Vitako MV 2022 - Resiliente Verwaltung in Krisenzeiten

Manuel (HonkHase) Atug

Manuel (HonkHase) Atug

- 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 KRITISche Infrastrukturen?

Die 10 Kritische Infrastruktur Sektoren in Deutschland

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

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

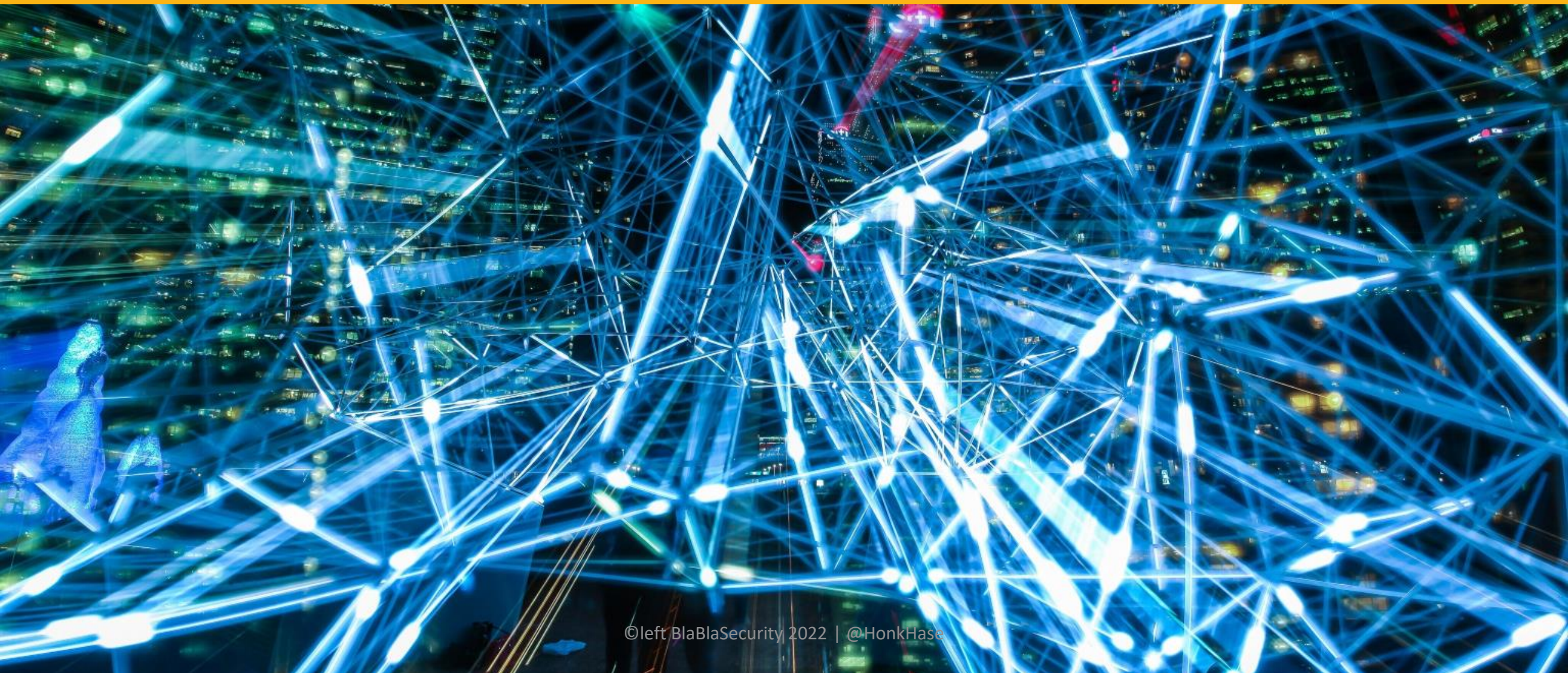
- **Vertraulichkeit**

Vertrauliche Informationen werden unberechtigt zur Kenntnis genommen oder weitergegeben

*BSI Grundschutz

Öffentliche Verwaltung und Ihre Fachverfahren sind kritisch für die Bevölkerung!

