Phish-Bot 2025

Manuel ‚HonkHase‘ Atug

KRITIS, Cloud und KI

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
- Experte der European Research Executive Agency (EU REA)
- Mitgründer der AG KRITIS: ag.kritis.info

AG KRITIS

~~@HonkHase~~ @HonkHase@chaos.social

@honkhase.bsky.social

Ich habe #KRITIS im Endstadium

Verwaltung & Cybersicherheitsgesetzgebungen

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

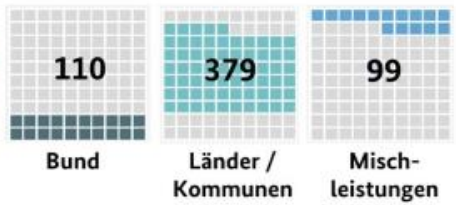
IT-Planungsrat

Bundes-CIO + Landes-CIOs
Kommunale Spitzenverbände

Zielsetzungen bis 2022

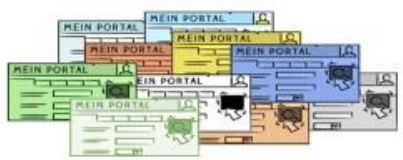
bis **2023**: Umsetzung **Single-Digital-Gateway-VO** (= EU-OZG)

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 Deutschlands ➔

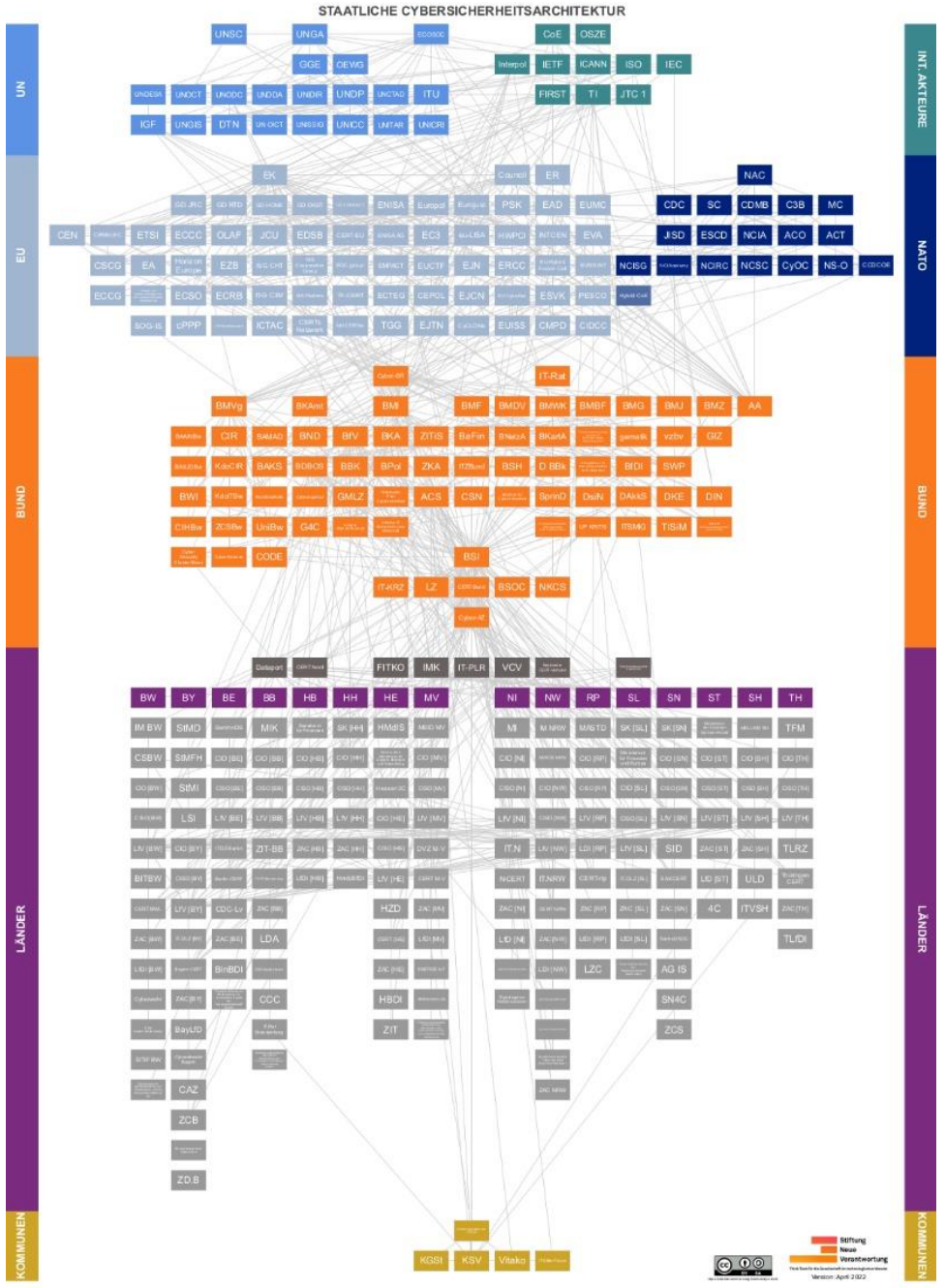
UN

Europe

Germany

Federal States

Municipalities



Int. Actors

NATO

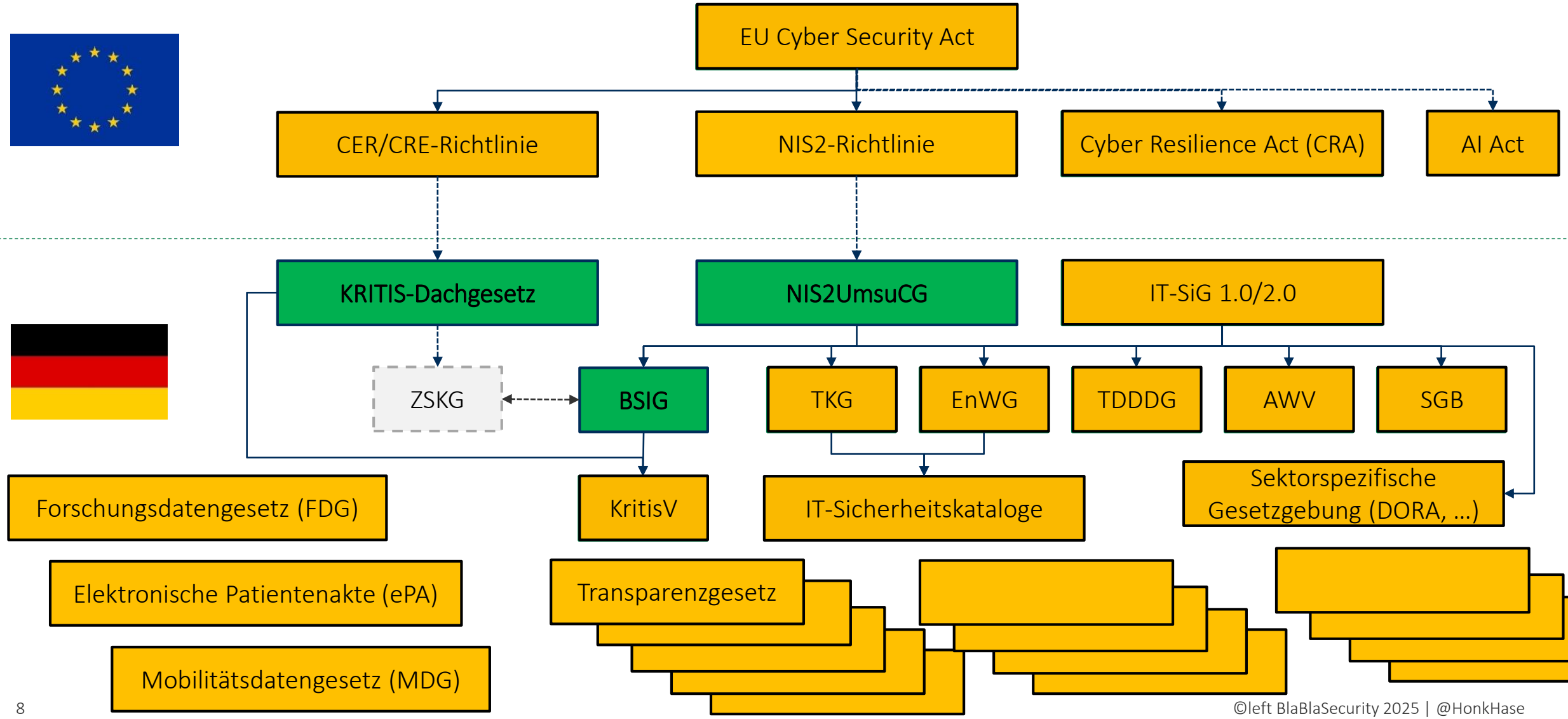
Germany

Federal States

Municipalities

Übersicht zur (Cybersicherheits-)gesetzgebung

(naja, so ein bischen halt)



