TROTZ SPITZENTECHNIK VERWUNDBAR? PRO GOVERNANCE KOMMUNALER CYBERSICHERHEIT

Kirstin Scheel

03.05.2022

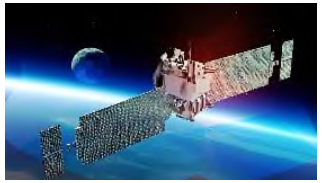
Fraunhofer SIT

KLEINE AUSWAHL AUS 2022 – BEISPIELHAFTE VORFÄLLE

- Stichwort **Datenschutz** (Ende 01/2022):
  - 33.000 hochsensible Mails aus dem **Ausländeramt Lübeck** bei eBay verkauft

- Stichwort **Ransomware** (Ende 01/2022):
  - KRITIS Betreiber: Cyberangriff legt **Oiltanking-Tanklager** deutschlandweit vollständig lahm – Tankwagen-Beladung außer Betrieb

- Stichwort vermutlich Kollateralschaden **Cyberwar** (24.2.2022):
  - Ausfall des **Satellitennetzwerks** KA-SAT hat Auswirkungen auf Windräder



- Stichwort **Phishing** (Anfang 03/2022):
  - Mitarbeiter der **Stadt Bochum** fallen auf Phishing herein

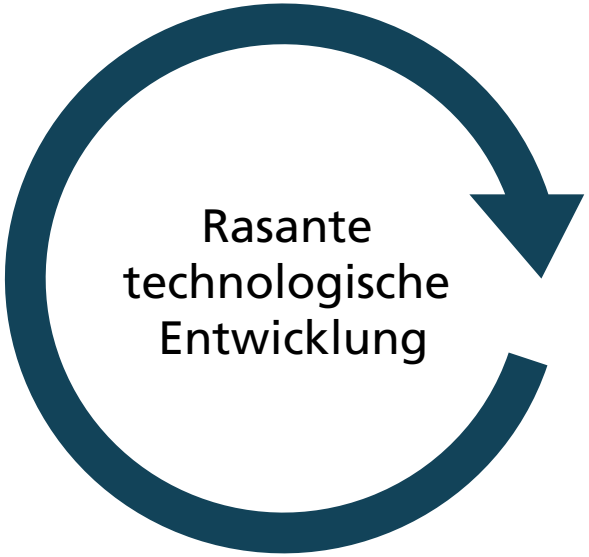
KLEINE AUSWAHL AUS 2022 – BEISPIELE FÜR ERFOLGREICH ANGEGRIFFENE EINRICHTUNGEN

- **Ransomware-Angriffe auf Städte**
  - Stadt Suhl (10.3.2022)
  - Stadt Dingolfing (21.3.2022)
- **Ransomware-Angriff auf Klinik**
  - Kliniken am Bodensee (14.1.2022)
- **Angriffe auf Hochschulen**
  - Münster (Internetserver, Prüfungsserver, 26.1.2022)
  - Aschaffenburg (29.3.2022)
- **Instagram-Accounts mehrerer Kultureinrichtungen** durch **Phishing** übernommen (02/2022ff)

Instagram-Account gehackt: Krupp-Stiftung
Instagram-Account gehackt: Kunstmuseum Stuttgart
Instagram Account gehackt: HMKV Hartware MedienKunstVerein
Instagram Account gehackt: Kunstmuseum Ulm
Instagram Account gehackt: Schauwerk Sindelfingen
Instagram Account gehackt: Hamburger Kunstverein
Instagram Account gehackt: Berliner Fotozentrums C/O

GRÜNDE FÜR DIE UNSICHERHEIT HEUTIGER IT

- Geringes **Bewusstsein** für Risiken
- Geringe **Anreize** für bessere Sicherheit, negative Anreize durch Kostendruck
- Geringer **Markterfolg** bekannter Technologien
- **Social Engineering** und Innentäter
- Schlechte **Benutzbarkeit** und geringe Automatisierung von Sicherheit für Administratoren und Endnutzer
- Unsichere **Bestandssysteme**
- Geringe **Software- u. Hardwarequalität**, schwierige Konfiguration und Integration



