FRIEDRICH NAUMANN STIFTUNG Für die Freiheit.

Friedrich Naumann Stiftung

Staatsziel Digitale Transformation

Manuel ‚HonkHase' Atug

FRIEDRICH NAUMANN STIFTUNG Für die Freiheit.

Cyber-Krisenmanagement - Von Anhalt-Bitterfeld bis zur Ukraine

Manuel ‚HonkHase‘ Atug

Manuel (HonkHase) Atug

Head of Business Development bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- > 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für das IT-SiG 2.0 im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz

- Mitgründer der AG KRITIS: ag.kritis.info

AG KRITIS

- Mitgründer der AGND: www.agnd.eu

AGND

@HonkHase

Ich habe #KRITIS im Endstadium

Was sind die Ziele von Cybersicherheit?

- **Verfügbarkeit**

Autorisierte Benutzer werden am Zugriff auf Informationen und Systeme behindert

- **Integrität**

Die Korrektheit der Informationen und der Funktionsweise von Systemen ist nicht mehr gegeben

- **Vertraulichkeit**

Vertrauliche Informationen werden unberechtigt zur Kenntnis genommen oder weitergegeben

*BSI Grundschutz

Schutzziele für KRITIS

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

- Forschung im Bevölkerungsschutz - Band 28: „Definition von Schutzzielen für Kritische Infrastrukturen “
- 492 Seiten sektorspezifische Forschung zum Thema Schutzziele für KRITIS

Wie ist Cybersicherheit in Deutschland organisiert?

Europäische Kommission

Your Europe
European Union

Single Digital Gateway: Einheitliches digitales Zugangstor zu den Verwaltungsleistungen der EU und der Mitgliedstaaten

EU-Mitgliedsstaaten

EU-Fristen einhalten. EU-Anforderungen mitdenken. EU-Komponenten nachnutzen.

Funktioniert das?

Bundeskanzleramt

Bundeskanzlerin
Chef des Bundeskanzleramtes
Staatsministerin für Digitalisierung

Gruppe Digitalpolitik, IT-Steuerung

Beide Projekte perspektivisch verbinden.

Digital Service 4Germany

dit.bund
DIT ist Innovation

Bundesministerium des Innern, für Bau und Heimat

Der Beauftragte der Bundesregierung für Informationstechnik

Bundesinnenminister
CIO der Bundesregierung

Abteilung Digitale Gesellschaft

Reicht der politische Wille?

BKAmt und BMI verantworten und koordinieren Umsetzung.

Monitoring auf solide Grundlage stellen! Orientierung geben!

Konferenz der Regierungschefinnen und Regierungschefs der Länder

Ministerpräsidenten

Chefs der Staats- und Senatskanzleien

Reicht der politische Wille?

Es braucht ein echtes politisches Controlling!

Die Bundesregierung

Digitalkabinett

Digitalrat der Bundesregierung

Vorschläge müssen umgesetzt werden.

daten ethik kommission

z.B. IMK WMK 2019

Fachministerkonferenzen

Reicht die Unterstützung?

Die Bundesregierung

IT-Konsolidierung Bund

IT-Rat

Informationstechnikzentrum Bund

ITZ Bund

Leistungs- und Unterstützungsfähigkeit muss erhöht werden.

FITKO

Zu wenig Personal!

unterstützen konzeptionell und operativ

KoSIT

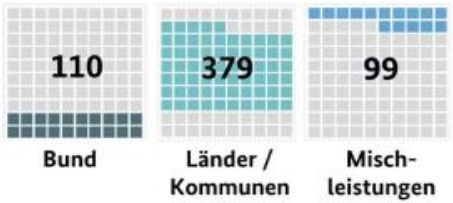
IT-Planungsrat

Bundes-CIO + Landes-CIOs
Kommunale Spitzenverbände

Zielsetzungen bis 2022

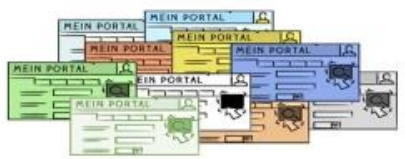
bis **2023**: Umsetzung **Single-Digital-Gateway-VO** (= EU-OZG)

1. Umsetzung der 588 **OZG-Leistungen**



2. Verknüpfung der Portale aller Ebenen zu einem **Portalverbund** (inkl. Servicekonten)

bund.de BETA
Verwaltung digital



Bundesministerien

AA | BK | BMAS
BMBF | BMEL | BMF
BMFSFJ | BMG | BMI
BMJV | BMU | BMVI
BMVG | BMWi | BMZ

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutzfragen zu Registern und Datencockpit klären.

