Wie sicher ist meine Kommune?

Reiner Schmidt
Landesamt für Sicherheit in der Informationstechnik

Agenda

- Landesamt für Sicherheit in der Informationstechnik & Kommunen
- Daten und deren Wert
- Vorfälle
- Angriffsvektoren
- Kriminelle Dienste im Internet – Darknet
- Nach einem Sicherheitsvorfall und Notfallmanagement
- Lösungsansätze und Leistungen des LSI
- Kommunale Behördennetze und Allianzen

Das Landesamt für Sicherheit in der Informationstechnik (LSI)

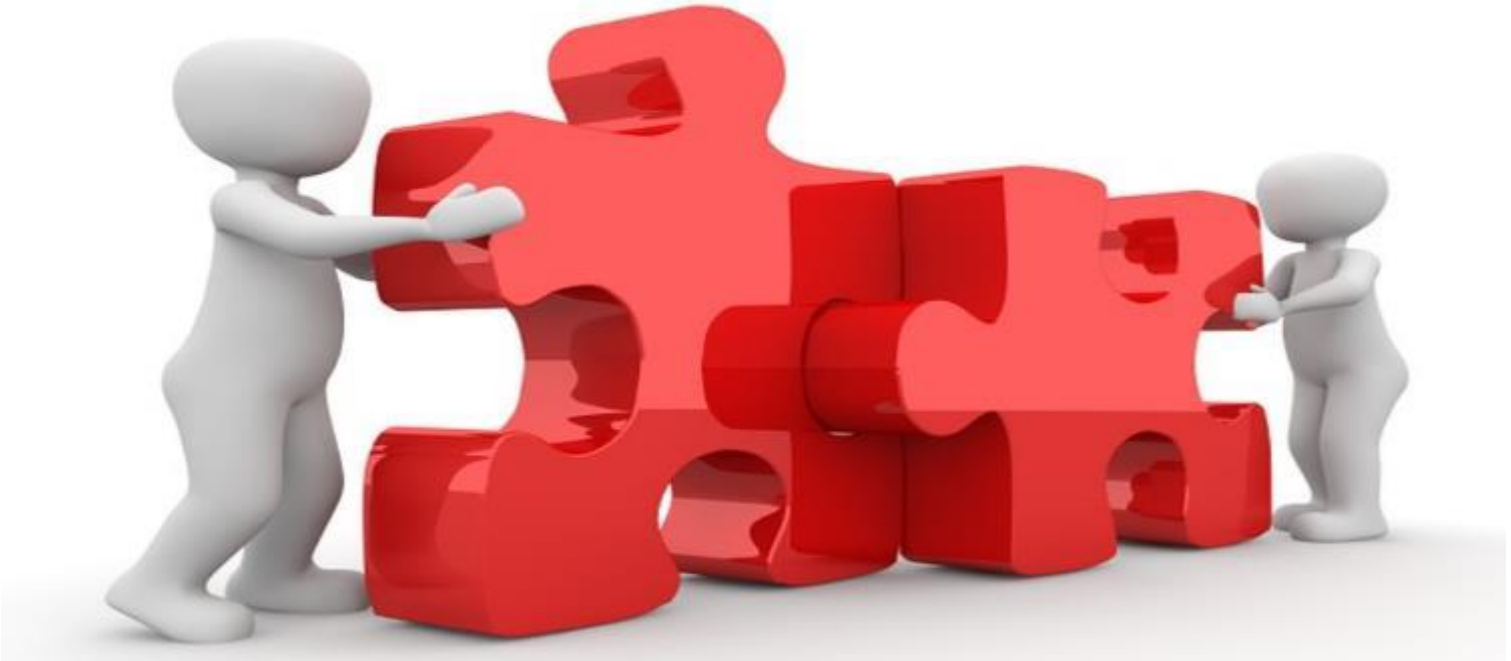
- Bayern erstes Bundesland mit eigenem Landesamt
- Gründungszeitpunkt: 01.12.2017
- Standorte:

Nürnberg

Ast. Bad Neustadt a.d.Saale

Ast. Würzburg

Das LSI = Partner der Kommunen



Kommunen

- Kommunen sind das Rückgrat unserer Gesellschaft

- In den Kommunen liegen die Kronjuwelen unserer Gesellschaft - Daten sind die Währung in der Informationsgesellschaft

Online Zugangsgesetz (OZG)

- Weit über hundert Fachanwendungen müssen in Kommunen betreut werden

- Alle diese Fachanwendungen müssen zusätzlich noch online und vor allem SICHER angeboten werden

Daten und deren Wert

Die Währung - Big Data

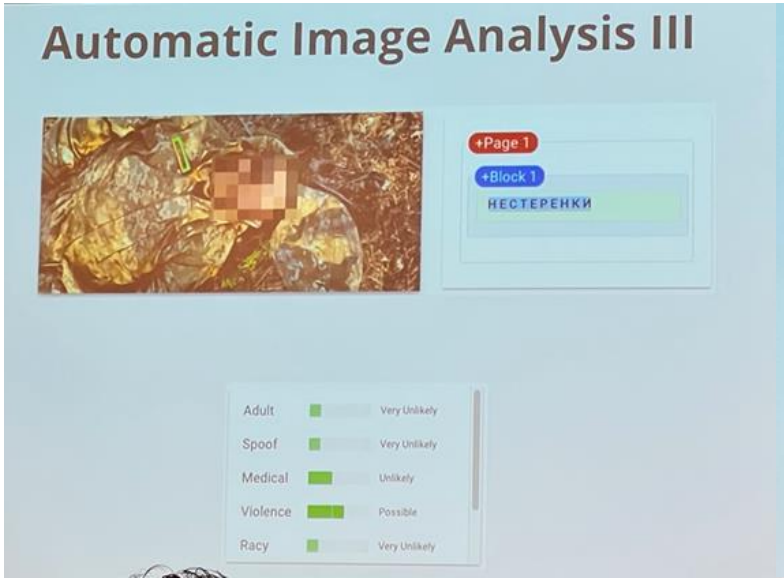
Was passiert in den Sozialen Medien?

