POLIZEI

BADEN-WÜRTTEMBERG

POLIZEIPRÄSIDIUM MANNHEIM

Polizeipräsidium Mannheim | L 6, 1 | 68161 Mannheim

Cybercrime-Ermittlungen

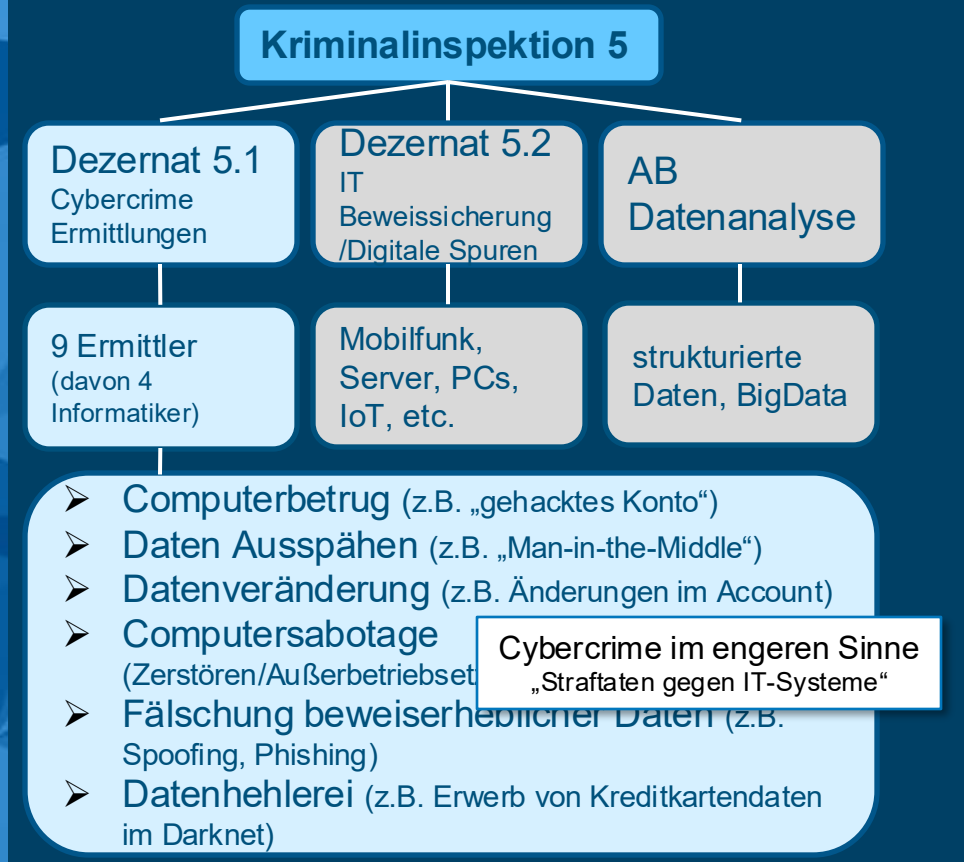
- Ransomware, DDoS und Co. -

Polizeipräsidium Mannheim
Kriminalpolizeidirektion Heidelberg
Kriminalinspektion 5
Dezernat 5.1 – Cybercrime-Ermittlungen

KOK Böder, MSc.
KOK Herbert, MSc.

Wer wir sind

Dezernat 5.1 beim
Polizeipräsidium Mannheim



Besonderheiten von CyberCrime

im Vergleich zu anderen Straftaten

Technisch anspruchsvolles Deliktsfeld

Stetige Zunahme von CC Delikten

- Häufig Banden, die sich firmenartig strukturiert haben (OK)
- Cybercrime-as-a-Service
- Auch minderjährige Täter („Skript-Kiddies“)
- Vermehrt staatliche Akteure (z.B. RU, CN)

i.d.R. lange Verfahrensdauer (> 1 Jahr)

99% der Angriffe anonymisiert

täglich neue Angriffsvektoren und Techniken

durch das Internet so gut wie immer Auslandsbezug

IT-Sicherheitsfirmen oft in Konkurrenz zur Polizei

Spezielle Einrichtungen

Polizei / Justiz / Land / Bund

- **Schwerpunktstaatsanwaltschaft** CC in Mannheim
- Generalstaatsanwaltschaft mit **Cybercrime-Zentrum** in Karlsruhe

StA

- **ZAC** (Zentrale Ansprechstelle Cybercrime @LKA BW)
- **Sonderlaufbahn** „Cyberkriminalist“ (Quereinstieg als Informatiker u.ä.)