Datenschutzfragen zu Registern und Datencockpit klären.

DSK Landes-Datenschützer

IT-Dienstleister der Länder & Kommunen

IT-Unternehmen, Start-Ups

Länder und Kommunen

294 Landkreise, ca. 11.000 Gemeinden

Deutscher Städtetag | DStGB | Deutscher Landkreistag

Prinzipien

Digital First
(digitale Verfahren als Regelfall)

Once Only
(Daten nur noch einmal angeben)

Transparenz verbessern!

Bund, Länder und Kommunen entwickeln gemeinsam Lösungen.

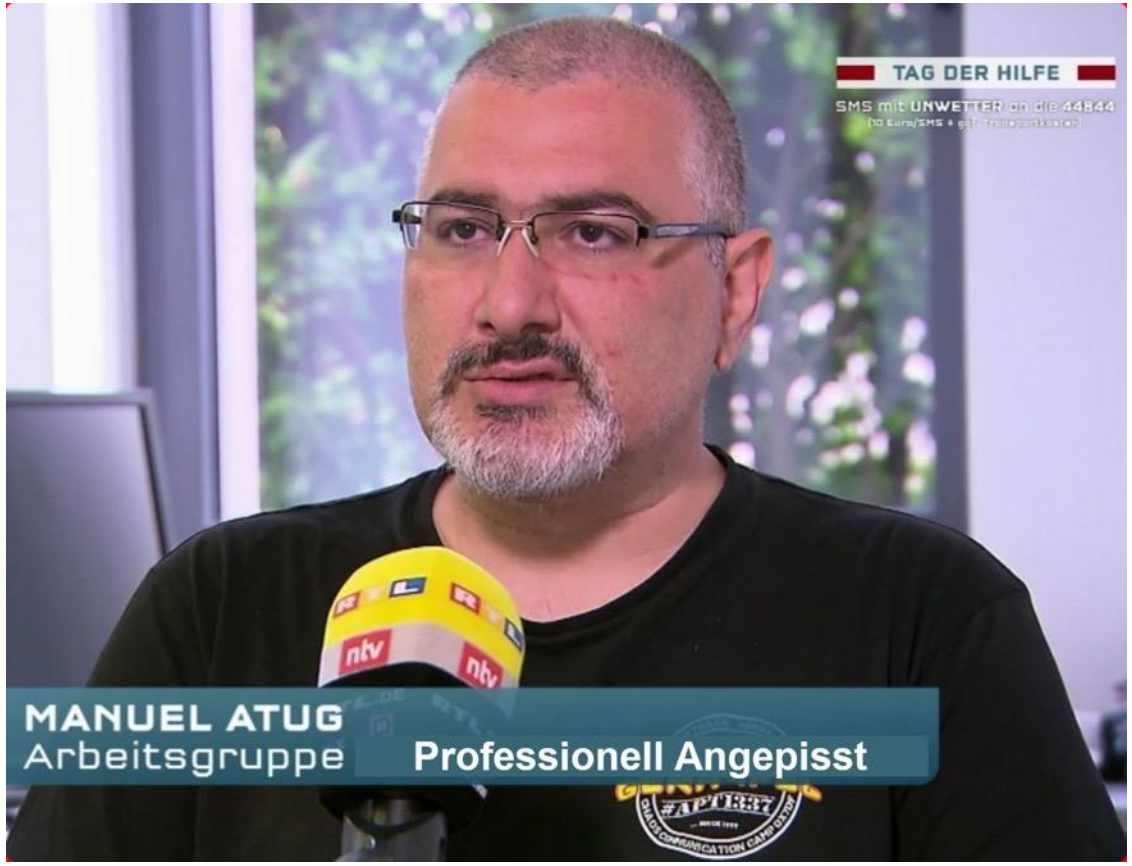
Privates IT-Know-How besser einbinden! FIT-Store-Konzept anpassen.

Bund gibt zusätzlich 3 Mrd. Euro!

Flächendeckung fraglich! Es bleiben nur noch 2 Jahre Zeit!

