

Was ist Cyber Security und warum ist der Schutz digitaler Systeme wie sensibler Daten so wichtig?

WELCOME

In der heutigen vernetzten digitalen Welt sind Angriffe aus dem Cyberspace eine reale Bedrohung. Cyber Security ist der Schutz vor diesen digitalen Gefahren.

Cyber Security | Davos



Rainer Kessler – Moderator

LL.M. M.B.A., Dozent FHGR & Cyber-Security Experte

Cyber Security | Davos



**Video-Grussbotschaft
Philipp Wilhelm,
Landammann**



Patrick Schaller – Referent

**Digitale Sicherheit - Geschichte, Herausforderungen,
Möglichkeiten, Beiträge ETH**

Senior Scientist am

Institut für Informationssicherheit ETH Zürich

zu meiner Person



- Dipl. Math ETH (1999)
- Bootcamp Cisco Systems (danach bei grossem ISP, CISO)
- Selbständig, Software-Entwicklung, Beratung
- “NDK Informatik ETH” (CAS Computer Science, Fokus Information Security)
- PhD in Information Security (Security Protokolle, formale Verifikation)
- Software Entwickler, Security Engineer
- Security Architekt
- Selbständig, Beratung, Prototypenbau, Entwicklung, Dozent ETH
- Wissenschaftlicher Projektleiter CYD Campus armasuisse
- Senior Scientist am Institut für Informationssicherheit der ETH Zürich

Digitale Sicherheit

Geschichte, Herausforderungen, Möglichkeiten, Beiträge ETH

Patrick Schaller

Senior Scientist am Institut für Informationssicherheit ETH Zürich

30.11.2023

Geschichte Informationssicherheit

- Bis 60er Jahre ausschliesslich für Staaten und Militär von Interesse
- Sicherheitseigenschaft von Interesse: Geheimhaltung
- Erster programmierbarer Computer, um Verschlüsselung der Wehrmacht im 2. Weltkrieg zu brechen (Colossus, Bletchley Park)
- Alain Turing: Theoretische Grundlagen der heutigen Informatik
- Claude Shannon: “Mathematical Theory of Communication” (1948)
- 60er Jahre Computer werden für die Industrie interessant (ARPANET: Vorgänger des heutigen Internets)
- 70er Jahre Entwicklung des Verschlüsselungsstandards DES (zertifiziert durch NIST 1976)



Geschichte Informationssicherheit



- 1976 asymmetrische Kryptographie
- 1980er Jahre Personal Computer (PC)
- 1990er Jahre HTTP, HTML, e-Mails, Verbreitung des Internets
- 2000er Jahre grossflächige Verbreitung Internet («I love you»-Virus)
- 2009 Satoshi Nakamoto setzt Bitcoin in die Welt
- 2010 Stuxnet (komplexe Schadsoftware gegen iranische Nukleareinrichtungen)
- 2013 Edward Snowden enthüllt Überwachungs- und Spionagepraktiken von westlichen Geheimdiensten
- 2015+ Carbanak (Bankraub > 1 Mia), NotPetya (Schadsoftware, Schaden >10 Mia),...
-

Entwicklung Informatik



- “isolierte” Systeme
- auf einzelne Aufgaben zugeschnitten
- verschiedene Systeme nicht kompatibel

- graphische Benutzeroberfläche
- mehrere Programme
- Vernetzung/Kommunikation

- interoperable Systeme
- vernetzte Systeme
- Online-Dienste

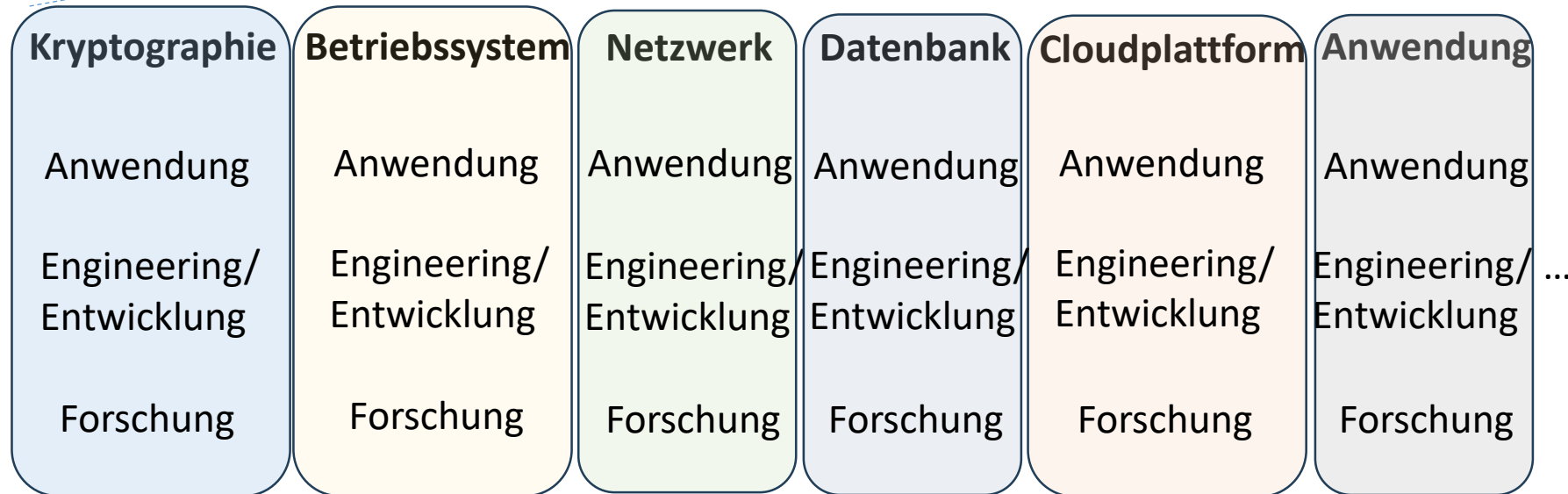
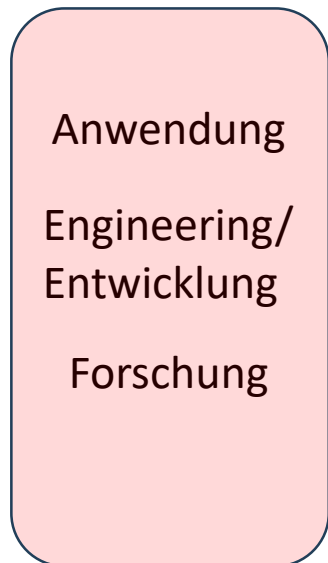
- Cloud-basierte Dienste
- soziale Netzwerke
- künstliche Intelligenz
- autonome Systeme

Rechenleistung, Datenspeicher, Benutzerfreundlichkeit, Anwendungsgebiete

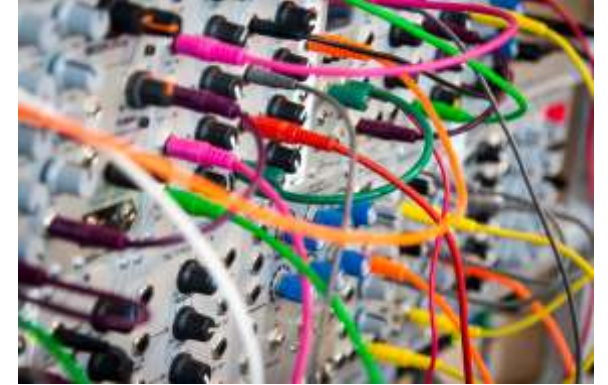


Spezialisierung, Informationsmenge, Abhängigkeit, Komplexität

Entwicklung Informatik



Komplexität



- Abstraktion und Modularisierung erlauben uns Komponenten wiederzuverwenden
- Wir erhöhen damit die Entwicklungsgeschwindigkeit und verringern die Entwicklungskosten (wirtschaftlicher Anreiz)
- Aus Benutzersicht vereinfacht sich vieles (Bsp. Navigation mit dem Smartphone), gleichzeitig wachsen die Abhängigkeiten und die Komplexität
- Bruce Schneier: «Complexity is the worst enemy of security»^{*}
- Thomas Dullien: «The anomaly of cheap complexity»^{**}

(^{*}): https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

(^{**}): <https://www.youtube.com/watch?v=q98foLaAfX8>

Schutzmassnahmen



- Bewusstsein
 - Abhängigkeiten
 - Komplexität
- Selbstverantwortung
- Gemäss dem «Digital Defense Report 2023» von Microsoft* kann man mit »Cyber-Hygiene« 99% der Cyber-Angriffe verhindern:
 - Multifaktor-Authentisierung
 - Umsetzung von «Zero-Trust»-Prinzipien
 - Verwenden von Werkzeugen die Angriffe entdecken und Virenschutz
 - Verwendete Software up-to-date halten
 - Kenntnis der eigenen Daten, deren Speicherort und Kritikalität => entsprechende Schutzmassnahmen

(*): <https://www.microsoft.com/en/security/security-insider/microsoft-digital-defense-report-2023/>

