Bedrohungslage Cybercrime

MORITZ HUBER

KRAUTHEIM – 27. APRIL 2016

Baden-Württemberg
LANDESKRIMINALAMT

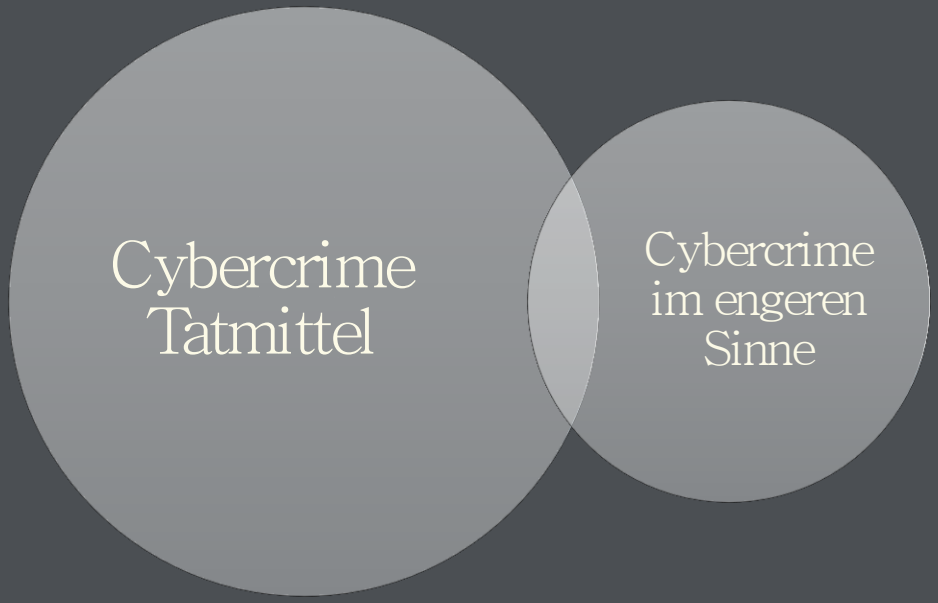
Agenda

- Aktuelle Phänomene und Präventionsmöglichkeiten
- Entwicklung der Kriminalitätslage
- Organisation der Polizei Baden-Württemberg

Agenda

- Aktuelle Phänomene und Präventionsmöglichkeiten
- Entwicklung der Kriminalitätslage
- Organisation der Polizei Baden-Württemberg

Cybercrime



Quelle: https://www.bitkom.org/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709_Studienbericht_Wirtschaftsschutz.pdf