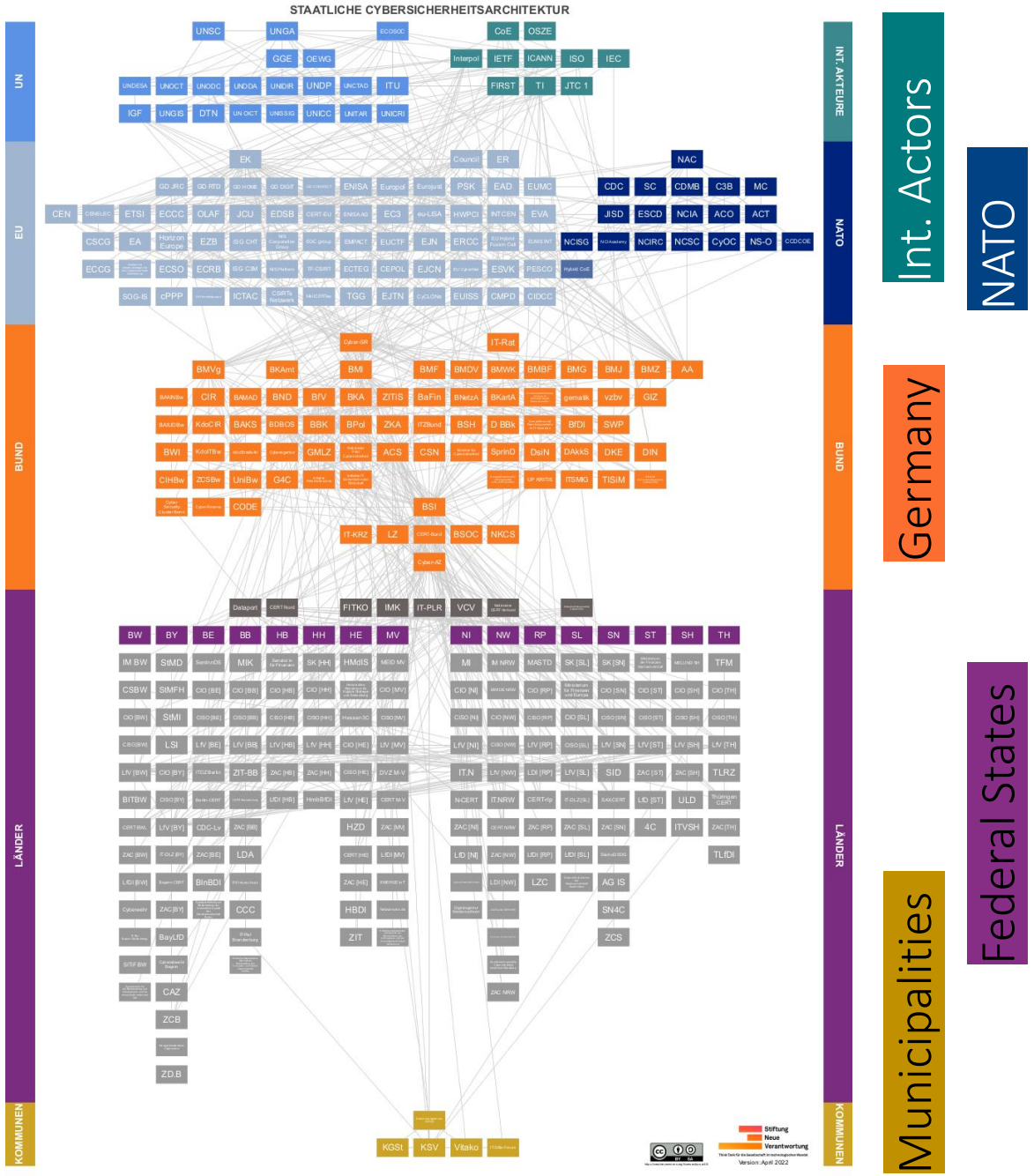
Sind alle nötigen Mittel eingeplant (**1,5 Mrd. Euro**)?

KRITIS Sektor Staat und Verwaltung digital handlungsfähig?



Die staatliche Cybersicherheitsarchitektur:

Errr… wait O_o



UN

Europe

Germany

Federal States

Municipalities

Int. Actors

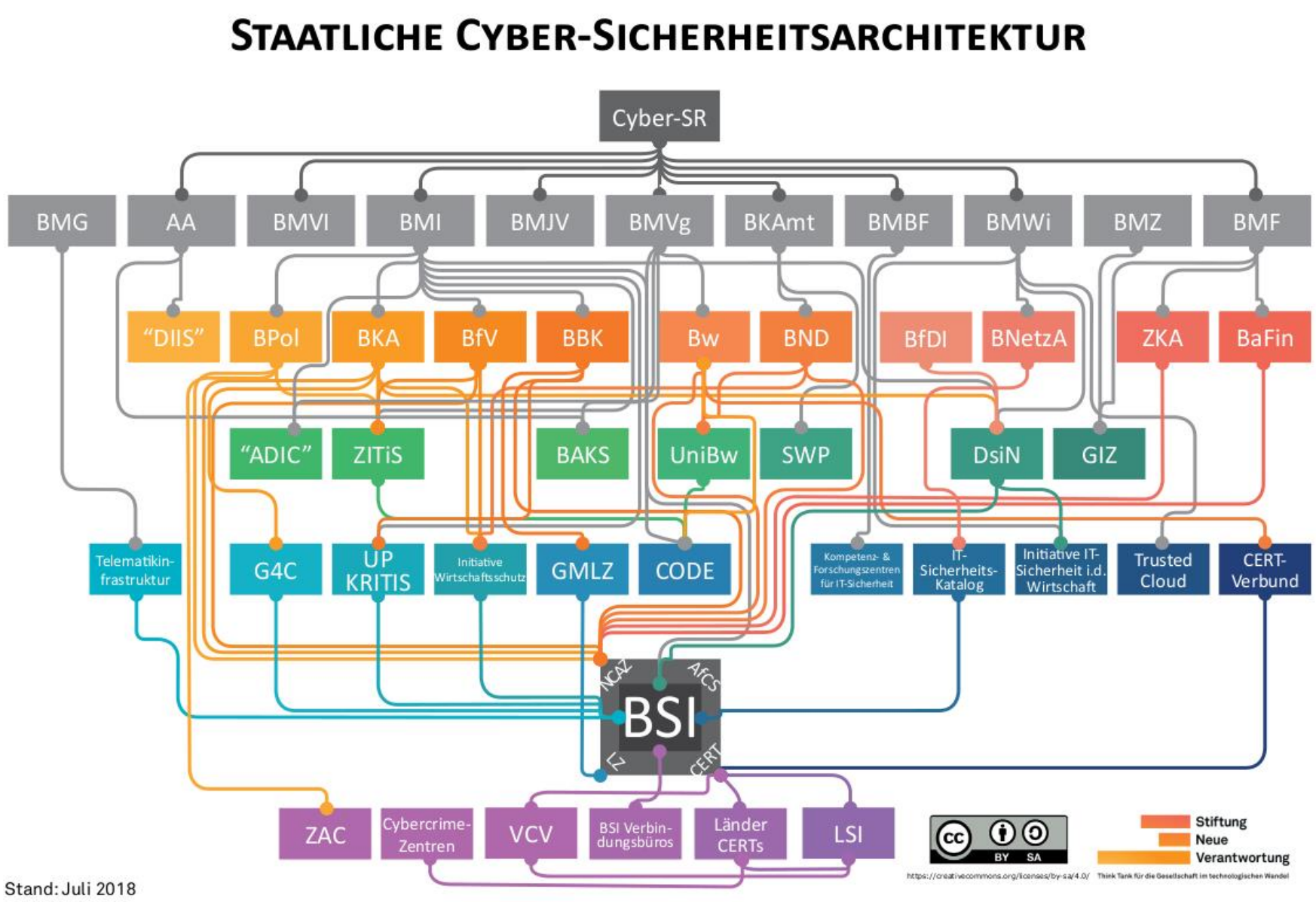
NATO

Germany

Federal States

Municipalities

2018 zum Vergleich



Cyberhotlines

Cyberhotline Berlin:

Die Cyberhotline der Digitalagentur Berlin
(**Werktags, 9 - 17 Uhr**)