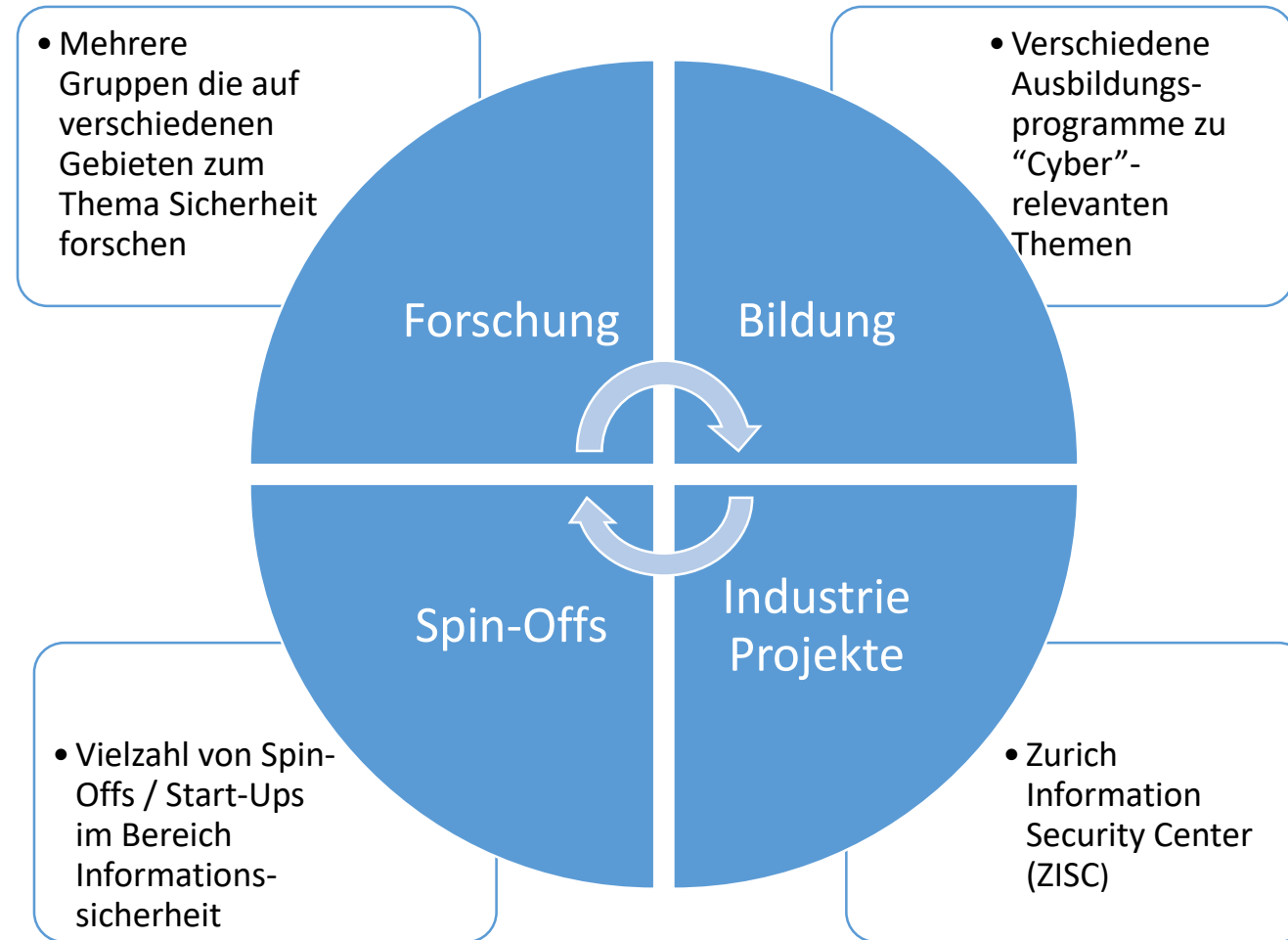
Schutzmassnahmen

- Resilienz
 - «Zero-Trust»-Prinzipien
 - Notfallnummern, -plan, -szenarien
 - Szenarien durchdenken/spielen
- Bewusstsein
- IKT-Minimalstandard* (Bundesamt für wirtschaftliche Landesversorgung BWL)
 - Leitfaden zur Analyse der eigenen Situation/»Readiness«
 - Konkrete Handlungsweisen zur Verbesserung der eigenen IKT-Resilienz



(*): https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html

Beiträge ETH



Forschung

- Institute of Information Security
 - Prof. David Basin: Information Security Group
 - Prof. Srdjan Capkun: System Security Group
 - Prof. Kenny Paterson: Applied Cryptography Group
 - Prof. Adrian Perrig: Network Security Group
 - Prof. Shweta Shinde: Secure & Trustworthy Systems Group
 - Prof. Florian Tramèr: Machine Learning and Information Security
- Institute of Theoretical Computer Science
 - Prof. Dennis Hofheinz: Foundations of Cryptography Group
 - Prof. Ueli Maurer: Information Security & Cryptography Group
- Related groups:
 - Examples: Machine learning, secure programming, software verification
- Over 100 researchers in Information Security

Bildungsprogramme Informationssicherheit

Continuing Education

CAS Cyber Security

- 10 ECTS

CAS Computer Science

- 20 ECTS
- Spec. Information Security

DAS Cyber Security

- 35 ECTS

Master's Programs

Master of Science

- Computer Science
- Track Information Security

Master of Science

- Cyber Security
- Joint Master EPFL/ETHZ

Bachelor's Program

Bachelor of Science

- Computer Science

Zurich Information Security Center (ZISC)





- Verbindung Academia – Industry
- Gemeinsame Forschungsprojekte zu “Cyber”-relevanten Themen
- Gemeinsames Angehen der “Cyber”-Herausforderungen von heute und morgen
- Mehr Informationen: <https://zisc.ethz.ch>
- Partner:



Swiss Support Center for Cybersecurity (SSCC)

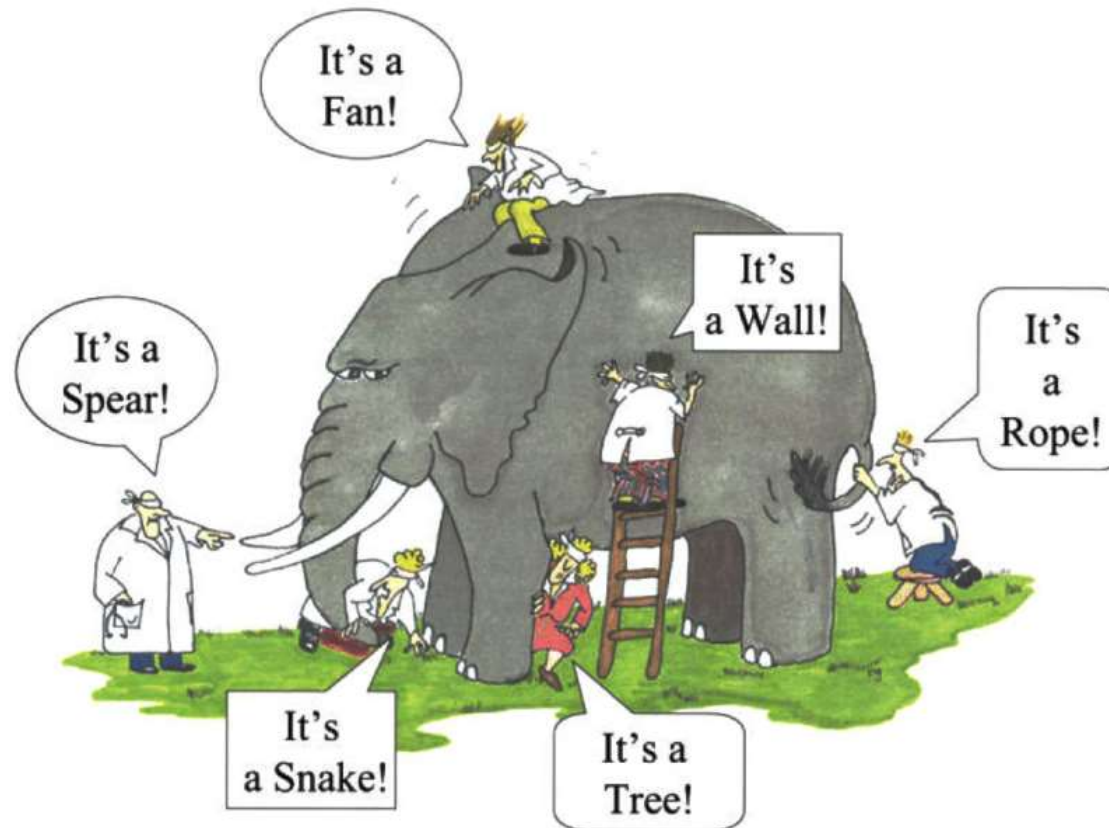
- Gemeinsame Initiative mit EPFL (mehr Hochschulen geplant)
- Ursprung in der nationalen Cyber Strategie (NCS 2018 – 22)
- Unterstützung von Verwaltung und Industrie sowie der Schweizer Bevölkerung als Ganzes in Bezug auf heutige und zukünftige Herausforderungen auf dem Gebiet der “Cyber”-Sicherheit
- Aktivitäten:
 - Akademische Arbeitsgruppen
 - Think Tanks
 - Unterstützung von Ausbildungsprogrammen zum Thema “Cyber”-Sicherheit
- Für mehr Informationen: <https://sscc.ethz.ch>

Information Security bezogene Spin-Offs / Start-Ups

-  : truly secure networking
-  : access control based on proximity
- **FUTURAE**  : two factor authentication
-  CHAINSECURITY : automated formal audit for blockchains
- **xorlab**: effective cyber threat prevention
- ... and many more

Ende

Danke für Ihre Aufmerksamkeit!



Cyber Security | Davos



Fragen?



Monika Stucki – Referentin

Datenschutz - Warum wir uns wirklich mit dem Thema beschäftigen sollten

**Team Leader & Lead Security Consultant bei Redguard AG
Lehrbeauftragte FHGR**

zu meiner Person

- Bachelor- und Master-Absolventin der früheren HTW Chur (Informationswissenschaft)
- Lehrbeauftragte IT Security und Gastdozentin Datenschutz an der FHGR
- Teamleiterin Datenschutz sowie Sicherheits- und Datenschutzbeauftragte bei der Redguard AG
- Datenschützerin durch und durch sowohl im geschäftlichen, als auch im privaten Alltag



Datenschutz

Warum wir uns wirklich mit dem Thema beschäftigen sollten

Monika Stucki, 25.01.2024

Alles, was Recht ist

- Bundesverfassung Art. 13 (Schutz vor Missbrauch der persönlichen Daten)
- Datenschutzgesetz (DSG) & Verordnung (DSV) (für Bundesorgane und Private)
- 24 kantonale Datenschutzgesetze (für kantonale und kommunale Behörden)

Datenschutz bezweckt die Wahrung der Persönlichkeit und Grundrechte von **betroffenen Personen** bei der **Bearbeitung** von **Personendaten**.