Betroffene Unternehmen

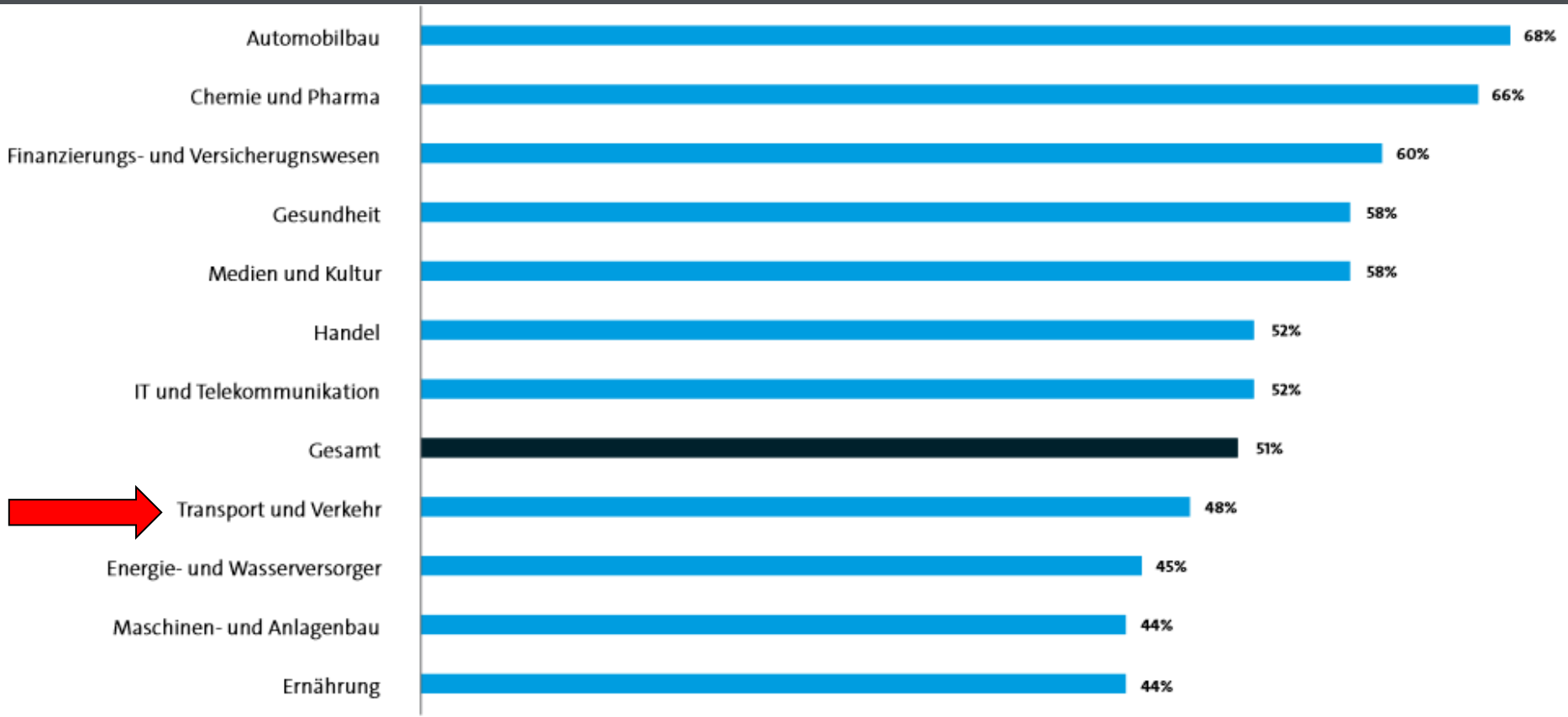


Abbildung 2: Betroffene Unternehmen nach Branchen

Basis: Alle befragten Unternehmen (n=1.074) | Quelle: Bitkom Research

Cyberwar

DDos-Attacke

Internet-of-Things

CEO Fraud

Spoofing (DNS, Call-ID, IP)

Scareware

Ransomware

Botnetz

OK

Brute-Force-Attacke

Darknet

Social Engineering

Abmahnfalle

Baden-Württemberg
LANDESKRIMINALAMT

Quelle: http:// www.t-online.de/computer/sicherheit/id_75009016/hacker-manipuliert-narkosegeraet.html

