

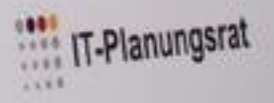


5. Kommunal IT-Sicherheitskongress

23. und 24. April 2018 in Berlin



mit Unterstützung durch



Verfolgung von Cybercrime im Land Berlin



5. Kommunalen IT - Sicherheitskongress

Berlin – 23. April 2018



Agenda:

- I. Staatsanwaltschaft Berlin
- II. Herausragende Einzelfälle
- III. Verfolgungshindernisse
- IV. Fazit und Ausblick

I. Staatsanwaltschaft Berlin (1):

- Größte Staatsanwaltschaft in Deutschland
- Derzeit ca. 315 Planstellen für Staatsanwältinnen / Staatsanwälte, ca. 850 Folgekräfte
- Organisiert in 8 Hauptabteilungen mit 36 Abteilungen
- 3 Standorte in Berlin – Moabit

I. Staatsanwaltschaft Berlin (2):



I. Staatsanwaltschaft Berlin (3):

Zuständigkeiten im Bereich Cybercrime:

- *Cybercrime im weiteren Sinne*: Bearbeitung in den allgemeinen Erwachsenen-, Jugend- und ggf. Wirtschaftsabteilungen („Alltagskriminalität“)
- Spezielle Zuständigkeiten einzelner Spezialabteilungen: KiPo, politisch motivierte Straftaten („Hasskriminalität“), Mandatsträger als Täter und Opfer

I. Staatsanwaltschaft Berlin (4):

Abt. 257 – organisierte IT – Kriminalität:

- Eingerichtet zum 01. August 2015
- Besetzung derzeit:
Abteilungsleiter, Vertreterin und 2,66
Dezernentinnen, 1 N.N. (bislang unbesetzte) Stelle,
3 Folgekräfte (Geschäftsstellenmitarbeiterinnen)

I. Staatsanwaltschaft Berlin (5):

Zuständigkeiten Abt. 257 nach GVP:

- *Cybercrime im engeren Sinne* - (IT ist Tatmittel o. Angriffsziel) UND Organisierte Begehung
- Oder wenn - IT-Kriminalität + *Pilotverfahren*, d.h. es handelt sich um ein neues Kriminalitätsphänomen
- Ausnahme: IT-Tat nachrangig oder Ermittlungen ersichtlich erfolglos !!!

I. Staatsanwaltschaft Berlin (6):

Weitere Zuständigkeiten Abt. 257:

- **Unterstützung:**

Hilfe bei der Bearbeitung von Verfahren durch Mustererstellung, Kontaktvermittlung u.ä.

- **Aus- und Fortbildung, Networking:**

Selbststudium, Teilnahme, Organisation und Abhalten von Fortbildungsveranstaltungen („*lernen und lehren*“)



II. Herausragende Einzelfälle (1.1):

Waffenhandel im „Darknet“:

- Anlassunabhängige Ermittlungen des BKA bei „hidden services“ im TOR – Netzwerk
- Deutschsprachiger bietet diverse Schusswaffen und Munition an
- Positive Bewertungen durch Käufer (analog ebay)!

Exkurs: hidden services:

Bestsellers

- Walther P22**
\$762.65
[Add to Cart](#)
- Glock 17 & Gemtech Tundra**
~~\$2,223.45~~ \$1,599.99
[Add to Cart](#)
- Beretta PX4 Storm Type F**
\$1,223.90
[Add to Cart](#)

BlackMarket Reloaded
http://5onwrsplvuk7cwk.onion

Home Your Account Your Purchases Forum

Categories: Weapons > Firearms

AK 47 saige full auto + 1 mag of ammo = 900 euro

Price: 111.08967 BTC
\$ 1,111.23 £ 707.29 € 900.00

Ship from: europe
Ship to: worldwide
Stock: 2
Created in: 2012-07-18 22:13 UTC
Last update: 2012-08-05 01:36 UTC

Your balance isn't enough to buy this item! Please deposit the needed funds before.

Description

- 1x AK 47 saige full auto + 1 mag of ammo = 900 euros each
- 2x glocks f19 gen 4 + 3 clips of ammo = 500 euros each
- 1x glocks 22 .40 + 2 clips of ammo + 450 euros each

ACT NOW!