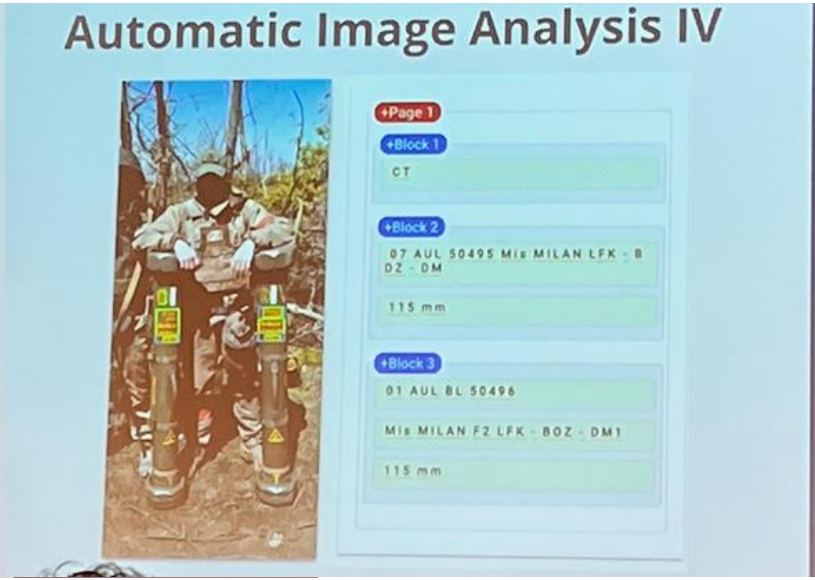
splunk>

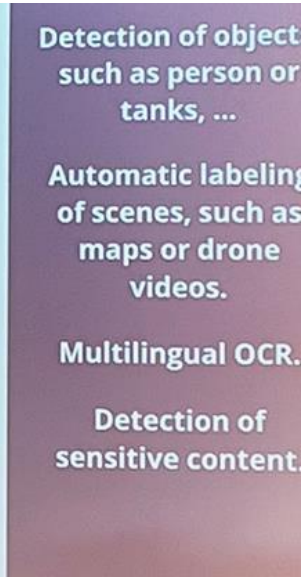
Log-Files
&
Graphen

23andMe.com
GesundheitsApp
Telemetriedaten

Auswertungen via Telegram (API)







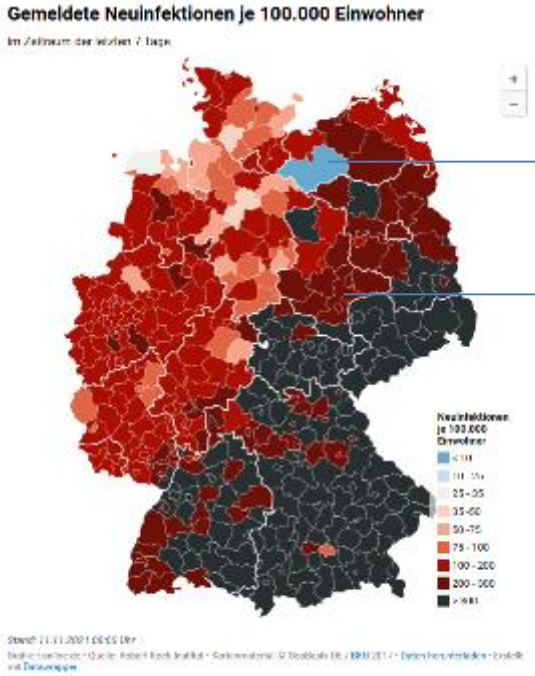
Die Einschläge (auch bei Kommunen) kommen näher - werden häufiger und heftiger

Satellitensystems KA-SAT

Quelle: https://www.golem.de/news/ukraine-krieg-satelliteninternet-ka-sat-ausgefallen-2202-163468.html
https://www.heise.de/news/Angriff-auf-Satellitennetzwerk-KA-Sat-Experten-suchen-nach-dem-Ursprung-6544706.html

- Ausfall des KA-SAT-Satellitennetzwerk Europa am 24. Februar um 4 Uhr UTC (Weltzeit)
- Betroffen: Ukraine, Deutschland, Griechenland, Ungarn und Italien (Kollateralschäden)
- SAT-Modems gehen kaputt
- Modems von Ipcopter betroffen
  (stattet Feuerwehren und Rettungsdienste mit Satellitensystemen für die Notfallkommunikation aus)

Angriffsziel Landkreise



Landkreis Ludwigslust-Parchim (15.10.2021)
Gemeinsamen IT-Dienstleister mit Schwerin

Landkreis Anhalt-Bitterfeld (05.07.2021 – K-Fall 09.07.2021)

Nach Cyber-Angriff- Erreichbarkeit der Ämter der Kreisverwaltung per E-Mail

Nach dem Cyber-Angriff auf das Netzwerk der Kreisverwaltung wird am Montag (19.07.2021) der Notbetrieb aufgenommen. Das bedeutet, dass alle Ämter wieder per Mail kommunizieren sowie Mails empfangen und bearbeiten können. Die bisherigen E-Mail Kontakte, die auch auf dieser Homepage auf den Fachseiten zu finden sind, können nicht mehr benutzt werden!

Bis auf Widerruf gelten nachstehende E-Mail Kontakte.

Meldungen auf der Homepage vom 15.11.2021

Angriffsziel Kommunen

Services und Erreichbarkeit der Verwaltung: Was geht? Und wie?

Seit dem Hacker-Angriff am 17.10.2021 ist die Stadt [redacted] nur eingeschränkt erreichbar. Wie erreichen Sie uns?

- **Telefon**
  Die Telefonanlage ist wieder in Betrieb. Gespräche könnten aber noch ruckeln oder abbrechen. Bitte sprechen Sie nicht auf Anrufbeantworter. Manche ABs springen zwar an, aber die Nachrichten können nicht abgehört werden.
- **E-Mails**
  Emails funktionieren zur Zeit gar nicht.
- **Termine**
  Die Verwaltung hat auf ihre (Online-)Kalender keinen Zugriff und kann Ihnen deshalb Termine auch nicht absagen. Für Dienstleistungen, die schon wieder laufen, können telefonisch mit den zuständigen Ämtern Termine vereinbart werden.
- **Post**
  Bitte schreiben Sie an:

Angriffsziel Kommunen

Sie sind hier: Startseite > Hackerangriff auf das Rathaus

Hackerangriff auf das Rathaus

23. Mai 2022

Das Rathaus wurde Opfer … ren Schäden entstehen, waren wir … zu nehmen. Aus diesem Grund könn… ienste nur sehr eingeschränkt …erden.

…aben eine **Notfall** Email-Au…

unter der das Rathaus zu erreichen ist:

[redacted]@gmx.de

Diese bitten wir nur in dringenden Fällen zu verwenden.
Sobald die Sicherheit wiederhergestellt ist, werden wir wieder zum Normalbetrieb zurückkehren.