Internet of Things

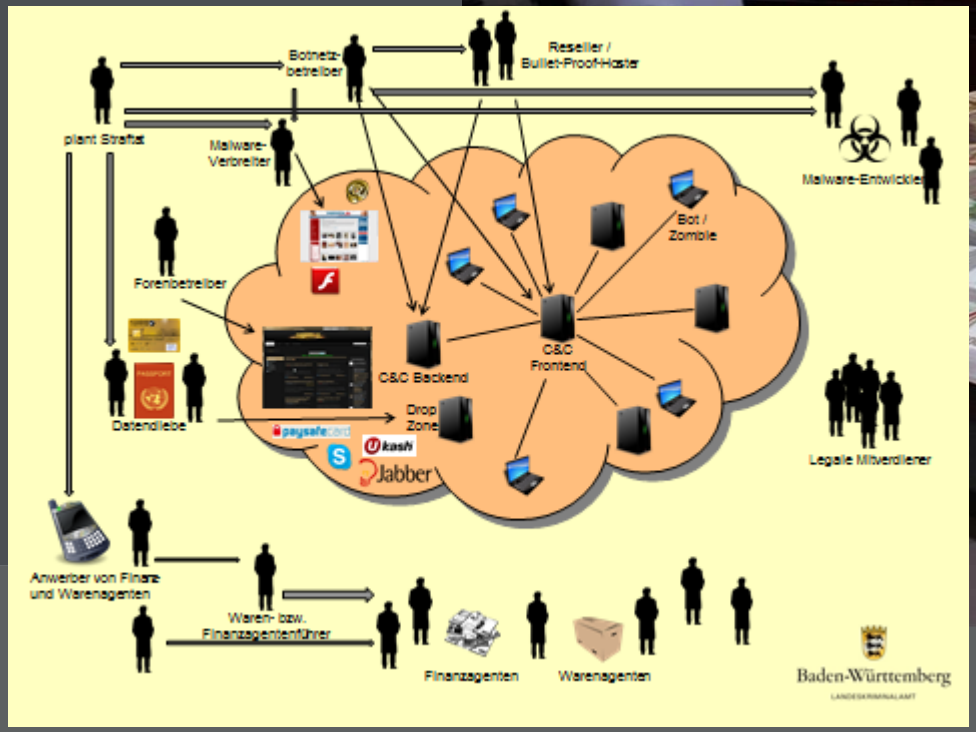
Beatmung gestoppt

Hacker übernimmt Narkosegerät

10.08.2015, 10:51 Uhr | t-online.de

Hacker konnte Beatmungsgerät manipulieren (Quelle: Science Photo Library/imago)

Organisierte Kriminalität



Baden-Württemberg
LANDESKRIMINALAMT

Underground Foren

Crime

Fraud
Geld verdienen mit geklauten Kreditkarten/Paypals etc

Real Crime
Überfälle, Raubzüge etc

Drogen
Herstellung von Drogen, Diskussionen, Mischungen etc.

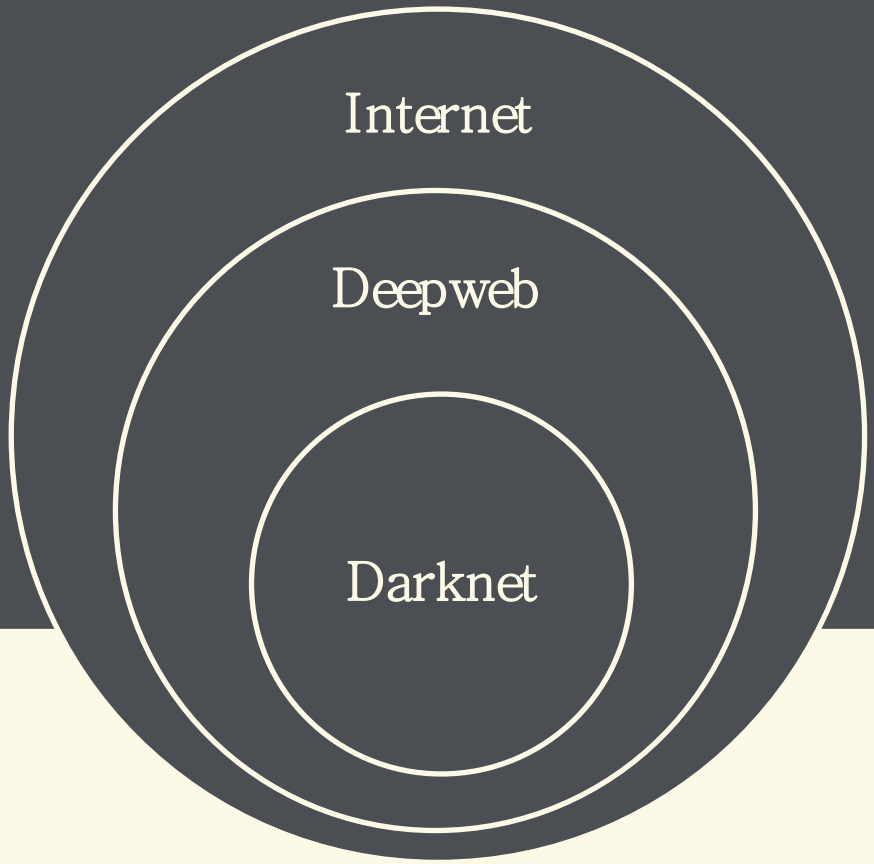
Webhacking/Websecurity/Coding
Exploits, SQL Injection, XSS etc

