Thüringen zwischen Faxgerät und firesale - IT-Sicherheit in der Verwaltung

Madeleine Henfling (MdL)

Manuel ‚HonkHase' Atug

IT-Sicherheit der Kommunen

Manuel (HonkHase) Atug

Manuel (HonkHase) Atug

Principal bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- Weit über 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

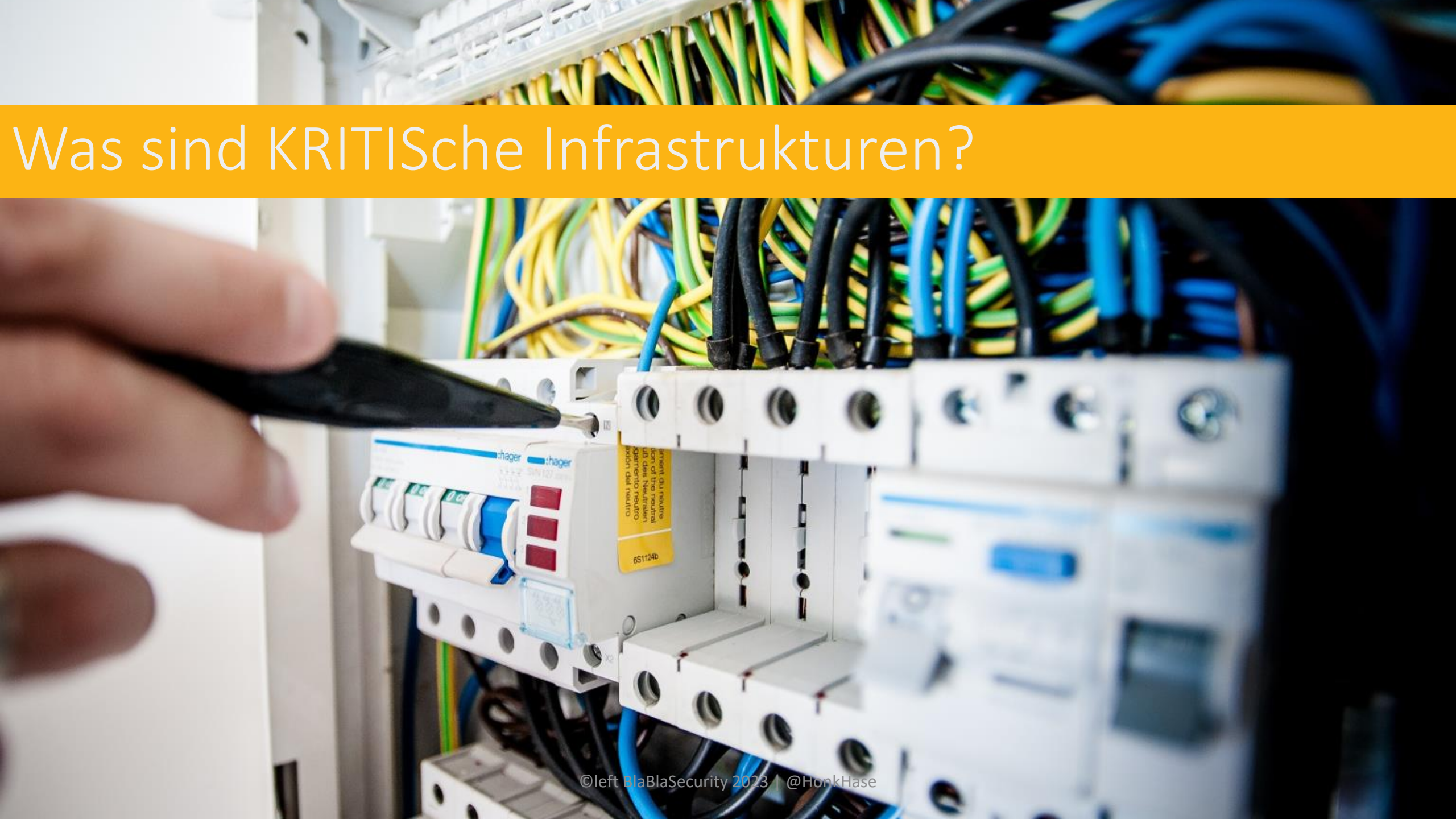
- Mitgründer der AG KRITIS: ag.kritis.info

- Mitgründer der AGND: www.agnd.eu

@HonkHase @HonkHase@chaos.social

Ich habe #KRITIS im Endstadium

Was sind KRITISche Infrastrukturen?



