net [213.165.64.20]) by mx.kundenserver.de (node=mxeu2) with ESMTP (Nemesis) id 0MKpdM-1K3x7X3Aj1-0006XV for rmbpa3@online.de; Wed, 04 Jun 2008 19:49:59 +0200Received: (qmail 21470 invoked by uid 0); 4 Jun 2008 17:49:59 -

Phishing

- Kunstwort aus Password und fishing

- Allgemein: **identity theft** beschreibt das Ausspähen von
- Zugangsdaten für Banken (Online banking), Versandhäuser,
- Internet-Auktionshäuser, E-Mail Konten, Kontaktportale, .
- Mit den gestohlenen Zugangsdaten können die Täter einen Vermögensschaden oder Rufschaden bewirken.
- In Baden-Württemberg von Jan. bis Nov. 2005 ca. 210 Schadenfälle (incl. sog. Financial Agents) mit einer Summe von 1,3 Mio. €

- in ca. der Hälfte der Fälle Aufforderung per E-Mail
- bei den restlichen Fällen Einsatz eines Trojaners

Pharming

- Durch Manipulation der Hosts-Datei (z.B.
- c:\WINDOWS\system32\drivers\etc\hosts bei WindowsXP)
- von Web Clients werden Anfragen auf gefälschte Webseiten umgeleitet

- DNS-Spoofing (Domain Name System); hierzu müssen DNS-Server bzw. DNS-Anfragen manipuliert werden.

Polizei Baden-Württemberg

Vielen Dank für Ihre Aufmerksamkeit

POLIZEI
BADEN-WÜRTTEMBERG

Björn Schemberger

Herzlich willkommen

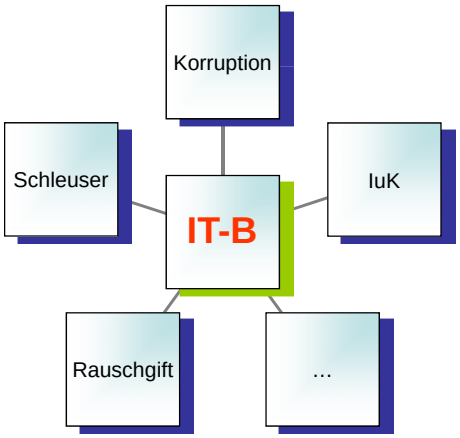
Ich präsentiere Ihnen Heute Abend meine persönliche Meinung, Einstellung und Erkenntnisse, nicht die des LKA

Forensik

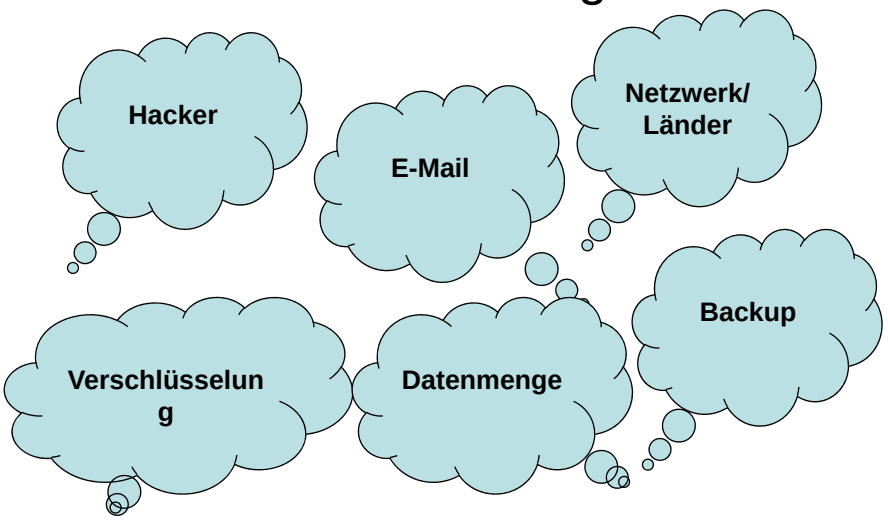
- Live Analyse

- Post-mortem-analyse

IT-B als Dienstleister



Einsatzvorbesprechung / -vorbereitung



Durchsuchung

- Übe[illegible]verschaffen
- Strukturiere[illegible]tzwerk)
- Absprache mit de[illegible]rchsuchungsleiter
- Sicherungsplan erstellen
- Sichern (die üblichen Probleme)

DOKUMENTIEREN

- Soweit die Theorie…

Objekt X

- Bekannt war:
  - Verschlüsselung
  - separates Stromnetz
- Vorbereitung:
  - Coldboot - Passwörter
  - FireWireHack - Passwörter

Unrealircd

- Anruf: Kollege hat Logs mit den verschlüsselten IPs

-> Vorratsdatenspeicherung ?

-> Code reversed

-> Bruteforcer-Injektion fehlgeschlagen

-> Nachprogrammieren war zu knapp

Alles hinterlässt Spuren

- Mutter ermordet, Sohn streitet die Tat ab
- ICQ-Logfiles zur Tatzeit
- Hinweis auf weitere Zeugen

→ Junge gesteht den Mord

Verfahren X

- 3 Durchsuchungen à 10 Objekte
- Mehrere Firmen
- Mehrere Länder
- 10 TB Daten!

Fragen?

Vielen Dank für Ihre Aufmerksamkeit