



Kanton Zürich
Direktion der Justiz und des Innern
Staatsanwaltschaft Kanton Zürich



cybercrime-quo vadis

Möglichkeiten und Grenzen der Cybercrime-Strafverfolgung

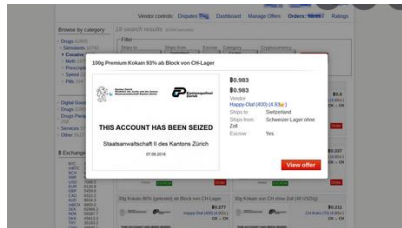
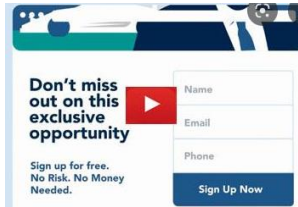
Referat am 12. Technology Forum 2022 by Studerus

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

Was ist Cybercrime?

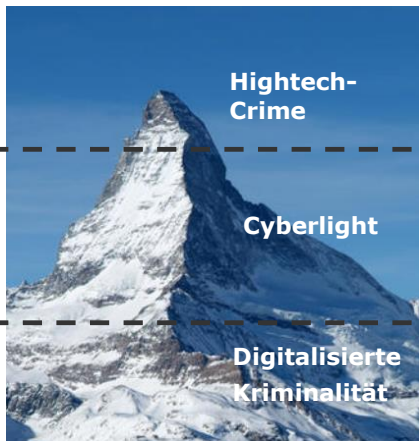
- Cyberkriminalität im engeren Sinn betrifft Straftaten, die mit Hilfe der Informations- und Kommunikationstechnologien (IKT) verübt werden oder sich Schwachstellen dieser Technologien zu Nutzen machen. Diese kriminellen Aktivitäten sind neu und werden durch diese Technologien erst möglich.
- Cyberkriminalität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

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/>

MITRE ATT&CK [®]													
Matrices Tactics ▾ Techniques ▾ Mitigations ▾ Groups Software Resources ▾ Blog  Contribute Search 													
ATT&CK Matrix for Enterprise													
layouts ▾ show sub-techniques hide sub-techniques													
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Collection	
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Clipboard Data	
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	Develop External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Dynamic Resolution (2)	
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (2)	Encrypted Channel (2)	
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Direct Volume Access	Deploy Container	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (2)	Encrypted Channel (2)	
Phishing for Information (3)	Obtain Capabilities (6)		Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Dynamic Resolution (2)	Encrypted Channel (2)	
Search Closed Sources (2)	Stage Capabilities (5)		Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Exploitation for Defense Evasion	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Ingress Tool Transfer	
Search Open Technical Databases (3)		Supply Chain Compromise (3)	Shared Modules	Create or Modify System Process (4)	Escape to Host	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Multi-Stage Channels	Non-Standard Port	
Search Open Websites/Domains (2)		Trusted Relationship	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Hide Artifacts (7)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Non-Standard Port		
Search Victim-Owned Websites		Valid Accounts (4)	System Services (2)	Exploitation for Privilege Escalation	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Standard Port		
			User Execution (3)	Hijack Execution	Impair Defenses (7)	Impair Defenses (7)	Steal Application Access Token	Network Share Discovery		Data Staged (2)			
			Windows Management Instrumentation					Password Policy Discovery					

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.

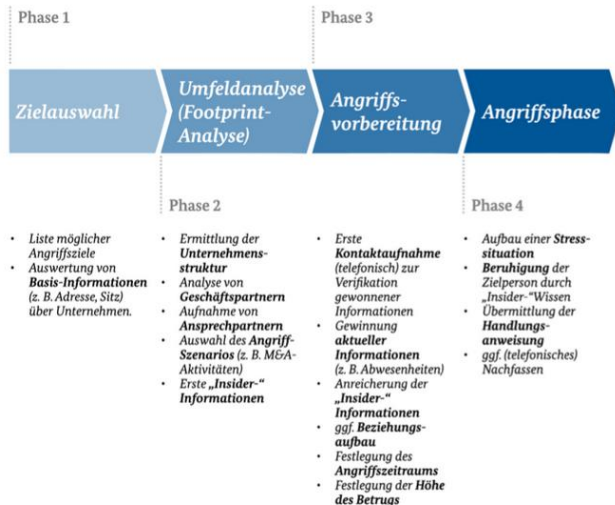
Regards,

Fabiola.

CEO-Fraud

– Modus operandi:

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



Quelle: BSI

Themen Organisation

Kanton Zürich • Direction der Justiz und des Innern • Staatsanwaltschaft • Staatsanwaltschaft II

Staatsanwaltschaft II

Wir sind spezialisiert auf die Strafverfolgung im Bereich der Schwerpunktkriminalität und Cybercrime. Ausserdem führen wir besondere Untersuchungen. Hier finden Sie Informationen zu unserer Organisation, zu unseren Abteilungen sowie die Kontaktangaben.