Malware
Hier handelt sich alles um Trojaner/Malware

Account/Stuff Base
Free Stuff wie CCs, Accounts, Keys etc.
+ Public Stuff

Baden-Württemberg
LANDESKRIMINALAMT

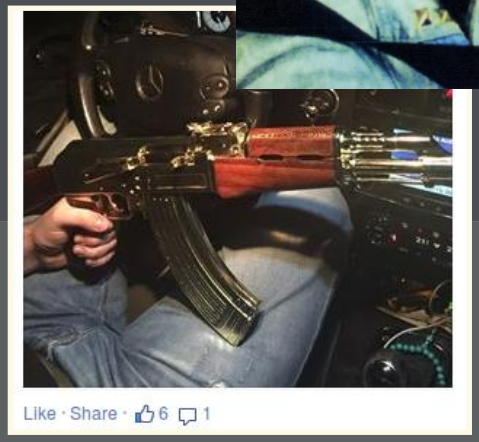
Darknet



- TOR
- I2P
- FREENET
- …

Baden-Württemberg
LANDESKRIMINALAMT

Drogendealer NRW



Social Engineering

„ *Die zwischenmenschliche Manipulation, mit dem Ziel (unter Vortäuschung falscher Tatsachen) unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen.* “

Es werden nicht die technischen Möglichkeiten ausgenutzt!

→ **„Sozial-Ingenieure hacken Menschen.“**

Baden-Württemberg
LANDESKRIMINALAMT

CEO-Fraud / Fake President

Baden-Württemberg
LANDESKRIMINALAMT

CEO-Fraud / Fake President

Von: Geschäftsführer@firma.de <Geschäftsführer@presidency.com>

An: Finanzbuchhalter@firma.de

Sehr geehrter Hr. Buchhalter!

Sind Sie im Moment verfügbar?

Hochachtungsvoll
Geschäftsführer

Baden-Württemberg
LANDESKRIMINALAMT

CEO-Fraud / Fake President

Von: Geschäftsführer@firma.de <Geschäftsführer@presidency.com>

An: Finanzbuchhalter@firma.de

Sehr geehrter Hr. Buchhalter,

Ich befinde mich derzeit in Asien zur Vorbereitung einer Firmenübernahme. Da Sie sich in der Vergangenheit als loyaler und vertrauenswürdiger Mitarbeiter erwiesen haben, möchte ich Ihnen eine wichtige Aufgabe übertragen, die nur SIE alleine ausführen können…

Hochachtungsvoll
Geschäftsführer

Baden-Württemberg
LANDESKRIMINALAMT

Quelle: http:// news.softpedia.com/news/belgian-bank-loses-70-million-to-classic-ceo-fraud-social-engineering-trick-499388.shtml

Indikatoren CEO Fraud

- „muss streng vertraulich behandelt werden“
- „Vertragsstrafen und Sanktionen“
- „Kontakt zu französischem Ber
- „vermeiden Sie in
  Anspielung
-
- innerhalb unseres

Baden-Württemberg
LANDESKRIMINALAMT

Prävention

- Sensibi… Mitarbeiter
- Überprü… Mails
- Restriktive Datenm…
- Verhaltensrichtlinie bei Ve…
- Vier-Augen-Prinzip
- Entwickeln Sie ein Notfallkonzept, für den Sc…

!!! Prüfen Sie die Maßnahmen auch auf Ihre tatsächliche Wirksamkeit !!!

- Nutzung digitaler Signaturen

Baden-Württemberg
LANDESKRIMINALAMT

Quelle: http://www.sueddeutsche.de/digital/hackerangriff-computervirus-legt-klinik-in-neuss-lahm-1.2861656

Crypto-Ransomware

Süddeutsche Zeitung
SZ.de Zeitung Magazin

12. Februar 2016, 16:36 Uhr Hackerangriff

Computervirus legt Klinik in Neuss lahm

- Ein Computervirus legt das städtische Krankenhaus in Neuss lahm. Es werde gearbeitet wie vor 15 Jahren, sagt eine Sprecherin.
- Cyberangriffe auf Krankenhaus-IT nähmen zu, es gebe auch Fälle von Erpressung, teilt die Krankenhausgesellschaft mit.