Darum geht's

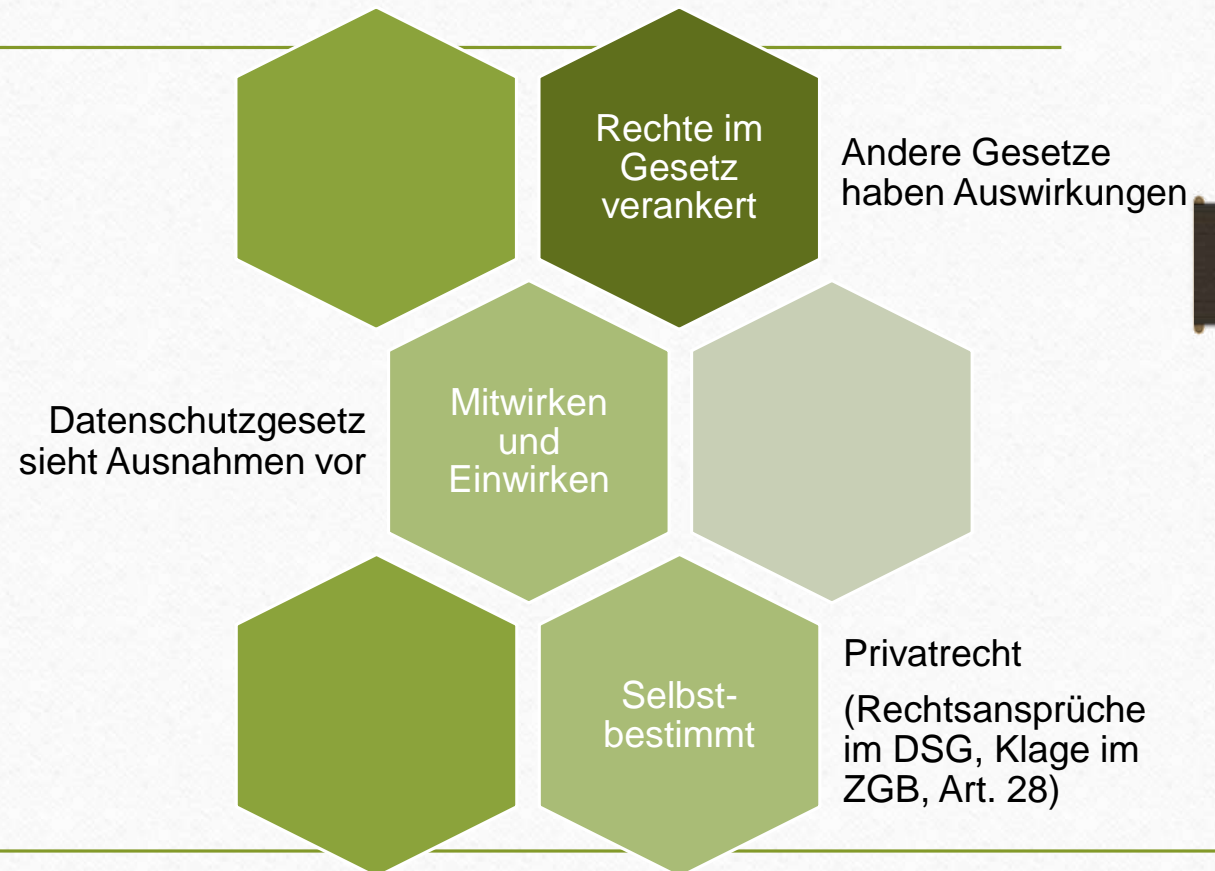
- Über **betroffene Personen** bearbeiten wir (Personen-)Daten
- **Personendaten** beziehen sich auf eine bestimmte Person oder ermöglichen eine Identifikation dieser Person
 - "normale" Daten wie Vor- und Nachname, Geburtsdatum, Lohndaten, etc.
 - Besonders schützenswerte Personendaten wie Gesundheitsdaten, Daten über Intimsphäre, Rasse Ethnie, ...

- Jeder Umgang mit Persondaten ist eine **Bearbeitung**



Unsere Rechte (als Betroffene)

- Information
- Auskunft
- Datenherausgabe und –übertragung
- Berichtigung
- Einschränkung der Bearbeitung
- Widerspruch gegen Bekanntgabe
- Widerruf einer Einwilligung
- Löschung



Unsere Pflichten (als Bearbeitende)

- Einhaltung der Grundsätze
 - Keine Bearbeitungen, die gegen gesetzliche Vorgaben verstossen (Rechtmässigkeit)
 - Nur so, wie die Betroffenen es erwarten dürfen (Treu und Glauben / Transparenz)
 - So wenig wie möglich und so viel wie nötig für die Aufgabe (Verhältnismässigkeit)
 - Keine Bearbeitung (auch keine Sammlung), wenn kein Zweck besteht (Zweckbindung)
 - Löschen/Vernichten/Anonymisieren, sobald nicht mehr benötigt (Datensparsamkeit)
 - Daten sind im Kontext korrekt und aktuell oder zu berichtigen (Richtigkeit)
 - Datenschutz von Anfang an und als Standard (Privacy by Design/Default)

Unsere Pflichten (als Bearbeitende)

- Die Betroffenen über die Bearbeitung ihrer Daten informieren (Informationspflicht) und ihre Rechte sicherstellen
- Dokumentationen und Risikoanalysen erstellen (Verzeichnis der Bearbeitungstätigkeiten, Datenschutz-Folgenabschätzungen)
- Auftragsbearbeiter verpflichten (vertraglich) und kontrollieren
- Datensicherheit gewährleisten (durch angemessene technische und organisatorische Massnahmen) und Meldung erstatten bei Verletzung der Datensicherheit
- Unsere berufliche Schweigepflicht einhalten
- Mitwirken, wenn die Aufsichtsbehörde (EDÖB) kommt

Datenschutz

Warum wir uns **wirklich** mit dem Thema beschäftigen sollten



Darum sollten wir uns damit beschäftigen!

Datenschutz ist eine kollektive Verantwortung, denn...

... wir alle sind

- Kunden, Patienten, Klienten von Unternehmen und damit Betroffene
- täglich im Umgang mit Daten von Familie, Freunden, Bekannten und allen anderen, die wir über 7 Ecken kennen

Datenschutz “in a Nutshell”

Es gibt noch viel zu tun.

Vielen Dank für Ihre Aufmerksamkeit.



Cyber Security | Davos



Fragen?

Cyber Security | Davos



Ingo Barkow – Referent

Cyber Security - Mythen aufgeklärt und wie man sich trotzdem schützen kann

Professor & Leiter des Schweizerischen Instituts für Informationswissenschaft (SII)

**Gute Besserung,
Ingo!**

zu meiner Person



- Seit 2015 an der FH Graubünden beschäftigt, Dozent für Datenmanagement, seit 2017 als Professor und seit 2019 als Institutsleiter des Schweizerischen Institut für Informationswissenschaft.
- Data Manager am Deutschen Institut für Internationale Pädagogische Forschung (DIPF) in Frankfurt, Fachbereiche Forschungsdatenzentrum (FDZ) Zentrum für Technologiebasiertes Assessment (TBA)
- Geschäftsführer ein IT-Schulungsunternehmen im Raum Würzburg. Trainer für Firmenschulungen/Lehrbeauftragter in den Bereichen Datenbankadministration, Datenbankentwicklung, Datenintegration, Datenanalyse, Netzwerkadministration

Zehn Mythen über Cybersecurity



MYTHOS 1

*«MEINE DATEN SIND FÜR HACKER
NICHT INTERESSANT»*

BEDROHUNG

**IMMER STÄRKERES AUFKOMMEN VON
RANSOMWARE ODER BOTNETZEN**

MYTHOS 2

*«HACKINGANGRIFFE BETREFFEN
NUR MITTLERE UND GRÖßERE
UNTERNEHMEN»*

BEDROHUNG

**HACKING UND SABOTAGE AUCH BEI
KMU ODER PRIVATPERSONEN**

MYTHOS 3

*«HACKINGANGRIFFE SIND DIE FOLGE
VON UNGESCHULTEM PERSONAL»*

BEDROHUNG

**SCHULUNGEN NICHT REGELMÄSSIG,
INHALTE WERDEN DURCH
NICHTAUFTRETEN VERGESSEN**

MYTHOS 4

«*CYBERSECURITY IST NUR AUF
COMPUTERN RELEVANT*»

BEDROHUNG

**IMMER MEHR HACKING AUF
SMARTPHONES, TEILWEISE AUCH
LEGAL DURCH SOFTWAREANBIETER**

MYTHOS 5

*«HACKING E-MAILS SIND DEUTLICH
ERKENNBAR Z.B. AN SCHREIBFEHLERN»*

BEDROHUNG

**IMMER MEHR «TAILOR-MADE» MAILS
MIT SPEZIFISCHER AUSRICHTUNG AN
DEN ADRESSATEN**

MYTHOS 6

*«HACKING IST EIN REIN TECHNISCHER
PROZESS»*

BEDROHUNG

**DIE MAJORITÄT VON
HACKINGANGRIFFEN FUNKTIONIERT
ÜBER SOCIAL ENGINEERING**

MYTHOS 7

*«DER SCHADEN VON HACKING
ANGRIFFEN IST SCHNELL ERKENNBAR»*

BEDROHUNG

**DIE MAJORITÄT VON
HACKINGANGRIFFEN WIRD VON DEN
BETROFFENEN NICHT ERKANNT**

MYTHOS 8

*«ANTIVIRENSOFTWARE UND FIREWALL
REICHEN ALS SCHUTZ AUS»*

BEDROHUNG

**KONTUNIERLICHE VERBESSERUNG VON
HACKING TOOLS UND METHODEN**

MYTHOS 9

*«IT-SICHERHEIT WIRD HERGESTELLT
ÜBER STRIKTE RICHTLINIEN»*

BEDROHUNG

**STRIKTE RICHTLINIEN WERDEN VON
USERN WEGEN SCHLECHTER USABILITY
UMGANGEN**

MYTHOS 10

*«WIR SIND SICHER DA WIR NUR
EXTERNE DIENSTE IN DER CLOUD
VERWENDEN»*

BEDROHUNG

**REGELMÄSSIGE SICHERHEITSLLECKS
BEI KOMMERZIELLEN CLOUD
ANBIETERN**

FAZIT

SICHERHEIT IN REGELMÄSSIGEN
ABSTÄNDEN HINTERFRAGEN

DANN METHODEN PRAGMATISCH
UMSETZEN

Fachhochschule Graubünden
Pulvermühlestrasse 57
7000 Chur
T +41 81 286 24 24
info@fhgr.ch

Vielen Dank für Ihre Aufmerksamkeit.

Fachhochschule Graubünden
Scola auta specialisada dal Grischun
Scuola universitaria professionale dei Grigioni
University of Applied Sciences of the Grisons

swissuniversities



Cyber Security | Davos



Fragen?



Christoph Scherer – Referent

Cybercrime Dienste der Kantonspolizei Graubünden

Chef Cybercrime Dienste bei Kantonspolizei Graubünden |
MSc | Malware Analyst | Forensic Examiner

zu meiner Person



- Seit 2023 Chef Cybercrime Dienste der Kantonspolizei Graubünden, vorher Projektleiter und Koordinator Cybercrime, Dienste Mobile Forensic Examiner und Ermittler
- 2021 High Tech Analysis Unit (HTAU), Secondment Program (Manhattan District Attorney's Office)
- Frontend Developer bei Clear Minds Investment AG
- IF&HF Advisory Office | Associate Director, UBS



Kantonspolizei Graubünden
Polizia chantunala dal Grischun
Polizia cantonale dei Grigioni

Cyber Incident: die Rolle der Polizei

GZD Cyber Security Veranstaltung Davos



Kantonspolizei
Graubünden



Digitale Ziele Kanton GR



Die Bündner Regierung, Foto: Ständekanzlei Graubünden

Die Bündner Regierung schickt die Kantonspolizei in den Cyber-Kurs. Zudem soll im Kanton enger mit Hochschulen zusammengearbeitet werden.



Die Bündner Regierung hat neben Klima und Vielfalt auch Innovation und Digitalisierung als Pfeiler des kantonalen Erfolgs definiert. Man wolle sich damit als innovativer Gebirgskanton positionieren, heisst es seitens der Exekutive. Die politische Strategie, die bis 2024 festgelegt wurde, geht nun in die Umsetzungsphase.