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)

Kontakt

Staatsanwaltschaft II des Kantons Zürich

Mehr erfahren →

Güterstrasse 33
Postfach
8010 Zürich
Route (Google)
Adresse kopieren

+41 43 258 23 00

kanlei.sta2@jz.zh.ch

Diese E-Mail ist nur für allgemeine Anfragen gedacht. Anfragen zu konkreten Verfahren richten Sie bitte direkt an den zuständigen Staatsanwalt oder die zuständige Staatsanwältin. Strafanzeigen, die per E-Mail eingereicht werden, müssen gemäss Art. 110 Abs. 2 StPO mit einer qualifizierten elektronischen Signatur versehen sein.

Falsche Unterstützungsanfragen

Windows Defender Alert :
Zeus Virus Detected In
Your Computer !!

Please Do Not Shut Down or Reset Your
Computer.



The following data will be compromised if you continue:

1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.

Call Technical Support Immediately at **(844) 7618-171**

**Call Microsoft Technical
Department: (844) 7618-
171 (Toll Free)**



WARNING!

**SYSTEM MAY HAVE DETECTED
VIRUSES ON YOUR COMPUTER**

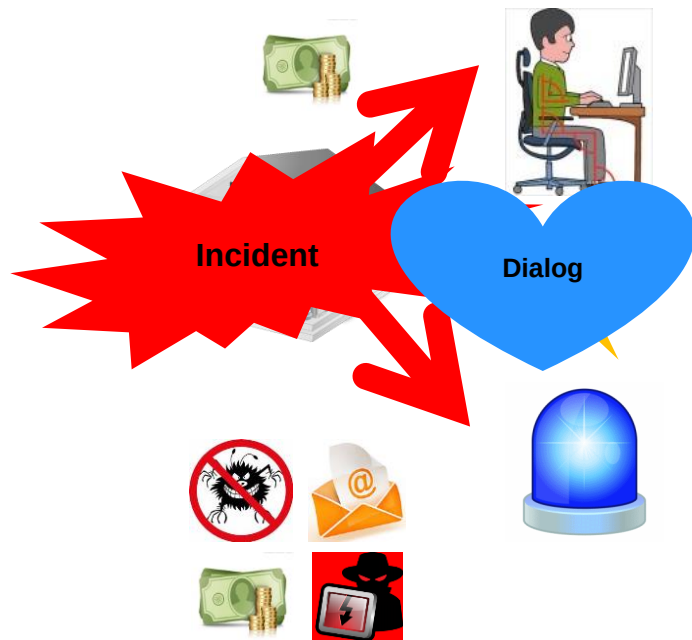
System May Have Found (2) Malicious Viruses: *Rootkit.Sirefef.Spy* and *Trojan.FakeAV-Download*. Your Personal & Financial Information **MAY NOT BE SAFE.**

For Help Removing Viruses, Call Tech Support Online Right Away:

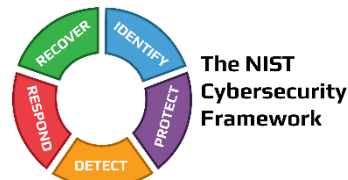
1(855) 970-1892
(TOLL-FREE, High Priority Call Line)

Your IP Address: [redacted] | Generated on 02-18-2014 | Priority: Urgent

Public Private Partnership



Cyber-Security



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

Strafverfolgung

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

IST-Lagebild: "Eisberg-Prinzip"



SOLL-Lagebild / Fallübersicht

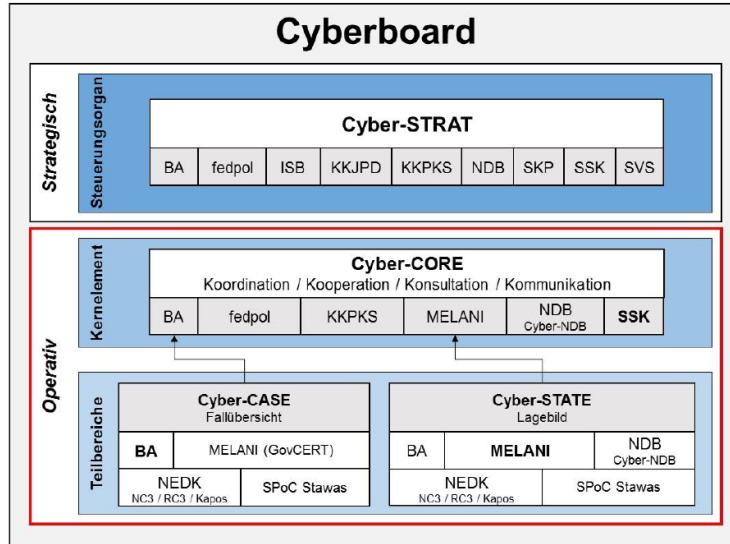
- Ereignis: Modus-Operandi, Anzahl, Tatort/Erfolgsort, Deliktsumme/Schaden
- Anzeige Polizei: Pendente Ermittlungen, Täter-ID pos./neg, Lokalisation, SOMA
- Geschäft STA: Zuständigkeit, Phänomenkomplex, operatives Verfahren, Rechtshilfe



