Kanton Zürich
Direktion der Justiz und des Innern
Staatsanwaltschaft Kanton Zürich

cybercrime-quo vadis

Möglichkeiten und Grenzen der Cybercrime-Strafverfolgung

Referat am 12. Technology Forum 2022 by Studerus

stv. LSTA lic.iur. Stephan Walder
Staatsanwaltschaft II des Kanton Zürich

Was ist Cybercrime?

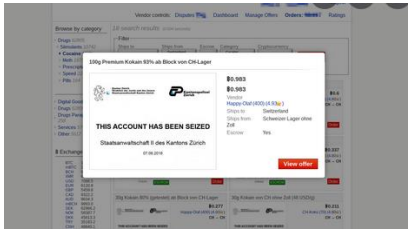
- Cyberkriminalität im engeren Sinn betrifft Straftaten, die mit Hilfe der Informations- und Kommunikationstechnologien (IKT) verübt werden oder sich Schwachstellen dieser Technologien zu Nutzen machen. Diese kriminellen Aktivitäten sind neu und werden durch diese Technologien erst möglich.

- Cyberkriminalität im weiteren Sinn nutzt das Internet als Kommunikationsmittel, wobei die sich bietenden Möglichkeiten wie bspw. der E-Mail-Verkehr oder der Austausch respektive das Bereitstellen von Dateien für unlautere Zwecke missbraucht werden. Diese kriminellen Aktivitäten sind nicht neu, sondern die dabei verwendeten Tat- und Speichermedien (Email, Whatsapp, Snapchat, Instagram, Telegramm bzw. elektronische Datenträger statt Papier, Cloudservices etc.).

Quelle: Allianz der schweizerischen Strafverfolgung zur Bekämpfung der Cyberkriminalität, Protokoll der 1. Sitzung vom 2. September 2016

Staatsanwaltschaft
Kanton Zürich

Was ist Cybercrime?