THESE GUNS ARE FOR SALE ONLINE

II. Herausragende Einzelfälle (1.2):

- Scheinankauf von Munition erfolgreich; Versand erfolgte von Berlin über Packstation
- Observation: Täter geht hoch konspirativ vor
- Sodann „kleiner Lauschangriff“ auf das vom Täter genutzte Fahrzeug, Durchsuchung, Beschlagnahme umfangreichen Beweismaterials, Haftbefehl

Täter beim Einwurf des Pakets:



II. Herausragende Einzelfälle (1.3):

- Beschlagnahme von ca. 2.000 (!) Schuss Munition verschiedener Kaliber im Wohnwagen des Täters
- Anklage vor dem Landgericht Berlin – 23 Einzelfälle von Verkäufen
- Hauptverhandlung am 12.09.2016 Angeklagter ist vollumfänglich geständig - 4 Jahre Gesamtfreiheitsstrafe – inzwischen rechtskräftig!

Durchsuchung beim Täter:



II. Herausragende Einzelfälle (2.1):

DDoS - Angriff an die Webauftritte der SPD, CDU und Sigmar Gabriels (2015):

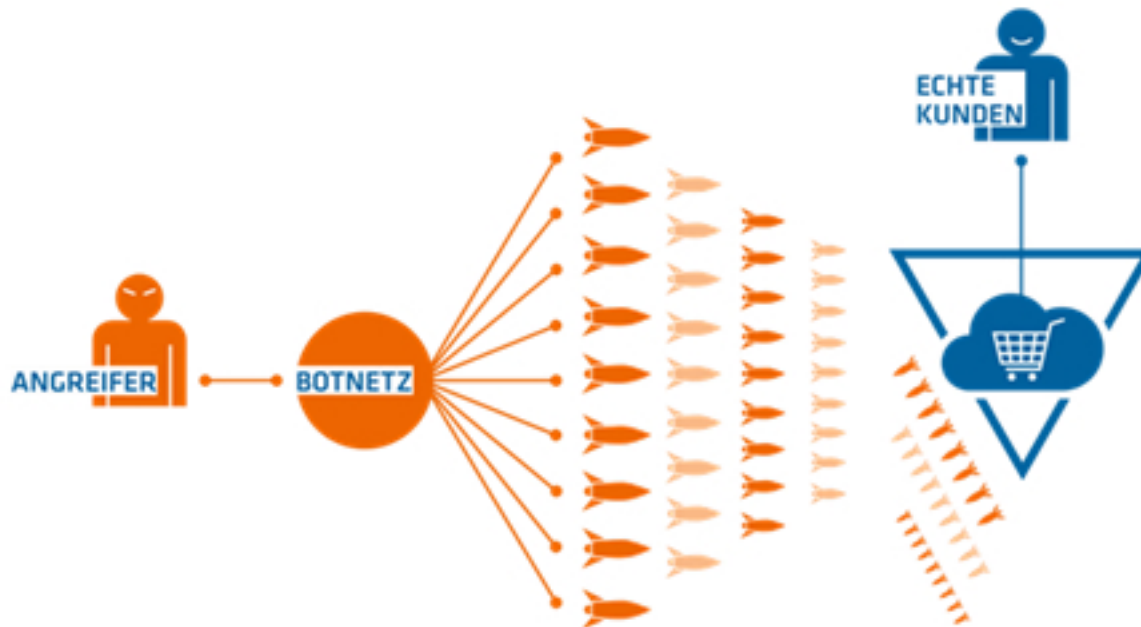
- Täter ärgert sich über die beabsichtigte Wiedereinführung der Vorratsdatenspeicherung
- Verschafft sich Zugriff auf Botnetze und greift mehrfach (erfolgreich) die o.g. Webauftritte an – legt diese über Stunden lahm
- Berichtet „stolz“ in sozialen Netzwerken über seinen Erfolg!

II. Herausragende Einzelfälle (2.2):

DDoS – Angriff – was ist das eigentlich?