Polizei

- Cyber-Sicherheitsagentur BW (**CSBW**) + **CyberWehr BW**

Land

- **ZITiS** (Zentrale Stelle f. Informationstechnik im Sicherheitsbereich)
- Teilnahme „Convention on CyberCrime (**CCC**)“ („Budapest Convention“)
- Teilnahme an **Europol** & **Eurojust**

Bund

Polizei bei Cyber-Vorfällen

Häufige Vorurteile

„Die Polizei kennt sich im IT-Bereich sowieso nicht aus“

„Die Polizei beschlagnahmt all unsere Server als Beweismittel“

„Die Polizei behindert nur unsere IT“

„Wer weiß, was die Polizei in unseren Daten alles findet, was sie gegen uns verwenden kann“

„Der Täter wird sowieso nie gefunden“

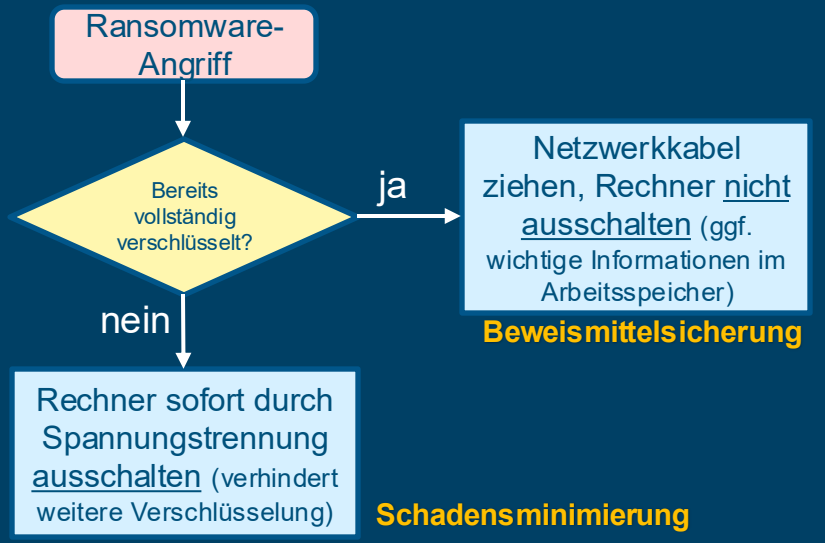
Polizei vs. Incident Responder

Warum sie uns auf jeden Fall auch hinzuziehen sollten

- Sie und Ihre Firma stehen für uns an 1. Stelle
- Polizei hat kein wirtschaftliches Interesse sie zu unterstützen
- Die Wiederherstellung ihres Betriebs hat oberste Priorität
- Auch die Polizei hat IT-Experten
- Expertise durch zahlreiche ähnlich gelagerte Fälle
- Internationale Ermittler-Teams
- Andere rechtliche / technische Möglichkeiten
- Jeder Fall ist ein Mosaik-Steinchen im großen Cybercrime Puzzle und unterstützt die Ermittlungen (weltweit)
- Gewonnene Informationen können helfen, andere Unternehmen zu warnen / vor Schaden zu bewahren
- Strafverfolgung (Cybercrime) zunehmend erfolgeich

Sofort-Maßnahmen im Schadensfall

Ransomware



Setzen Sie die Polizei so früh wie möglich in Kenntnis
(ZAC BW od. beliebige Dienststelle)

Falls möglich, Systeme nicht löschen — Beweismittel-sicherung

Folgen sie ihrem Notfall-Plan

Ziehen Sie (BSI-zertifizierte) IT-Dienstleister (IR) hinzu

Informieren Sie Mitarbeiter und Kunden/Partner (frühzeitig)