Dieses Jahr soll besonders die Kooperation des Kantons mit Hochschulen gefördert werden. 2021 werde eine

Sonderprofessur Life Science mit der Einrichtung einer neuen Assistenzprofessur an der Universität Zürich umgesetzt, wie es in der Strategie heisst. Zudem will der Kanton die Fachhochschule Graubünden national und international besser positionieren, dafür soll ein Hochschulzentrum gebaut werden.

Ein weiterer Schwerpunkt ist die Umsetzung der Cyberstrategie der Kantonspolizei. 2021 werde eine Ausbildungsoffensive lanciert, heisst es. Alle Mitarbeitenden der Kantonspolizei würden eine Grundausbildung in den Themenbereichen Cybersicherheit, Phänomene, Spurensicherung, Mobiltelefone und cyberspezifisches Vorgehen bei einer Tatbestandsaufnahme absolvieren. Für jene Polizisten, die direkt in Sachen Cyberkriminalität ermitteln, wird ein vertiefender Kurs durchgeführt.

Zugleich werde mit der Arbeit zum Aufbau einer spezialisierten IT-Umgebung begonnen, so die Regierung. Diese diene dazu, dass Ermittlungen im Internet anonym und ohne technische Restriktionen durchgeführt werden können. Zudem sollen die Integrität, Vertraulichkeit und Verfügbarkeit von beweisrelevanten Daten sichergestellt werden.

Jahresprogramm 2021

Diese Digitalthemen packt Graubünden dieses Jahr an

Mi 13.01.2021 - 11:15 Uhr
 von René Jaun und Iha

Im Rahmen seines Regierungsprogramms der kommenden vier Jahre setzt der Kanton Graubünden einen Schwerpunkt auf die Digitalisierung. Noch dieses Jahr will er unter anderem die digitale Quellensteuerdeklaration ermöglichen, sowie die Polizei für den Bereich Cybercrime schulen lassen.



"Die Bündner Regierung schickt die Kantonspolizei in den Cyber-Kurs.."



Kantonspolizei Graubünden

Kantonspolizei Graubünden

- 527 MA (davon 108 in Kripo)
- 2022: 11'234 Straftaten

Cybercrime Dienste (CYCD)

- Dienst in der Kriminalpolizei
- Seit 2017 (2003 – 2017 IT Forensik)
- 13 Mitarbeitende (zivil & inkorporierte)
- 3 Fachdienste:
 - IT-Forensik
 - Cybercrime Ermittlung
 - Kriminalanalyse



Fachdienste im CYCD



CYC Forensik

- Sicherstellungen von Computer, Server, Mobilgeräte, IoT, Fahrzeuge
- Gerichtsverwertbare Beweismittelsicherung
 - Datensicherung
 - Extraktionen
 - Aufbereitung
- Technische Analyse



CYC Ermittlungen

- Ermittlungsunterstützung Cybercrime im weiteren Sinn und digitale Ermittlungen
- Fallbezogenes OSINT
- Ermittlungen Cybercrime im engeren Sinn
- Malware-Analyse & Reverse Engineering
- Tracing Kryptowährungen
- Technische Überwachungen
- Darknet
- P2P Monitoring
- Unterstützung VF / VE im virtuellen Raum (z.B. virtuelle Pädokriminalität)



CYC Kriminalanalysestelle

- Strategisch: Statistiken/Muster für strategische Führung (Resource Allocation)
- Taktisch: Lagebild zur seriellen (Cyber-)Kriminalität
- Operationell: Auswertung einzelner Fälle oder Serie mit Visualisierungen, Hypothesen und Empfehlungen
- Massendatenanalyse
- Systematisches OSINT



Sind wir alleine? Teamwork



Fedpol / BKP / Interpol / Europol

Partnerorganisationen koordinieren internationale Zusammenarbeit oder übernehmen in bestimmten Fällen die Fallführung

Anderes Polizeikorps

Aufgrund bestehendem Sammelverfahren oder getätigten Ermittlungen kann der Fall an eine andere Strafverfolgungsbehörde abgetreten werden
Beispiele: Kantonspolizei Zürich
übernahme Verfahren Reteffe



Lage "Cybercrime"



Schweizer Unternehmen ungenügend geschützt

CYBERANGRIFF

Websites der St.Galler Freitagmorgen offline

Hackerangriff auf St. Gallen

Audio & Podcast

Cyberkriminalität in der Erziehung

Cyberkriminalität: Daten gestohlen, Terabyte weggeschickt, Schülerin...

Autor:in: Nina G
10.05.2023, 17:30

Der Bundesrat

Schweizerische Eidgenossenschaft
Confederaziun Svizra
Confederaziun Svizra

Der Bundesrat
Das Portal der Schweizer Regierung

Suchen

Themen A-Z

Startseite > Dokumentation > Medienmittellungen > Hackerangriff auf die Firma Concevis: Auch die Bundesverwaltung ist betroffen

Hackerangriff auf die Firma Concevis: Auch die Bundesverwaltung ist betroffen

Bern, 14.11.2023 - Das Software-Unternehmen Concevis wurde Opfer eines Ransomware-Angriffes, bei dem sämtliche Server der Firma verschlüsselt wurden. Unter den entwendeten Daten befinden sich nach aktuellem Kenntnisstand mutmasslich auch ältere, operative Daten der Bundesverwaltung. Die vertieften Analysen laufen derzeit noch.

Hackerangriff zeigt, wie abhängig der Bund von Xplain ist

Aus Rundschau vom 08.10.2023

News > Schweiz >

Wegen Hackerangriff auf Xplain – Polizeisoftware teils offline

Bei der Stadtberner Fremdenpolizei funktioniert eine App nicht mehr. Die Abhängigkeit der Behörden von Xplain zeigt sich auch andernorts.

Die Hackergruppe Play hat am 24. März den Medienverlag NZZ und die CH Media angegriffen.



Häufigste Tatbestände



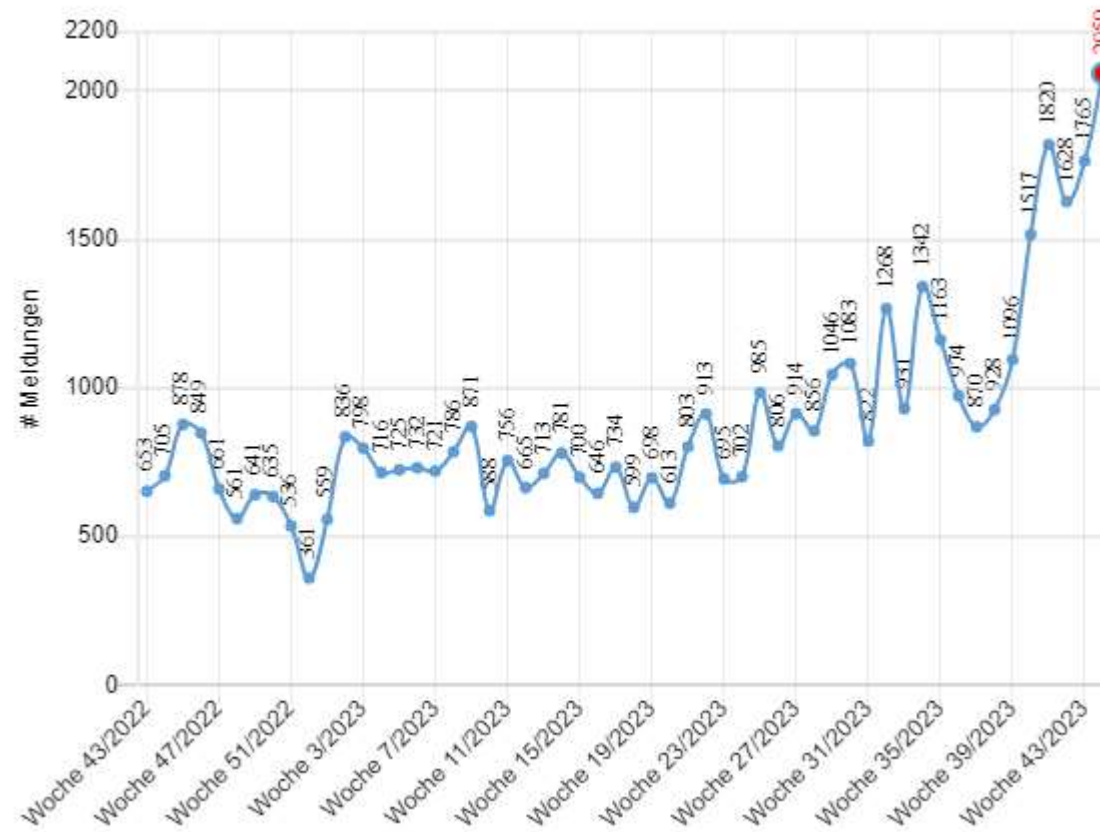


Tatbestände mit hoher Deliktssumme

CEO-Fraud
Ransomware
Boiler Room Fraud
Romance Scam



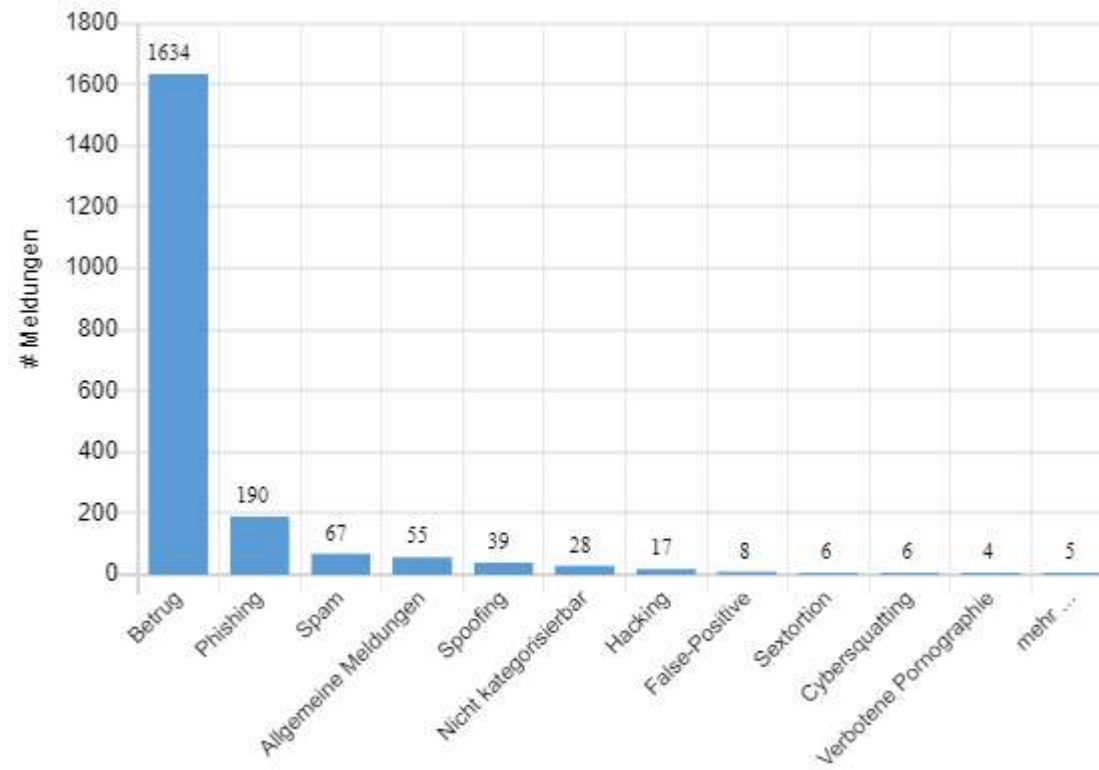
NCSC Meldungen



Entwicklung der Meldungen der letzten 12 Monate / Quelle: www.ncsc.admin.ch (Stand 07.11.2023)