- „*Verteilte Dienstblockade – Dienstverweigerung*“
- Durch Dritte *bewusst und gewollt* (vorsätzlich) herbei geführte Überlastung eines Systems führt zu dessen Zusammenbruch
- Täter verwenden zur Tatausführung sog. Botnetze

Exkurs: DDos - Angriff:



Exkurs: Illegale Dienstleistungen

Botnet Rental for Installs

- Load Service: Buy \$110 / 1K installs (USA)

CONTACTS:
Support #1: ICQ 59612
Support #2: ICQ 59076
Support #3: ICQ 975

OUR PRICE:

United States	\$110
All world	\$16
Mix with no Asia	\$30



Optima

HTTP
ICMP
SYN
UDP

DARKNESS X
Powerful DDoS Bot with premim admin-panel "Optima"
[From Russia with love]

4 types of DDoS Attacks / Additional modules / 7 packages / Amazing Support
2009-2012. SW_Team

II. Herausragende Einzelfälle (2.3):

- Ermittlungen durch BKA SO 45 – Außenstelle Berlin
- IP – Ermittlungen komplett sinnlos, da diese zu „gekaperten“ Rechnern („BOT's“) führten
- Twitter – Auskunftersuchen nicht zielführend, da von dort erfahrungsgemäß keine Antwort
- Aber: Täter nennt in Tweet seine Skype – Adresse!

II. Herausragende Einzelfälle (2.4):

- Die Lösung: **Skype – Tracking!**
- Beschluss gemäß § 100 g StPO an Microsoft führte zu einer „frischen“ IP aus dem Bereich der Telekom
Auskunftersuchen, § 100 j StPO,
- Identifizierung eines 16 jährigen Schülers aus Gießen
- Abgabe an ZIT (GStA Frankfurt/Main) gemäß §§ 3, 42 JGG

II. Herausragende Einzelfälle (3.1):

Phishing – Angriff auf online geführte Girokonten von Kunden der Commerzbank AG (2013):

- Commerzbank AG erstattet in Frankfurt/Main Strafanzeige gegen unbekannt wegen unberechtigter Verfügungen von Konten wohlhabender Kunden mit der Besonderheit, dass durch die Täter Festgeldkonten aufgelöst und Wertpapiere verkauft wurden („*cherry – picking*“)
- Ermittlungen zunächst durch das BKA SO 41 und der ZIT

II. Herausragende Einzelfälle (3.2):

- Zugriffe auf Opferkonten über verschlüsselte Kanäle („VPN - Tunnel“) und betrügerisch angemieteten virtuellen Server
- Überwachung des virtuellen Servers gemäß § 100 a StPO („**Server – TKÜ**“) ergab eine IP, von der auf Konten von Finanzagenten (stellen ihr Girokonto gegen Bezahlung Dritten zur Verfügung) regelmäßig zugegriffen wurde
- IP – Ermittlungen führten zu Provider mit „Quasi – statischer“ IP – Vergabe und einem Anschluss in Berlin

II. Herausragende Einzelfälle (3.3):

- Anschluss durch 2 Personen aus der Ukraine (?) genutzt, die sich unangemeldet in der betreffenden Wohnung aufhalten
- Durchsuchung (§§ 102, 105 StPO) erbrachte diverses Beweismaterial, u.a. Rechner und Mobiltelefone
- AG Gießen (Ermittlungsrichter) erlässt Haftbefehl wegen des dringenden Verdachts des banden- und gewerbsmäßigen Computerbetruges (§§ 263 a, 263 Abs. 3, 5 StGB)

II. Herausragende Einzelfälle (3.4):

- Übernahme des Verfahrens durch die StA Berlin aufgrund des Tatortprinzips, § 7 StPO
- Weitere Ermittlungen des LKA Berlin zu Finanzagenten
- Anklageerhebung im November 2013: 33 Fälle; Schaden ca. € 130.000,00
- Verurteilung der Täter im September 2014


II. Herausragende Einzelfälle (4.1):

Wenn einer eine Reise tut – betrügerische Bestellungen hochwertiger DB - Tickets:


- Phänomen bekannt seit Sommer 2012
- Täter bieten auf Mitfahrportalen DB – Tickets zu äußerst günstigen Preisen an
- Tickets stammen angeblich aus Firmenkontingenten, Ersatzleistungen aufgrund Verspätungen u.ä.

Exkurs: DB Online - Ticket

- Reisender benötigt Internetzugang mit E – Mail – Account
- Bezahlung durch Abbuchung **oder Kreditkarte**
- Kreditkartennummer, Ablaufdatum und CVC Ziffer ausreichend!
- Identifizierung im Zug entweder mit Kreditkarte **oder Ausweisnummer!**



Online-Ticket
Bitte auf A4 ausdrucken



Barcode bitte nicht trennen!