Wir bitten um ihr Verständnis.

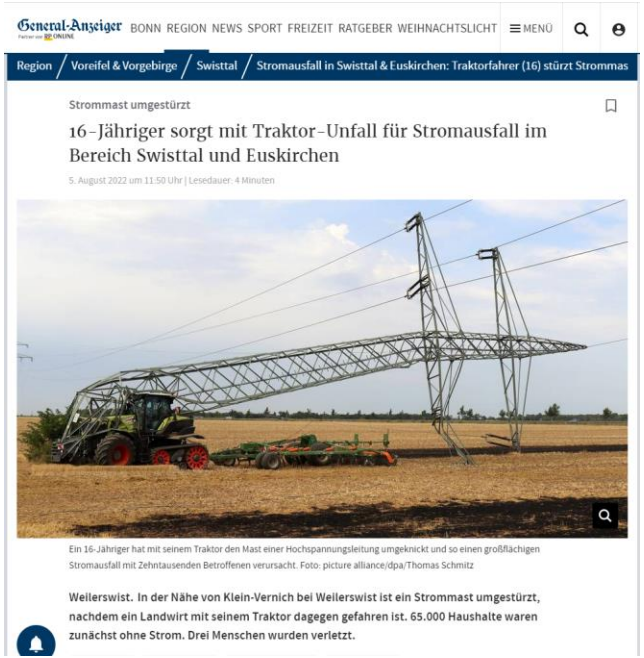
Zwischen Mai und Juni 2022 sieben kommunale Sicherheitsvorfälle

Technische und organisatorische Defizite

Wie ist es bestellt um:

- Heiraten
- Geburten und Sterbefälle
- Einwohnerwesen - Pass
- Rechnungen
- Gehälter
- Vergabeverfahren
- Wahlen
- Wirtschaftsförderung
- Termine und Termintreue
- …

Stromausfall Swisttal und Euskirchen



General-Anzeiger BONN REGION NEWS SPORT FREIZEIT RATGEBER WEIHNACHTSLICHT ≡MENÜ

Region / Voreifel & Vorgebirge / Swisttal / Stromausfall in Swisttal & Euskirchen: Traktorfahrer (16) stürzt Strommas

Strommast umgestürzt

16-Jähriger sorgt mit Traktor-Unfall für Stromausfall im Bereich Swisttal und Euskirchen

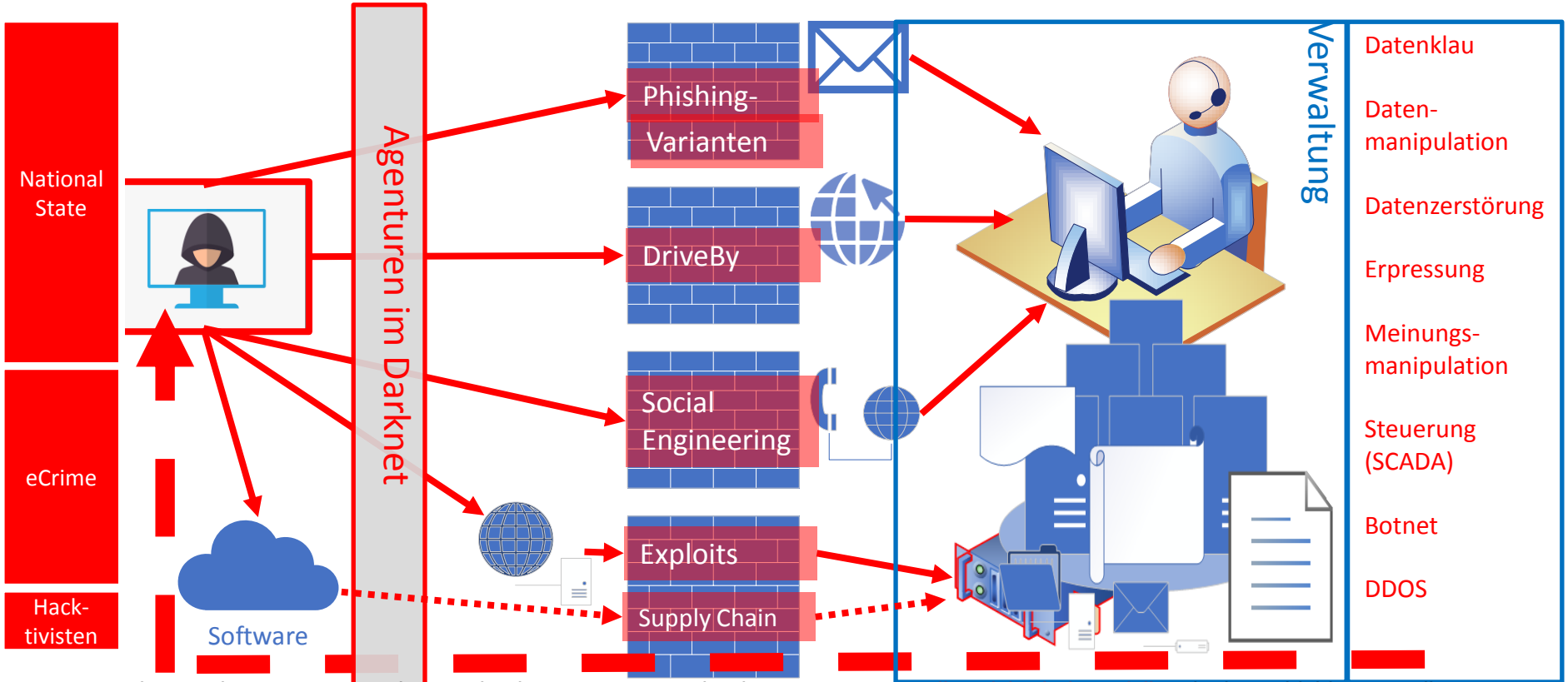
5. August 2022 um 11:50 Uhr | Lesedauer: 4 Minuten

Ein 16-Jähriger hat mit seinem Traktor den Mast einer Hochspannungsleitung umgeknickt und so einen großflächigen Stromausfall mit Zehntausenden Betroffenen verursacht. Foto: picture alliance/dpa/Thomas Schmitz

Weilerswist. In der Nähe von Klein-Vernich bei Weilerswist ist ein Strommast umgestürzt, nachdem ein Landwirt mit seinem Traktor dagegen gefahren ist. 65.000 Haushalte waren zunächst ohne Strom. Drei Menschen wurden verletzt.

