Herausforderung IT-Sicherheit

IT-Infotage Pegnitz

Lukas Knorr
Zentralstelle Cybercrime Bayern

Strafverfolgung in Bayern

Seit 01.01.2015

Zentralstelle Cybercrime Bayern

(errichtet bei der Generalstaatsanwaltschaft Bamberg)

- **Aufgaben:**
  - **Bearbeitung herausgehobener Verfahren der Computerkriminalität**
  - Aus- und Fortbildung der bayerischen Justiz
  - Zentrale Ansprechstelle für Cyberkriminalität

Eigene Ermittlungstätigkeit

Die ZCB ist originär für folgende Ermittlungsverfahren zuständig:

- **Tatbegehung aus dem Bereich der organisierten Cyberkriminalität**
- **Auswirkungen auf bedeutende Wirtschaftszweige und kritische Infrastrukturen**
- **Angriffe auf Computer- und Informationstechnik durch neue oder mit hohem Gefährdungspotential verbundene Begehungsweisen**
- **hoher Ermittlungsaufwand im Bereich der Computer- und Informationstechnik**
- **Angriffe auf die IT-Struktur von Behörden oder anderen öffentlichen Einrichtungen**

Cybercrime als allgegenwärtige Bedrohung

Einige Schlagzeilen …

Mehr Kosten durch Cybercrime als durch Drogenhandel

Studie sieht Cybercrime weiter auf dem Vormarsch

Unterschätzte Gefahr: „Cybercrime wird jeden treffen“

EUROPOL | 30.09.2015

Cybercrime wachsende Bedrohung für Europa

Angriffe auf Brandenburg

Cybercrime verursacht Millionenschaden

CYBERCRIME BOOMT UND SCHADET KMU

Ansteigende Fälle beim Phishing? Cybercrime nimmt laut BKA deutlich zu

Cybercrime-Versicherungen erwarten Boom in Europa

Interpol beziffert Schaden durch Cybercrime in Europa auf 750 Milliarden Euro

Im Visier der Hacker

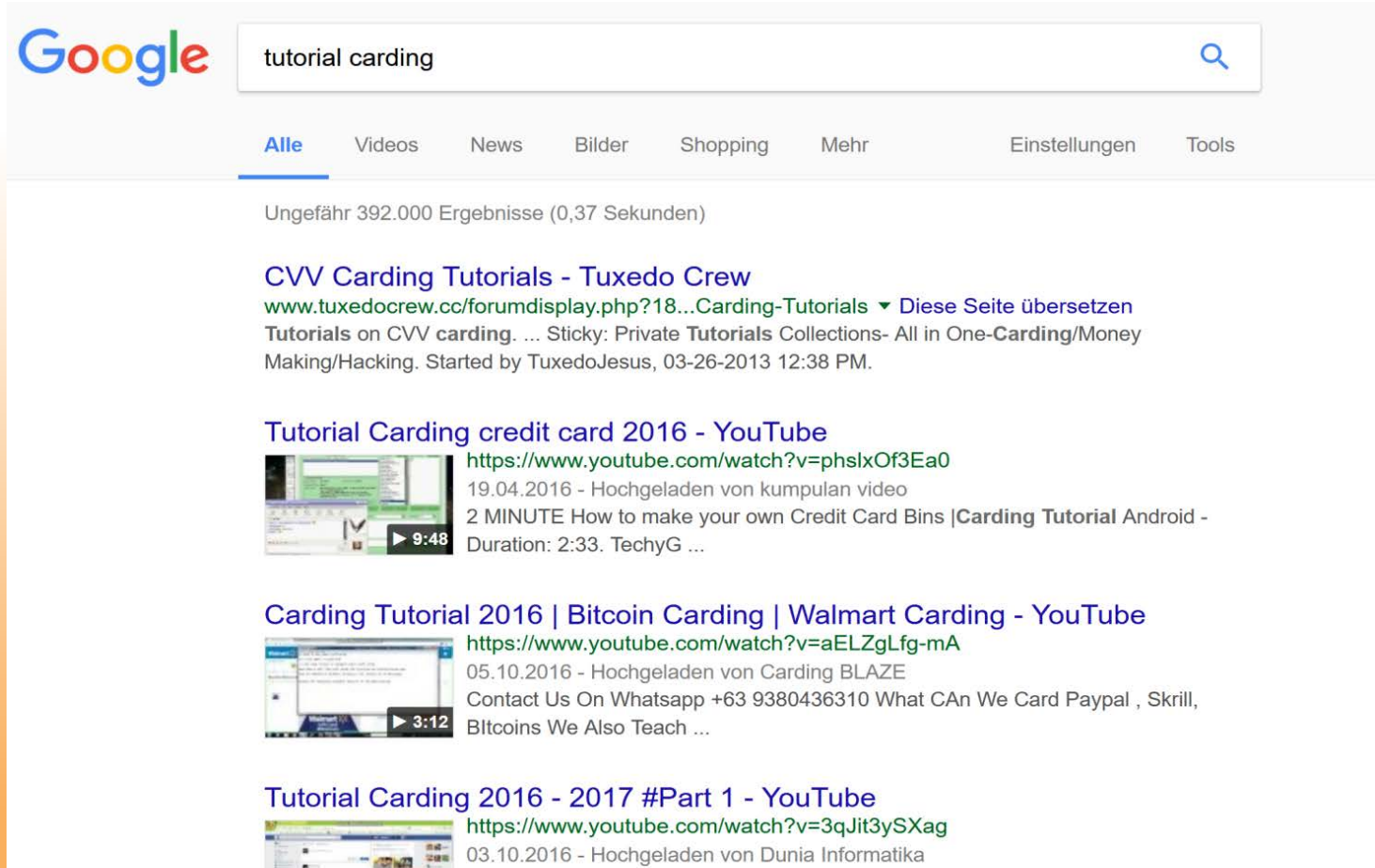
Cyber-Angriffe machen Staat und Wirtschaft ratlos

