Abteilung Cybercrime und Digitale Spuren LKA BW

FRAUNHOFER SIT

Reinhard Tencz
Tel.: 0711 5401-2500
Mobil: 0162-2530753
Reinhard.tencz@polizei-bwl.de

September 2017

Baden-Württemberg

LANDESKRIMINALAMT

Phishing

Identitätsdiebstahl

Malware

Scareware

Cyberwar

Carding

Botnetz

Espionage

Brute-Force-Attacke

Filesharing

Darknet

Spoofing (DNS, Call-ID, IP)

Spam

Abmahnfalle

Digitale Erpressung

APT

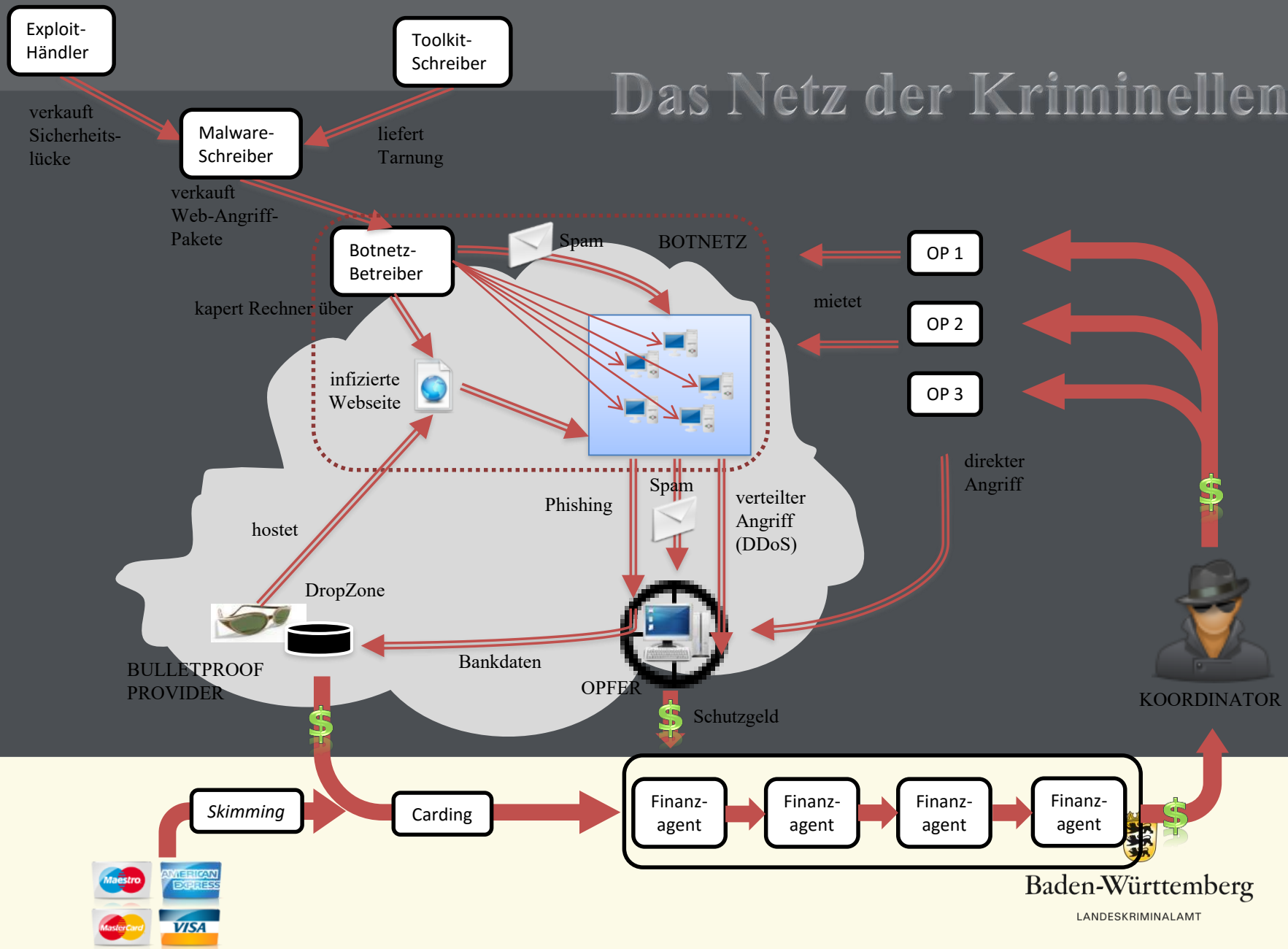
DDos-Attacke

Social Engineering

Cybercrime

- Transnationale Kriminalität
- Kriminelle Infrastrukturen
- Underground-Economy (Baukasten-Systeme)
- Kryptierung, Anonymisierung (geringes Entdeckungsrisiko)
- Cybercrime-as-a-Service
- Bedeutung digitaler Währungen

Das Netz der Kriminellen



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

Quelle: http://www.stuttgarter-nachrichten.de/inhalt.kinderpornografie-nicht-zuzumuten.54d5e6ef-68b7-47cf-b57b-08d0ff00647f.html

Kinderpornografie

STUTTGARTER-NACHRICHTEN.DE

Kinderpornografie

Nicht zuzumuten

Franz Feyder, 29.08.2015 09:14 Uhr

Staatsanwälte leiteten auf Grundlage von Ermittlungen des baden-württembergischen Landeskriminalamtes (LKA) weltweit in diesem Jahr bereits 11 753 Strafverfahren wegen des Besitzes und der Verbreitung von Kinderpornografie ein.