ICE Fahrkarte

Gültigkeit: 26.10.2012 - 25.11.2012 Hinfahrt bis 27.10.2012
Rückfahrt an 2 aufeinanderfolgenden Tagen innerhalb der Gültigkeit

Normalpreis (Hin- und Rückfahrt)

Klasse: 2, 1. Erw. NormalkVG 23.10.2012 Rostock München ICE 2
Erw. Preis: 15,00 € 2012 BMWKVG 23.10.2012 Rostock München ICE 2
Hinfahrt: Rostock → München, mit ICE
Rückfahrt: München → Rostock, mit ICE
Über: 2012 VIA: (L'SLF'N/HH'H'GOE'FD'WUE)
15 EUR ENTGELT FÜR UMTAUSCH/ERSTATTUNG AB 1. GELTUNGSTAG

Zahlungspositionen und Preis				
Positionen	Preis	Mwst D: 19%		
ICE Fahrkarte	1 270,00€	270,00€	43,11€	
Reservierungen	3 8,00€	8,00€	1,28€	
Summe	278,00€	278,00€	44,39€	

Kreditkartenzahlung

Betrag 278,00€ VU-Nr 455695619 Transaktions-Nr 288043
Datum 23.10.2012 Gen-Nr 635484

Ihre Kreditkarte wurde mit dem oben genannten Betrag belastet. Die Buchung Ihres Online-Tickets erfolgte am 23.10.2012. DB Fernverkehr AG/DB Regio AG, Stephensonstr. 1, 60326 Frankfurt, Steuernummer: 045 231 28552.

Hinfahrt: 20G8 7HFW 8MF
Zeitpunkt: 26.10.2012
Gültig ab:

Rückfahrt: 22GU DVMY T4D
Zeitpunkt: 26.10.2012
Gültig ab:

Frau [REDACTED]
ID-Karte: **Personalausweis (DE11) 7820**
Auftragsnummer: [REDACTED]

Ihre Reiseverbindung und Reservierung Hinfahrt am 26.10.2012

Halt	Datum	Zeit	Gleis	Fahrt	Reservierung
Rostock Hbf	26.10.	ab 08:25	3	IC 2217	1 Sitzplatz, Wg. 8, Pl. 57, 1 Gang, Großraum, Nichtraucher
Hamburg Hbf	26.10.	an 10:16	11a/b	ICE 587	1 Sitzplatz, Wg. 23, Pl. 41, 1 Fenster, Großraum, Nichtraucher
München Hbf	26.10.	an 17:00	15		

Ihre Reiseverbindung und Reservierung Rückfahrt am 29.10.2012

Halt	Datum	Zeit	Gleis	Fahrt	Reservierung
München Hbf	29.10.	ab 12:16	24	ICE 788	1 Sitzplatz, Wg. 4, Pl. 14, 1 Gang, Großraum, Nichtraucher
Hamburg Hbf	29.10.	an 18:04	14a/b		
Hamburg Hbf	29.10.	ab 18:35	6b	RE 4317	
Rostock Hbf	29.10.	an 20:51	6		


Hinweise:

- Die Fahrkarte muss ausgedruckt vorliegen und gilt nur zusammen mit der beim Kauf angegebenen eigenen gültigen Identifizierungskarte
- Bei Normalpreisen auch in anderen Zügen als in der Reiseverbindung angegeben innerhalb der Geltungsdauer gültig (ggf. Aufpreis für anderen Weg erforderlich)
- Erstattung oder Rücknahme über www.bahn.de, in DB ReiseZentren oder die in Ihrer Auftragsbestätigung angegebene Serviceadresse. Keine Erstattung oder Rücknahme in Reisebüros
- Das Online-Ticket gilt nur für den unter "Fahrkarte" angegebenen Reiseabschnitt. Die Übersicht "Ihre Reiseverbindung" enthält ggf. Reiseinformationen zu Teilstrecken (z.B. mit dem Bus), für die ein weiteres Ticket erforderlich ist
- Wenn Ihr Ticket die City-Option beinhaltet, gilt diese nur am Ankunftsstag der Hinfahrt bzw. am Abfahrtsstag der Rückfahrt (Reisetage wie unter "Ihre Reiseverbindung" angegeben)
- Für Fahrten im City-Gebiet mit City-Ticket oder City mobil muss die Echtheit des Online-Tickets durch den Zangenabdruck des Zugbegleiters bestätigt werden
- Es gelten die Beförderungsbedingungen der DB AG bzw. besondere Regelungen für bestimmte Strecken und Angebote (z.B. innerhalb von Verkehrsverbänden, Tarifgemeinschaften, Ländertarife).