Baden-Württemberg
LANDESKRIMINALAMT

Quelle: http://www.heise.de/security/meldung/Erpressungs-Trojaner-Locky-schlaegt-offenbar-koordiniert-zu-3104069.html

Crypto-Ransomware Locky

Baden-Württemberg
LANDESKRIMINALAMT

Falsche Bewerbung / PETYA

Sehr geehrter Herr **Müller**,

Durch meine mehr als **5-jährige Berufserfahrung als Dachdecker** und die kontinuierliche, selbständige Weiterbildung bin ich davon überzeugt, die mit der herausfordernden Stelle als Dachdecker verbundenen Anforderungen zu Ihrer Zufriedenheit erfüllen zu können. Daher bewerbe ich mich hiermit gerne bei Ihrem Unternehmen.

Mittlerweile arbeite ich seit mehr als fünf Jahren als Dachdecker. Bereits während meiner Ausbildung hatte ich die Möglichkeit, Tätigkeiten die geforderten Tätigkeiten kennenzulernen.

Mit freundlichem Gruß

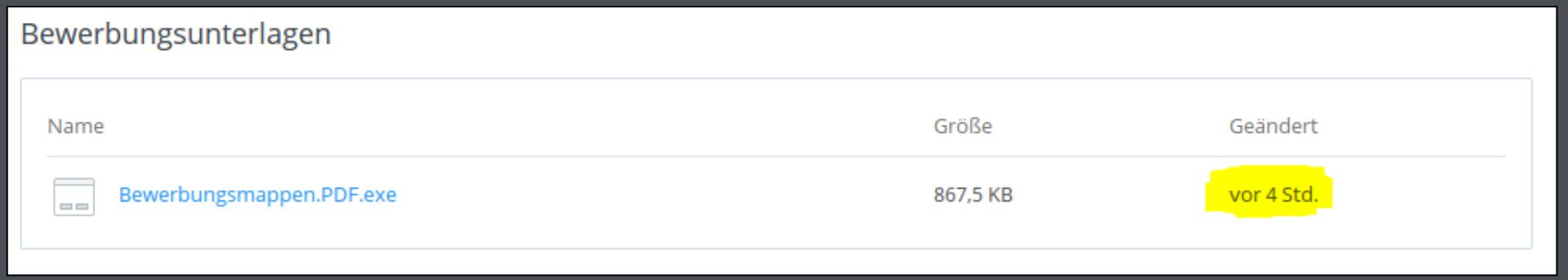
Tobias Täter

Bewerbungsunterlagen und Zertifikate: **https://www.dropbox.com/sh/Beispiellink/123456?dl=0**

Ich konnte die Unterlagen nicht anhängen, dennoch müssen Sie sich nicht extra anmelden um die Bewerbung anzusehen, Entschuldigen Sie bitte die Unannehmlichkeiten!

Baden-Württemberg
LANDESKRIMINALAMT

Falsche Bewerbung / Ransomware



Baden-Württemberg
LANDESKRIMINALAMT

Prävention

- Sensibi… …ihre Mitarbeiter
- Prüfen Sie … …ils sorgfältig
- Achten Sie auf die tat… …ung
- Entwickeln Sie ein Notfallkonzept… …eintritt

!!! Prüfen Sie die Maßnahmen auch auf Ihre tatsächliche Wirksamkeit !!!

- Sichern Sie Ihr System mit aktueller Schutzsoftwa…
- Erstellen Sie regelmäßig externe Backups

Baden-Württemberg
LANDESKRIMINALAMT

Agenda

- Aktuelle Phänomene und Präventionsmöglichkeiten
- Entwicklung der Kriminalitätslage
- Organisation der Polizei Baden-Württemberg

Baden-Württemberg
LANDESKRIMINALAMT

Lageentwicklung

PKS	2011	2012	2013	2014	2015	Tendenz
Tatmittel Internet	20.988	16.912	18.804	17.949	18.676	→

POLAS BW	2011	2012	2013	2014	2015	Tendenz
Tatmittel Internet (Täter unbekannt oder im Ausland)	6.166	11.362	14.944	18.562	21.129	↗