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

Bitkom Studie

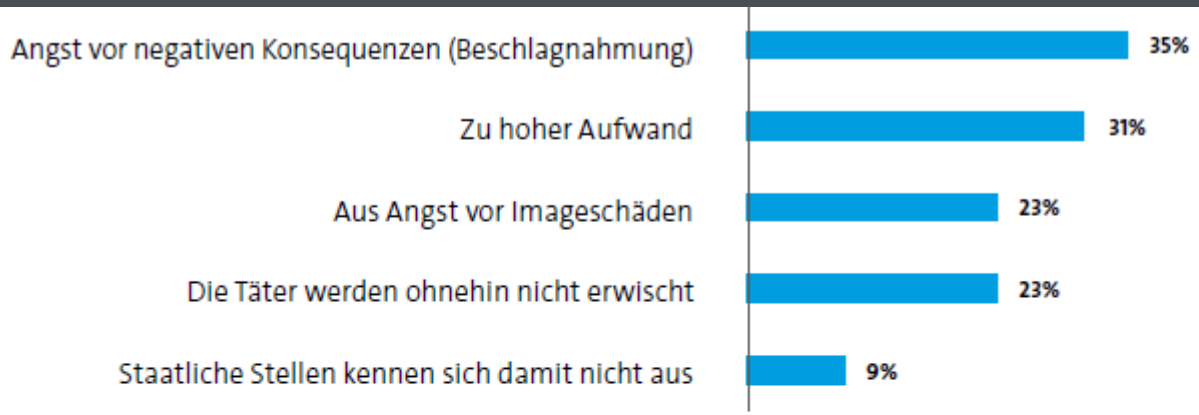


Abbildung 12: Gründe für das Nicht-Einschalten von staatlichen Stellen

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren und keine staatliche Stellen bei der Untersuchung eingeschaltet haben (n=440)

Mehrfachnennungen möglich | Quelle: Bitkom Research

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

Aufgetretene Delikte

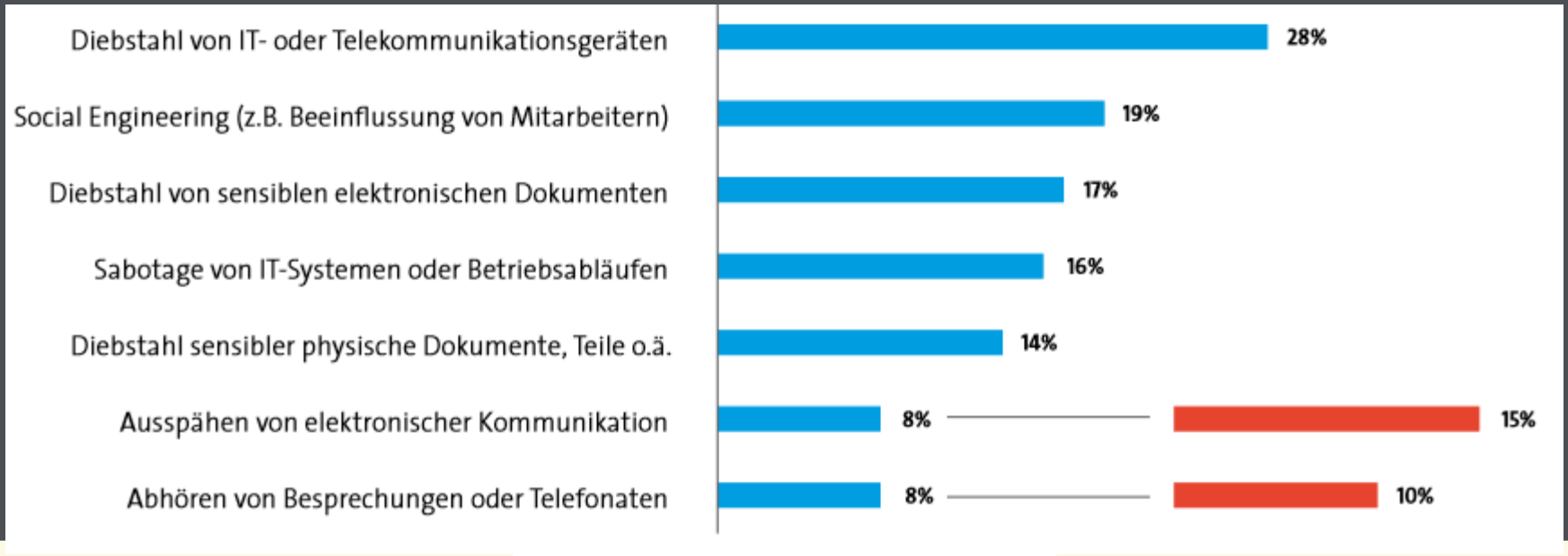


Abbildung 4: Aufgetretene Delikte

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

Betroffen

ab 500 Mitarbeiter: Betroffen

Baden-Württemberg
LANDESKRIMINALAMT

uelle: http://www.nbcnews.com/tech/security/ubiquiti-networks-says-it-was-victim-47-million-cyber-scam-n406201