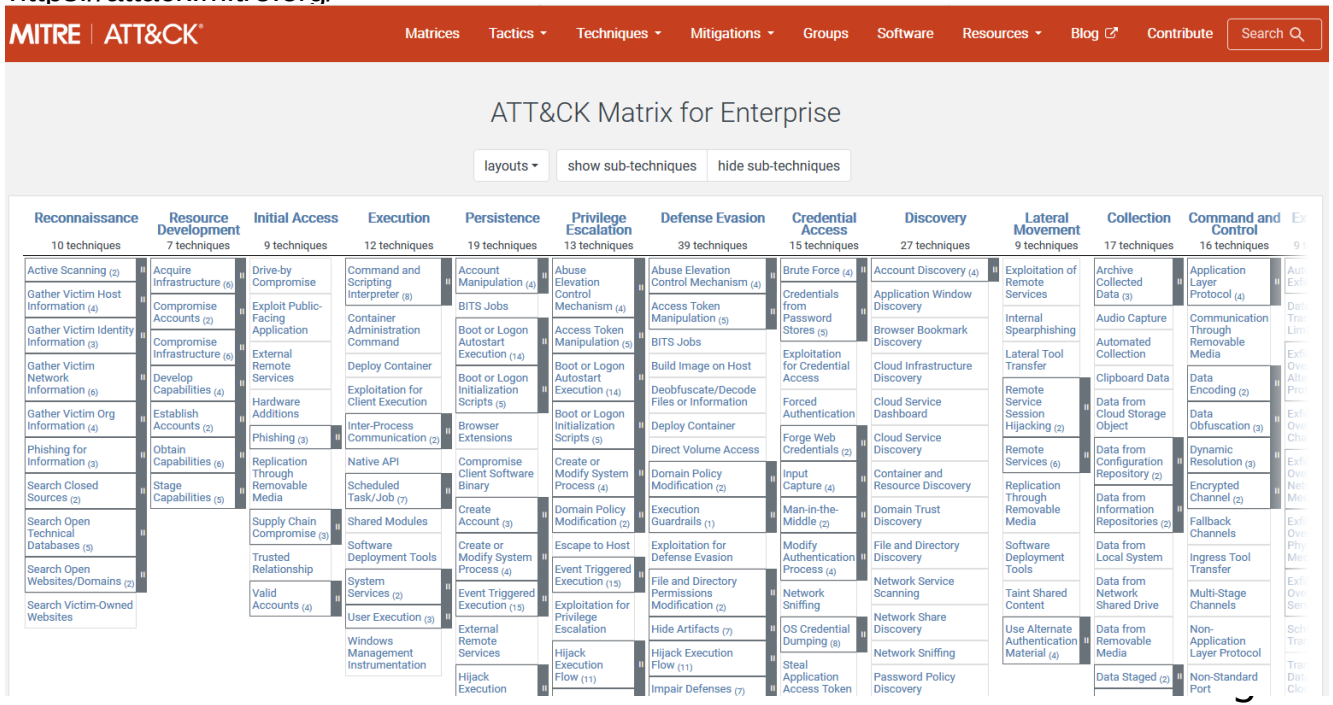


Cybercrime Definition

- Cybercrime ist kein Deliktsfeld, sondern eine Ermittlungsmethode
- Primärziel: Identifikation/Lokalisation der Täterschaft
- Definition ist abhängig von der Komplexität der Ermittlungen:
  - **Hightech-Crime**: Erforderlichkeit eines operativen Verfahrens
  - **Cyberlight**: Komplexe Ermittlungen, ohne operative Massnahmen
  - **Digitalisierte Kriminalität**: Delikte mit EDV-Device als Tat- oder Beweismittel

Ransomware

- Cyber-Kill-Chain (Lockheed-Martin)
- https://attack.mitre.org/



CEO-Fraud

From: Fabiola Gianotti <fabiola.gianotti@cern.ch>
Date: Monday, 19 October 2020 at 10:29
To: [redacted]
Subject: Re: CERN LOGISTICS SUPPORT REQUEST

Hello [redacted]

Thank you for your email reply and I am glad you are well and in good health.

Apologies for the troubles, I need your assistance with a transfer of 2,875 Euros, for CERN logistics support payment.

Our treasurer is not able to process the transfer due to a family emergency, and I'm having some troubles with international transfers without my bank access token while on vacation.

Kindly let me know if you can help with the transfer, and if I can forward you the details to transfer the payment on behalf of CERN?

Rest assured the amount will be fully reimbursed back to you as soon as our treasurer is back in office.

Look forward to your return email for transfer details if you can help.

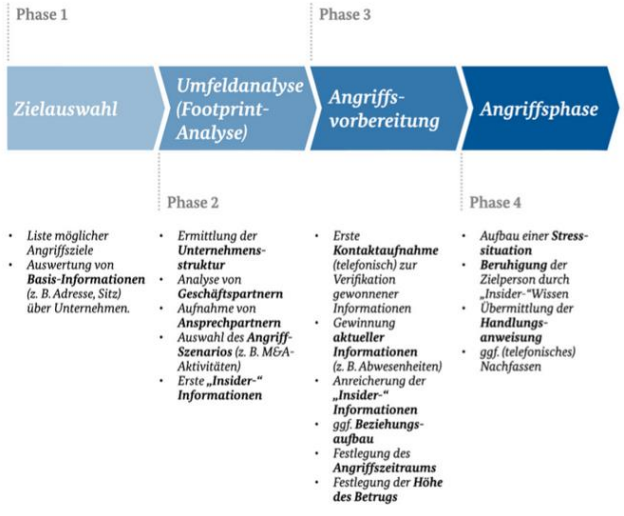
Regards,

Fabiola.

CEO-Fraud

– Modus operandi:

Die Kriminellen gehen beim CEO Fraud strukturiert vor und richten Ihre Angriffe nach Effizienzkriterien / Erfolgsaussichten aus.



Quelle: *BSI*

Organisation

Leitung
lic.iur. Urs Hubmann, Leitender Staatsanwalt

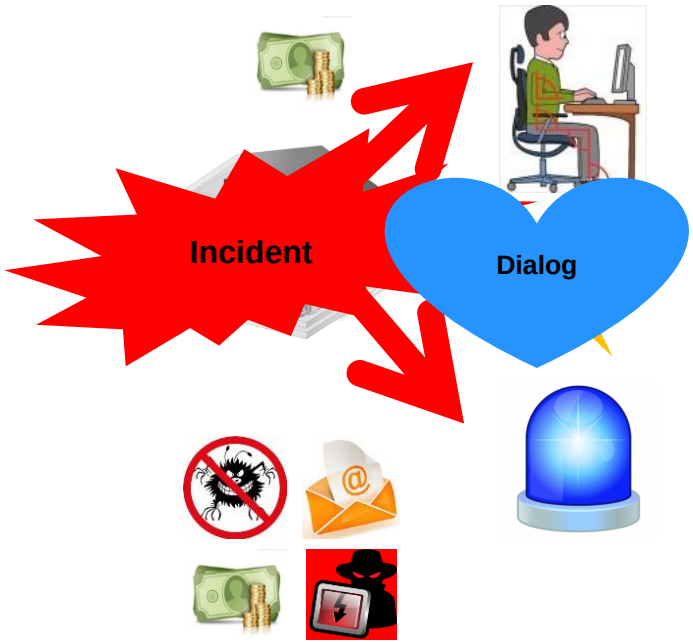
lic.iur. Stephan Walder, Stv. Leitender Staatsanwalt