Cyber-Attacken kosten uns 43 Milliarden Euro im Jahr

US-Studie: Deutschland besonders betroffen, 15 bis 20 Prozent der Wertschöpfung im Netz vernichtet

Justiz digital

Cybercrime leicht gemacht



Phänomen *„crime as a service“*

- Infrastructure-as-a-Service
  - z. B. Miete von Botnetzen
- Data-as-a-Service
  - z. B. Kreditkartendaten
- Pay-per-Install-Services
  - z. B. Verbreitung von Schadsoftware mit Bezahlung nur bei Erfolg
- Hacking-Services
  - z. B. Infiltration bestimmter Systeme “auf Bestellung”
- Translation-Services
  - z. B. Übersetzung von Phishing-Mails
- Moneylaundering-Services
  - z. B. Vermittlung von Finanzagenten

Justiz digital

Herausforderungen für die Strafverfolgung

Ermittlungs- und Strafverfahren in diesem Bereich sind mit <u>besonderen Problemlagen</u> konfrontiert:

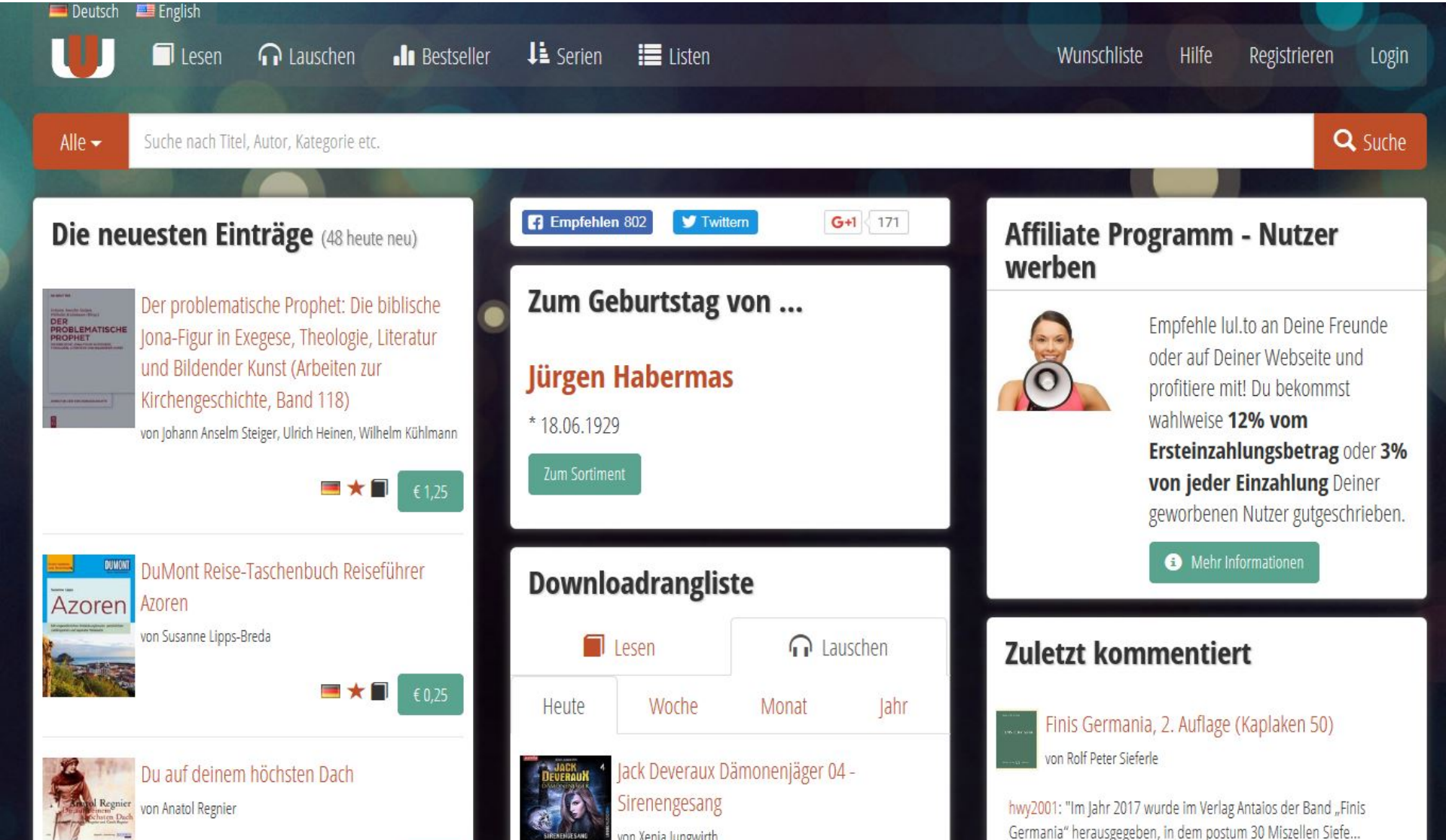
- **geringe Anzeigebereitschaft bei den Geschädigten**
- **Flüchtigkeit digitaler Spuren ⇔ viel zu späte Anzeigeerstattung**
- **regelmäßig Auslandsbezug**
- **Notwendigkeit der Auswertung großer Datenmengen**
- **Verschlüsselung**
- **besondere Probleme im Darknet**

Aktuelle Verfahren (Beispiele)