Social Engineering

Baden-Württemberg

LANDESKRIMINALAMT

Zentrale Ansprechstelle Cybercrime

Warnmeldung für Firmen

Stuttgart, 17. September 2015

E-Mails vom vermeintlichen Geschäftsführer: LKA warnt Firmen vor Betrugsmasche

Seit kurzem gehen vermehrt Hinweise auf eine seit längerem bekannte Betrugsmasche beim Landeskriminalamt Baden-Württemberg ein.
Dabei nutzen die Täter gezielt die Abwesenheit der Geschäftsführung aus, um mit gefälschten E-Mail-Absenderangaben an Firmengelder zu gelangen. Mit d
versuchen die Betrüger Firmen zu täuschen, teilweise kam es bereits zu U
und Schäden von mehreren Millionen Euro.

Neugier

Anerkennung

Hilfsbereitschaft

Angst

Druck

Folgen

- Strukturen
  - Neu
  - Kooperationen
  - Cyberwehr
- Personal
  - Laufbahnen
  - Aus- und Fortbildung
- Ausstattung
  - Infrastruktur
  - Hard- und Software
  - Finanzierung
- Recht
  - Internationale Rechtshilfe
  - StPO (Bsp. Datenhehlerei, Prof. Sieber, Begrifflichkeiten StPO -1879)

Abteilung 5
Cyberkriminalität / Digitale Spuren

Führungsgruppe ZAC

Inspektion IuK – Ermittlungen

- Ermittlungen Auswertung
- Internetrecherche Ansprechstelle KiPo
- Ermittlungsinformatiker