Landkreis Anhalt-Bitterfeld

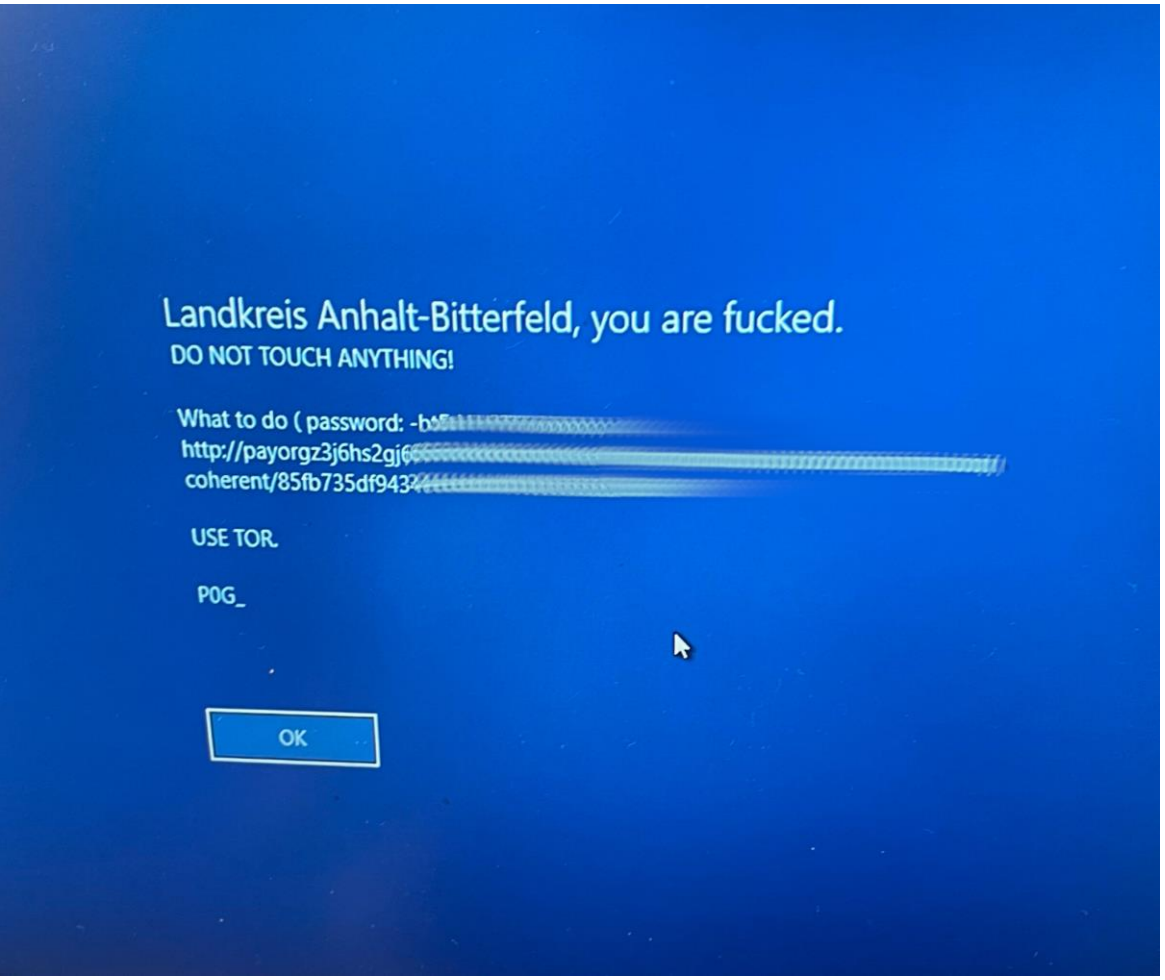


Cybercrime – Ransomware as a Service

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

Sicherheitsvorfall Ransomware



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 Mio €
- Fachverfahren: Sozialabgaben vs KFZ-Zulassung

Schutzmaßnahmen im Cyberraum

It‘s all about „Kultur“

- gute und gesunde Organisationskultur
- freundliche und wertschätzende Kommunikationskultur
- offene Fehlerkultur

- Heutzutage hat der patriarchale und autoritäre Chef ausgedient!

Cyber-Verteidigung

(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*

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? (ID Wallet, Luca App)

  →Können wir damit die Cyberresilienz im KRITIS Sektor Staat und Verwaltung erhöhen?