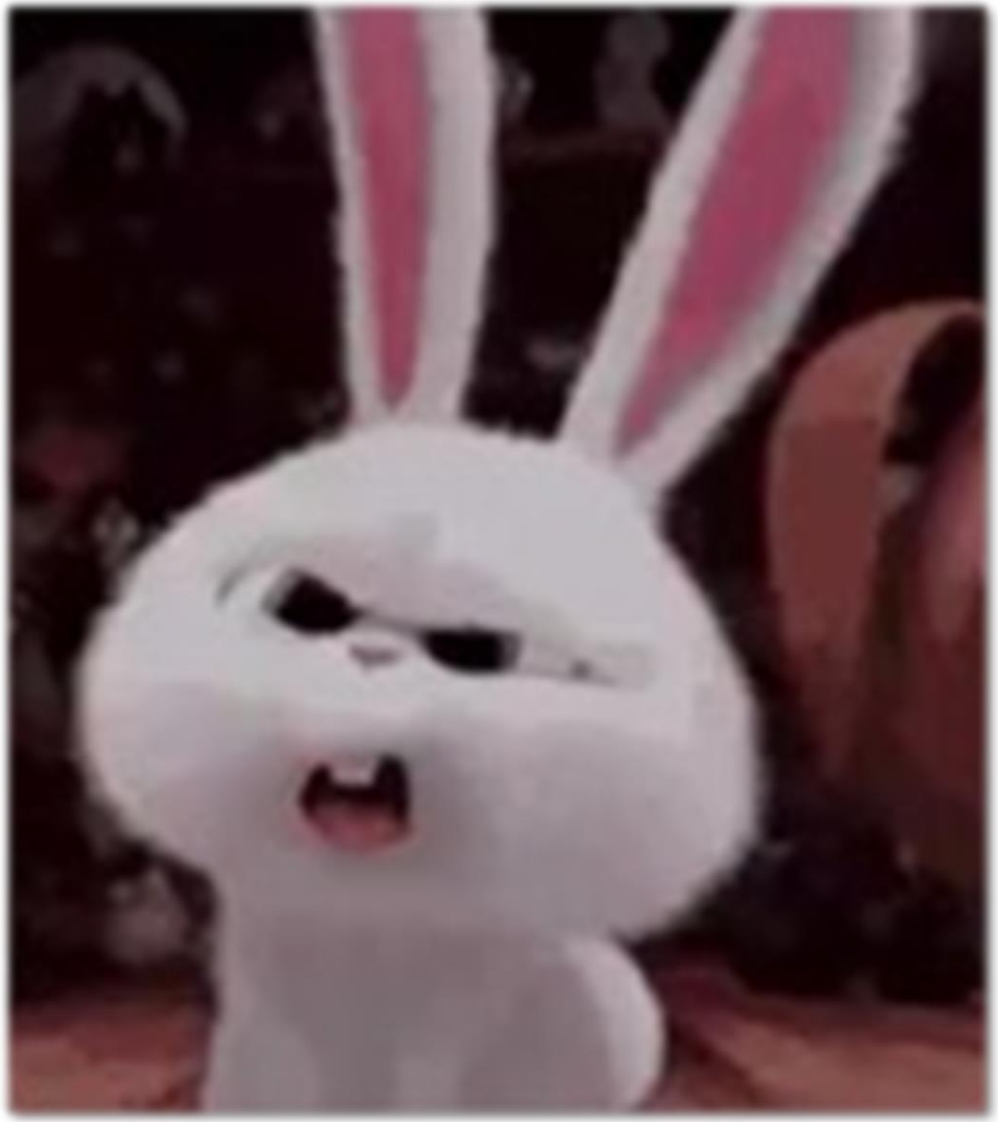
Cyberhotline Eurobits

Bochum, Essen und Gelsenkirchen
(**Werktags von 8 - 18 Uhr**)