Inspektion IT-Beweissicherung Digitale Spuren

- IT-Beweissicherung
- Datenanalyse Massendaten-auswertung
- Bild Video Audio

Inspektion Telekommunikations-überwachung

- TKÜ-Zentrum
- Operative IT
- IMSI WLAN FIS

Zentrale Ansprechstelle Cybercrime

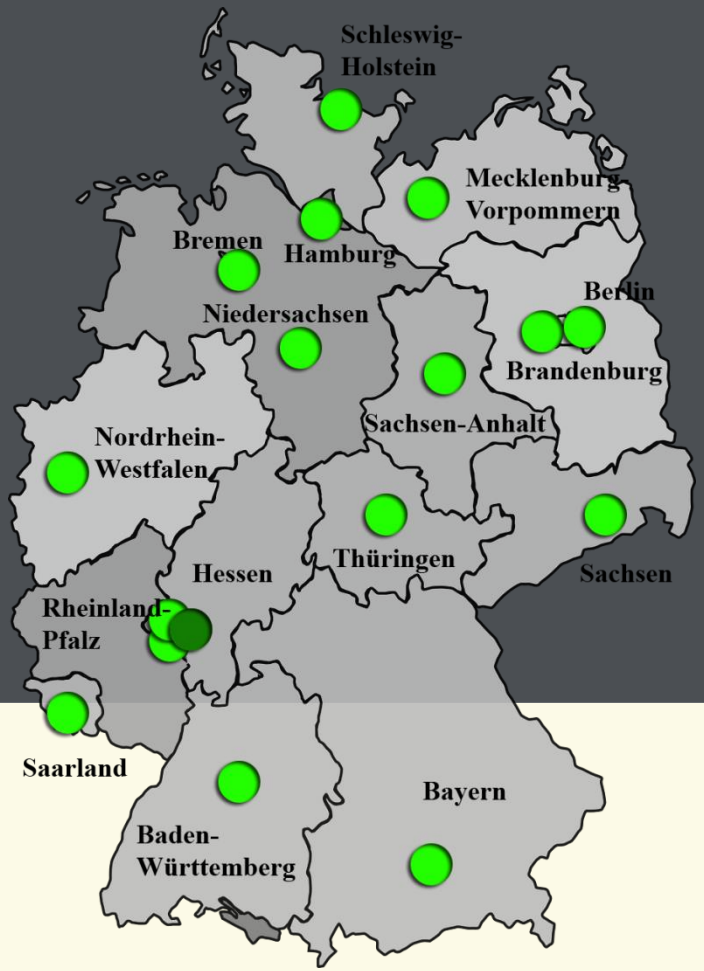
ZAC

Damit Sie im Netz niemandem ins Netz gehen

Für Behörden und Unternehmen

0711 5401-2444
cybercrime@polizei.bwl.de

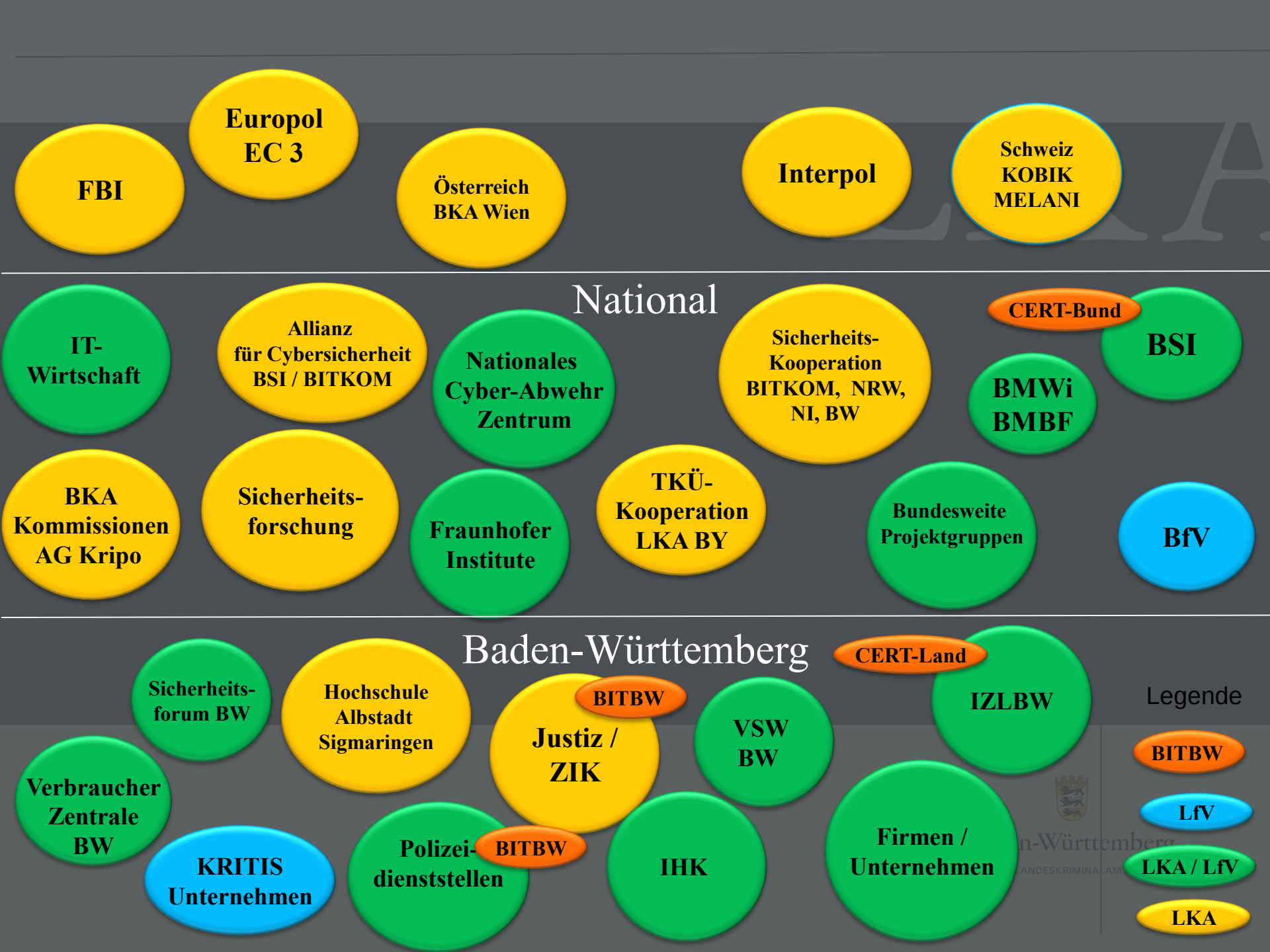
ZAC-Dienststellen



Bundeskriminalamt

Landeskriminalamt

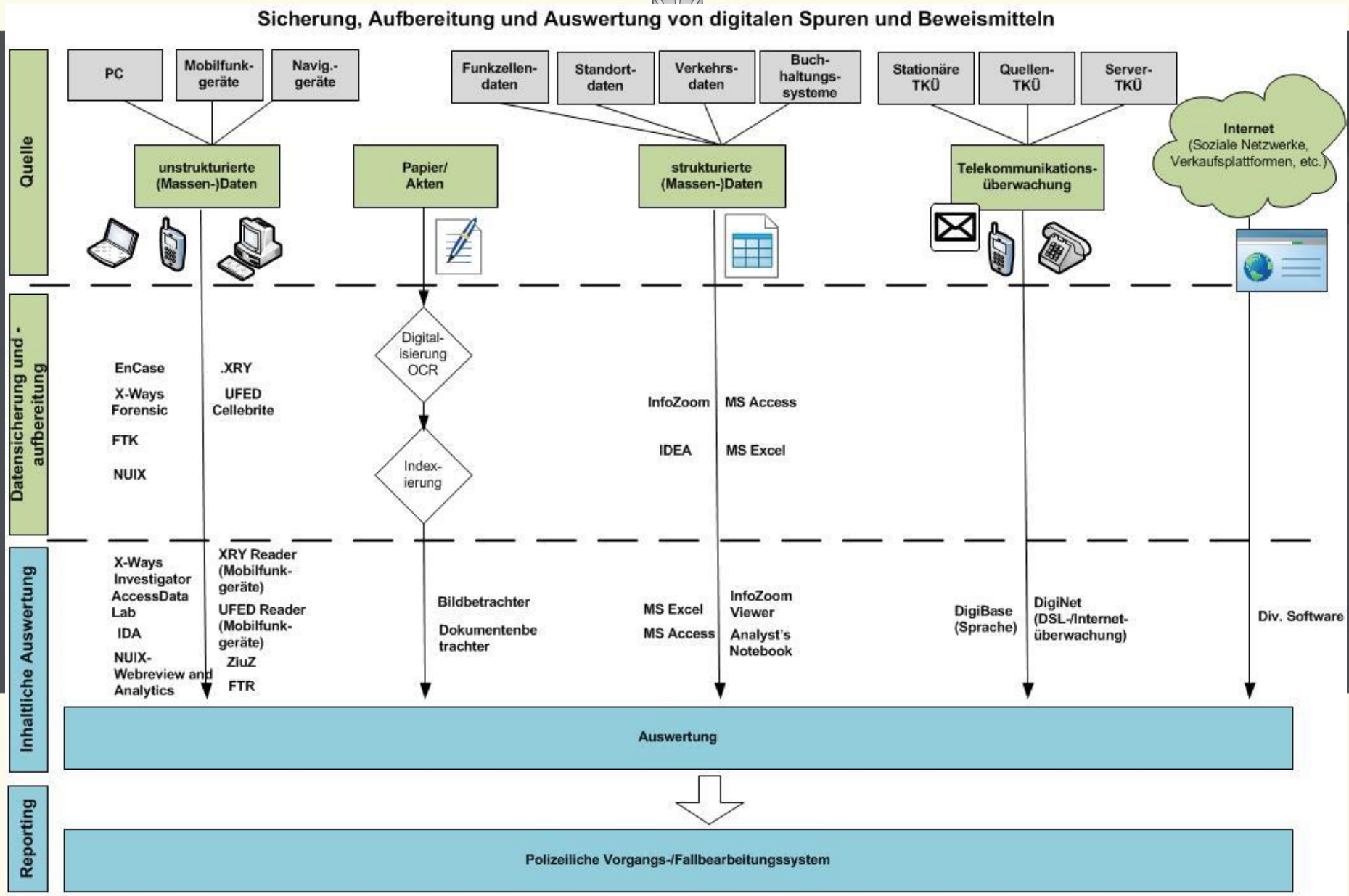
Baden-Württemberg
LANDESKRIMINALAMT


Europol
EC 3
FBI
Österreich
BKA Wien
Interpol
Schweiz
KOBIK
MELANI
National
IT-
Wirtschaft
Allianz
für Cybersicherheit
BSI / BITKOM
Nationales
Cyber-Abwehr
Zentrum
Sicherheits-
Kooperation