  →Was ist eine gute Digitalisierung?

Cyber-Verteidigung

(…die langweiligen Basics der IT-Security)

Büroalltag in der Defense

Haben wir ein Backup?

Ist es frisch oder fermentiert es vor sich hin?

Haben wir das sogar Offline vorliegen?

Haben wir mal die Wiederherstellung getestet?

Braucht das Wiedereinspielen viel zu lang?

Firewall? Same!

Nutzerverwaltung? Same! …

Nachhaltigkeit in der Digitalisierung

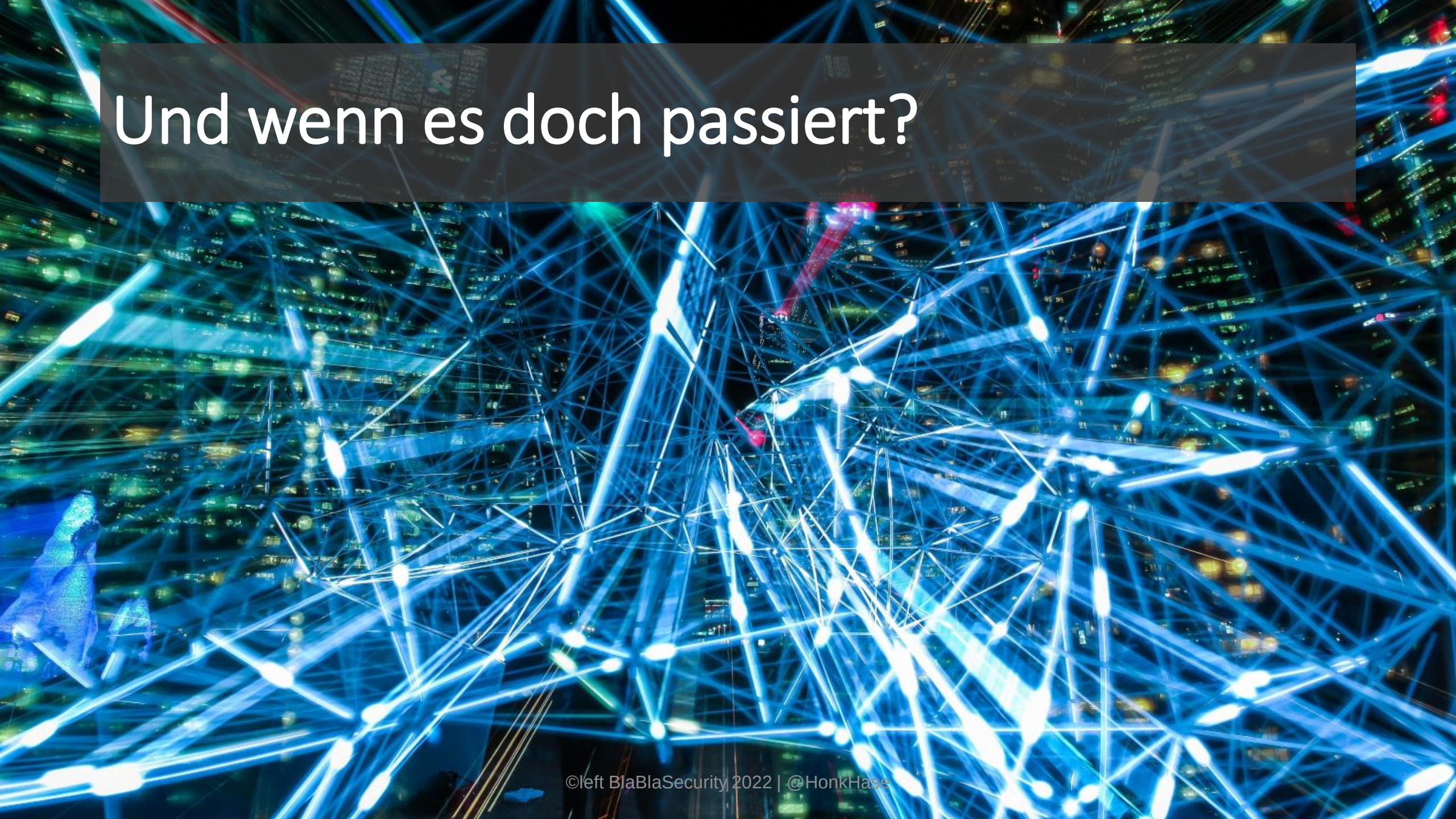
- Bei der digitalen Transformationen verantwortungsvolle Maßnahmen einzuleiten und gewissenhaft durchzuführen, also zu operationalisieren, ist daher gleichsam eine technische wie ethische Aufgabe!
- Vermeidet daher technische Schulden an kommende Generationen
- Hinter jedem Datensatz steht ein Mensch
- 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 wenn es doch passiert?