Mehr Information gibt es unter www.bahn.de/onlineticket. Informieren Sie sich unter www.bahn.de/reiseplan zeitnah über Ihre Verbindung. Wir danken Ihnen für Ihre Buchung und wünschen Ihnen eine angenehme Reise!

26 10

Aktuelle Infos aufs Handy!



Fahrpläne, Pünktlichkeit, Alternativen zur Fahrt und mehr! m.bahn.de

Exkurs: www.mitfahrgelegenheit.de

Angebot

[← zurück](#) [Merktzettel hinzufügen](#) [Drucken](#)

Strecke	von	Berlin
	über	Hamburg
	über	Düsseldorf
	über	Köln
	über	Frankfurt/Main
	über	Stuttgart
	nach	München
Zeitpunkt	Datum	Do, 22.08.13
	Uhrzeit	17.00 Uhr
Freie Plätze		4

Bezahlung Barzahlung bei der Fahrt

28 €

Preis pro Person

So funktioniert's

1. Stellen Sie eine kostenlose Buchungsanfrage. Sie erhalten dann die Telefonnummer des Fahrers.
2. Rufen Sie den Fahrer an und klären Sie offene Fragen, bevor er Ihre Anfrage bestätigt.

Noch Fragen?

[Zur Buchung](#)

Fahrer



eri schnei
★★★★★ (-)

Bitte einloggen, um das Kurzprofil dieses Nutzers einzusehen.

Details	Raucher	nein
	Kosten	28 €/Person

Bahnmitfahrgelegenheit

Ich biete ihnen hier die Möglichkeit, vergünstigte ICE-Bahn-Tickets zu erwerben. Sie können die Fahrt individuell nach Wunschzeit antreten. Umsteigen in S-Bahn, RB...zur Anfahrt kleinerer Bahnhöfe/Städte ist auch möglich und kostengleich.

Aufgrund der vielen Anfragen, bitte bevorzugt per E-Mail kontaktieren. Gerne werde ich ihnen unverbindlich weitere Infos zukommen lassen:

mail (at) erich-schneider (punkt) net

Mit freundlichen Grüßen
Erich Schneider

Diese Mitfahrgelegenheit wird täglich angeboten.
Letztmalig aktualisiert am Mo 19.08.2013 13:36

[Missbrauch melden](#)

II. Herausragende Einzelfälle (4.2):

- Täter verwenden zur „Bezahlung“ abhandengekommene Kreditkartendatensätze
- Bereits nach kurzer Zeit erhebliche Schäden, da massenhafte Begehung
- Ticket – Käufer regelmäßig gutgläubig, Erwerb einer „echten“ Fahrkarte
- Keine Kontrolle durch Zugbegleiter auf betrügerische Erlangung

II. Herausragende Einzelfälle (4.3):

- November 2012: Ermittlung von 2 Tätern, insgesamt Buchungen von 2.366 Tickets
- Verurteilungen im August 2013 zu jeweils unbedingten Freiheitsstrafen (2 Jahre 10 Monate; 3 Jahre 3 Monate)
- September 2014: Identifizierung eines Täters, verantwortlich für ca. 5.000 betrügerische Buchungen
- Täter einschlägig vorbestraft (2 Jahre mit Bewährung) begeht Taten nunmehr von Thailand aus

II. Herausragende Einzelfälle (4.4):

- Internationaler Haftbefehl wegen 1.823 Taten
- Passenzugsverfahren, Mitteilung an thailändische Behörden, da illegaler Aufenthalt in Thailand!
- September 2015: Festnahme durch Immigration Police – Täter kommt in (öffentlich rechtliche) Abschiebehaft
- BKA – Zielfahnder übernehmen Beschuldigten in Bangkok, Rückführung und U – Haft in JVA - Moabit