- **Vorkasse-Betrug** (Fake-Shops, Online-Notare)
- **Schadsoftware** (insb. Ransomware)
- **Spearphishing**-Attacken auf Unternehmen (CEO-Fraud)
- **Underground Economy** (Carding, Trojaner, Bot-Netze, Hacking)
- **DDoS**-Angriffe
- **UrhG** (Pay-TV-Streaming)
- **Zahlungswirtschaft** (Manipulation von Online-Banking und Geldautomaten)
- **Kinderpornografie** (geschlossene Foren)
- **Swatting**

Justiz digital

“Lesen und Lauschen”



Generalstaatsanwaltschaft Bamberg
Zentralstelle Cybercrime Bayern

Diese Plattform und der kriminelle Inhalt wurden beschlagnahmt

durch das Landeskriminalamt Sachsen im Auftrag der Generalstaatsanwaltschaft Bamberg - Zentralstelle Cybercrime Bayern.

The platform and the criminal content have been seized
by the State Office of Criminal Investigation Saxony (LKA) on behalf of Attorney General's Office Bamberg.

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

SN4C CyberCrime Competence Center Sachsen

Ransomware

Ransomware = Schadsoftware, die Daten des Benutzers auf einem IT-System verschlüsselt. Für die Entschlüsselung verlangen die Täter die Zahlung
eines Lösegelds

