



**Hochschule  
Albstadt-Sigmaringen**  
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

# Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen ECSM

Tobias Scheible, M.Eng.

# Tobias Scheible, M.Eng.

- 1999 GeoCities Website, 2000 eigene Domain, 2001 Kundenprojekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I: IT-Sicherheit von Netzwerken Hochschulzertifikatsprogramm
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
- Buch- & Zeitschriftenautor, Blogger, Referent, ...



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

.....  
13.10.2022 | ECSM

Tobias Scheible, M.Eng.

# Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 32 Bachelor- und Masterstudiengänge

Fakultät  
Engineering



Fakultät  
Business Science  
and Management



Fakultät Life  
Sciences



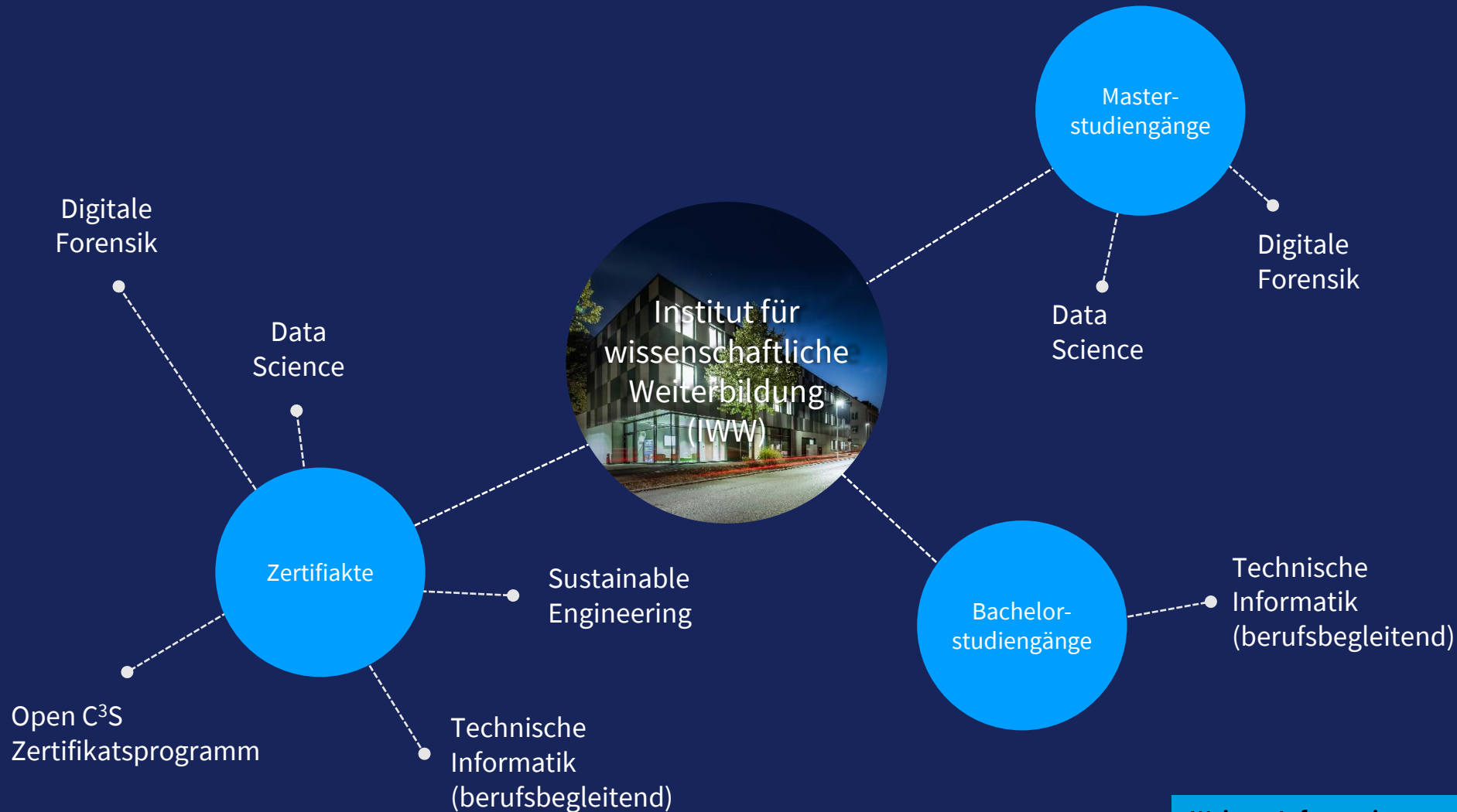
Fakultät  
Informatik



**Cybercrime as a Service (CaaS)  
& Ransomware-Bedrohungen**

# Institut für wissenschaftliche Weiterbildung

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen



**Weitere Informationen:**  
[www.hs-albsig.de/iww](http://www.hs-albsig.de/iww)

# Agenda

- **Schadsoftware**

- Nutzung von Standardfunktionen
- Ausnutzung von Schwachstellen
- Krimineller Hintergrund

- **Ransomware**

- Verschlüsselungstrojaner
- Angriffsszenario
- Social Engineering
- Fallbeispiel Locky

- **Cybercrime**

- Entwicklungsphasen
- Organisierte Kriminalität
- Cyber-Banden Interna

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Hinweis

Die komplette Präsentation wird im Anschluss unter [www.scheible.it](http://www.scheible.it) bereitgestellt.



# Schadsoftware



# Nutzung von Standardfunktionen

1949

John von Neumann, einer der Väter der Informatik, beschreibt die Theorie von sich selbst reproduzierenden Automaten.

1981

Der Begriff Computervirus wird zum ersten Mal von Prof. Leonard M. Adleman verwendet, dieser hat später das RSA-Kryptosystem mitentwickelt.