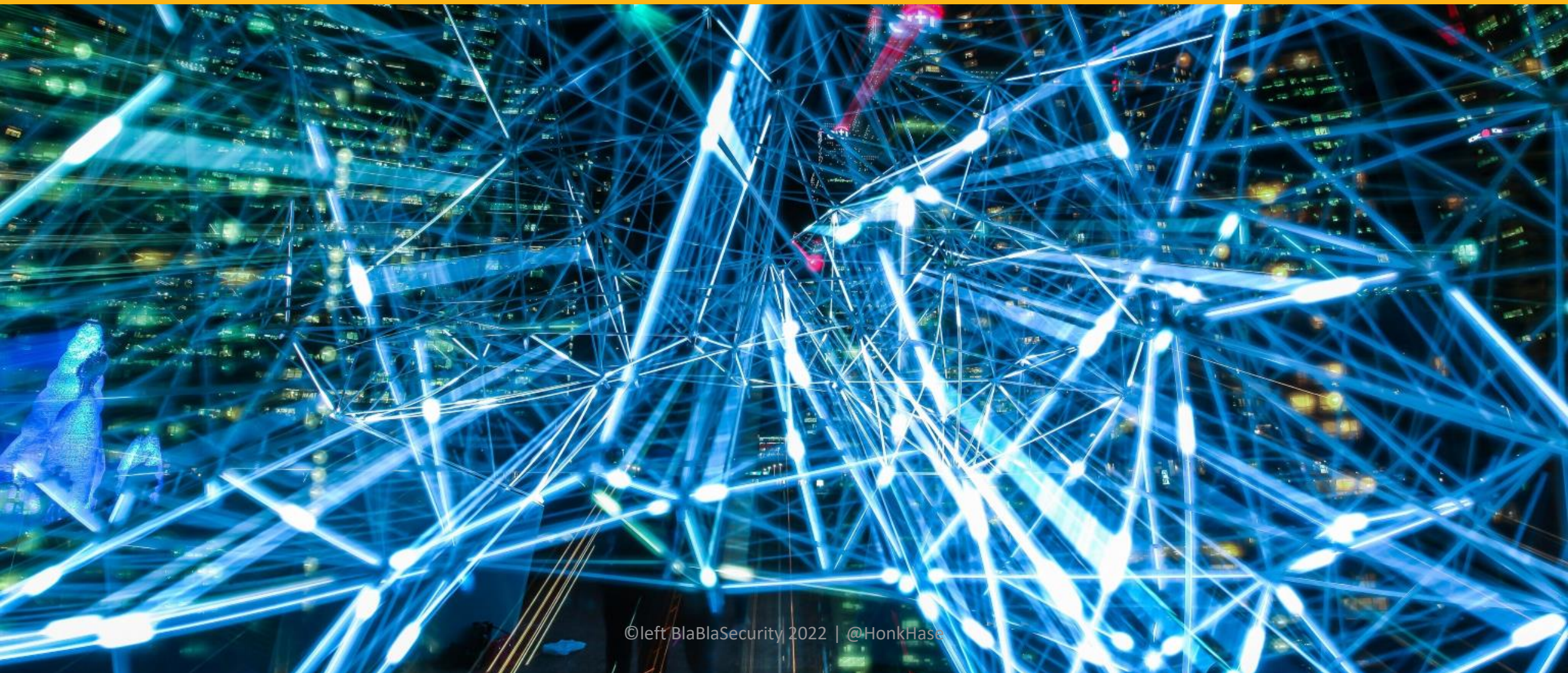
BSI Cyber-Sicherheitsnetzwerk

Bundesweite Hotline Nummer 0800-274 1000

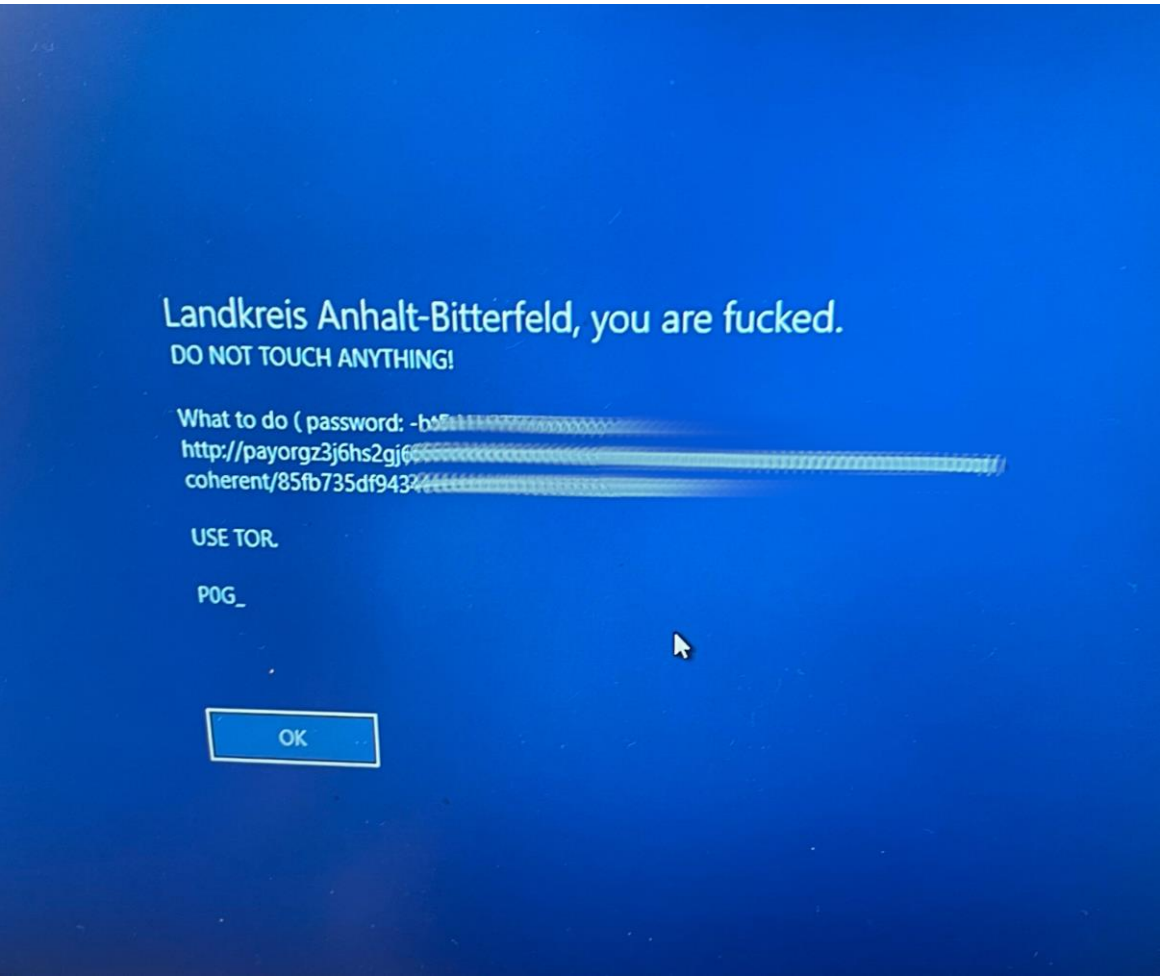
Das wird uns retten?!? O_o



Landkreis Anhalt-Bitterfeld



Cybercrime – Ransomware as a Service



Oder: Wie man viele hundert Millionen Dollar im Jahr macht!

- Alles vollverschlüsselt via Ransomware
- Über 1.000 Clients und Server an sieben Standorten