Die 10 Kritische Infrastrukturen Sektoren in Deutschland

Quelle https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html

Funktioniert das?

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.

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.

datenethikkommission

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

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

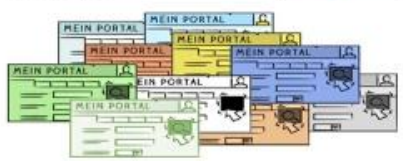
110	379	99
Bund	Länder / Kommunen	Misch-leistungen

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

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

bund.de BETA
Verwaltung digital

NAME@DE
LOGIN



Bundesministerien

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

Datenschutzfragen zu Registern und Datencockpit klären.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutzfragen zu Registern und Datencockpit klären.

DSK Landes-Datenschützer

IT-Dienstleister der Länder & Kommunen

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

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!

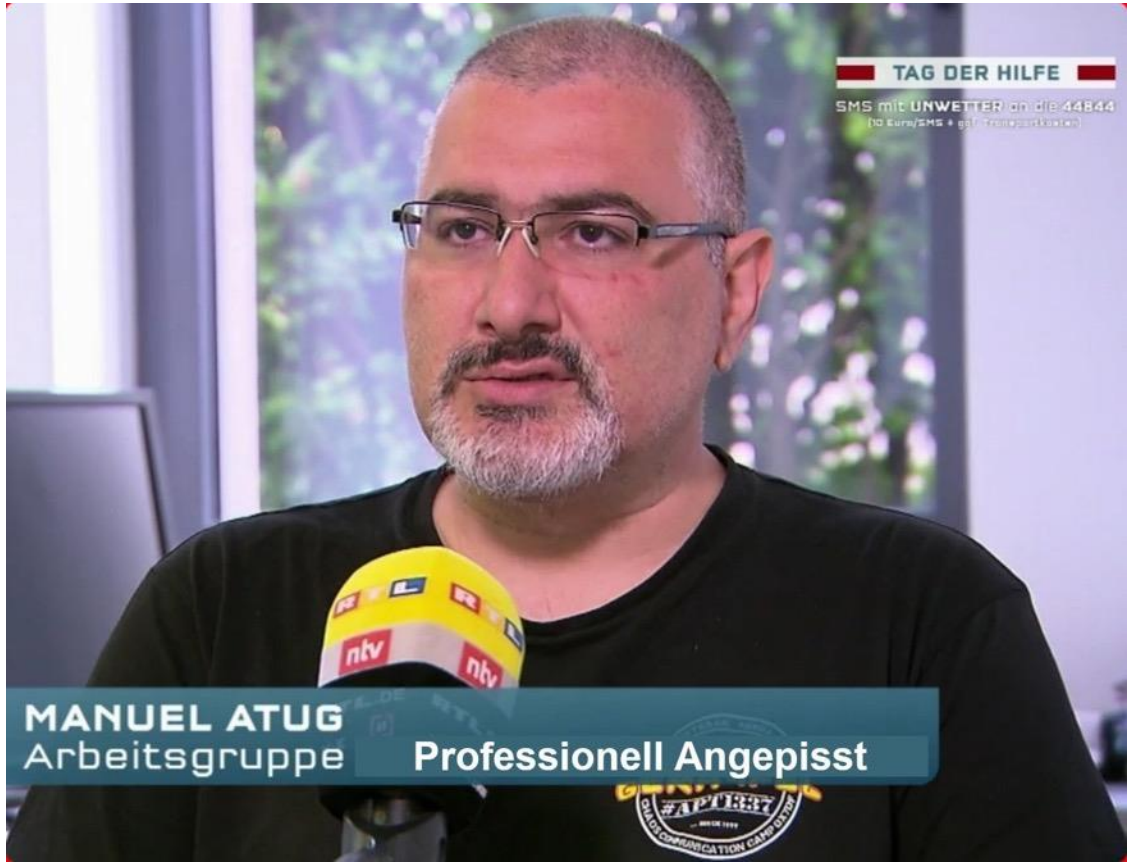
Bund, Länder und Kommunen entwickeln gemeinsam Lösungen.