Exkurs:

- *Thiery I. auf dem Heimweg ...*



II. Herausragende Einzelfälle (4.5):

- Frühjahr 2016: Hauptverhandlung vor dem Landgericht Berlin – Große Strafkammer
- Zunächst ca. 20 Verhandlungstage bis Oktober 2016 angesetzt
- Nach zwischenzeitlicher Unterbrechung der Hauptverhandlung: Umfassendes Geständnis
- Rechtskräftiges Urteil: 5 Jahre 3 Monate Gesamtfreiheitsstrafe

III. Verfolgungshindernisse (1):

- Wiedereinführung der Vorratsdatenspeicherung und Möglichkeit der Datenerhebung durch Strafverfolgungsbehörden praxisfern und untauglich:
 - Differenzierung zwischen Verkehrs- und Standortdaten nicht nachvollziehbar (10 Wochen, bzw. 4 Wochen)
 - Verkehrsdatenerhebung als offene (!) Maßnahme
 - Lückenhafter und widersprüchlicher Katalog in Rechtsgrundlage, § 100 g Abs. II StPO:
Verwertungsdelikt (Strafandrohung 6 Monate) erfasst,
nicht Grunddelikt (Verbrechen 1 Jahr Mindeststrafe)

III. Verfolgungshindernisse (2):

- Vereinfachung bei Vermögensabschöpfung erforderlich – Beweislastumkehr – Täter müssen nachweisen, dass Vermögensgegenstände rechtmäßig erworben wurden
- Gesetzliche Regelung der sog. Quellen – TKÜ würde Rechtsunsicherheit beseitigen – wirksames Ermittlungsmittel bei OK und Terrorismus
- Vereinfachte Opportunitätsentscheidungen bei offensichtlich rein zivilrechtlich motivierten Strafanzeigen

III. Verfolgungshindernisse (3):

- **Big Data:** Auswertung großer Datenmengen zeitaufwendig und bei Vergabe an auswärtige Dienstleister sehr teuer
- Social – Media – Dienste oft nicht sehr kooperativ, Verweis auf den (formellen) Rechtshilfeweg
Nachteil: Zeitaufwendig bei ungewissen Erfolgsaussichten
- Täter setzen vermehrt (wirksame) Verschlüsselungstechniken (z.B.: Kommunikation über VPN – Tunnel; Verwendung von TrueCrypt u.ä. Werkzeugen)

III. Verfolgungshindernisse (4):

- Starker Mangel an qualifizierten Personal bei Polizei und Justiz
- Pensionierungswelle bei Polizei und Justiz führen zu Lücken, die auf absehbare Zeit nicht zu schließen sind
- Dienst bei Berliner Behörden aufgrund unzureichender Alimentierung zunehmend unattraktiv, starke Konkurrenz durch Bundesbehörden und andere Bundesländer mit weitaus besserer Besoldung
Folge: Stellen können nicht mehr adäquat besetzt werden

IV. Fazit und Ausblick (1):

- Von einer erheblichen Dunkelziffer bei Cybercrime - Delikten ist auszugehen.
- Strafanzeigen werden aufgrund von Reputationsverlust-ängsten nicht oder nur selten erstattet („schlechte Presse“)
- Enge Zusammenarbeit von Wirtschaft und Ermittlungsbehörden wünschenswert und erforderlich
- Sicherung der Unternehmens-, bzw. Behördeninfrastruktur ist erfahrungsgemäß eher rudimentär

IV. Fazit und Ausblick (2):

- „Hase und Igel – Prinzip“; Täter haben sich als äußerst innovationsfreudig bei der Entwicklung neuer „Geschäftsmodelle“ gezeigt. Reaktionen darauf stets verzögert
- Angriffe auf kritische Infrastrukturen jeglicher Art sind zu erwarten. Motive der Täter können sowohl politischer als auch krimineller Natur sein. Grenzen allerdings fließend!
- Ohne signifikante Änderungen an Besoldungsverhältnissen kann der trotz Widrigkeiten erreichte hohe Standard bei der Verfolgung von Cybercrime nicht gehalten werden



***Haben Sie noch Fragen oder
Anregungen?***

Ansonsten:

Vielen Dank für`s Zuhören