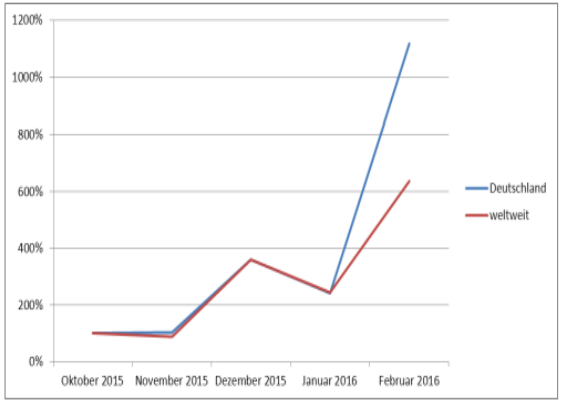
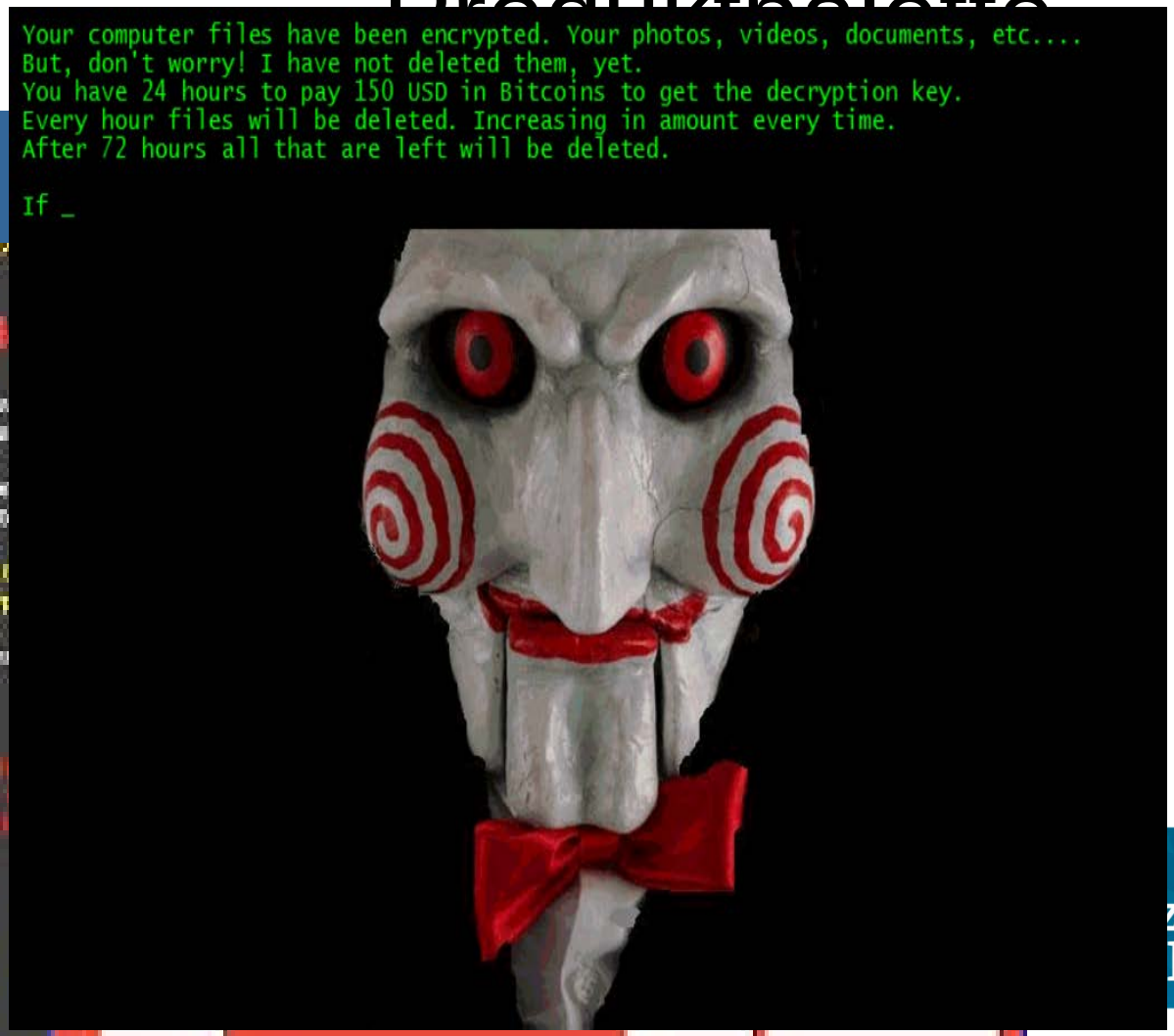


Abbildung 1: Trend der Ransomware-Detektionen in Deutschland Oktober 2015 – Februar 2016, Quelle: BSI

Breite Produktpalette



Was hilft?

Kein Backup?
Kein Mitleid!