1983

Fred Cohen präsentiert das Konzept eines Virus und implementiert einen Prototyp, der innerhalb von wenigen Minuten auf allen Rechnern volle Zugriffsrechte hatte.

1985

Erste Viren, meist Scherzprogramme, sind außerhalb von Laborumgebungen anzutreffen und in Deutschland wird zum ersten Mal über Computerviren berichtet.

1988

Zum ersten Mal wird das Konzept „Würmer“ bekannt. Schadsoftware, die sich selbst weiter verbreiten kann.

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

Nutzung von Standardfunktionen  
Ausnutzung von Schwachstellen  
Krimineller Hintergrund

### Ransomware

### Cybercrime

# Schadsoftware - AIDS

- Erste Angriffe mit Ransomware bereits 1989
- Schadsoftware wurde per 5,25“ Diskette mit der Post verschickt
- Nach 90 Starts wurden die Dateinamen verschlüsselt
  - Eine italienische AIDS Organisation verlor Forschungsergebnisse aus 10 Jahren
  - Ersteller der Ransomware wurde 1990 verhaftet

```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
```

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

Nutzung von Standardfunktionen  
Ausnutzung von Schwachstellen  
Krimineller Hintergrund

### Ransomware

### Cybercrime



# Ausnutzung von Schwachstellen

1989

Erste polymorphe Viren erscheinen, die selbstständig ihre Code-Struktur verändern, um nicht von Antivirensoftware erkannt zu werden.

1990

Das *European Institute for Computer Antivirus Research* (EICAR) wurde gegründet und spielt heute noch eine wichtige Rolle bei der Erforschung von IT-Bedrohungen.

1995

Alternative Verbreitungswege über Makros werden aufgegriffen.

1997

Schadsoftware nutzt Schwachstellen in Anwendungen und Betriebssystemen aus.

1998

MacOS ist nun ebenfalls betroffen, erste Backdoors wurden gesichtet und Schadsoftware konnte einen kompletten Rechner unbrauchbar machen.

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

Nutzung von Standardfunktionen  
Ausnutzung von Schwachstellen  
Krimineller Hintergrund

### Ransomware

### Cybercrime

# Krimineller Hintergrund

„1990 in Bulgarien und 1998 in Russland entstanden infolge von Wirtschaftskrisen Hackerfabriken und später in Russland auch Hackerschulen. In ihnen wurde im gewerbsmäßigen Stil Hacking-Angriffe und Malware-Programmierung als Auftragsarbeiten gegen Geld ausgeführt.“ S. 15, *Eine kurze Geschichte der Cybercrime*; Dieter Kochheim

1991

Erste Plattform für den illegalen Handel von gestohlenen Bankdaten.

2000

Der „I-love-you“ Virus überschrieb Daten und griff Informationen ab und infizierte ca. 10 % aller vernetzten Computer – ein Schaden von über 10 Milliarden Dollar entstand.

2004

Schadsoftware wird von nun an vermehrt von organisierten Kriminellen eingesetzt, die sich zu Banden zusammenschließen, um gezielt illegales Geld zu verdienen.

2005

Andere Systeme wie Symbian (Smartphone OS) oder Windows CE werden jetzt auch angegriffen. Ebenfalls gibt es Schwachstellen bei der Bluetooth Schnittstelle.

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

Nutzung von Standardfunktionen  
Ausnutzung von Schwachstellen  
Krimineller Hintergrund

### Ransomware

### Cybercrime



Ransomware

# Verschlüsselungstrojaner

Bei Ransomware (auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner genannt) handelt es sich um Computer-Schadsoftware, das sich heimlich auf dem Computer eines Opfers installiert. Die Schadsoftware führt einen Kryptoangriff durch (verschlüsselt alle oder wichtige Dateien) und fordert dann eine Art Lösegeld, um den Computer zu entsperren oder die Daten zu entschlüsseln.



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

#### Ransomware

- [Verschlüsselungstrojaner](#)
- [Angriffsszenario](#)
- [Verschlüsselungstrojaner](#)
- [Social Engineering](#)
- [Verschlüsselungstrojaner](#)
- [Fallbeispiel Locky](#)

### Cybercrime

# Angriffsszenario



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime



# Verschlüsselungstrojaner

## Was bewirkt Ransomware?

- Sie verschlüsselt Dateien, sodass sie nicht mehr verwendet werden können.
  - Dabei werden Dateien verschlüsselt, auf die der Benutzer ganz normal Zugriff hat. Dadurch müssen keine Sicherheitslücken ausgenutzt bzw. Rechteausweitungen durchgeführt werden.
  - Partielle Verschlüsselung von Daten für mehr Geschwindigkeit (August 2022).
- Zusätzlich wird gedroht, Daten zu veröffentlichen, wenn keine Zahlung erfolgt.
  - Teils mit Drohung an Personen, dass ihre Daten veröffentlicht werden, wenn das Opfer bzw. die Quelle nicht zahlt.
- Deaktiviert bestimmte Anwendungen (z. B. Taskmanager, Webbrowser, ...).
- Sie hindert eventuell, dass auf die Computer zugegriffen werden kann.

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime



# Verschlüsselungstrojaner

## Wie gelangt Ransomware auf einen Computer?

- In den meisten Fällen erfolgt eine Ransomware-Infektion per Phishing-Mail. Hierbei kommen Social Engineering Methoden zum Einsatz.
- Ebenfalls spielen Drive-By Infektionen mittels Exploit-Kits eine Rolle, zumeist bei Systemen ohne aktuelle Sicherheitsupdates.
- Schwachstellen in Servern werden ausgenutzt, um eine Ransomware in ein zentrales System einzuschleusen.
- Ebenso werden ungeschützte oder schwach gesicherte Fernzugänge ausgenutzt, um auf dem damit erreichbaren System eine Ransomware Infektion auszuführen.
- In einigen Fällen gab es spezialisierte Angriffe mit USB-Sticks, die per Paketdienst als gefälschte Bestellung versendet wurden.

### Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

#### Schadsoftware

##### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

#### Cybercrime

# Social Engineering

- Neuer Phishing Ansatz – Angreifer stellen eine Konversation her



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

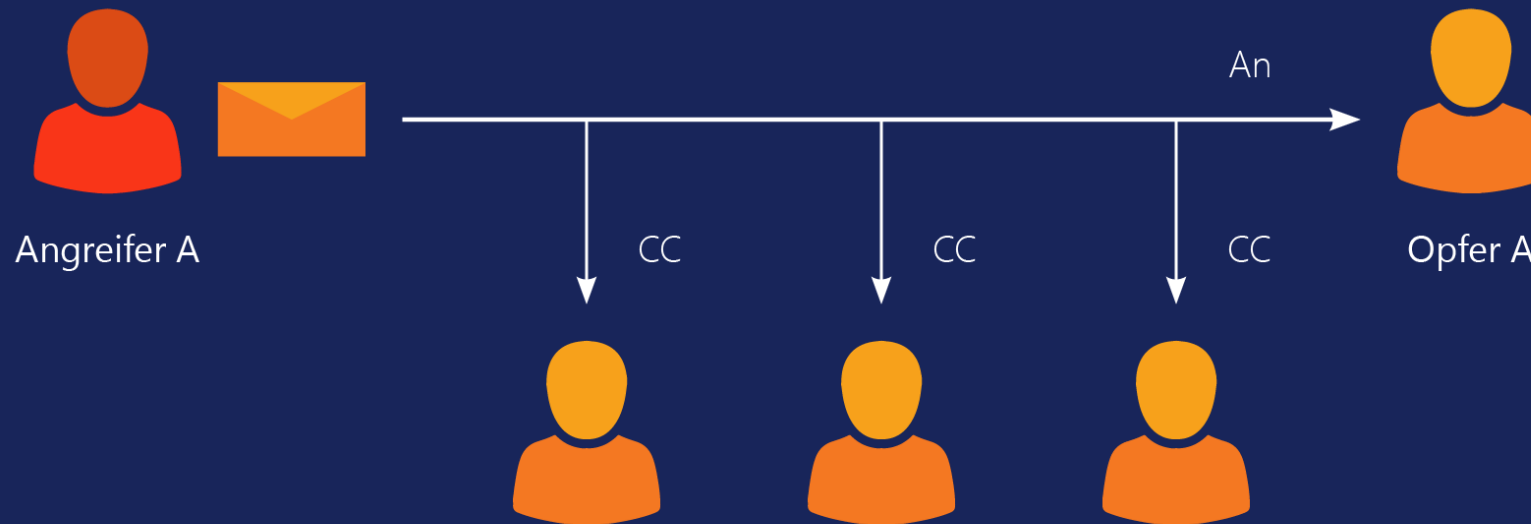
#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime

# Social Engineering

- Neuer Phishing Ansatz – Angreifer stellen eine Konversation her



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

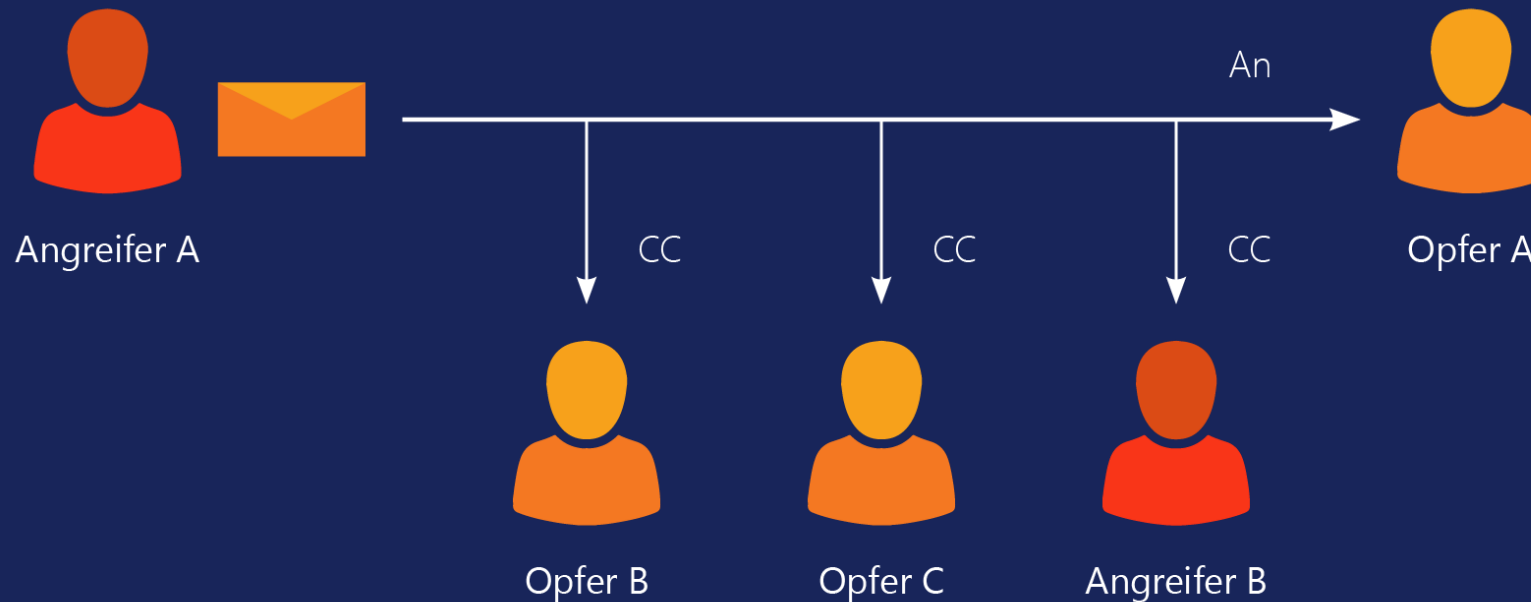
#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime

# Social Engineering

- Neuer Phishing Ansatz – Angreifer stellen eine Konversation her



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

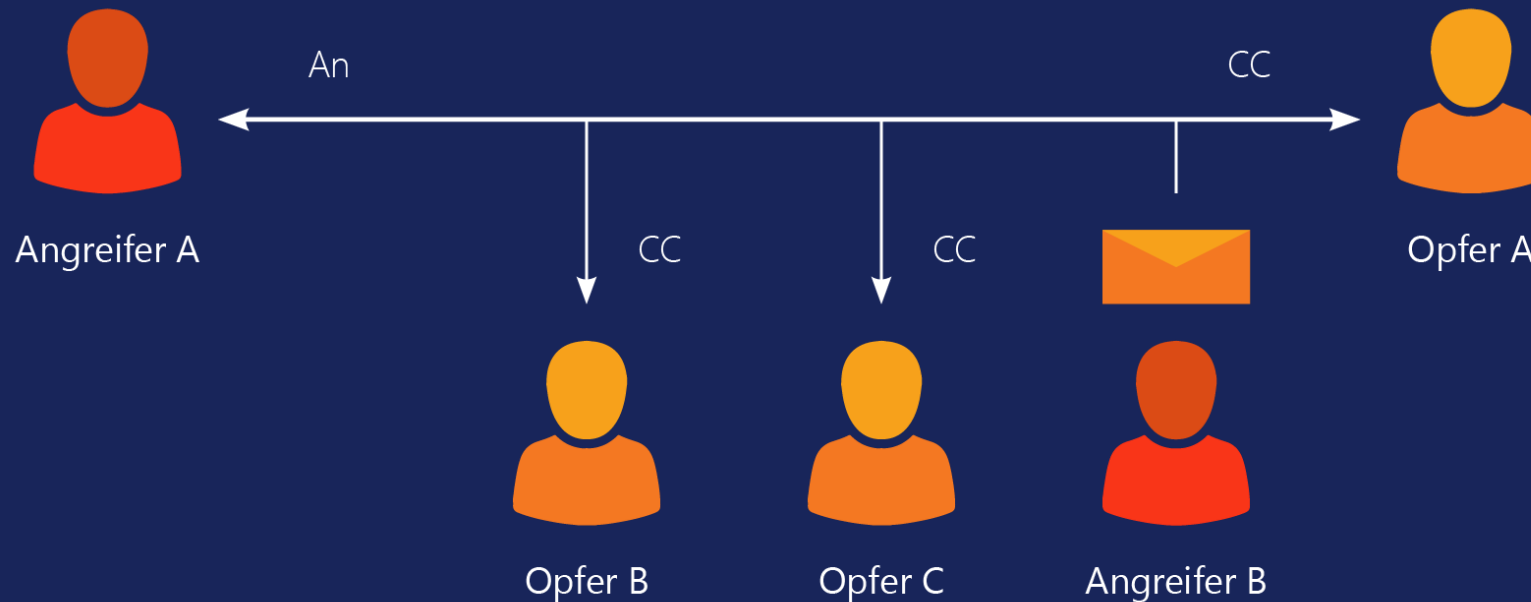
#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime

# Social Engineering

- Neuer Phishing Ansatz – Angreifer stellen eine Konversation her



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

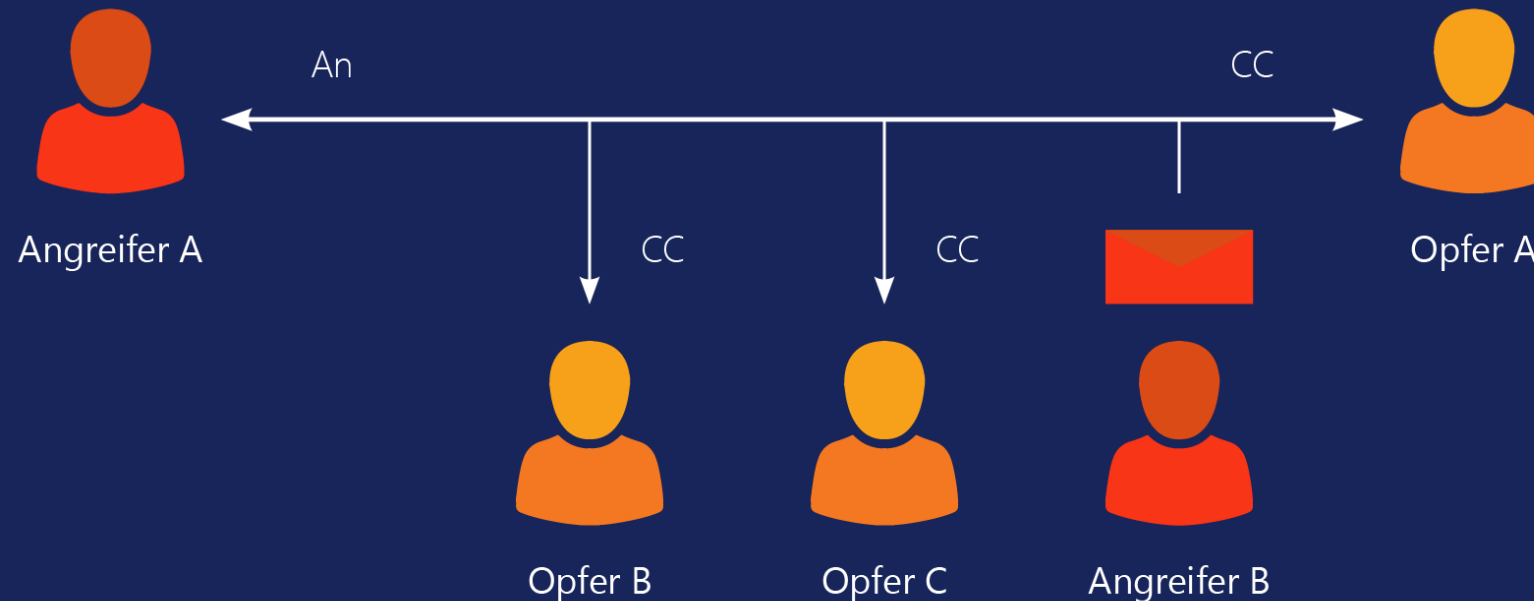
#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime

# Social Engineering

- Neuer Phishing Ansatz – Angreifer stellen eine Konversation her



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime



# Verschlüsselungstrojaner

## Sollte das Lösegeld gezahlt werden?

- Nein, denn damit werden die Banden der Cyber-Kriminellen finanziert und es werden noch mehr Angriffe auf andere Unternehmen durchgeführt.

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime

# Kryptotrojaner / Ransomware

**PCGames**  
VIDEOGAMES · TECHNIK · FILME · SERIEN

Suche

PCG  PUR

Login

Registrieren

155 User online

NEWS TESTS TIPPS VIDEOS SPIELE FORUM HARDWARE FILME QUIZ HEFT & ABO

Neuer Newsletter Elden Ring Elden Ring Tipps PC-Spiele 2022 PS5 & PS4-Spiele 2022 Jobs für Gamer Mehr

gamesworld

STARTSEITE / SPIELEMARKT

**MediaMarkt**

2

## Ransomware-Angriff auf MediaMarkt: Erpresser verlangen 240 Millionen Dollar Lösegeld

Onlinekriminalität ist schon lange kein Kavaliersdelikt mehr und die Folgen eines Cyberangriffs hat gerade erst MediaMarkt, die gigantische Handelskette für Elektronikgeräte in jeder Form und Farbe, zu spüren bekommen. Mit einem Ransomware-Angriff wurden 3100 Server des Unternehmens verschlüsselt, die Erpresser verlangten 240 Millionen Dollar Lösegeld.

QUELLE: MEDIA MARKT

Quelle: [pcgames.de](https://www.pcgames.de) (7)

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

### Ransomware

- Verschlüsselungstrojaner
- Angriffsszenario
- Verschlüsselungstrojaner
- Social Engineering
- Verschlüsselungstrojaner
- Fallbeispiel Locky

### Cybercrime

.....  
13.10.2022 | ECSM

Tobias Scheible, M.Eng.

# Verschlüsselungstrojaner

## Wie können die Dateien wiederhergestellt werden?

- Grundsätzlich sollten die IT-Systeme so konzeptioniert sein, dass nach einem Angriff in möglichst kurzer Zeit der Produktivzustand wiederhergestellt werden kann.
- Eine gute Backupstrategie ist das wichtigste Element gegen Ransomware.
- Zum Teil wird die Schadsoftware geknackt und es ist eine Entschlüsselung mit spezieller Software wieder möglich.
  - Allerdings kann der Zeitraum sehr lange sein oder zum Teil ist es niemals möglich.

### Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

#### Schadsoftware

#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

#### Cybercrime

# EXKURS Entschlüsselung

 ID Ransomware  Identifizieren  FAQ  Notify Me  Donate

 Deutsch



## ID Ransomware

Lade eine Lösegeldforderung und/oder eine verschlüsselte Beispieldatei hoch, um die Ransomware zu identifizieren, die deine Daten verschlüsselt hat.

*Wissen ist halb gewonnen!*  
GI Joe —

### Dateien hochladen

#### Lösegeldforderung ?

Die Datei, welche die Lösegeld- und Zahlungsinformationen anzeigt.

Keine Datei ausgewählt.

#### verschlüsselte Datei ?

Eine Datei, die verschlüsselt wurde und nicht geöffnet werden kann.

Keine Datei ausgewählt.

#### Addresses

Optionally, you may enter any email addresses or hyperlinks the ransomware gives you for contact (if there is no ransom note).