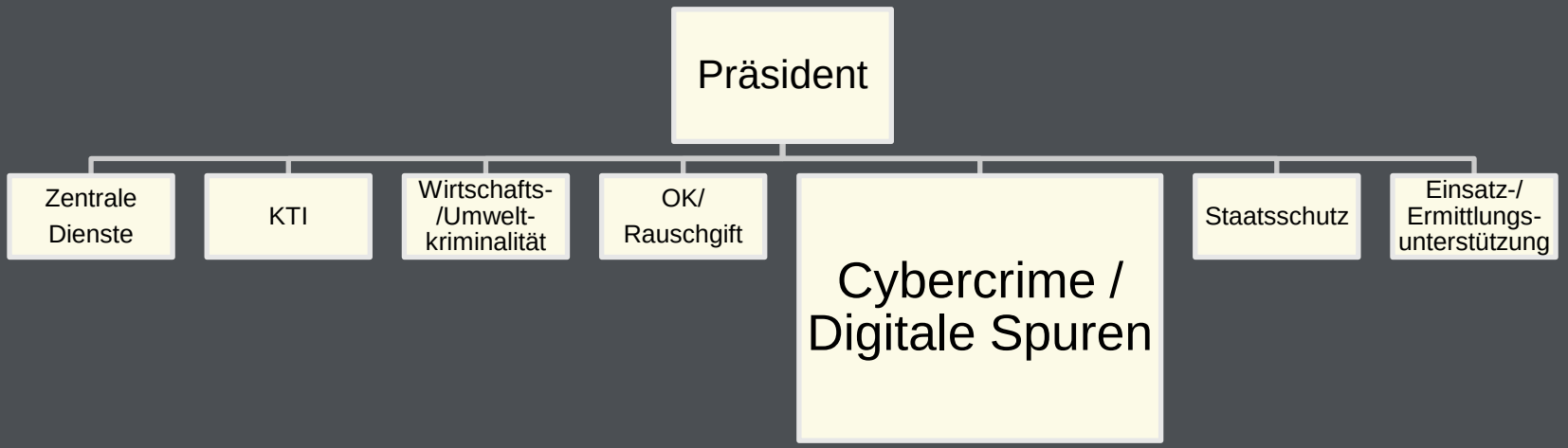
Baden-Württemberg
LANDESKRIMINALAMT

Agenda

- Aktuelle Phänomene und Präventionsmöglichkeiten
- Entwicklung der Kriminalitätslage
- Organisation der Polizei Baden-Württemberg