Justiz digital

Unsere Täter:

- **„klassische“ (meist männliche) Einzeltäter mit hervorragenden IT-Kenntnissen und oftmals geringem Unrechtsbewusstsein**
- **hochgradig arbeitsteilig und international operierende Banden**
- **aber auch: Einzeltäter/lose Gruppierungen ohne besondere IT-Kenntnisse, die sich die notwendigen Fähigkeiten/Tools im Dark und Surface Web zukaufen**

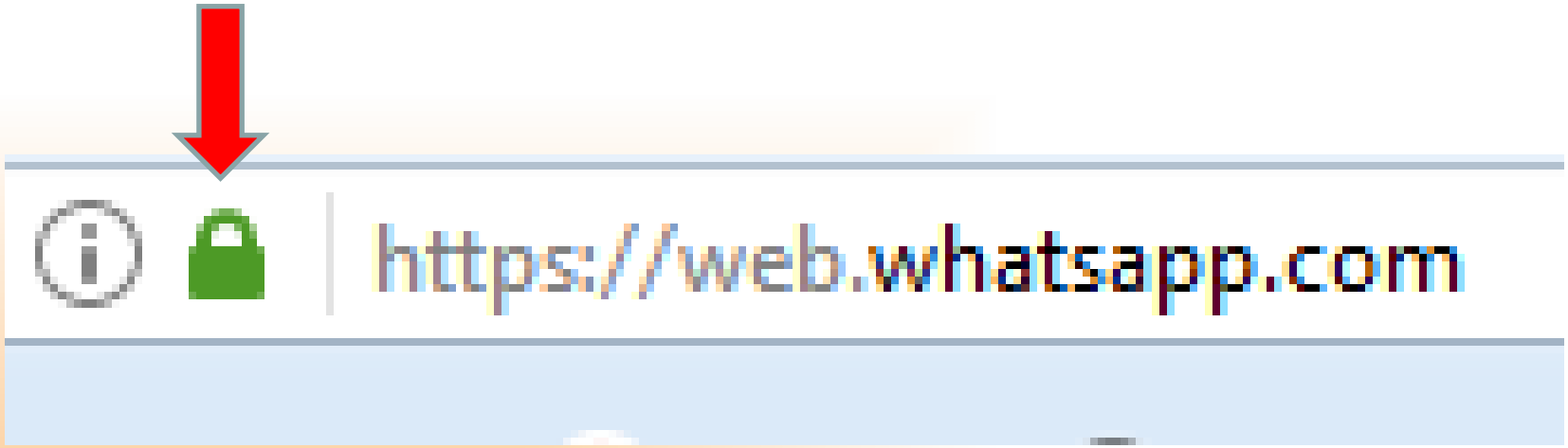
Nach wie vor:
Gefährdung durch die üblichen „Verdächtigen“

Infektionen mit Schadsoftware:

- **E-Mail mit**
  - **Verlinkung (erst dann Drive-by-Infektion)**
  - **Anhang**

- **Ausspähen von Zugangsdaten**
  - **Preisgabe über Phishing**
  - **Voreinstellungen unverändert**
  - **Erratbare oder simple Passwörter**
  - **„Abhandenkommen“ beim Provider und Mehrfachverwendung bei verschiedenen Diensten**
  - **Trojaner auf Rechner**
  - **Ganz selten: Zettel unter der Tastatur**

https://...ist doch sicher!



Zugriff auf private Accounts über verschlüsselte Zugänge erhöhen das Risiko einer Infektion!

Justiz digital

Wie kann ich mich und meine Behörde schützen?

- ***„kommt darauf an …“*: Verschiedene IT-Strukturen erfordern unterschiedliche Maßnahmen!**
- **Das Stereotyp „Nicht ob, sondern wann kommt der Angriff?“ ist leider zutreffend. Auch Behörden erleiden bei „ungezielten“ Angriffen Kollateralschäden.**
- **Awareness aller Mitarbeiter ist wichtig!**
- **Unterschätzen Sie nicht die Kreativität der Täter!**

Die ZCB empfiehlt:

- **Je schneller Strafanzeige erstattet wird, desto höher der Ermittlungserfolg (begrenzte Verbindungsdatenspeicherung).**
  -Telefonische Absprache ist zu empfehlen!-
- **Ruhe bewahren!**
- **Bereinigung und forensische Sicherung planen und dokumentieren!**
- **Beweismittel sichern und isolieren, nicht vernichten.**

Entwicklung der Zentralstelle Cybercrime Bayern

- **Beschluss der Staatsregierung im Sommer 2016 → massiver Ausbau zur nach derzeitigem Stand größten staatsanwaltschaftlichen Zentralstelle zur Bekämpfung von Cybercrime bundesweit**

- **vorgesehen sind:**
- **01.10.2017 + 2 Staatsanwälte/-innen**
  + 2 IT-Fachkräfte (ab 01.01.2018)
- **01.10.2018 + 3 Staatsanwälte/-innen**
  + 2 IT-Fachkräfte

Justiz digital

Herausforderung IT-Sicherheit

IT-Infotage Pegnitz

Lukas Knorr
Zentralstelle Cybercrime Bayern