Kanton	Ereignis	Anzeige	Untersuchung
	 		
			
			
			
			
	 		
			

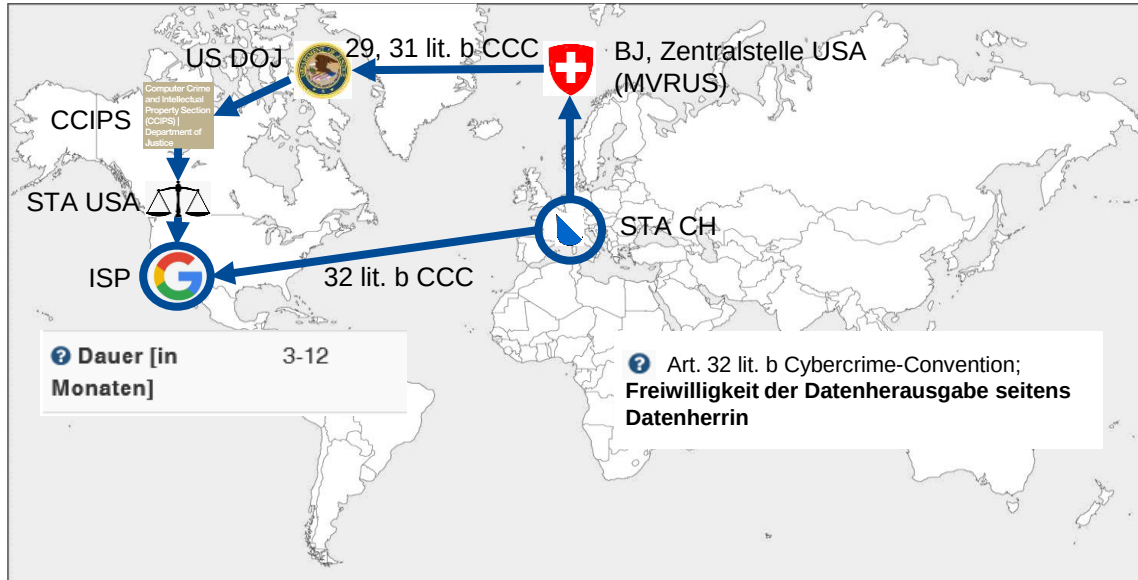
Nationale Koordination von Fallkomplexen

- 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 Verbundaufgabe



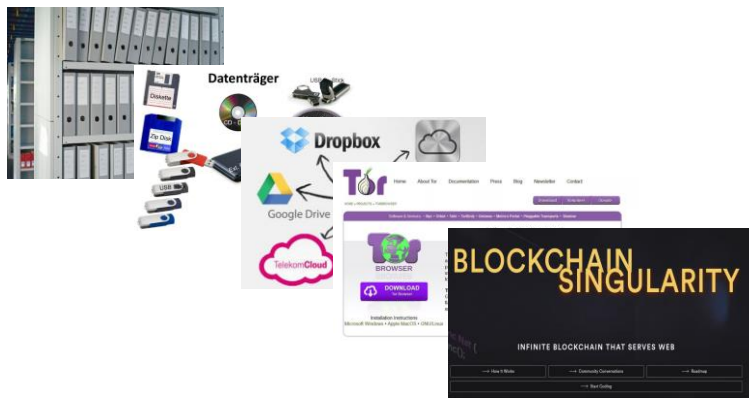
Key Challenge: Datenerhebung im Ausland

- 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

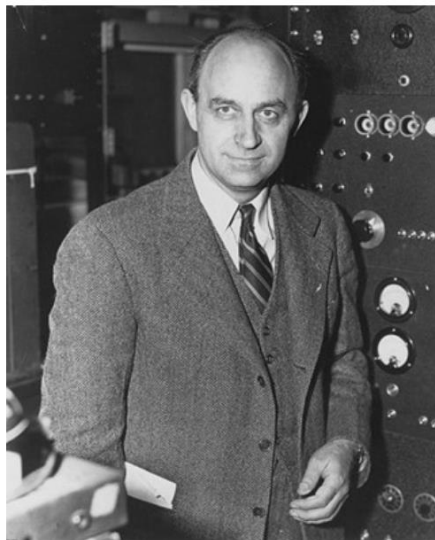
- "Die Nutzung des Internets, etwa von sozialen Netzwerken, steht grundsätzlich jedermann zu, auch Strafbehörden für **Online-Ermittlungen** (vgl. Art. 139 Abs. 1 i.V.m. Art. 306 Abs. 1-2 und Art. 312 Abs. 1 StPO)."
- "Falls "Gefahr im Verzug" ist, dürfen die Strafbehörden jedoch **Beweisgegenstände**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