Krisenmanagement

in 7 Schritten

Schritt 1
Wen brauche
ich im Krisenfall?

Schritt 2
Wo treffen wir uns in der Krise?

Schritt 3
Wie kommuniziere ich?

Schritt 4
Was mache ich im Krisenfall?

Schritt 5
Was brauche ich an
Dokumentation?

Schritt 6
Köpfe kennen in der Krise

Schritt 7
Cyber-Versicherung

Schritt 0: Basisabsicherung

Die beste Notfallplanung ist, wenn kein Notfall eintritt!

z. B. die Leitfäden des BSI zur Basisabsicherung und zu Ransomware nutzen

Und Backups, Backups, Backups

Offline Backups & regelmäßig testen

Empfehlungen des BSI

Cyber-Sicherheit für KMU

(Die TOP 14 Fragen)

Frage 1: Wer ist verantwortlich?

Frage 2: Wie gut kennen Sie Ihre IT-Systeme?

Frage 3: Führen Sie regelmässig eine Datensicherung durch?

Frage 4: Spielen Sie regelmässig Updates ein?

Frage 5: Haben Sie Makros deaktiviert?

Frage 6: Verwenden Sie Virenschutzprogramme?

Frage 7: Haben Sie eine Richtlinie für sichere Passwörter festgelegt?

Frage 8: Haben Sie eine Firewall eingerichtet?

Cyber-Sicherheit für KMU

(Die TOP 14 Fragen)

Frage 9: Wie sichern Sie Ihre Mailaccounts ab?

Frage 10: Wie trennen Sie unterschiedliche IT-Bereiche?

Frage 11: Haben Sie IT-Risiken im Homeoffice und bei Geschäftsreisen im Griff?

Frage 12: Wie informieren Sie sich? Wie sensibilisieren Sie Ihre Mitarbeiter?

Frage 13: Deckt Ihre Versicherungspolice auch Cyber-Risiken ab?

Frage 14: Wissen Sie, wie Sie bei einem Cyber-Angriff reagieren müssen?

BSI & Deutscher Landkreistag

BSI IT-Notfallkarte

Die Informationen auf der IT-Notfallkarte richten sich primär an die IT-Anwenderin und den IT-Anwender in der Organisation. Sie stellen drei Botschaften in den Vordergrund:

1. Kenntnis der Ansprechpartner für IT-Notfälle in der Organisation und deren Erreichbarkeit.

2. Sofortige Weitergabe entscheidender Informationen zu IT-Notfällen.

3. Gegenmaßnahmen nur nach Absprache/Anweisung mit den für IT-Notfällen zuständigen Ansprechpartnern.

Weiterführende Link Empfehlungen

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
  - Informationen und Hilfestellungen für KMU
    https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html

  - Informationssicherheit für kleine und mittelständische Unternehmen (KMU)
    https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Grundschutz-Profile/it-grundschutz-profile_node.html

Weiterführende Link Empfehlungen

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
  - IT-Notfallkarte „Verhalten bei IT-Notfällen“ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html
  - BSI Newsletter für KMU https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen_node.html

Weiterführende Link Empfehlungen

- **Deutscher Landkreistag**
  - Informationssicherheit für Landrätinnen und Landräte: IT-Grundschutz in den Landkreisen https://www.landkreistag.de/images/stories/themen/ITSicherheit/211217_Handlungsleitfaden_IT-Grundschutz.pdf

- **Allianz für Cyber-Sicherheit (ACS)**
  https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/topservice_hidden_node.html

- **Linus Neumann**
  - CCC Congress 36C3 “Hirne Hacken”
    https://www.youtube.com/watch?v=BreKdM7CKnY


Fragen? :)


DANKE :)