Ransomware-Vorfall

weitere Empfehlungen und Hinweise

Solange der Umfang des Angriffs nicht zu 100% aufgeklärt ist, gehen sie davon aus, dass alles was sie am laufenden System (Server, Client, Telefon, Fax, Smartphone, Drucker, etc.) machen, vom Täter beobachtet werden kann!
=> nutzen sie möglichst keine Unternehmens-E-Mail-Adressen und Telefone zur Kommunikation

Von Lösegeldzahlungen wird grundätzlich abgeraten

- trotz Zahlung keine Garantie, dass alle Daten wiederhergestellt werden
- Täter werden animiert weitere Firmen anzugreifen
- Täter informieren andere Gruppierungen, dass gezahlt wurde
- Sanktionen in manchen Ländern möglich **(Stichwort: Terrorfinanzierung)**

Ransomware-Vorfall

weitere Empfehlungen und Hinweise

Sollte eine Zahlung in Betracht gezogen werden:

- Lösegeld kann in den meisten Fällen verhandelt werden
- Klären sie (intern) frühzeitig, wie gezahlt werden soll (Stichwort: Kryptokonto)

Prüfen Sie ihre Versicherungen bzgl. Einschluss Cybervorfälle

Kontakt zu Tätern nur über gesicherte Kanäle (VPN, neutrale E-Mail-Adresse)

Möglichst keine E-Mail aus dem (infiltrierten) Unternehmensnetz an die Polizei (Täter liest mit)

Ransomware-Angriff

Vorgehensweise der Täter

Die häufigsten Angriffsvektoren

- Phishing
- Sicherheitslücken
- (RDP-)Brute-Force

Täter lassen sich häufig Zeit, das System zu erkunden.
Verschlüsselung ggf. erst nach Monaten im System

Varianten

Single Extortion
(Verschlüsselung der Daten)

Double Extortion
(Verschlüsselung + Datenexfiltration)

Triple Extortion
(Verschlüsselung + Datenexfiltration + DDoS-Angrif)

Multi-Extortion
(zusätzlich Angriff von Partnern/Kunden, Drohung mit Meldung des Vorfalls an Behörden (falls meldepflichtig), Daten werden Konkurrenz gezielt angeboten, etc.)

Vermeidung von Cybervorfällen

Empfehlungen und Hinweise

Legen sie (regelmäßig) Backups an!

3-2-1 Regel

3: Erstellen Sie drei separate Kopien Ihrer Daten

2: Speichern Sie diese Kopien auf zwei verschiedenen Medien (z.B. HDD, USB-Laufwerk, Cloud-Speicher, Bänder)

1: Lagern Sie mindestens eine dieser Kopien an einem externen Standort (z.B. eine andere Stadt, ein Rechenzentrum, eine Cloud)

Regelmäßig Sicherheitspatches installieren

Remotezugänge absichern (VPN + MFA)

Schulung und Assessment der Mitarbeiter

... weitere (siehe Empfehlungen BSI[1])

1) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/Top-10-Ransomware-Massnahmen/top-10-ransomware-massnahmen.html

Weitere Unterstützung, Links, etc.

Empfehlungen und Hinweise

ZAC BW[1]
(**Z**entrale **A**nsprechstelle **C**ybercrime beim LKA BW)

CSBW[2]
(Cyber Sicherheitsagentur BW)

BSI[3]
(Bundesamt für Sicherheit in der Informationstechnik)

CyberWehr[4]
(Unterstützung für KMU)

CyberSicherheitsForum BW[5]

IHK[6]
(z.B. Cybersicherheitscheck)

Cybersecurity Community[7]
(Arbeitsgruppe für RN-Region)

1) https://lka.polizei-bw.de/zentrale-ansprechstelle-cybercrime/
2) https://www.cybersicherheit-bw.de/sicherheitsvorfall
3) https://www.bsi.bund.de/
4) https://cyberwehr-bw.de/
5) https://cybersicherheitsforum-bw.de/
6) https://www.ihk.de/stuttgart/fuer-unternehmen/innovation/digitale-wirtschaft/internet-recht/it-sicherheit-basisberatung-6078176
7) https://www.smart.industries/news/cybersecurity-community/

Vielen Dank für Ihre Aufmerksamkeit!

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM MANNHEIM