Angriffsvektoren

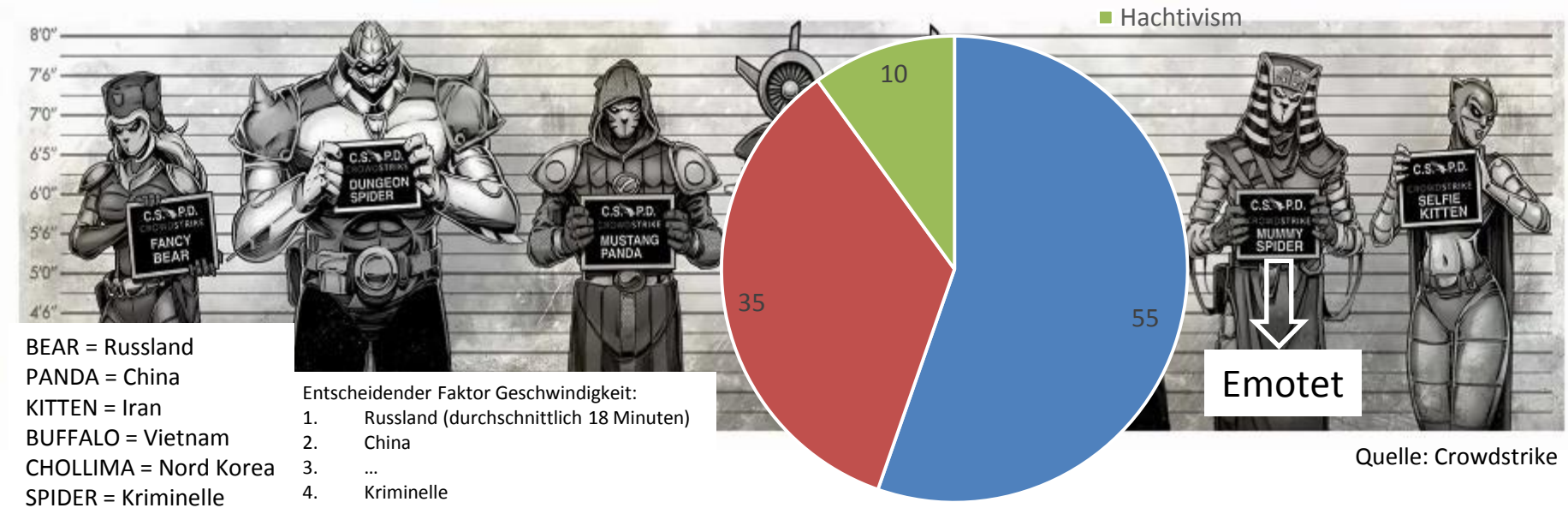
Angriffsvektoren



Laut dem Verizons Data Breach Investigations Report 2020 beginnen 96 Prozent aller Sicherheitsvorfälle mit einer Phishing-E-Mail

Kriminelle Dienste im Internet - Darknet

Über 140 professionelle Gruppen aktiv



BEAR = Russland
PANDA = China
KITTEN = Iran
BUFFALO = Vietnam
CHOLLIMA = Nord Korea
SPIDER = Kriminelle

Entscheidender Faktor Geschwindigkeit:

1. Russland (durchschnittlich 18 Minuten)
2. China
3. …
4. Kriminelle

Quelle: Crowdstrike

Staatliche Akteure

GRU – Militärischer Geheimdienst

SVR - Auslandsgeheimdienst

FSB- Inlandsgeheimdienst

STRONTIUM / APT28
➔ Datendiebstahl / Phishing
IRIDIUM / Sandworm
➔ Datenzerstörung

NOBELIUM
➔ Phishing

ACTINIUM / Gamaredon
➔ Datendiebstahl / Phishing
BROMINE / EnergeticBear
➔ Datendiebstahl
KRYPTON / Turla
➔ Aufklärung / Phishing

Ausschnitt krimineller Dienste im Darknet

Infection as a Service
Ransomeware as a Service
Malware as a Service

Service	Preis in US $ (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner		
▪ **Desktop-Version**	1.000 - 10.000 $	bei Kauf
▪ **Mobile-Version**	1.000 - 10.000 $	bei Kauf
RAT (Remote Administration Tool)	60 - 530 $ ca. 3.000 $	pro Monat bei Miete bei Kauf
Mining Bots	50 – 150 $	pro Monat bei Miete
Crypting	0 - 100 $ 30 - 500 $	bei Kauf von einem Crypt bei einem Wochen-Abo mit 50 Crypts pro Tag
DDoS-as-a-Service	80 - 1.500 $	pro Monat bei Miete
Bulletproof Hosting		
▪ **Shared**	5 - 50 $	pro Monat bei Miete
▪ **Dedicated**	50 - 700 $	pro Monat bei Miete
Counter-AV-Service	10 $	pro Monat und 300 Scans
Infection-on-Demand (Phishing-Services o.ä.)	Ab 100 $	pro Monat
Stealer Logs	5 -15 $ 400 – 900 $	pro Stück pro Monat für Abonnement

Quelle: BKA – Bundeslagebild Cybercrime 2021

Akteur Conti

Quelle:
https://www.heise.de/news/FBI-gibt-Hilfestellung-zur-Erkennung-von-Lockbit-Befall-6355209.html