BITKOM, NRW,
NI, BW
CERT-Bund
BSI
BMWi
BMBF
BKA
Kommissionen
AG Kripo
Sicherheits-
forschung
Fraunhofer
Institute
TKÜ-
Kooperation
LKA BY
Bundesweite
Projektgruppen
BfV
Baden-Württemberg
Sicherheits-
forum BW
Hochschule
Albstadt
Sigmaringen
BITBW
Justiz /
ZIK
VSW
BW
CERT-Land
IZLBW
Legende
BITBW
LfV
LKA / LfV
LKA
Verbraucher
Zentrale
BW
KRITIS
Unternehmen
Polizei-
dienststellen
BITBW
IHK
Firmen /
Unternehmen

Digitale Spuren

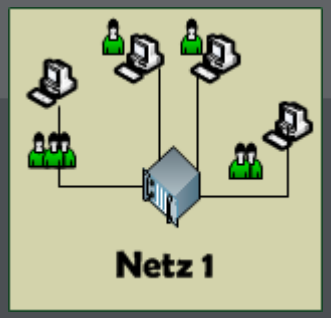
- Kfz-Vernetzung (eingebaute SIM-Karten, Kfz-Elektronik,
- autonomes Fahren etc.)
- Netzwerkforensik
- Mobile Devices
- Smart Home
- Telekommunikationsüberwachung
- Industrie 4.0
- Internet der Dinge
- Bitcoin-Ermittlungen
- Social Media Analytic
- BIG-Data Analysen (Data Scientist)
- Multi-Media-Forensik