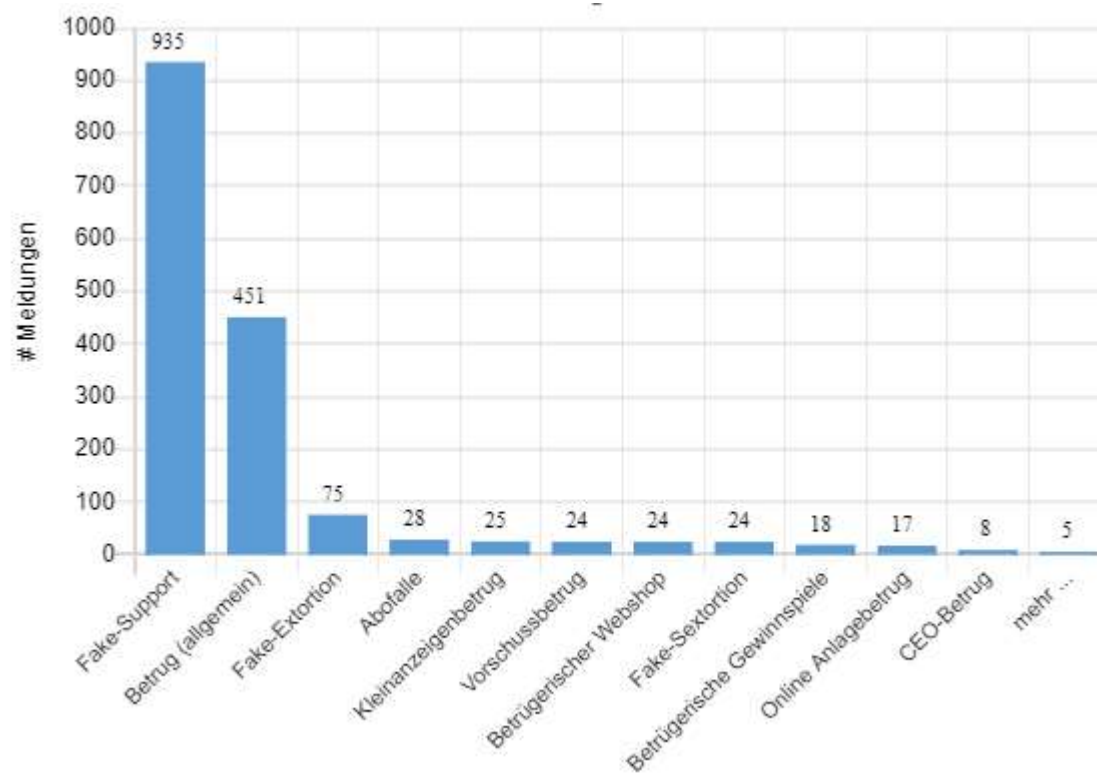
NCSC Meldungen Kategorien



Detaillierte Statistik der am häufigsten gemeldeten Cybervorfälle nach Hauptkategorien pro Woche / Quelle: www.ncsc.admin.ch (Stand 07.11.2023)



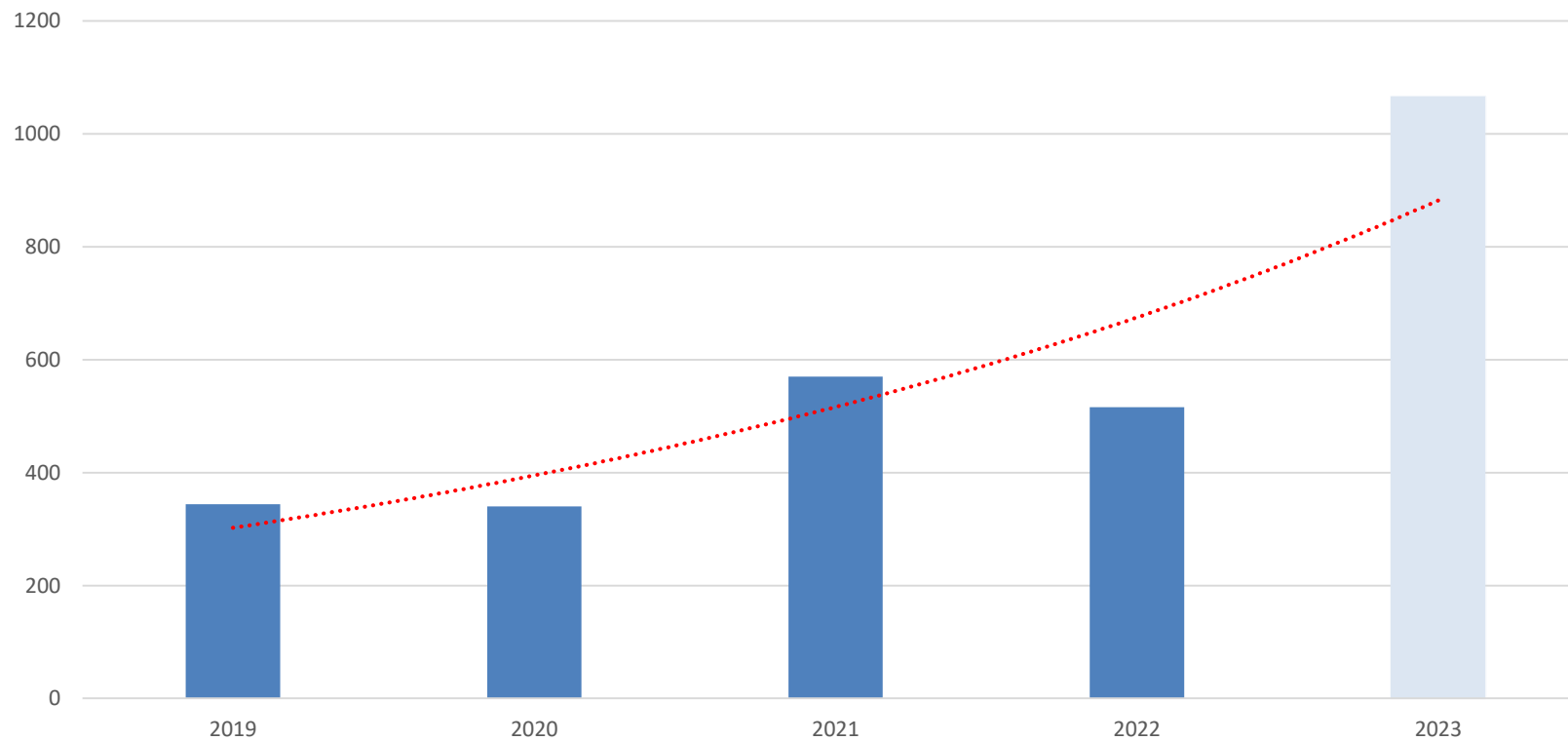
NCSC Meldungen Betrug





Entwicklung Cyberdelikte GR

Straftaten mit einem Modus Operandi der digitalen Kriminalität, Kanton Graubünden

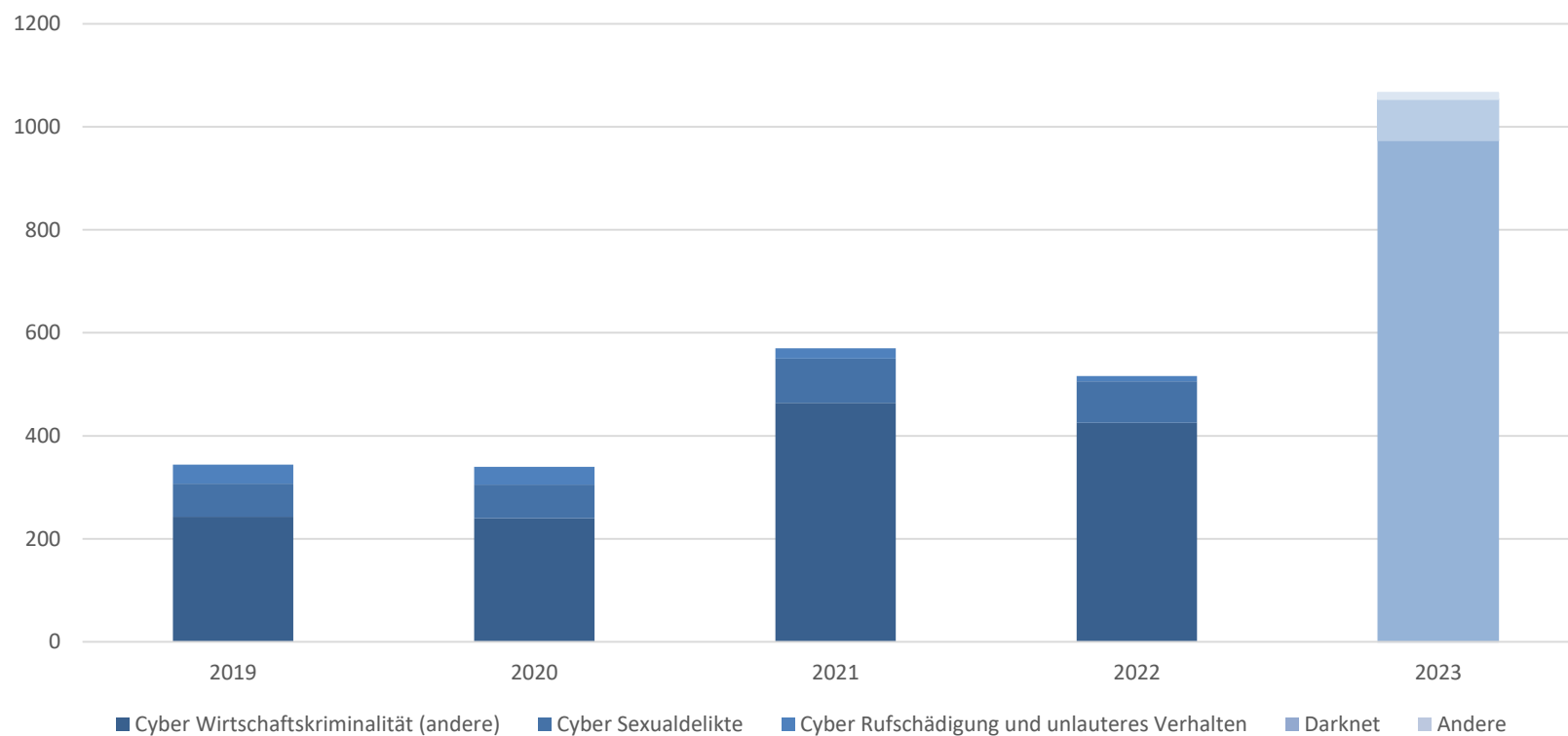


Quelle: PKS (Straftaten mit einem Modus Operandi der digitalen Kriminalität Kanton Graubünden)
2023 ist eine lineare Hochrechnung aufgrund der PKS Zahlen Januar bis September 2023 mit einem arithmetischen Mittel des Trends



Entwicklung Cyberdelikte GR

Straftaten mit einem Modus Operandi der digitalen Kriminalität, Kanton Graubünden



Quelle: PKS (Straftaten mit einem Modus Operandi der digitalen Kriminalität Kanton Graubünden)
2023 ist eine lineare Hochrechnung aufgrund der PKS Zahlen Januar bis September 2023 mit einem arithmetischen Mittel des Trends



Was macht die Polizei?