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

### Cybercrime

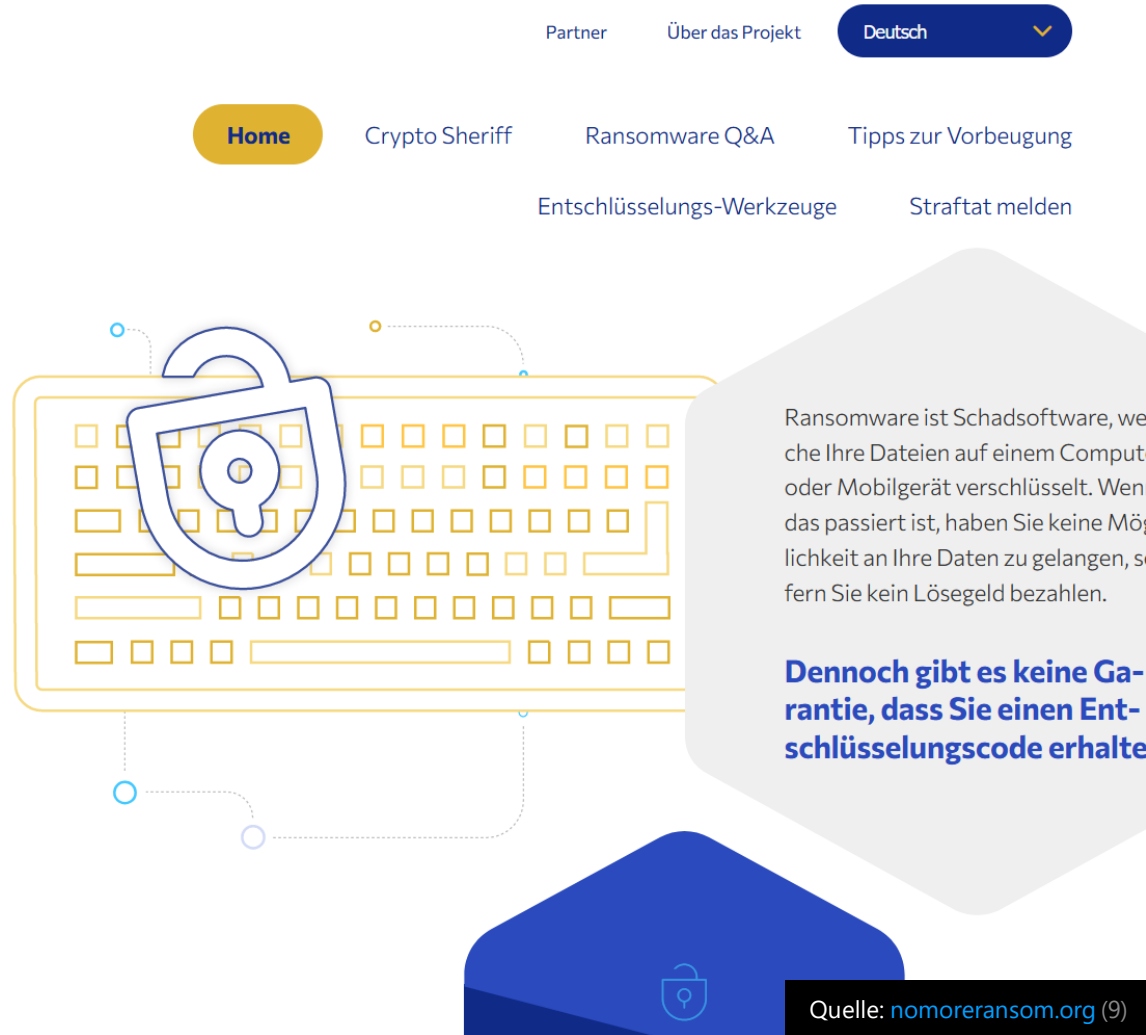
# EXKURS Entschlüsselung

<🔒/>  
**NO MORE  
RANSOM**

**Brauchen Sie  
Hilfe  
zum Entriegeln  
Ihres digitalen  
Lebens, ohne da-  
bei Lösegeld zu  
zahlen\*?**

JA

NEIN



Partner Über das Projekt Deutsch

Home Crypto Sheriff Ransomware Q&A Tipps zur Vorbeugung

Entschlüsselungs-Werkzeuge Straftat melden

Ransomware ist Schadsoftware, welche Ihre Dateien auf einem Computer oder Mobilgerät verschlüsselt. Wenn das passiert ist, haben Sie keine Möglichkeit an Ihre Daten zu gelangen, sofern Sie kein Lösegeld bezahlen.

**Dennoch gibt es keine Garantie, dass Sie einen Entschlüsselungscode erhalten.**

Quelle: nomoreransom.org (9)

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

#### Ransomware

- Verschlüsselungstrojaner
- Angriffsszenario
- Verschlüsselungstrojaner
- Social Engineering
- Verschlüsselungstrojaner
- Fallbeispiel Locky

#### Cybercrime

13.10.2022 | ECSM

Tobias Scheible, M.Eng.

# Fallbeispiel Locky

- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien, auch auf Netzwerklaufwerken
- Zeitlicher Ablauf:
  - 15.02.2016 Locky wird als Schläfer aktiviert (Makros)
  - 22.02.2016 Gefälschte Unternehmensrechnung (JScript)
  - 24.02.2016 Gefälschtes Sipgate Fax (JScript)
  - 26.02.2016 Neue Infektionstechnik mit Batch-Dateien
  - 02.03.2016 Gefälschte BKA E-Mail (EXE-Datei)

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

### Schadsoftware

#### Ransomware

Verschlüsselungstrojaner  
Angriffsszenario  
Verschlüsselungstrojaner  
Social Engineering  
Verschlüsselungstrojaner  
Fallbeispiel Locky

#### Cybercrime



The background is a dark, textured surface with a grid of small, glowing blue squares. These squares are arranged in a pattern that resembles a digital or data landscape, with some squares appearing brighter than others. The overall effect is a sense of depth and digital connectivity.

