

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

Mehr Kosten durch Cybercrime als durch Drogenhandel

Einige Schlagzeilen ...

EUROPOL | 30.09.2015

Cybercrime wachsende Bedrohung für Europa

Studie sieht Cybercrime weiter auf dem Vormarsch

Unterschätzte Gefahr: „Cybercrime wird jeden treffen“

Angriffe auf Brandenburg

Cybercrime verursacht Millionenschaden

Ansteigende Fälle beim Phishing? Cybercrime nimmt laut BKA deutlich zu

CYBERCRIME BOOMT UND SCHADET KMU

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



Cybercrime leicht gemacht

Google

[Alle](#) [Videos](#) [News](#) [Bilder](#) [Shopping](#) [Mehr](#) [Einstellungen](#) [Tools](#)

Ungefähr 392.000 Ergebnisse (0,37 Sekunden)

CVV Carding Tutorials - Tuxedo Crew
www.tuxedocrew.cc/forumdisplay.php?18...Carding-Tutorials [Diese Seite übersetzen](#)
Tutorials on CVV carding. ... Sticky: Private Tutorials Collections- All in One-Carding/Money Making/Hacking. Started by TuxedoJesus, 03-26-2013 12:38 PM.

Tutorial Carding credit card 2016 - YouTube
 <https://www.youtube.com/watch?v=phslxOf3Ea0>
19.04.2016 - Hochgeladen von kumpulan video
2 MINUTE How to make your own Credit Card Bins |Carding Tutorial Android - Duration: 2:33. TechyG ...

Carding Tutorial 2016 | Bitcoin Carding | Walmart Carding - YouTube
 <https://www.youtube.com/watch?v=aELZgLf-gmA>
05.10.2016 - Hochgeladen von Carding BLAZE
Contact Us On Whatsapp +63 9380436310 What CAn We Card Paypal , Skrill, Bitcoins We Also Teach ...

Tutorial Carding 2016 - 2017 #Part 1 - YouTube
 <https://www.youtube.com/watch?v=3qJit3ySXag>
03.10.2016 - Hochgeladen von Dunia Informatika
Di Video Saya yang pertama ini saya akan Share ke kalian Cara Dump Amazon dengan Havij 2016 ...

Carding Tutorials | HCKLEAKED - Hacked CC & DeepWeb



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



Herausforderungen für die Strafverfolgung

Ermittlungs- und Strafverfahren in diesem Bereich sind mit besonderen Problemlagen 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**



“Lesen und Lauschen”

Deutsch English

U Lesen Lauschen Bestseller Serien Listen Wunschliste Hilfe Registrieren Login

Alle Suche nach Titel, Autor, Kategorie etc. Suche

Die neuesten Einträge (48 heute neu)

 **Der problematische Prophet: Die biblische Jona-Figur in Exegese, Theologie, Literatur und Bildender Kunst (Arbeiten zur Kirchengeschichte, Band 118)**
von Johann Anselm Steiger, Ulrich Heinen, Wilhelm Kühlmann
€ 1,25

 **DuMont Reise-Taschenbuch Reiseführer Azoren**
von Susanne Lipps-Breda
€ 0,25

 **Du auf deinem höchsten Dach**
von Anatol Regnier

 **Jack Deveraux Dämonenjäger 04 - Sirenenesang**
von Xenia Jungwirth

Zum Geburtstag von ...
Jürgen Habermas
* 18.06.1929
Zum Sortiment

Downloadrangliste
Lesen Lauschen
Heute Woche Monat Jahr

Affiliate Programm - Nutzer werben

 Empfehle lul.to an Deine Freunde oder auf Deiner Webseite und profitiere mit! Du bekommst wahlweise **12% vom Ersteinzahlungsbetrag** oder **3% von jeder Einzahlung** Deiner geworbenen Nutzer gutgeschrieben.
Mehr Informationen

Zuletzt kommentiert

 **Finis Germania, 2. Auflage (Kaplaken 50)**
von Rolf Peter Sieferle
hwy2001: "Im Jahr 2017 wurde im Verlag Antaios der Band „Finis Germania“ herausgegeben, in dem postum 30 Miscellen Siefe...



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



**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

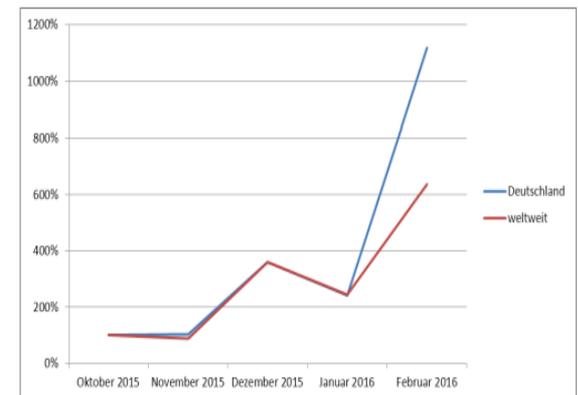


Abbildung 1: Trend der Ransomware-Detektionen in Deutschland Oktober 2015 – Februar 2016, Quelle: BSI

Breite

Produktplatte

Your computer files have been encrypted. Your photos, videos, documents, etc...
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If _



Your personal files

Your documents, photos, database encryption and unique key, generated

Private decryption key is stored on until you pay and obtain the private

You only have 24 hours to submit. If your files will be permanently cryp

Press 'View' to view the list of files

Press 'Next' for the next page.



WARNING! THE PRICE OF
YOUR FILES IS 150 USD IN
BITCOIN. IF YOU DO NOT
PAY WITHIN 24 HOURS,
YOUR FILES WILL BE
PERMANENTLY DELETED.

View



Was hilft?

**Kein Backup?
Kein Mitleid!**

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



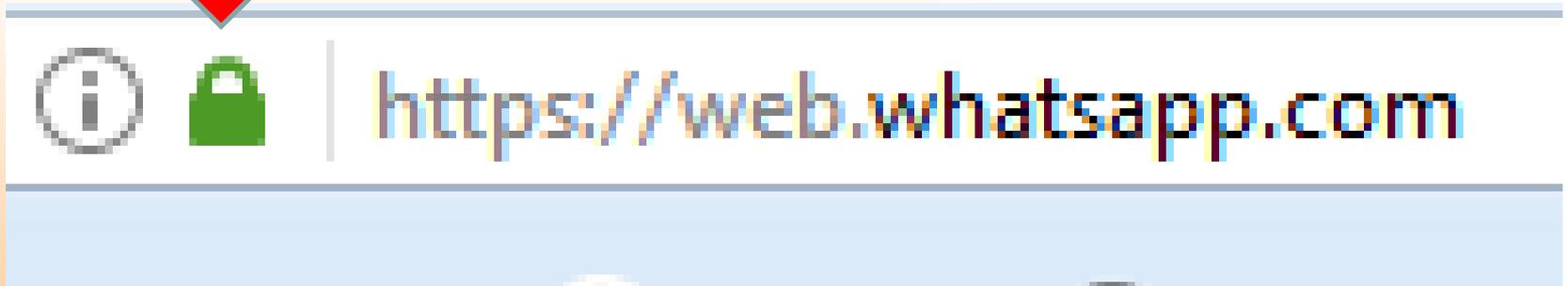
Nach wie vor: Gefährdung durch die üblichen „Verdächtigen“

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!**



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**



Herausforderung IT-Sicherheit

IT-Infotage Pegnitz

Lukas Knorr
Zentralstelle Cybercrime Bayern