Nationale Cyberstrategie (NCS)

Cyberdefence

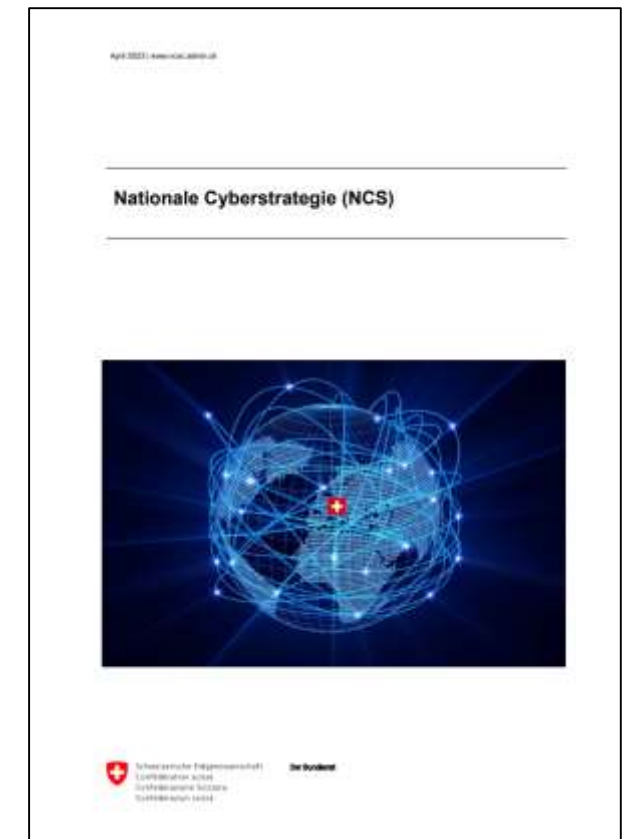
- Schutz der für die Landesverteidigung kritischen Systeme und Abwehr von Cyberangriffen
- Zuständigkeit: Armee

Cybersicherheit

- Bewältigung von Vorfällen und Verbesserung der Resilienz gegenüber Cyberrisiken
- Zuständigkeit: NCSC und Alle (Provider, Unternehmen, Private, Bund und Kantone)

Cyberstrafverfolgung

- Bekämpfung der Cyberkriminalität
- Zuständigkeit: Strafverfolgungsbehörden





Mission & Auftrag

Kantonsverfassung (Art. 79) und Polizeigesetz (Art. 2) definieren die Mission und den Auftrag der Kantonspolizei Graubünden.

- Wir sorgen für Ruhe und Ordnung
- Wir verfolgen Straftaten
- Wir beraten
- Wir helfen in der Not

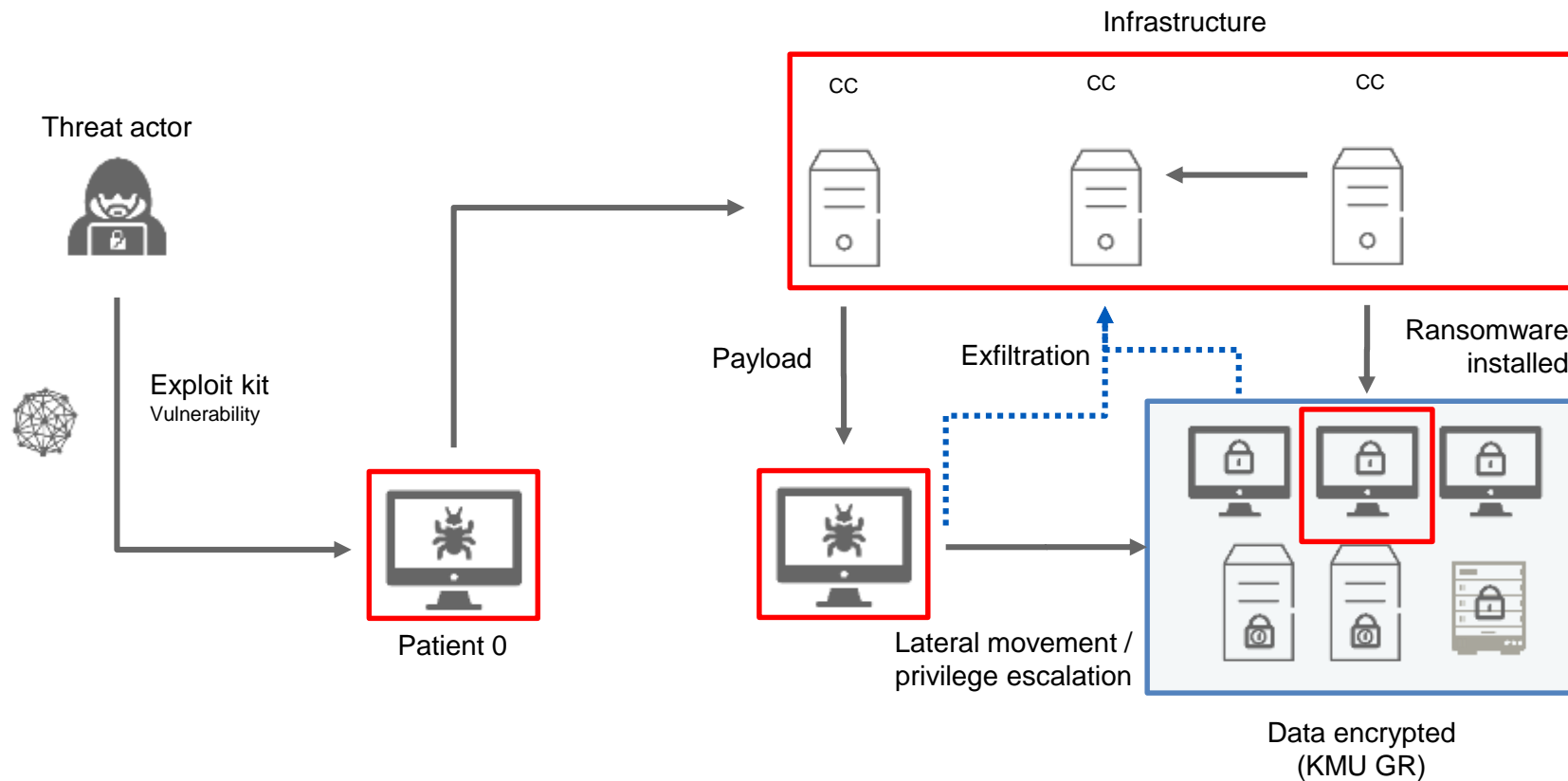


Polizei im virtuellen Raum

- Strafverfolgung: Wir **sichern Beweise**, **identifizieren** und **lokalisieren Straftäter**.
- Prävention: Wir **beraten** und **unterstützen** (potentielle) Geschädigte.
- Der Schutz und die Reparatur der Infrastruktur obliegt den Eigentümern.
- Wir sind nicht an Geschäftsgeheimnissen interessiert und wirken nicht auf die Infrastruktur ein.