Cybercrime

# Entwicklungsphasen

Phase I  
Die Anfänge

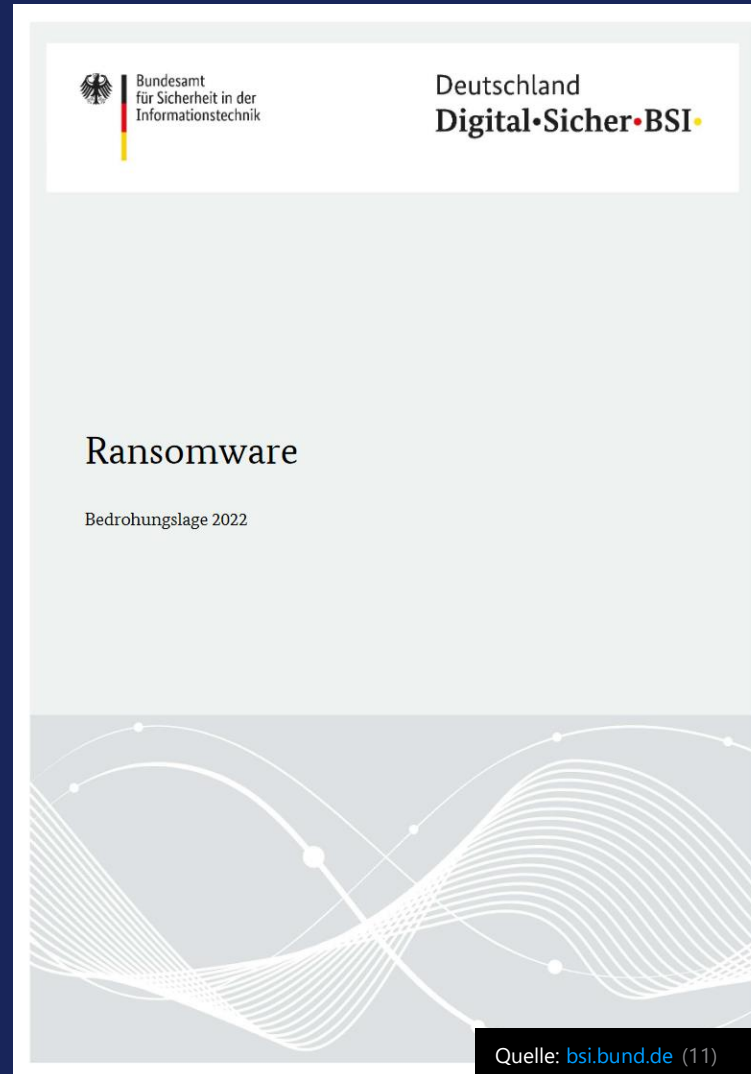
Phase IIa  
Effiziente Verbreitung und Zerstörung

Phase IIb  
Professionalisierung

Phase III  
Modularisierung

Phase IV  
Proliferation von Schadsoftware und Methoden

Phase V  
Criminal Service für alles



## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

Schadsoftware

Ransomware

Cybercrime  
Entwicklungsphasen  
Organisierte Kriminalität  
Cyber-Banden Interna

# Organisierte Kriminalität



Koordinator

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

Schadsoftware

Ransomware

Cybercrime

Entwicklungsphasen

Organisierte Kriminalität

Cyber-Banden Interna



# Cyber-Banden Interna

 heise online

heise +

Anmelden

Suchen



Menü

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: ENERGIE  UKRAINE  ELEKTROMOBILITÄT  KRYPTOGELD  PODCASTS 

heise online > Cybercrime > "Command&Control as a Service" – Cybercrime auf dem Weg in die Cloud

## "Command&Control as a Service" – Cybercrime auf dem Weg in die Cloud

Ein neues As-a-Service-Angebot hat im Cybercrime-Untergrund innerhalb weniger Monate bereits tausende Kunden gewonnen.

Lesezeit: 3 Min.

   20



(Bild: Blue Planet Studio/Shutterstock.com)

07.08.2022 09:30 Uhr | Security

Von Jürgen Schmidt

Quelle: [heise.de](https://heise.de) (12)

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

Schadsoftware

Ransomware

Cybercrime

Entwicklungsphasen

Organisierte Kriminalität

[Cyber-Banden Interna](#)

13.10.2022 | ECSM

Tobias Scheible, M.Eng.

# Cyber-Banden Interna

## Lockbit-Ransomware-Gruppe stellt sich professioneller auf

Die Erpresserbande hinter der Ransomware Lockbit hebt den Professionalisierungsgrad auf eine neue Stufe. Sogar ein Bug-Bounty-Programm hat sie aufgelegt.

Lesezeit: 3 Min.

   4



(Bild: Pixels Hunter/Shutterstock.com)

28.06.2022 13:37 Uhr | Security

Von Dirk Knop

Die Professionalisierung der Erpresserbande hinter der Lockbit-Ransomware hat eine neue Stufe erklommen. Dazu gehört markiges Marketing für eine

UNSERE EMPFEHLUNG

Quelle: [heise.de](https://heise.de) (13)

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

Schadsoftware

Ransomware

Cybercrime

Entwicklungsphasen

Organisierte Kriminalität

Cyber-Banden Interna

.....  
13.10.2022 | ECSM

Tobias Scheible, M.Eng.

# Cyber-Banden Interna

## Cybercrime und Trickbot-Leaks: "Wir zahlen Krankengeld und 13. Monatsgehalt"

Cybercrime goes Business: Ein Bewerbungsgespräch im Cybercrime-Untergrund zeigt eindrucksvoll, wie sehr sich organisiertes Verbrechen schon "normalisiert" hat.

Lesezeit: 4 Min.