Cyberdiarrhö

Offensive Lösungen

- Schon drölfzehn Mal verstorben:
  - Zombie Vorratsdatenspeicherung
- Sicherheitspaket
  - Massenüberwachung
  - Gesichtserkennung
  - Anlasslose Kontrollen
  - Wo ein Trog, da kommen…
- Wer uns ancybert, wird weggecybert
  - Hackback (manchmal auch Hackfirst)
- Schwachstellenmanagement
  - Verwalten (und ausnutzen) statt beheben

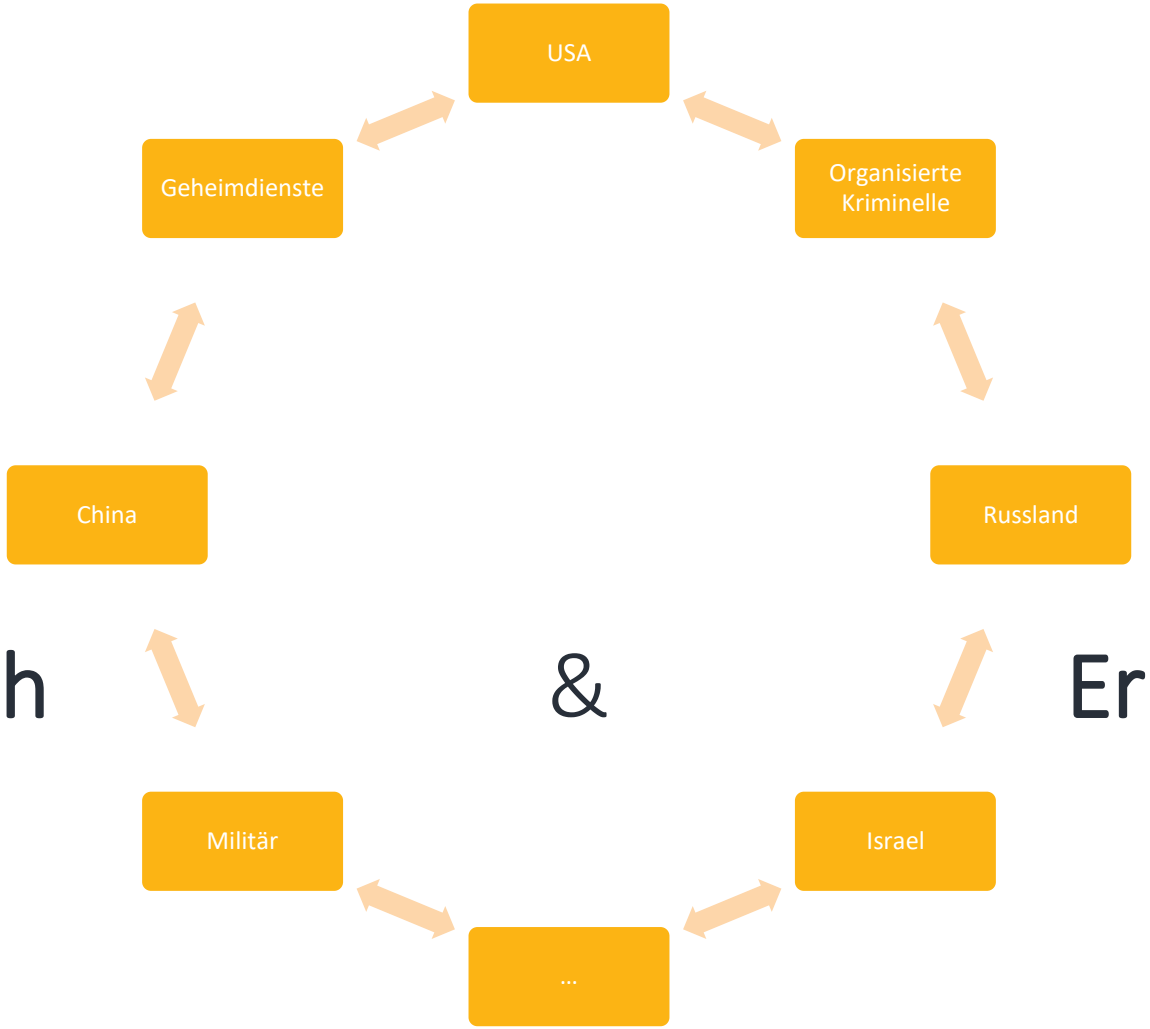
- Unhackbar! (by Law, nicht by Design)
  - nationale Sicherheit
  - öffentliche Sicherheit
  - Verteidigung & Militär
  - Kommunen
  - Landkreise
  - Strafverfolgungsbehörden
  - Geheimdienste

Zeitenwende

(angekündigt)

Organisierte Kriminalität, Geheimdienste und andere staatliche Akteure

Schutz vor was und wem?