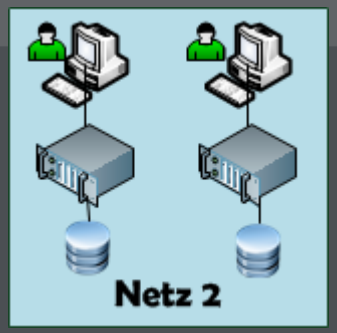
Status quo aus Sicht des Sachbearbeiters

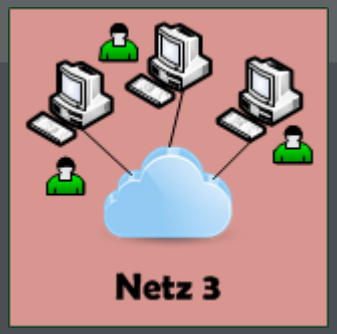


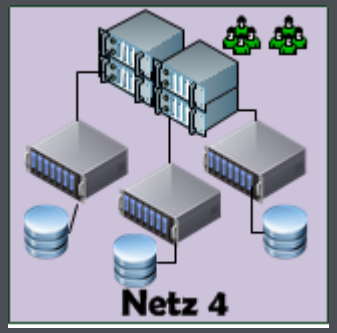
uwe.schlatter@polizei.bwl.de

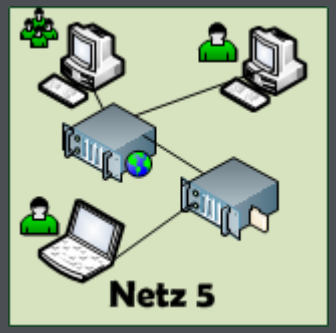
Gefahr von Insellösungen

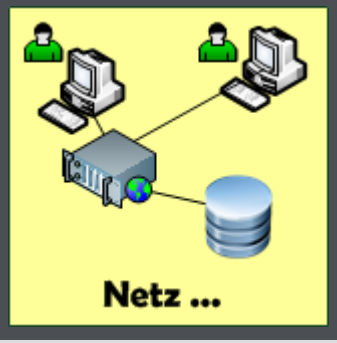












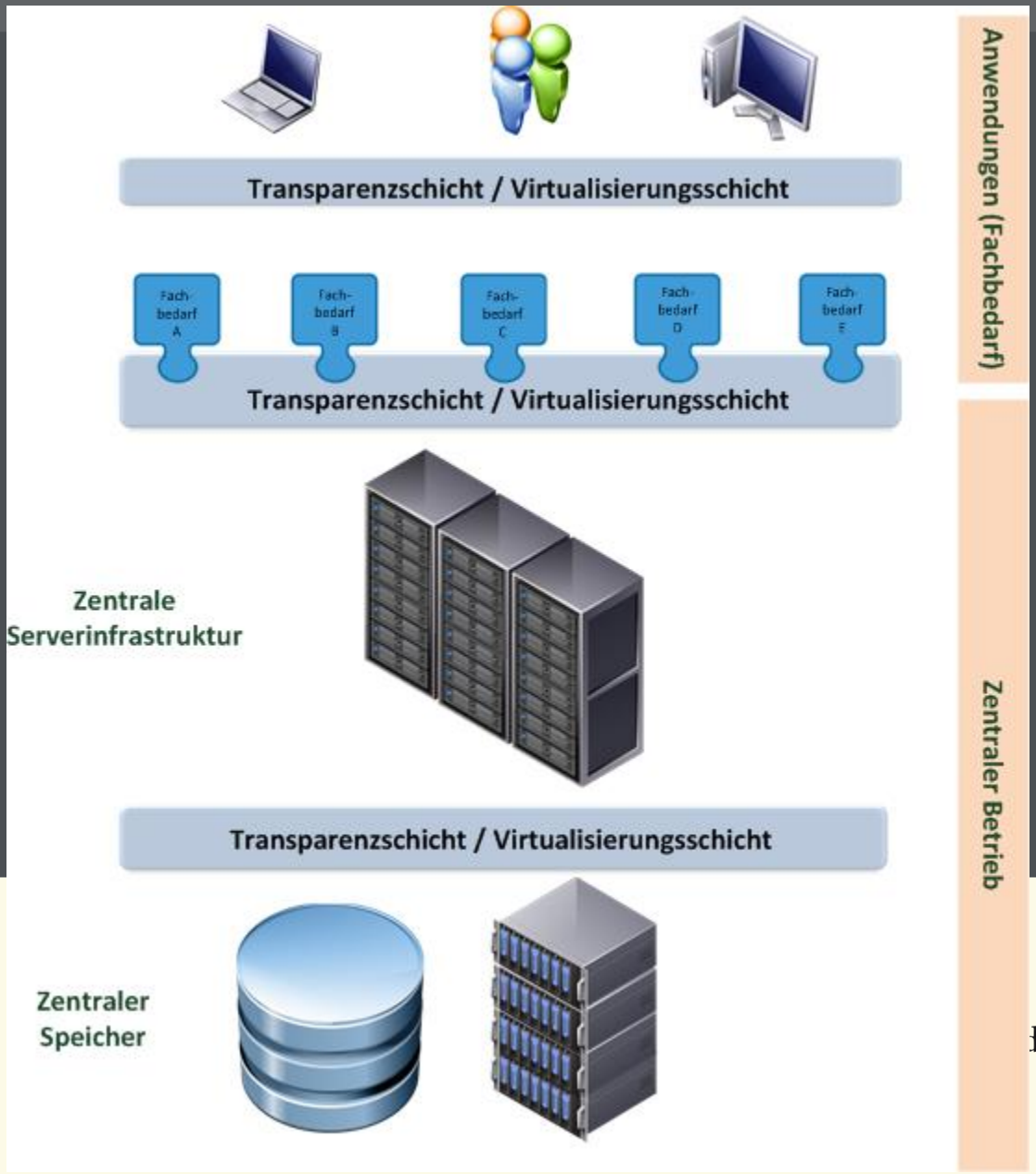
IT

- Fragmentierte IT-Architekturen
- Separate Datensilos
- Kein zentraler Betrieb
- Keine / unzureichende technische Standards
- Keine / unzureichende Berücksichtigung der Belange der IT-Sicherheit