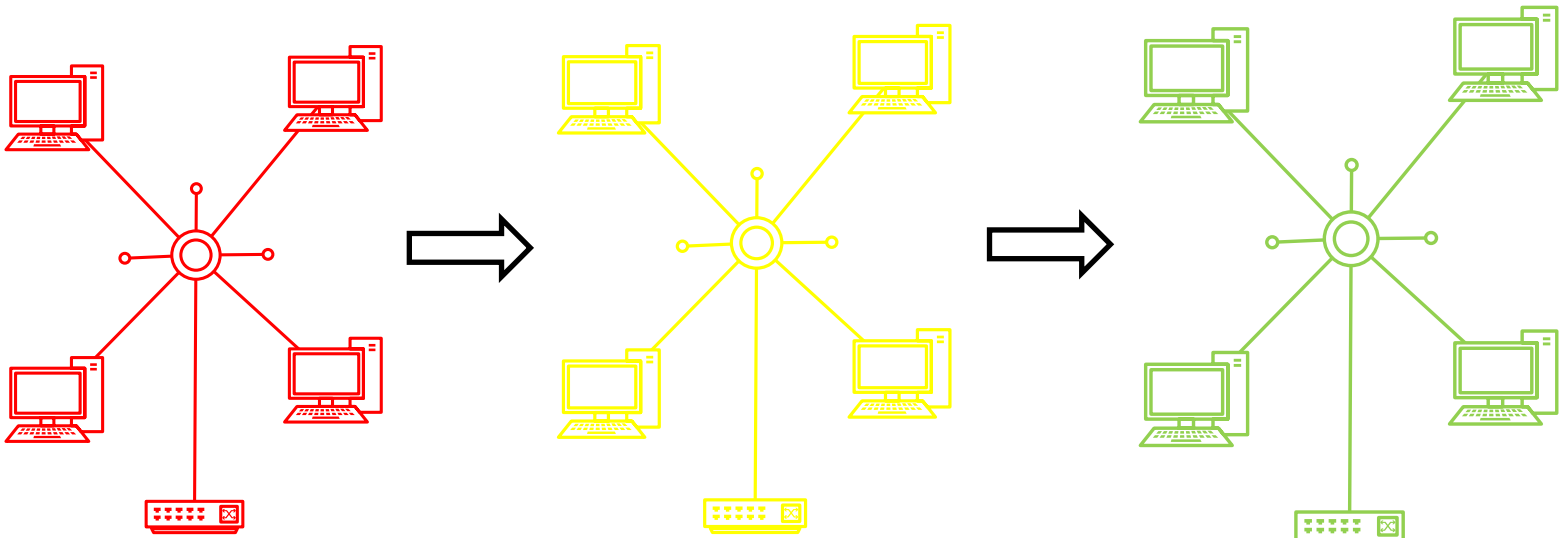
Bug Bounty
Fehlerprämie

- Wizard Spider
- Conti-Ransomware seit 2020
- Nachfolger von Ryuk
- St. Petersburg
- Ransomware direkt aber auch via RaaS
- Konkurrent Lockbit mit identischem Geschäftsmodell

- Offene Unterstützung für Russland ausgesprochen
  ➔ 60,000 Messages interne Chat-Logs wurden am 27.02.2022 geleaked (Unterstützer der Ukraine)

Nach einem Sicherheitsvorfall

Nach einem Sichereheitsvorfall



Betroffenes Netz

Säuberungs Netz

Ziel Netz

Lösungsansätze

Allgemeine Empfehlungen

- Orientierung am Stand der Technik
- Organisatorische Maßnahmen
- Investition in IT-Sicherheit
- Informationssicherheitsmanagementsysteme
- Stärkung der menschlichen Firewall
- Resilienz

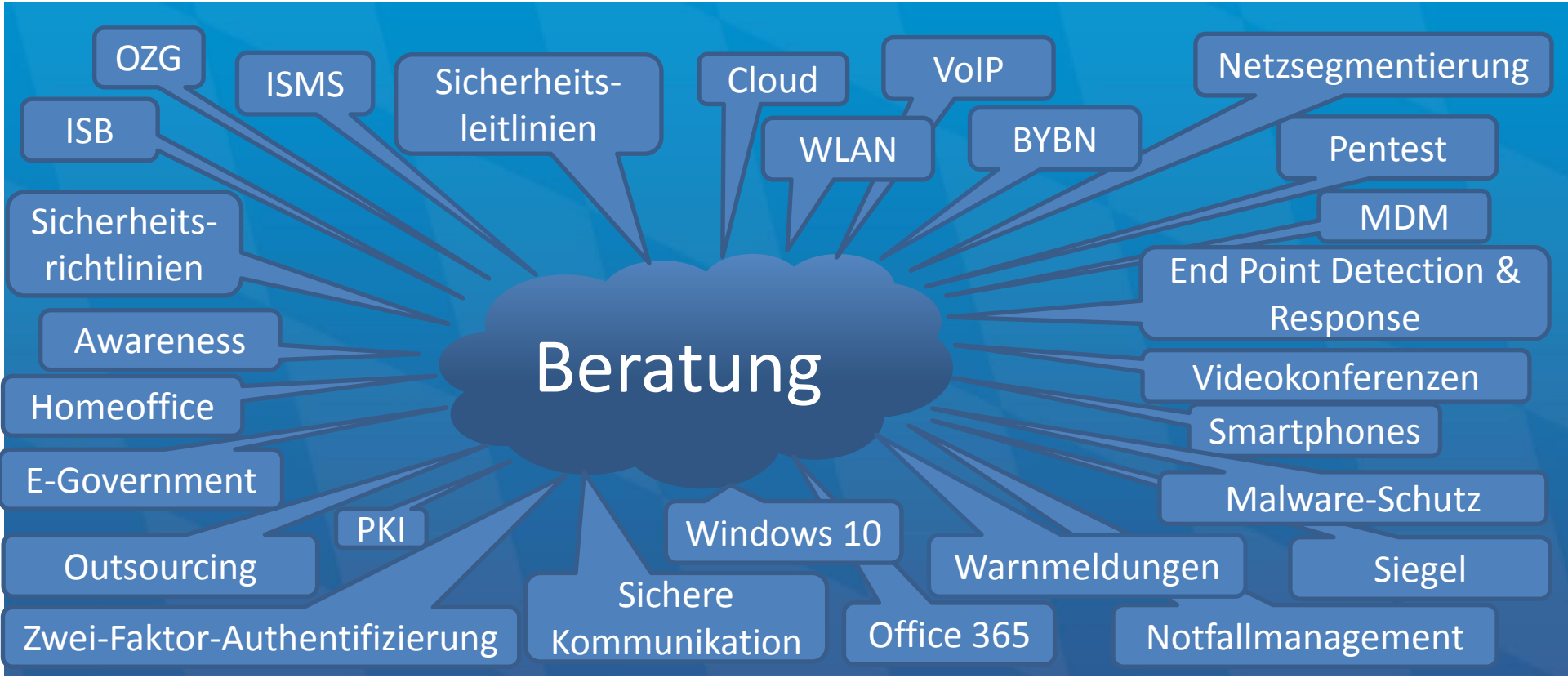
Resilienz

- Netzsegmentierung (Brandabschnitte)
- Offline Backup
- Malwareschutz
- Endpoint Detection & Response
- Patchmanagement
- Firewall MIT Regeln
- Awareness
- …

- ISMS
- Notfallmanagement

- Organisation

Leistungen des LSI


Beratung
OZG
ISMS
Sicherheits-
leitlinien
Cloud
VoIP
Netzsegmentierung
ISB
WLAN
BYBN
Pentest
Sicherheits-
richtlinien
MDM
End Point Detection &
Response
Awareness
Videokonferenzen
Homeoffice
Smartphones
E-Government
Malware-Schutz
PKI
Windows 10
Outsourcing
Warnmeldungen
Siegel
Sichere
Kommunikation
Office 365
Zwei-Faktor-Authentifizierung
Notfallmanagement

Siegel „Kommunale IT-Sicherheit“

Was haben gerade kleine bayerische Gemeinden, Märkte und Städte vom Siegel „Kommunale IT-Sicherheit“ des LSI?