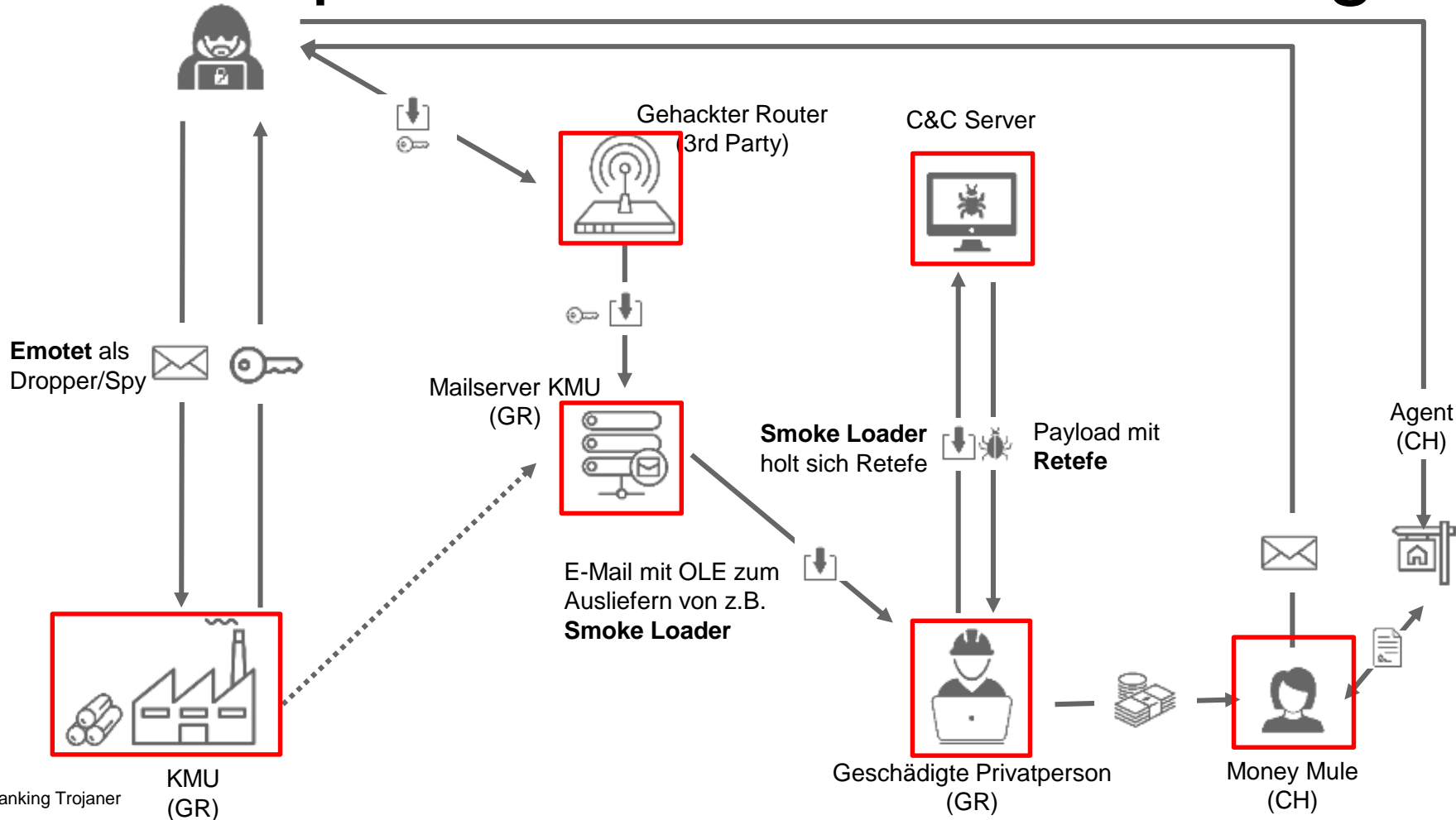


Beispiel: Beweismittelsicherung



Fiktives Beispiel Ransomware

Beispiel: Beweismittelsicherung



Fiktives Beispiel E-Banking Trojaner



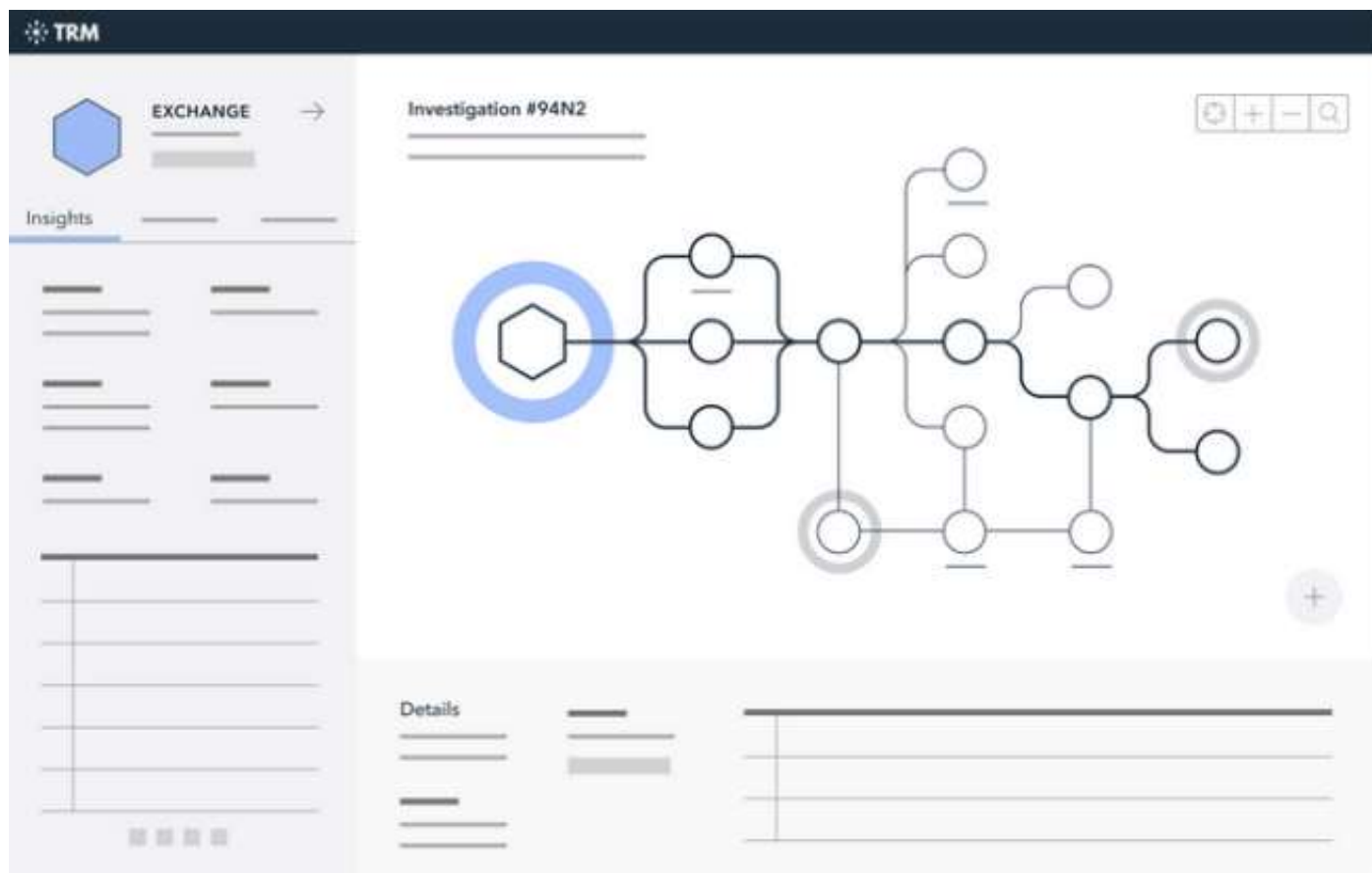
Beispiel: Identifikation

```
ext:00000001400022B7 E8 A4 FA FF FF      call    DecryptionAndRegistry ; Call Procedure
ext:00000001400022BC C7 44 24 34 00 10 00 00 mov     [rsp+20E8h+var_2084], 1000h
ext:00000001400022C4 48 8D 44 24 58          lea    rax, [rsp+20E8h+var_2090] ; Load Effective Address
ext:00000001400022C9 48 8D 0D 88 2B 00 00   lea    rcx, aAhr0cdov13d3dv_9 ; Base64:
ext:00000001400022C9                                     ; http://www.elsmap.com/banner.jpg
ext:00000001400022D0 48 8B F8              mov     rdi, rax
ext:00000001400022D3 48 8B F1              mov     rsi, rcx
ext:00000001400022D6 B9 2D 00 00 00        mov     ecx, 2Dh ; '-'
ext:00000001400022DB F3 A4                 rep movsb ; Move Byte(s) from String to String
ext:00000001400022DD C7 44 24 38 2C 00 00 00 mov     [rsp+20E8h+var_2080], 2Ch ; ','
ext:00000001400022E5 44 8B 4C 24 34          mov     r9d, [rsp+20E8h+var_20B4]
ext:00000001400022EA 4C 8D 84 24 C0 10 00 00 lea    r8, [rsp+20E8h+var_1028] ; Load Effective Address
ext:00000001400022F2 8B 54 24 38          mov     edx, [rsp+20E8h+var_2080]
ext:00000001400022F6 48 8D 4C 24 58          lea    rcx, [rsp+20E8h+var_2090] ; Load Effective Address
ext:00000001400022F8 E8 20 F0 FF FF        call   Base64Decryption ; Call Procedure
ext:0000000140002300 89 44 24 44           mov     [rsp+20E8h+var_20A4], eax
ext:0000000140002304 C7 44 24 3C 00 10 00 00 mov     [rsp+20E8h+var_20AC], 1000h
ext:000000014000230C 48 8D 84 24 88 00 00 00 lea    rax, [rsp+20E8h+var_2060] ; Load Effective Address
ext:0000000140002314 48 8D 0D 6D 2B 00 00   lea    rcx, aQzpcv2luzg93c1 ; C:\Windows\System32\conbase.dll
ext:0000000140002318 48 8B F8              mov     rdi, rax
ext:000000014000231E 48 8B F1              mov     rsi, rcx
ext:0000000140002321 B9 2D 00 00 00        mov     ecx, 2Dh ; '-'
ext:0000000140002326 F3 A4                 rep movsb ; Move Byte(s) from String to String
ext:0000000140002328 C7 44 24 40 2C 00 00 00 mov     [rsp+20E8h+var_20A8], 2Ch ; ','
ext:0000000140002330 44 8B 4C 24 3C          mov     r9d, [rsp+20E8h+var_20AC]
ext:0000000140002335 4C 8D 84 24 C0 00 00 00 lea    r8, [rsp+20E8h+var_2028] ; Load Effective Address
ext:000000014000233D 8B 54 24 40          mov     edx, [rsp+20E8h+var_20A8]
ext:0000000140002341 48 8D 8C 24 88 00 00 00 lea    rcx, [rsp+20E8h+var_2060] ; Load Effective Address
ext:0000000140002349 E8 D2 EF FF FF        call   Base64Decryption ; Call Procedure
ext:000000014000234E 8B 44 24 40          mov     [rsp+20E8h+var_20A0], eax
```