- Hohe finanzielle und personelle Aufwände
- Gefahr von nicht mehr beherrschbarer Komplexität
- Schwierige Planungen (ad hoc auftretende Beschaffungs-/Finanzierungsbedarfe)
- Beschränkte Skalierbarkeit der Insellösungen

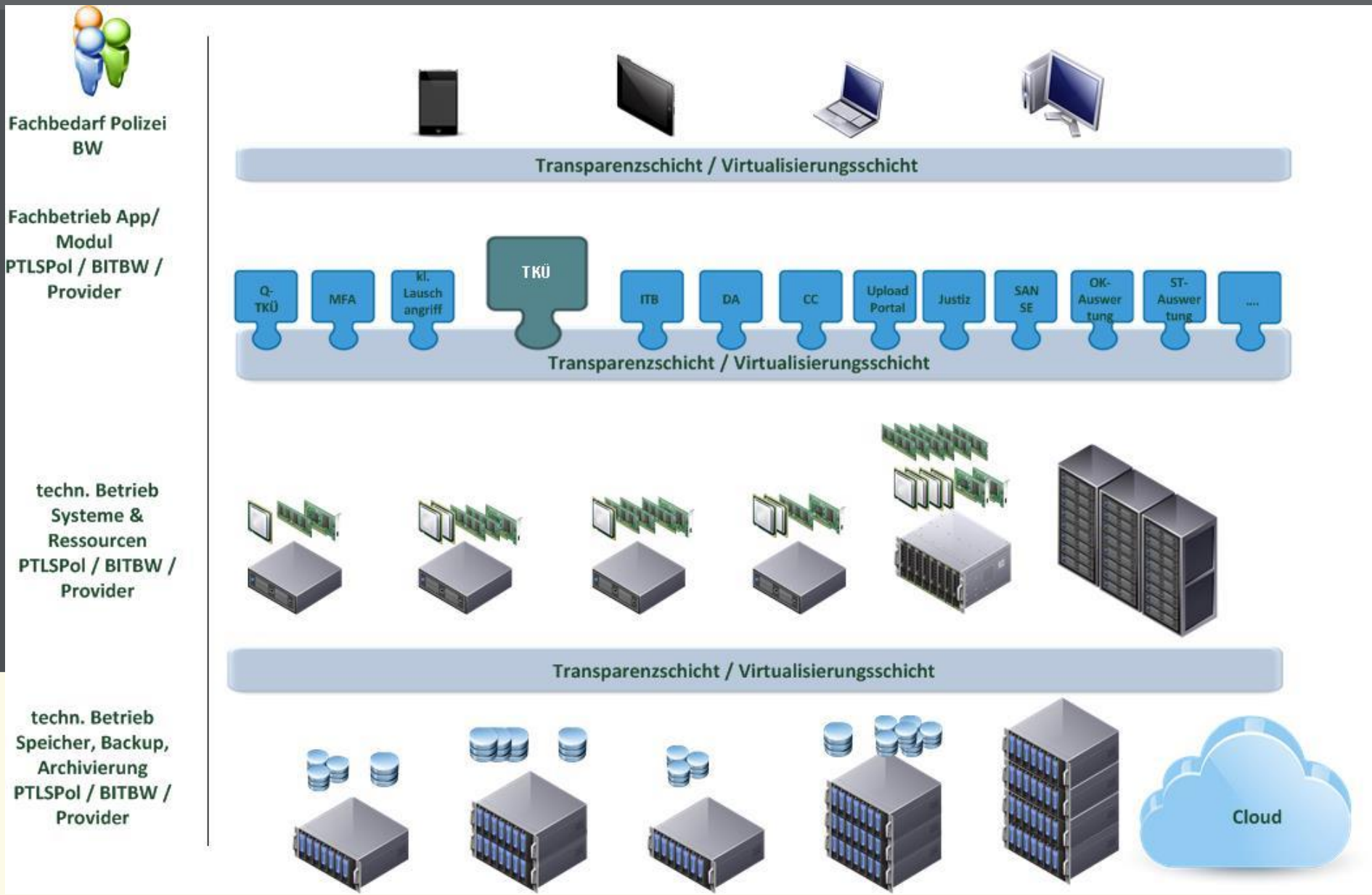
Sachbearbeiter

- Hohe Aufwände in der Auswertearbeit
- Keine / fehlende Auswertestandards
- Fragmentierte Geschäftsprozesse
- Keine Benutzerfreundlichkeit
- Medienbrüche
- Hohe Komplexität, durch zahlreiche unterschiedlich Auswerteprodukte
- Keine Mehrbenutzerfähigkeit