Abteilung A - Besondere Untersuchungen

Büro A-1:	lic.iur. Christine Braunschweig (Abteilungsleiterin)
Büro A-2:	lic.iur. Thomas Aerne
Büro A-3:	lic.iur. Stephan Keel
Büro A-4:	lic.iur. Christian Frei
Büro A-5:	lic.iur. Andrej Gnehm
Büro A-6:	lic.iur. Manfred Hausherr
Büro A-7:	lic.iur. Judith Vogel
Büro A-9:	Markus Landolt (Assistenzstaatsanwalt)

Falsche Unterstützungsanfragen

Public Private Partnership



Cyber-Security

The NIST Cybersecurity Framework

- Auftrag: **Schnelle Wiederherstellung/Gewährleistung des geschäftsprozessfördernden Zustands**

Strafverfolgung

- Beweissicherung (Verwertbarkeit)
- Lokalisation
- Identifikation
- Auftrag: **Sachverhaltsklärung**; **Täter überführen/bestrafen**

Staatsanwaltschaft
Kanton Zürich

IST-Lagebild: "Eisberg-Prinzip"

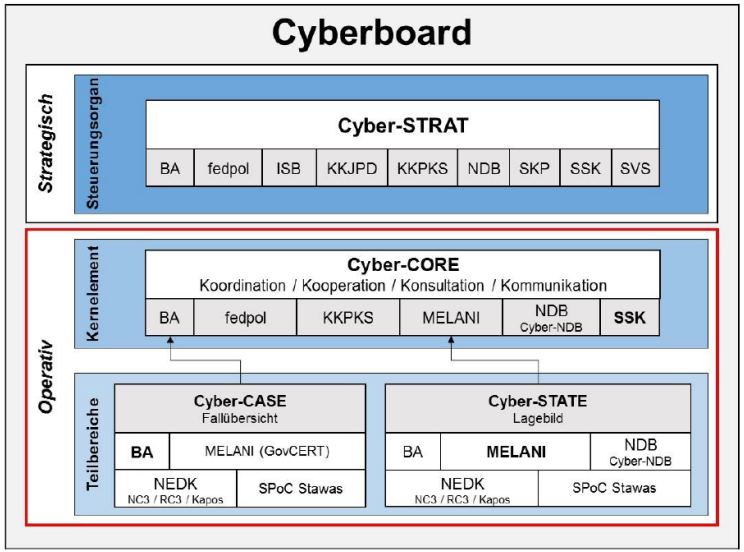
SOLL-Lagebild / Fallübersicht

- Ereignis: Modus-Operandi, Anzahl, Tatort/Erfolgsort, Deliktsumme/Schaden
- Anzeige Polizei: Pendente Ermittlungen, Täter-ID pos./neg, Lokalisation, SOMA
- Geschäft STA: Zuständigkeit, Phänomenkomplex, operatives Verfahren, Rechtshilfe

Kanton	Ereignis	Anzeige	Untersuchung

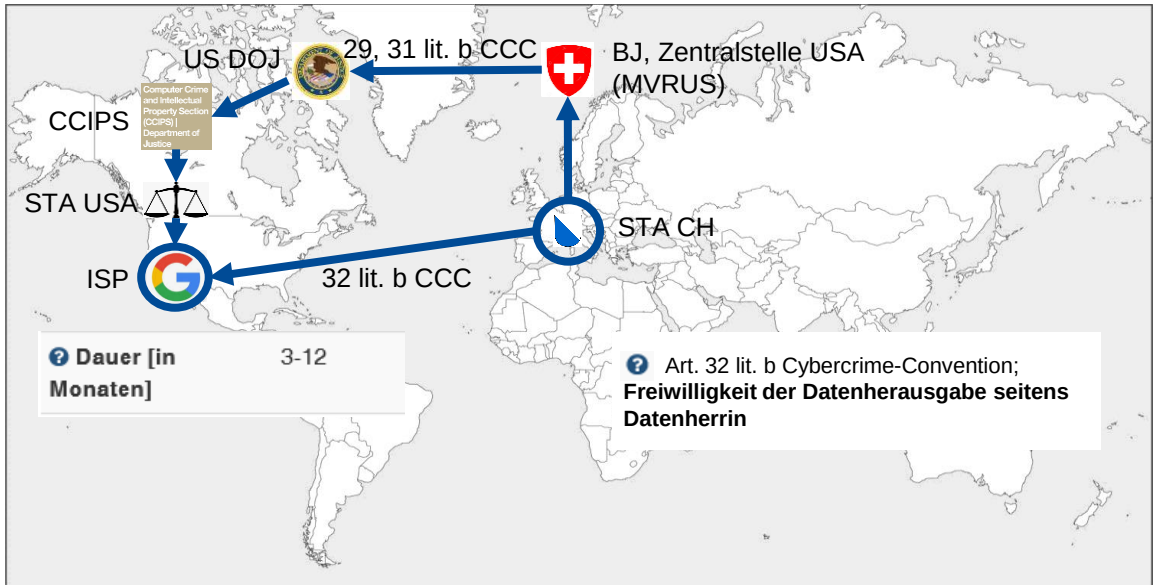
Nationale Koordination von Fallkomplexen