- ca. 160 Fachverfahren betroffen
- ca. 1 Jahr nicht arbeitsfähig
- Alle(!) Emails für immer weg und nicht wiederherstellbar
- Kosten von bisher über 2 Mio €
- Fachverfahren: Sozialabgaben vs KFZ-Zulassung

KRITIS in Putins Angriffskrieg gegen Ukraine

Ziel militärischer Cyber-Operationen im Hybrid Warfare

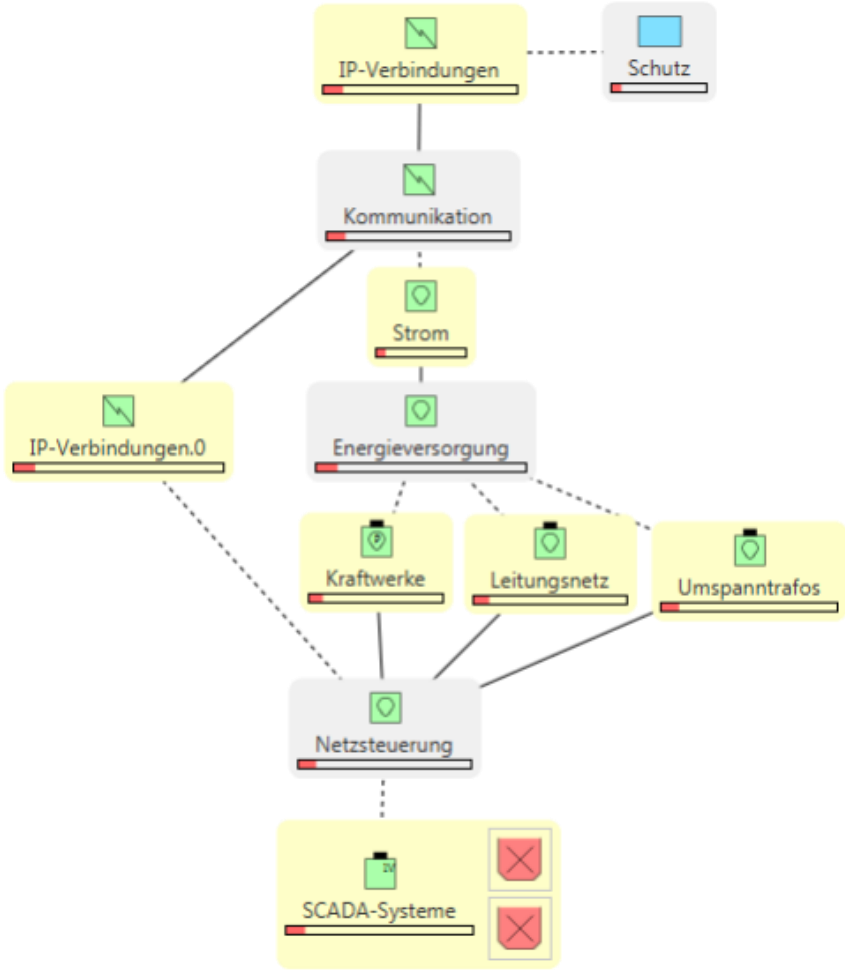
(durch militärischen Operationen „zur Aufklärung und Wirkung“)