   22



(Bild: Skorzewiak/Shutterstock.com)

18.07.2022 17:10 Uhr | Security

Von Jürgen Schmidt

Anfang des Jahres veröffentlichten Unbekannte interne Informationen der Trickbot-Bande, die bisher recht wenig Aufmerksamkeit erhielten. Dabei geben insbesondere die Chat-Protokolle einen unvergleichlichen Einblick in die Welt der

INHALTSVERZEICHNIS

1. Cybercrime und Trickbot-Leaks: "Wir zahlen

Quelle: [heise.de](https://heise.de) (14)

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

Schadsoftware

Ransomware

Cybercrime

Entwicklungsphasen

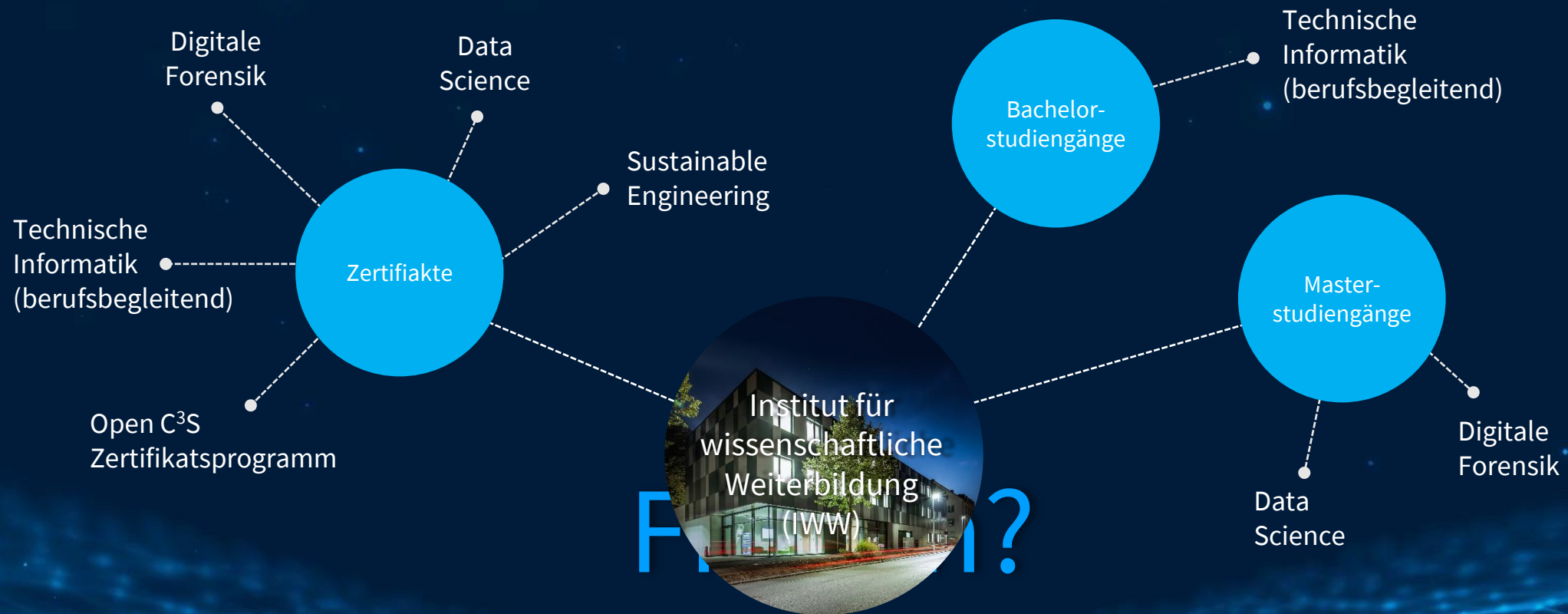
Organisierte Kriminalität

Cyber-Banden Interna

13.10.2022 | ECSM

Tobias Scheible, M.Eng.





# Vielen Dank für Ihre Aufmerksamkeit

Weitere Vorträge: [weiter-bildung.info](http://weiter-bildung.info) | Präsentation online unter: [scheible.it](http://scheible.it)

# Quellen

- 1) <https://www.cyberfahnder.de/doc/kurze-Geschichte-Cybercrime.pdf>, abgerufen am 12.10.2022
- 2) <https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>, abgerufen am 12.10.2022
- 3) [https://de.wikipedia.org/wiki/AIDS\\_\(Schadprogramm\)](https://de.wikipedia.org/wiki/AIDS_(Schadprogramm)), abgerufen am 12.10.2022
- 4) <https://www.avg.com/de/signal/history-of-viruses>, abgerufen am 12.10.2022
- 5) <https://de.wikipedia.org/wiki/Loveletter>, abgerufen am 12.10.2022
- 6) <https://de.wikipedia.org/wiki/Ransomware>, abgerufen am 12.10.2022
- 7) <https://www.pcgames.de/Spielemarkt-Thema-117280/News/Ransomware-Angriff-auf-MediaMarkt-Erpresser-verlangen-240-Millionen-Dollar-Loesegeld-1383228/>, abgerufen am 12.10.2022
- 8) [https://id-ransomware.malwarehunterteam.com/index.php?lang=de\\_DE](https://id-ransomware.malwarehunterteam.com/index.php?lang=de_DE), abgerufen am 12.10.2022
- 9) <https://www.nomoreransom.org/de/index.html>, abgerufen am 12.10.2022
- 10) <https://de.wikipedia.org/wiki/Locky>, abgerufen am 12.10.2022
- 11) [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2), abgerufen am 12.10.2022
- 12) <https://www.heise.de/news/Command-Control-as-a-Service-Cybercrime-auf-dem-Weg-in-die-Cloud-7204112.html>, abgerufen am 12.10.2022
- 13) <https://www.heise.de/news/Lockbit-3-0-Professionalisierung-der-Ransomware-Szene-7155742.html>, abgerufen am 12.10.2022
- 14) <https://www.heise.de/news/Cybercrime-und-Trickbot-Leaks-Wir-zahlen-Krankengeld-und-13-Monatsgehalt-7182800.html>, abgerufen am 12.10.2022

## Cybercrime as a Service (CaaS) & Ransomware-Bedrohungen

.....

13.10.2022 | ECSM

Tobias Scheible, M.Eng.