BayDiG
Art. 43 Abs. 1 Satz 2

- Beleg der **gesetzeskonformen Einführung** eines Informationssicherheitskonzeptes
- Feedback und **Beratung des LSI** zu TOMs und kontinuierlicher Verbesserung
- Sicheren IKT-Einsatz **Bürgern gegenüber** darstellen
- Verwendung des Siegel über **2 Jahre** (z.B. auf Homepage)

KOMMUNALE IT-SICHERHEIT

Stadt Musterhausen

vertreten durch

Herrn Ersten Bürgermeister
Dr. Max Mustermann

hat das
Siegel Kommunale IT-Sicherheit
des Landesamtes für Sicherheit in der Informationstechnik erworben.

Die Stadt misst der Informationssicherheit hohen Stellenwert bei und hat ein Konzept für Informationssicherheit nach BayEGovG erstellt.

Als Beauftragte(r) für Informationssicherheit (ISB) ist ernannt

Frau Eva Musterfrau

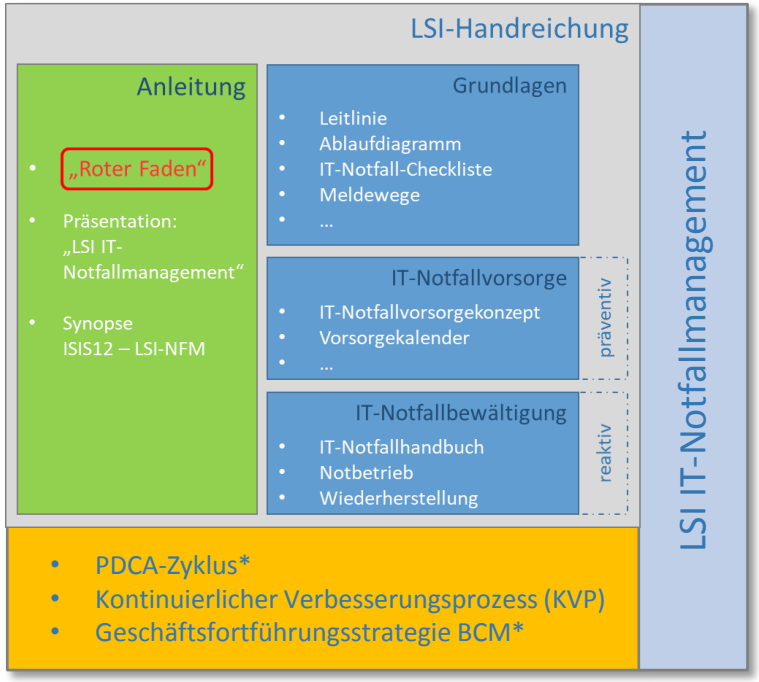
Geltungsbereich: Bacon ipsum dolor sit amet doner meatball jowl short ribs, chicken prosciutto salami frankfurter. Pig drumstick turducken short ribs, brisket meatloaf
Gültig bis: 1. Januar 2021

Nürnberg, Datum

Daniel Kleffel, Präsident
Landesamt für Sicherheit in der Informationstechnik

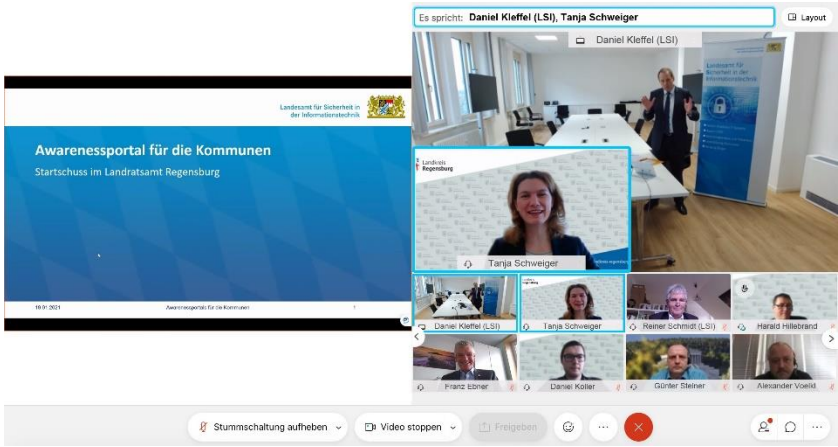
LSI Notfallmanagement

- Regelungen zum Ausrufen eines Notfalls, Alarmierungspläne, Notbetrieb, Wiederanlauf und der Nacharbeit.
- Notfallhandbuch, Vorlagen für Notfallkarte, Vorsorgekalender, Notfall-Checkliste und Pressemitteilungen.
- Vorlagen und Dokumente sind an das eigene Design anpassbar.