Machtmissbrauch & Erlösmaximierung

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

Dinge beim Namen nennen

Was ist KI?

- KI ist Software
  (und ganz viel Daten)
- Software kann man sicher entwickeln und betreiben.
  Oder eben auch nicht
- Software kann nicht denken

Wie nutze ich KI?

- Technologiehörigkeit vs Heilsversprechen
- Mittel zum Zweck vs Selbstzweck

Verlust der digitalen Souveränität über 3 Langzeit-Etappen

Hardware

- Speicherung der Daten
- Externe RZ Konzerne

Applikationen

- Verarbeitung der Daten
- Externe Cloud Konzerne

Daten

- Abgabe der Daten
- Externe KI Konzerne

Sicherer, robuster und nachvollziehbarer Einsatz von KI

- **Evasion/Adversarial Attacks**
  Durch eine Manipulation von Eingabedaten verleiten Angreifer das KI-Modell im Betrieb zu vom Entwickler nicht vorgesehenen Ausgaben

- **Data Poisoning Attacks**
  Manipulation der Trainingsdaten des KI-Modells, so dass dieses auf (bestimmte) Eingaben nicht wie vom Entwickler vorgesehen reagiert

Sicherer, robuster und nachvollziehbarer Einsatz von KI

- **Privacy-Attacks**
  Angreifer extrahieren Informationen hinsichtlich der Trainingsdaten aus dem Modell

- **Model Stealing Attacks**
  Angreifer extrahieren die Funktionalität des Modells

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf

>> All-Gefahren-Ansatz <<

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

** Hallo BBK*

Cyberwar vs. Realität

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

Resilienz ist das Mittel zum Zweck

(it‘s all about Cyber…)

Wie? Das ist doch quasi Magie… wie KI oder Blockchain…

Cyberresilienz! Zur Erhöhung der Widerstandsfähigkeit von KRITIS

** Fähigkeit eines Systems, Ereignissen zu widerstehen bzw. sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder möglichst schnell wieder zu erlangen*

Warum? Angriffe verpuffen wirkungslos durch Basis-Maßnahmen

** Hallo, BSI Grundschutz (ISMS mit BCM)*

Bedrohungen und Gefährdungen

- **Und alle: Cloud & KI**

- Was ist mit staatlichen Systemlandschaften?
- Was ist mit Betriebssystemen und Smartphones?
- Was ist mit Netzwerkequipment und Firewalls?
- Was ist mit Systemen zur Angriffserkennung?

Lieferkette: Israel XM Cyber

Ex-Mossad-Chef Tamir Pardo gründete ein Start-up, das Banken, Firmen und Regierungen berät. *Foto: picture alliance / dpa*

SICHERHEIT

»Tödlich wie die Atombombe«

Tamir Pardo warnt davor, das Zerstörungspotenzial von Cyberkriminellen zu unterschätzen

von Pierre Heumann

14.02.2021 11:06 Uhr

Von 2010 bis 2015 war er Direktor des Mossad.

Nach seinem Ausscheiden aus dem Geheimdienst vor fünf Jahren gründete er, zusammen mit zwei weiteren Ex-Mossad-Agenten, die Cyberfirma »XM Cyber«. Das Start-up hat eine vollautomatische Simulationsplattform für anhaltende Bedrohungen entwickelt, um Angriffe kontinuierlich aufdecken und den Handlungsbedarf lokalisieren zu können. Es zählt unter anderem Banken, Versicherungsfirmen, Flughäfen, Energiefirmen, Regierungen, Logistikfirmen und Börsen zu seinen Kunden.

Der Endgegner der Souveränität: Palantir

Palantir

- Autokratie-Etablierung durch Peter Thiel
- auch durch deutsche Steuergelder
- mittels deutscher Strafverfolgungsbehörden & Geheimdiensten
- USA als „CEO geführte Firma“ ohne Regulierung
- Vorstufe „Freedom Cities“
- Freiheit nicht mit Demokratie vereinbar

CyberCyber in der Lieferkette aka Systeme zur Angriffserkennung

- SzA vs. Antivirus vs. End Point Protection

- Alles oder nix?
  - Systemrechte und Vollzugriff oder zB passiv am Netzwerk?
- On-Prem oder in der Cloud?
  - Datenexport oder Souverän?
- Deutschland vs. USA vs. Israel?
  - Ist doch alles das gleiche Cyber?
- Sammeln und analsieren vs. Software Entwicklung vs. AGBs

- Crowdstrike vs Kaspersky vs. XM Cyber von Schwarz Gruppe / Schwarz Digits

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

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 können toxisch sein
- 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