Fiktives Beispiel Binärcode Analyse mit IDA

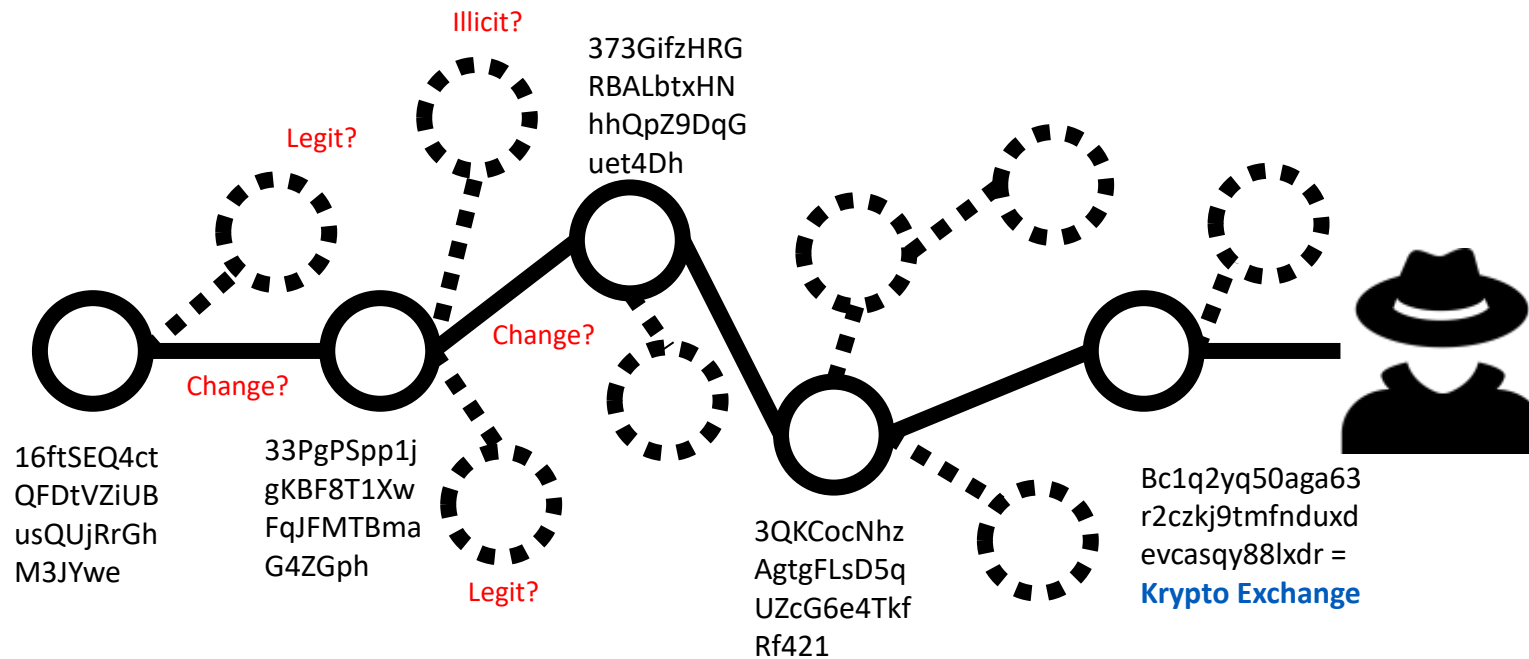


Beispiel: Identifikation





Beispiel: Identifikation



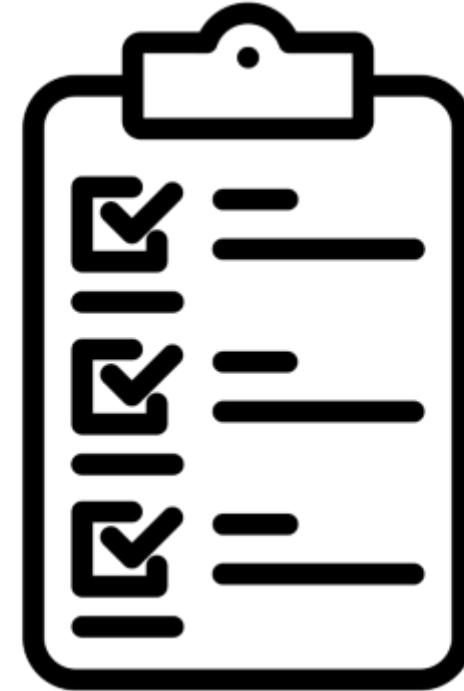
Fiktive Darstellung von Krypto Tracing mit bekannten public Adressen

Beispiel: Beratung

Massnahmen bei einem Ransomware Vorfall

(nicht abschliessend)

- Sofortmassnahmen
 - Trennen Internetverbindung / Netzwerk
 - Sichern Backups
 - Kontaktaufnahme mit Incident Responder
- Technische Massnahmen
 - **Beweismittel sichern**
 - **Identifikation der Ursache / Malware**
 - **Netzwerk** (Unterbindung Komm., DNS Resolver, Remote Zugänge schützen, IDS/Sensor etc.) **schützen/überwachen**
 - Logging aktivieren (insb. Sicherheits-Perimeter, log rotation deaktivieren)
 - User Accounts prüfen und bereinigen
- Recovery
 - Sicherheitslücken schliessen
 - Neuaufbau & Netzzonen einrichten
 - Übernahmen von Software Paketen und Daten prüfen
 - Neue Credentials setzen
- Organisatorische Massnahmen
 - Interne und externe Kommunikation
 - **Lösegeld / Verhandlung**
 - Meldung an Datenschutzbeauftragten bei Exfiltration



beraten / unterstützen

Rechtsmittel im globalen Kontext

- Hoheitliches Handeln der Strafverfolgungsbehörden ist **auf das eigene Territorium begrenzt**
 - Ausnahme Zugriffsprinzip
- **Rechtliche Instrumente** zur extra-territorialen Beweismittelerhebung
 - Rechtshilfe (unterschiedliche Erfolgsaussichten)
 - Cybercrime Convention (völkerrechtlicher Vertrag) zur Sicherung von Daten und freiwilliger Herausgabe von Daten
- Nicht alle Staaten haben bi- oder multilaterale [völkerrechtliche Verträge](#) mit CH oder sind CCC-Vertragsstaat



Warum immer Kontakt zur Polizei?

- Strafverfolgung & Repression
- Beratung
- Beitrag zu Lagebild
- Erkennen von Gefahren = Präventionsmassnahmen
- Möglichkeiten zur Anzeige
 - Persönlich am [Schalter](#)
 - [Onlineschalter](#) (Suisse ePolice)
 - Notrufe oder andere dringende Meldungen immer über die Notrufnummer 117





Wenn Sie betroffen sind

Die Kantonspolizei Graubünden empfiehlt Opfern von Cyberdelikten **schnellstmöglich** auf dem örtlichen Polizeiposten der Kantonspolizei Graubünden oder online **Strafanzeige zu erstatten**. Bitte bringen Sie folgende Dokumente mit:

Allgemein

- Transaktionsbestätigungen von Zahlungen (auch Kryptowährungen)
- Screenshots von täterischen Social Media Konten
- Originale E-Mails im digitalen Format
- Kopien sämtlicher Kommunikation
- Screenshots von betrügerischen Webseiten oder Inseraten

Bei zeitnaher Meldeerstattung steigen die Chancen Gelder zurückzuerlangen und Täter zu identifizieren. Zusammenarbeit mit Dritten.

Cyber Angriff (z.B. Ransomware)

- Zusätzlich Logfiles, Netzwerkprotokolle, Ransome Note, 4 Samples, Binaries/Executables, täterische URL/IP-Adressen



Ransomware Fall E-Mail Vorlage.msg

Herausforderungen für die Kapo

- Stetige Zunahme von Delikte
- Komplexität der Delikte
- Transnational operierende Täterschaft
- Professionelle Täterschaft und organisierte Kriminalität (finanzielle und personelle Ressourcen)
- Fachkräftemangel
- Fehlende Rechtsgrundlagen (z.B. Datenaustausch)
- Schneller technologischer Wandel





Prävention

5 Tipps Digitale Sicherheit

S wie «Sichern»

- Sichern Sie Ihre Daten regelmässig auf mindestens einem zweiten Medium.

U wie «Updaten»

- Updaten Sie Ihr System, Ihre Programme und Apps regelmässig mit der neusten Version.

P wie «Prüfen»

- Prüfen Sie bei Ihrem Gerät, ob ein Virenschutzprogramm installiert ist.

E wie «Einloggen»

- Verwenden Sie starke Passwörter
- Verwenden Sie wo möglich MFA

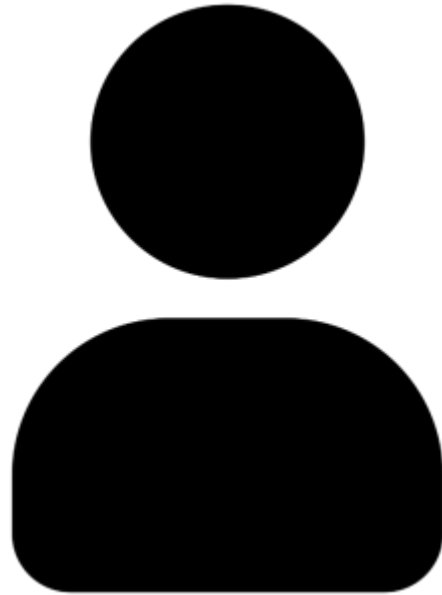
R wie «Reduzieren»

- Reduzieren Sie Betrugsrisiken im digitalen Raum mit einer gesunden Portion Misstrauen.





Privatpersonen



Cybercrime Dienst Kapo GR

- www.kapo.gr.ch/cybercrime

Schweizerische Kriminalprävention

- <https://www.skppsc.ch/de/>

Nationales Zentrum für Cybersicherheit NCSC

- <https://www.ncsc.admin.ch/>

EBAS (Hochschule Luzern)

- <https://www.ebas.ch/>

Cybercrimepolice.ch

- <https://www.cybercrimepolice.ch/>

iBarry

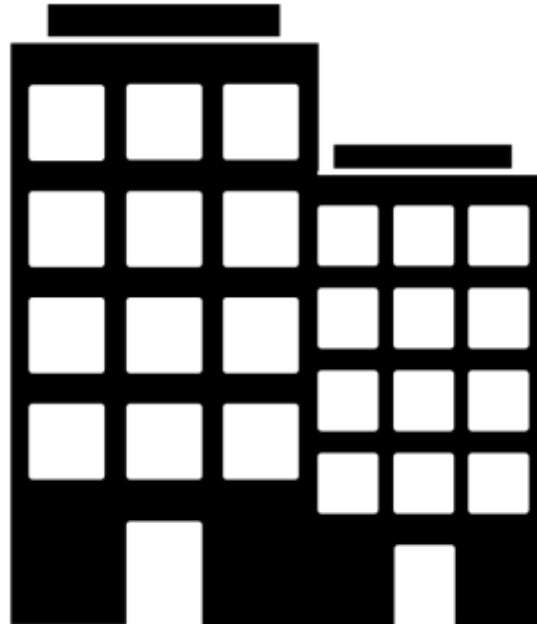
- <https://ibarry.ch/>

Nationale Sensibilisierungskampagne

- <https://www.s-u-p-e-r.ch/de/>



KMU



Cybercrime Dienst Kapo GR

- www.kapo.gr.ch/cybercrime

Nationales Zentrum für Cybersicherheit NCSC

- <https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html>

KMU Schnell-Check

- [KMU Schnell-Check | digitalswitzerland](#)

CyberSeal Gütesiegel

- [CyberSeal \(digitalsecurityswitzerland.ch\)](https://www.digitalsecurityswitzerland.ch)

iBarry Sicherheitschecks

- [Sicherheits Checks | iBarry](#)



Kontakt

Kantonspolizei Graubünden
Polizia chantunala dal Grischun
Polizia cantonale dei Grigioni

C Adj Christoph Scherer, MSc

C Cybercrime Dienst

Ringstrasse 2

7000 Chur

E-Mail: christoph.scherer@kapo.gr.ch

<http://www.kapo.gr.ch/cybercrime>

LinkedIn: www.linkedin.com/in/christoph-s-ba391722

Cyber Security | Davos



Fragen?



Schlussrunde



Apero – unser Dank gilt


Eine Veranstaltung der


Region **Prättigau/Davos**

Partner

 GEMEINDE
DAVOS

 **FH
GR** Fachhochschule Graubünden
University of Applied Sciences

 Kantonspolizei Graubünden
Polizia chantunala dal Grischun
Polizia cantonale dei Grigioni

 **Graubündner
Kantonalbank**

ETH zürich
KMU-Zentrum
Graubünden