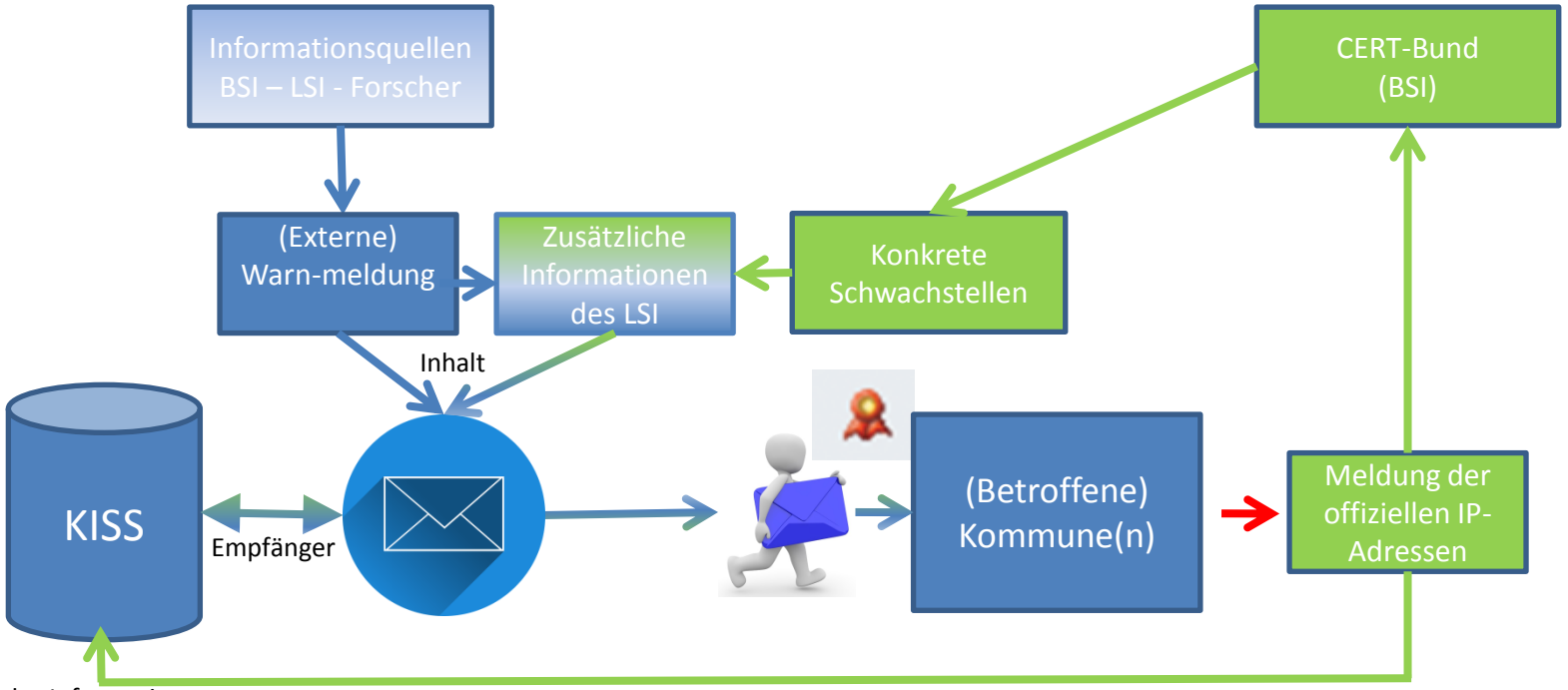


LSI Sensibilisierungskurse

- Kostenlose Sensibilisierungskurse für alle kommunalen Verwaltungen (Gemeinden, Märkte, Städte, Landratsämter und Bezirke)
- Didaktisch hochwertigen Kurse zur regelmäßigen Schulung des Personals
- Basis- und Aufbaukurse
- Teilnahme-Zertifikat kann als Nachweis ausgedruckt werden.
- Portal und Dokumente sind an das eigene Design anpassbar (Logo/Wappen, farbliche Anpassung)



Warn- und Informationsdienst



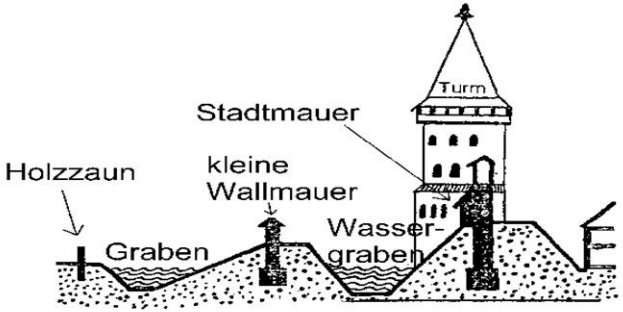
KISS = Kommunales Informationssystem

MISP - Malware Information Sharing Platform

- Sammlung, Zusammenfassung und Referenzieren von IoCs
- Anreicherung zusätzlicher Infos durch das LSI
- TLP: Green
  - nicht öffentliche Informationen
- Nur übers Behördennetz möglich
- Derzeit in Pilotierung

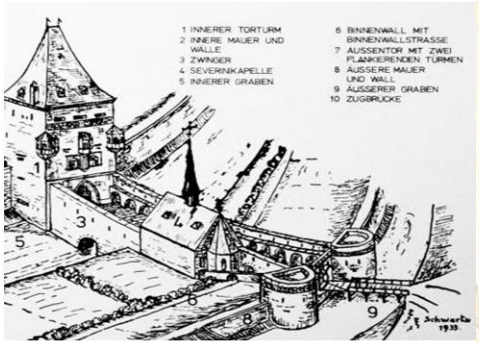
Weiter Empfehlungen

Verteidigungsanlagen



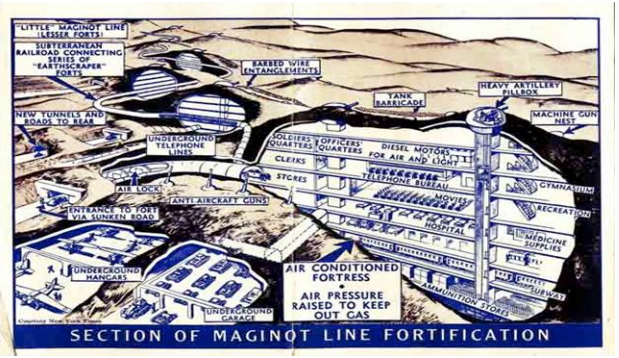
Quelle: http://ods.dokom.net/dortmund/verteidigung.html

Kleine Kommunen



Quelle: https://www.uni-muenster.de/Staedtegeschichte/portal/einfuehrung/aspekte/stadtbefestigungbildergalerie/index.html#Ringwallanlage