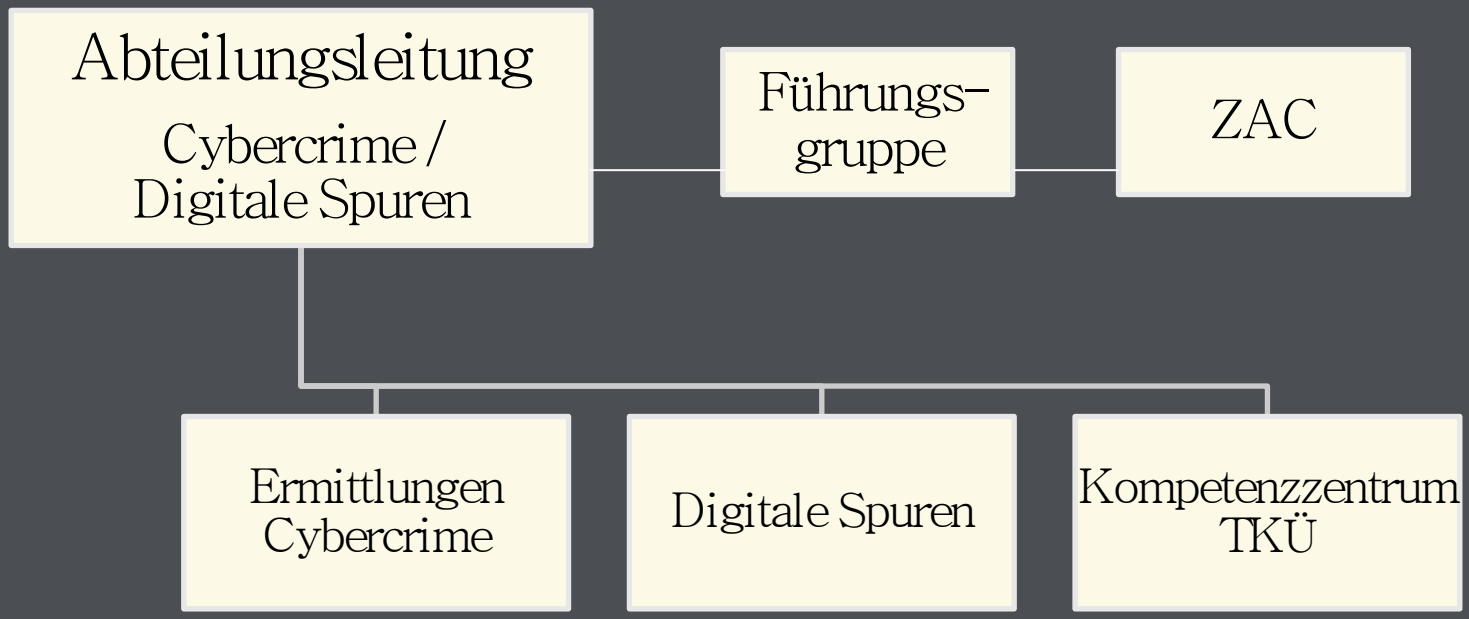
Baden-Württemberg
LANDESKRIMINALAMT

Landeskriminalamt



Baden-Württemberg
LANDESKRIMINALAMT

LKA BW – Abt. 5



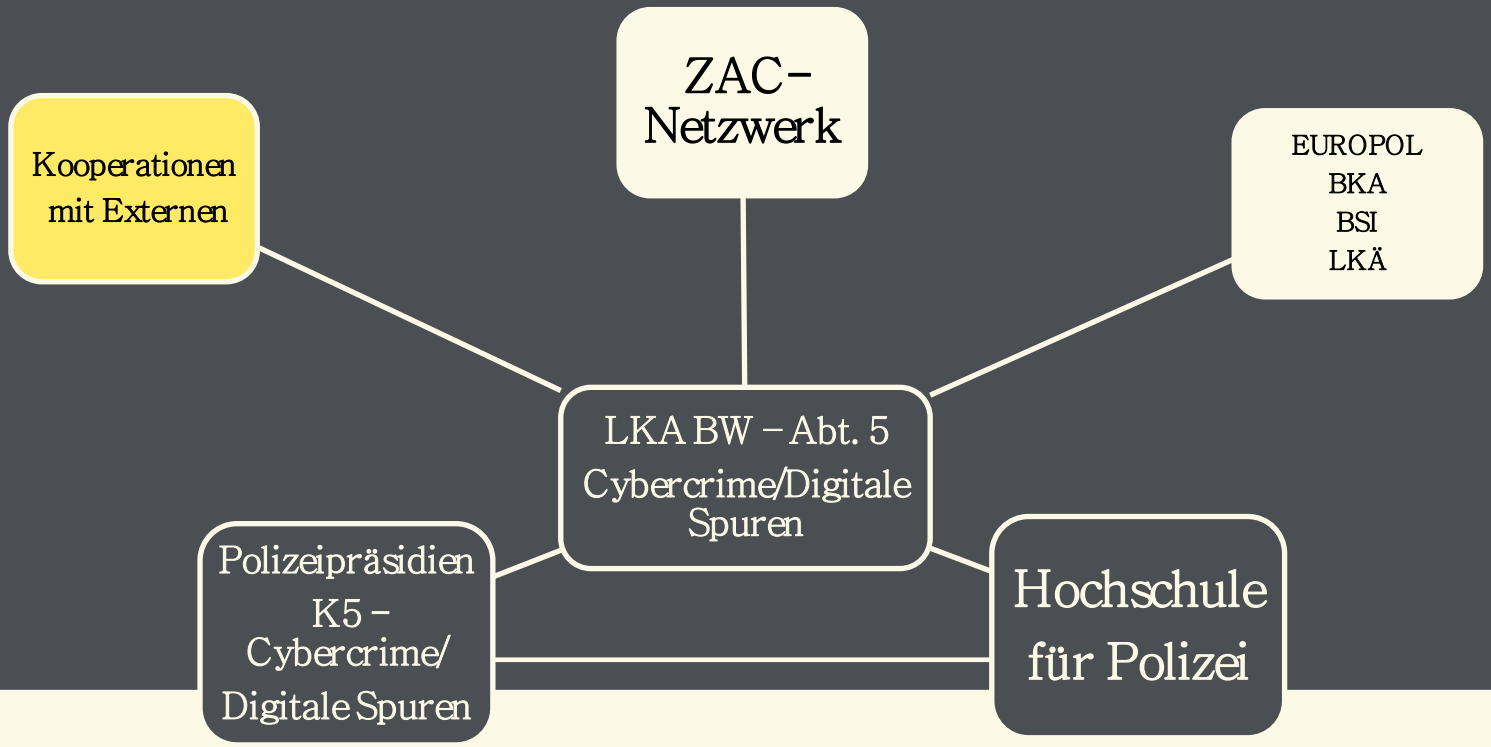
Baden-Württemberg
LANDESKRIMINALAMT

12 Polizeipräsidien

- Kriminalpolizeidirektion
  - K1
  - K2
  - K3
  - K4
  - **K5 Cybercrime / Digitale Spuren**
  - K6
  - K7
  - K8

Baden-Württemberg
LANDESKRIMINALAMT

Vernetzung der Abt. 5



Baden-Württemberg