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 Deutschlands ➔

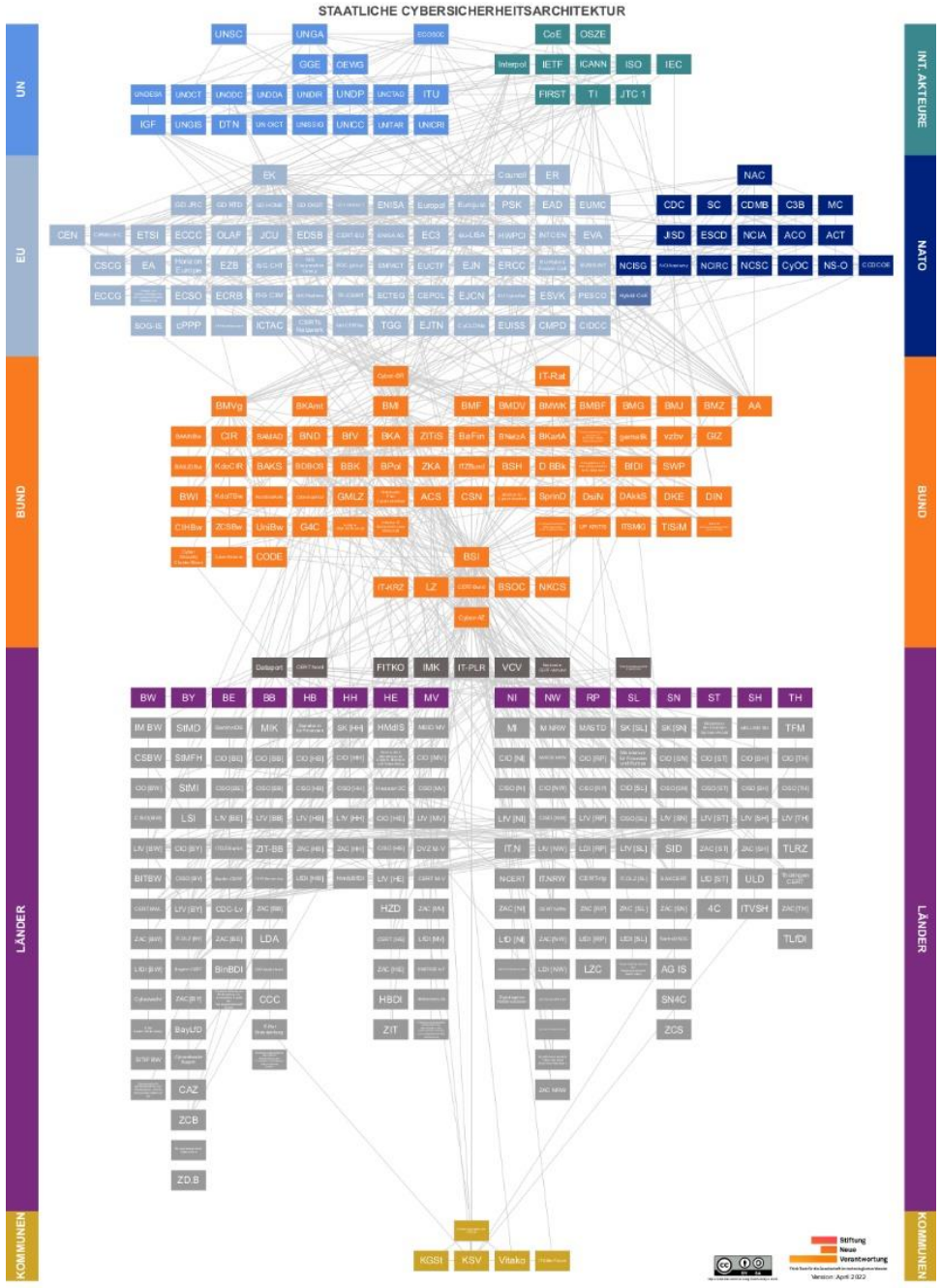
UN

Europe

Germany

Federal States

Municipalities



Int. Actors

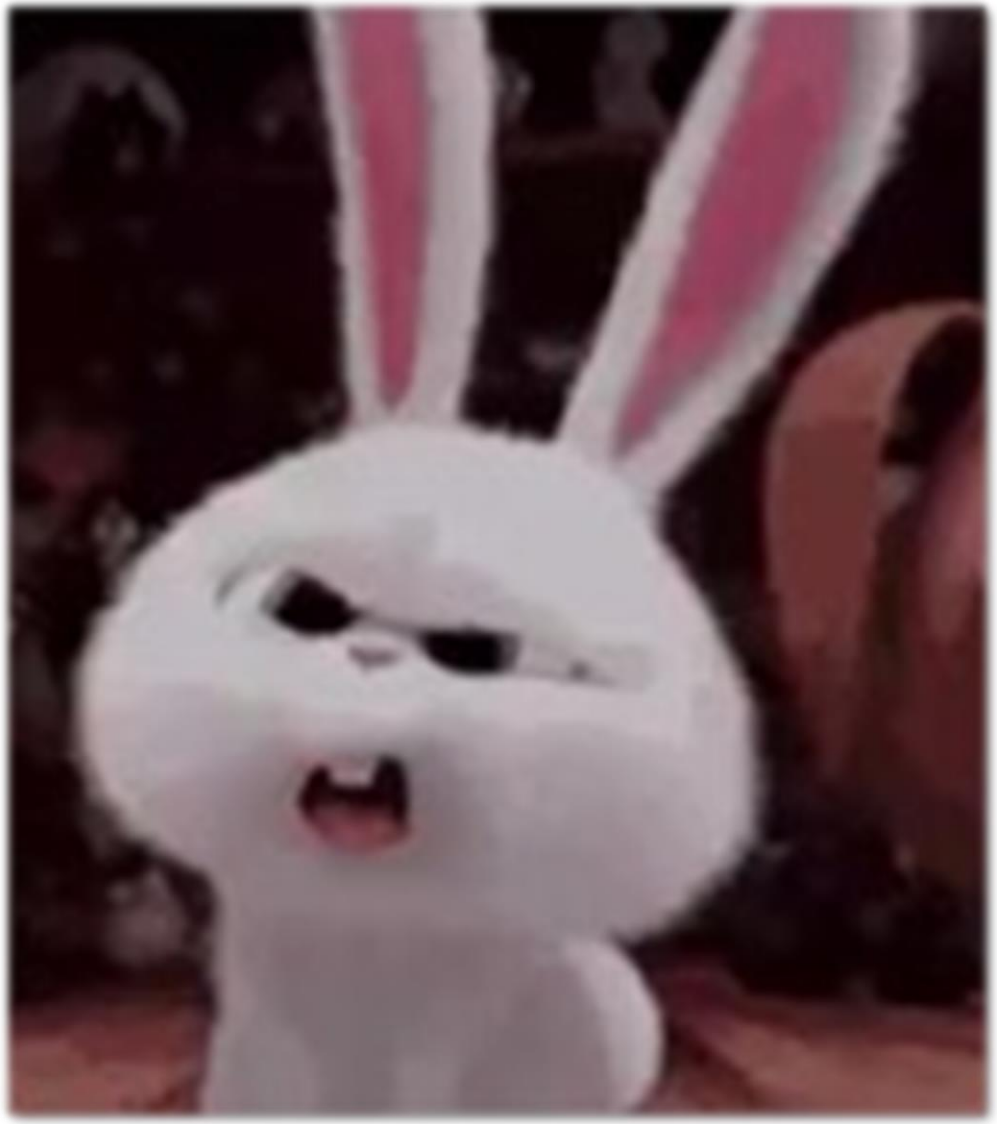
NATO

Germany

Federal States

Municipalities

Das wird uns retten?!? O_o