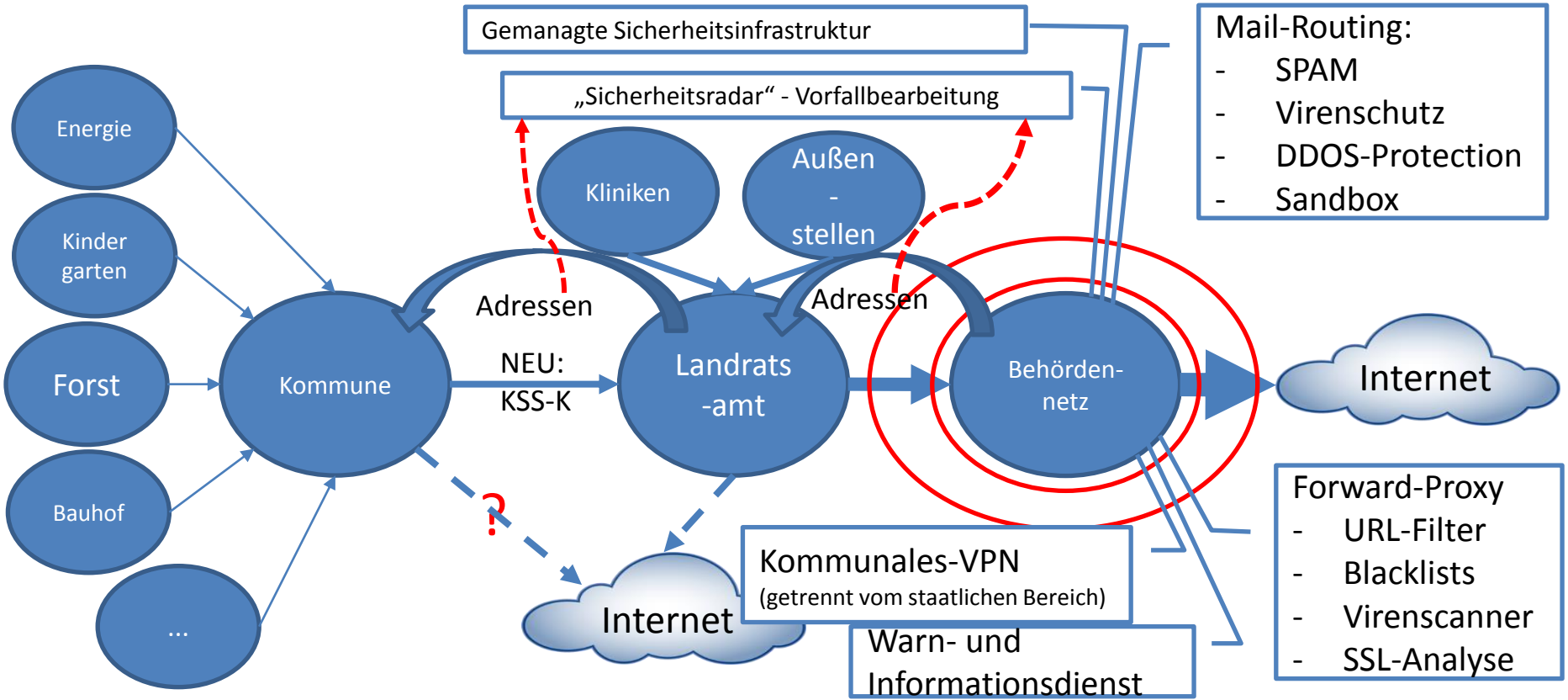
Städte Landkreise



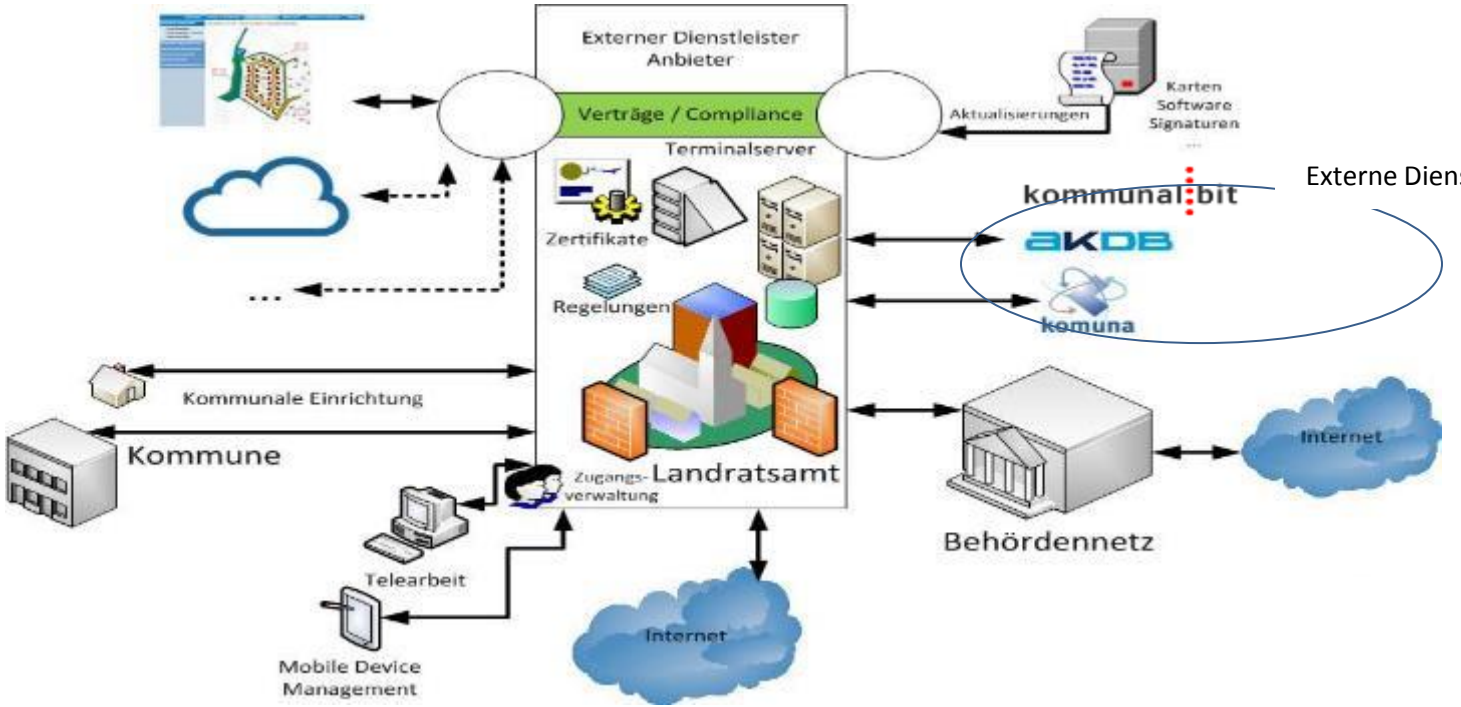
Quelle: https://tvtropes.org/pmwiki/pmwiki.php/UsefulNotes/MaginotLine

Große Städte Freistaat Bayern

Verteidigungsanlage Behördennetz



Kommunale Allianzen



Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Beratung für den kommunalen Bereich:

Beratung-Kommunen@lsi.bayern.de
Hotline: 0911 / 21549 - 523

Reiner.Schmidt@lsi.bayern.de
0911 / 21549 - 211