LANDESKRIMINALAMT

Zentrale Ansprechstelle Cybercrime

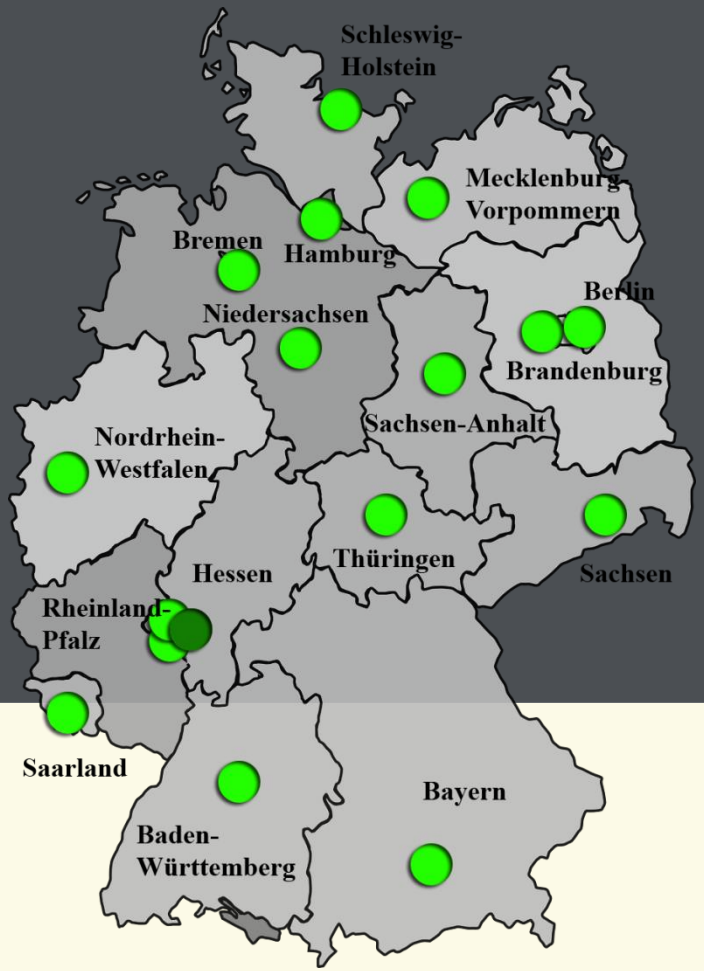
ZAC

Damit Sie im Netz niemandem ins Netz gehen

Für Behörden und Unternehmen

0711 5401-2444
cybercrime@polizei.bwl.de

ZAC-Dienststellen



Bundeskriminalamt

Landeskriminalamt

Baden-Württemberg
LANDESKRIMINALAMT

Zentrale Ansprechstelle Cybercrime

ZAC

Damit Sie im Netz niemandem ins Netz gehen

Für Behörden und Unternehmen

0711 5401-2444
cybercrime@polizei.bwl.de