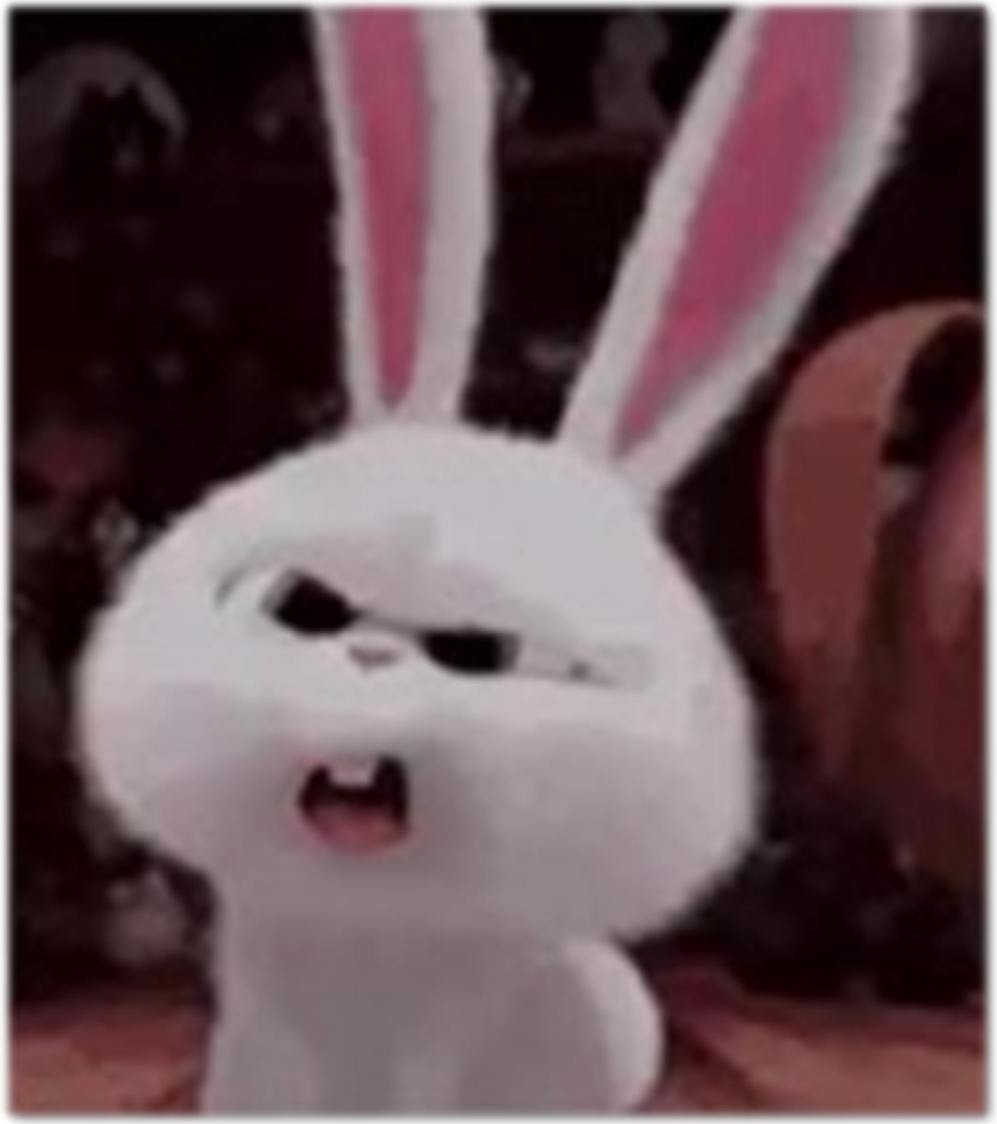


Nationale Sicherheitsstrategie

- **76 Seiten Strategie**
  - 62 x Cyber
  - 26 x Resilienz
  - 6 x kritische Infrastruktur
  - Glitzer-Hypes wie KI, Quanten und Blockchain kommen glücklicherweise kaum vor

- **Grundgesetzänderung**: „Schaffung einer Bundeskompetenz zur Gefahrenabwehr“
- **Hackfirst statt Hackback** „Abwehr eines laufenden oder unmittelbar bevorstehenden Cyberangriffs“

Und DAS wird uns retten?!? O_o



Öffentliche Verwaltung und Ihre Fachverfahren sind kritisch für die Bevölkerung!