Ziel: Gesamtintegration in ein zentralisiertes System



Ziel Gesamtintegration in ein zentralisiertes System



Think Tank

Entwicklungen	Gegenwart	2 Jahre	5 Jahre	10 Jahre	20 Jahre
Machine Intelligence • Spracherkennung • Bilderkennung • Kontextverstehen	F/P	F/P	P		
Artificial General Intelligence • Selbstlernende Systeme • Eigenständiges Entscheiden • Z.B. Fa. DeepMind	F	F	F	F/P	P
Fahrzeugtechnik • Fahrzeug-Fahrzeug Kommunikation (Car2X) • Fahrzeug-Internet (Car2X) • Car2Infrastruktur (Verkehrsleitsysteme, …) • Pay-as-you-drive • On Board Diagnose • Bordnetzarchitektur • Applikationen auf und mit Fahrzeugdaten	P				
Quantencomputer • Hohe Rechengeschwindigkeit • Quantenkryptographie	F	F	F	F/P	P
Industrie 4.0 • Logistik 4.0 • Services und Objekte in der Cloud • Autonome Cyberphysische Systeme • Avatare (über Smart Devices und Wearables) • Internet der Dinge • Dialog zwischen Produkt und Maschine • 3D-Drucker	F/P	F/P	F/P	P	

Legende

Forschungsstadium
Produkt

Baden-Württemberg
LANDESKRIMINALAMT

Entwicklungen	Gegenwart	2 Jahre	5 Jahre	10 Jahre	20 Jahre
Software Defined Networking • Bedarfsbasierte Bandbreitenanforderung • Trennung von Logik und Weiterleitung	F/P	P			
„Passive“ Robotik • Fertigung • Exploration menschenfeindlicher Umgebungen • Medizin (invasive Eingriffe) • Militär • Auch Exoskelette	P				
„Aktive“ Robotik • Assistenz, Partner des Menschen • Assistenz, Partner des Roboters • Verhaltensbasierte Robotik • „denkende Maschinen“ • Androiden	F	F	F	F/P	P
Big Data • Prognose Techniken (in Medizin, Gesellschaft und Finanzwesen) • DataScientist	F/P	P			

Entwicklungen	Gegenwart	2 Jahre	5 Jahre	10 Jahre	20 Jahre
Digitale Währungen • BitCoin • Ripple	F/P	F/P	P		
Nanotechnologien • Selbst-reinigende Materialen • Selbst-reparierende Materialien • Ultra-resistente Materialien • Medikamente	F/P	F/P	P		
Bildübertragung/Streaming • Bodycam • Carkamera • Soziale Medien • IP-gestützte Bildübertragung • Verkehrsüberwachung • Entwicklungen beim Fraunhofer Institut in Karlsruhe	P				
Virtuelle Realität • Avatare • VIPol • Produktentwurf • Virtuelle Räume	P				
Augmented Reality • Überlagerung mit Zusatzinformationen • Kombination von Realdaten mit virtuellen Daten	F/P	F/P	P		
Eigene Betriebssysteme • ReactOS • RedFlag Linux • Europäisches Betriebssystem	F/P	F/P	P		
Abrechnungs- und Nutzungsmodelle • Bodyleasing • Bedarfsgerechte Mobilität	P				

Legende

Baden-Württemberg
LANDESKRIMINALAMT

F orschungsstadium
P rodukt

Anmerkungen

- Innovations- und Produktzyklen (Wir sind zu langsam)
- Bedarf für eine Kriminalistik 4.0
- Forschungsbedarf Kriminologie 4.0
- Was kann/sollte zur Bekämpfung der Cybercrime finanziert werden ?
- Qualifizierungsoffensive Aus – und Fortbildung notwendig
- Zusammenarbeit im Alltagsgeschäft und in Sonderlagen zwischen IT-Spezialisten und Ermittlern (interdiszplinäres Vorgehen, Fallkonferenzen)
- Beweisführung wird immer professioneller (sachverständige Zeugen, Sachverständige)
- Beweisführung muss nachvollziehbar sein (Transformation in justizielle Prozesse)
- Akkreditierungs- und Zertifizierungsprozesse sind zwingend notwendig
- Zusammenarbeit zwischen Sicherheitsbehörden, Wissenschaft/Forschung, Wirtschaftsunternehmen und IT-Partnern muss deutlich intensiviert werden