- Die Staatsanwaltschaft leitet das Vorverfahren (Art. 15 Abs. 2 StPO)
- Die interkantonale Zuständigkeit regelt die Staatsanwaltschaft (Art. 31ff. StPO)
- Zuständigkeit → Anklage → Wirkung
- Cybercrime Strafverfolgung ist eine Verbundsaufgabe



Key Challenge: Datenerhebung im Ausland

- Grundsätzlich viel zu lange durchschnittliche Erstattungsdauer der Rechtshilfe
- Mangelnde Effektivität infolge Formalismus und restriktiver Praxis
- Die Cybercrime Convention (SR 0.311.43) hilft, aber nur in engen Schranken



Grundlagen Beweisrecht: Erhebung am Speicherort

- Früher: Technisch bedingt; Datenträger=Speicherort=Verfügbarkeit
- Heute: Dezentrale Speichermedien erlauben ortsunabhängig die weltweite Verfügbarkeit sämtlicher Daten in Echtzeit
- Morgen: "Internet Computer Ecosystem"; decentralized computing

BG 1B_29/2017 vom 24. Mai 2017

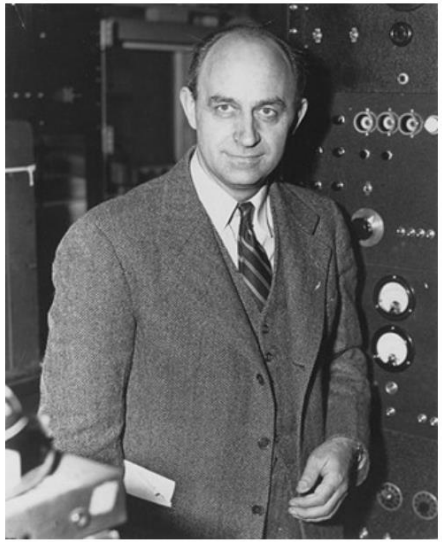
- "Die Nutzung des Internets, etwa von sozialen Netzwerken, steht grundsätzlich jedermann zu, auch Strafbehörden für **Online-Ermittlungen** (vgl. Art. 139 Abs. 1 i.V.m. Art. 306 Abs. 1-2 und Art. 312 Abs. 1 StPO)."
- "Falls "Gefahr im Verzug" ist, dürfen die Strafbehörden jedoch **Beweisgegenstände** bereits ***vorläufig*** **sicherstellen** (Art. 263 Abs. 3 StPO). Sichernde Zwangsmassnahmen sind namentlich zulässig, wenn die blosse Aufforderung zur Edition den Zweck der Massnahme vereiteln würde (Art. 265 Abs. 4 StPO)."

Counter-Strategy

- **Never Pay!**
  - Trittbrettfahrer, Black-Listing
  - Kein "Treu und Glauben" vs. Service-Infrastruktur zwecks Vertrauensbildung
  - Angebot (Bezahlen) schafft Nachfrage (Finanzierung von weiteren Angriffen)
- **Risk Management**
  - Save the Crown-Jewels
  - abgesicherte Zahlungsmethoden/Prozesse, 2-Factor-Authentification,
  - no logs, no prosecution (BCM, Security-Maturität; Zeitfaktor, zentraler Logserver mit Active-Directory-, Firewall- und Proxydaten)
  - Up-to-date Virus-Protection / Firewall
  - Backup (regelmässig, inkl. Rückspielungstests)
- **Resilience** (Täter gehen Weg des geringsten Widerstands)
- **Gesundes Misstrauen**

Fragen?

– Vielen Dank für Ihre Aufmerksamkeit.



‘We’re still confused, but on a higher level.’

Enrico Fermi
* 29.09.1901 Rom, † 28.11.1954 Chicago, einer der bedeutendsten Kernphysiker des 20. Jahrhunderts.
1938 Nobelpreis für Physik