- Cyber-Operationen
  - Spionage
  - Beeinträchtigung der Führungsfähigkeit
  - Sabotage Kritischer Infrastrukturen (KRITIS)
  - Defacement von regierungseigenen Webseiten und offiziellen Kommunikationswegen
  - Desinformation über soziale Medien
  - Blockade des nationalen Zugangs zum Internet

militärische Cyber-Wirkketten

(Theorie)

- **Cyberwirkung** löst häufig eine Kettenreaktion auf dem **Fähigkeits-Ressourcen-Netzwerk** aus
  - Angriff auf **SCADA-System** führt zum Ausfall der **Stromversorgung**
  - Ausfall der **Stromversorgung** führt zum Ausfall der **Telekommunikation**
  - Ausfall der **Telekommunikation** führt zum Ausfall/Einschränkung von **Schutzfunktion**



Es herrscht Krieg, aber ist das auch ein Cyberwar?

Cyberwar? Gübt’s hür nücht!

- Ja, das BMI nennt es „massive Cyberangriffe“
- Es waren eher Defacements und DDoS Angriffe auf Ministerien und Banken
- Joah, es gab auch 5 Wiper Angriffe
- KA-Sat Angriff auf Sateliten-Kommunikation
  ~30 Min Kommunikationsausfall
  Dafür Kollateralschäden:
  - ~30.000 Modems Offline
  - ~5.800 Windkraftanlagen ohne Remote Acces
  - Ausfall ELW2 Katastrophenschutz Fahrzeuge

Cyberwehr

Wir. Dienen. Neuland.

Aber es ist doch Züberkrieg!

Cyberwar? Äh nö sorry!

- Terabytes an Data Leaks russicher „Oligarchenfirmen“
- Conti Ransomware Group kooperiert mit dem FSB
  Best breed aus zwei Welten: Cybercrime & Geheimdienste
- Cyberwar vs Realität?
  - Cyberwar ist eher die bunte Powerpoint Foliengeschichte von Militärberatern, Rüstungsindustrie und zwielichtigen Securityproduktverkäufern
  - Realität ist ein permanentes Grundrauschen von Angriffen im Cyberraum
  - Dem einen Cyberraum für uns alle halt

©left BlaBlaSecurity 2022 | @HonkHase

Cyberwar vs. Realität

Der Cyberwar findet auf PowerPoint-Folien statt,
in der Realität ist es ein Krieg der Bomben und Granaten

Cyber Auswirkungen auf KRITIS?

Wie sehen also Cyber-typische Vorfälle im „Cyberwar“ aus?

- i.d.R. eher nicht langanhaltend, sondern temporär
- Wirtschaftliches Interesse (zB Ransomware)
- Spionage und Aufklärung
- Fake News und Propaganda

- Umfassende Kollateralschäden möglich, aber in der Risikoanalyse nicht kalkulierbar

Gibt es denn dann überhaupt Bedrohungen!?

- Digitalisierung?
  …schreitet bei KRITIS (langsam & schlecht) voran
- Ransomware wird mehr!
- Fachkräftemangel wird mehr!
- Naturereignisse werden mehr!

- Cyberwar-, Geheimdienste- & Hackback Szenarien bringen zukünftig mögliche Kollateralschäden

Cyberresilienz & Ausblick

- Ursache für eine Katastrophe ist für die Bevölkerung nicht relevant

- Aber: eine Krise (Pandemie) in der Krise (Putins Angriffskrieg) in der Krise (Ransomware) in der Krise (Gasmangellage) in der ***<beliebige Krise hier einfügen>*** braucht keiner!

- Kritische Fragen:

  → Ist Digitalisierung immer erforderlich? (ID Wallet, Luca App)

  →Können wir damit die Cyberresilienz von Produktionsumgebungen oder dem KRITIS Sektor Staat und Verwaltung erhöhen?

  →Was ist eine gute Digitalisierung?

Nachhaltigkeit in der Digitalisierung

- Bei der digitalen Transformationen verantwortungsvolle Maßnahmen einzuleiten und gewissenhaft durchzuführen, also zu operationalisieren, ist daher gleichsam eine technische wie ethische Aufgabe!

- Vermeidet daher technische Schulden an kommende Generationen

- Security by Design und Privacy by Design ist Menschenschutz

>> All-Gefahren-Ansatz <<

„Berücksichtigung aller Gefahrenarten (z. B. Naturgefahren, technologische Gefahren, etc.) im Rahmen des Risiko- und Krisenmanagements“

** Hallo BBK*

Und was mache ich, wenn alles nichts hilft?

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de