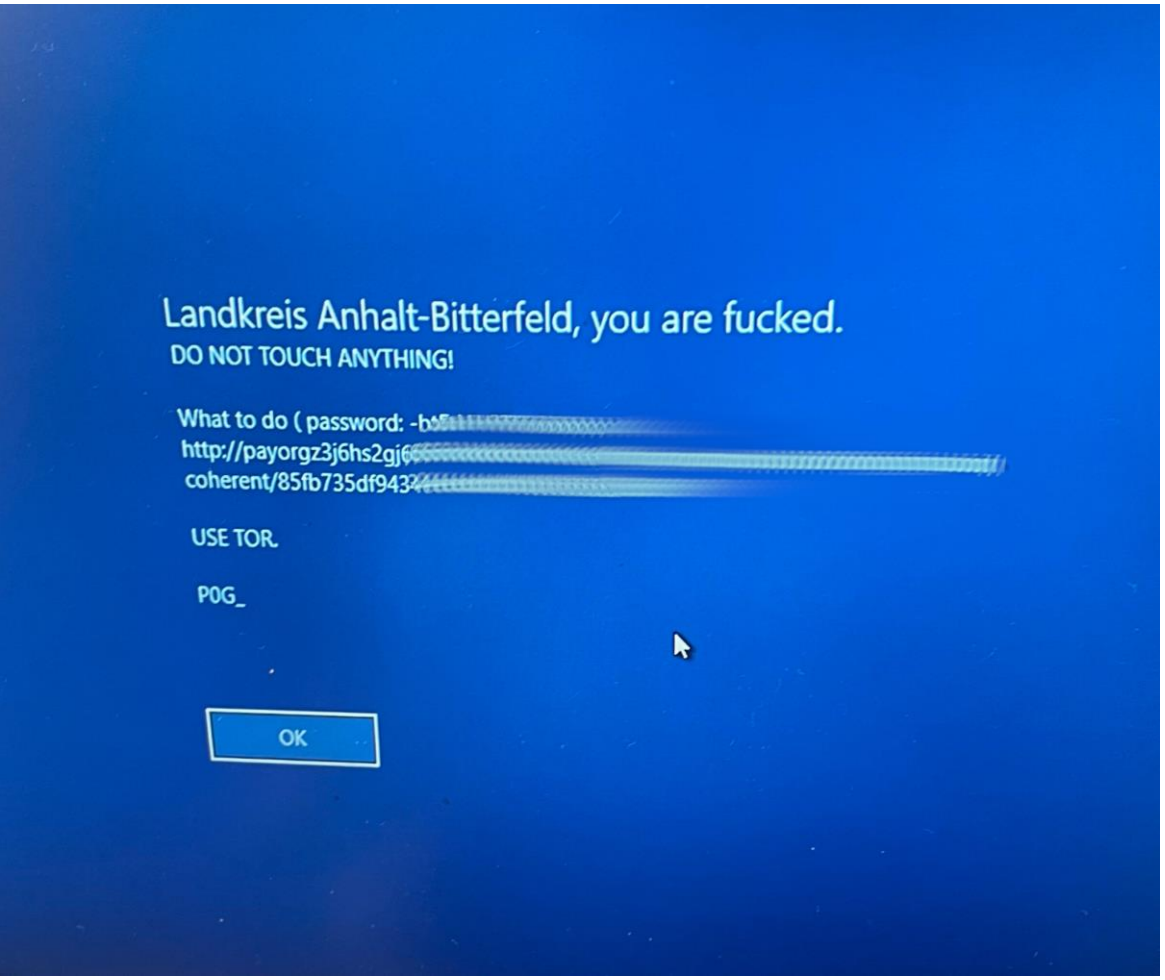
Gibt es denn Bedrohungen für KRITIS?

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

- „Cyberwar-“, Geheimdienste-, Hackfirst & Hackback Szenarien bringen zukünftig Kollateralschäden

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 7 Standorten
- ca. 160 Fachverfahren betroffen
- ca. 1 Jahr nicht arbeitsfähig
- Alle(!) Emails für immer weg und nicht wiederherstellbar
- Kosten von bisher über 2,5 Mio €
- Fachverfahren: Sozialabgaben vs KFZ-Zulassung

Sicherheitsvorfall Ransomware

Spear Phishing oder ungepatchte Systeme im Netz

- Email mit Link oder Anhang
  - Dropper wird geladen, dann Ransomware
  - Pivilege Escalation & Lateral Movement
  - Verschlüsselung
  - Double Extortion & Teilveröffentlichungen
- Ungepatchte Systeme im Internet erreichbar
  - Initial Access Broker (IAB) kompromittiert diese
  - Ransomware Gruppe kauft Zugang (zB 4.600 $)
  - Nutz RaaS Dienste im Abo mit 20 % Ransombeteiligung

Frage der Bevölkerung: Kommt morgen noch Strom & Wasser aus der Leitung?

Schutzmaßnahmen im Cyberraum

Was brauchen wir denn?

- Cyber-Resilienz!
- Krisenerfahrung und Übungen bei Verantwortlichen (Bürgermeisterinnen, Landrätinnen, you name it)
- Nein, keine Fachverfahren auf Windows 98 in 2021
- Sicherheitsanforderungen und Vorgaben für Staat und Verwaltung (vgl. BSI-Gesetz § 8a und Kritisverordnung)
- Kommunale CERTs mit Hilfe für alle kleinen Kommunen

Cyber-Hilfswerk!

Das CHW soll die existierenden Bewältigungskapazitäten für Großschadenslagen durch Cybervorfälle bei Kritischen Infrastrukturen kooperativ ergänzen!

https://ag.kritis.info/chw-konzept

Cyberresilienz ➔ Widerstandsfähigkeit gegen Ereignisse

- Ursache für Katastrophe oder Cybervorfall 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?

  →Können wir damit die Cyberresilienz 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
- Hinter jedem Datensatz steht ein Mensch ➔ Daten sind toxisch
- 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