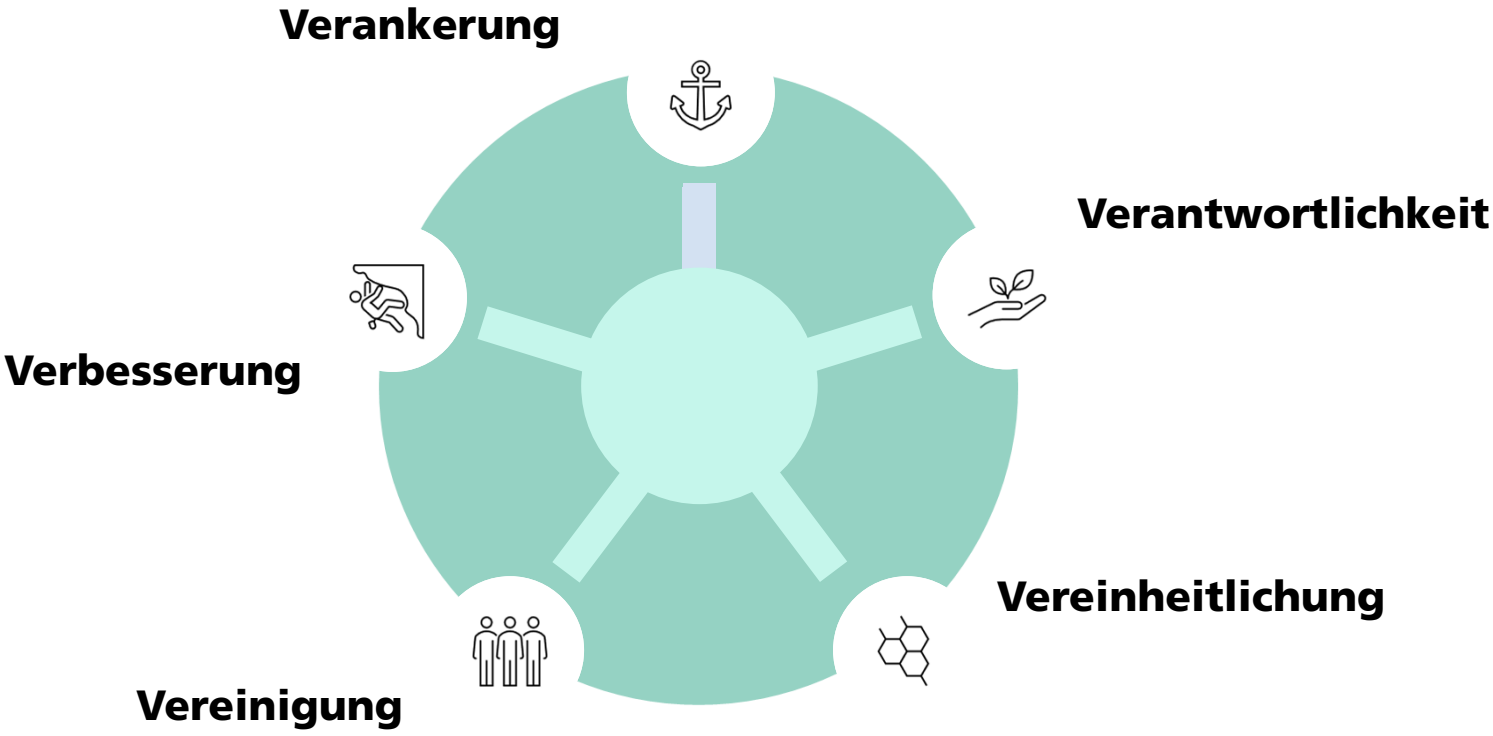
AUSZUG: HANDLUNGSLEITFADEN INFORMATIONSSICHERHEIT FÜR LANDRÄTINNEN UND LANDRÄTE
IT-GRUNDSCHUTZ IN DEN LANDKREISEN

[…]

- Übernahme der abschließenden **Gesamtverantwortung** der Behördenleitung, dazu Sicherstellung des Informationsflusses
- Ernennung einer/s **Informationssicherheitsbeauftragten**
- Initiierung der Erstellung und Fortschreibung einer **Informationssicherheitsleitlinie**
- **Unterstützung** der Informationssicherheitsbeauftragten mit dem Ziel der Einbindung in die relevanten Aktivitäten der Fachabteilungen/Dezernate
- Bereitstellung der erforderlichen Software als **Dokumentations- und Prozesssteuerungswerkzeuge**
- Aktives und widerspruchsfreies **Vorleben von Informationssicherheit**

[…]

EIN GOVERNANCE FRAMEWORK FÜR CYBERSICHERHEIT IN SMART COMMUNITIES



5 KONKRETE TIPPS – IM ÜBERBLICK:

- Jede Organisation braucht eine explizite **Cybersicherheitsstrategie** und explizite **Regeln**
- **Verantwortliche** müssen **benannt**, **Prozesse** definiert und alle Situationen, auch die Reaktion auf Cyberangriffe, müssen geübt werden
- Jede Organisation muss wissen, wie die eigene **Daten- und IT-Landschaft** aussieht, und sie **kontinuierlich auf Sicherheitsprobleme** überwachen
- Grundsicherungen wir **Backups, Updates und Patches** müssen regelmäßig durchgeführt werden
- Wenn eine kleine(re) Organisation nicht die internen Mittel hat, ihre Daten und IT selbst ausreichend gut abzusichern, können **externe Dienstleister und Rechenzentren** helfen.

FORENSIC READINESS - BEREIT FÜR DEN ERNSTFALL

- Erstellen Sie einen **Krisenplan** für Cyber-Angriffe (**Notfallkonzept**)
  - Kernprozesse müssen weiterlaufen können
  - während gleichzeitig die Suche nach Ursachen und Tätern möglich bleiben muss
- **Übungen -** Training der Abläufe im Vorfeld:
  - insbesondere Einspielen von Backups;
  - wann, wie und wo zur Anzeige bringen?;
  - was ist bzgl. Datenschutz zu beachten?
- Führen Sie eine **Kontaktliste** von
  - ihrer Cyberversicherung,
  - IT-Forensikunternehmen, etc.
- Bereiten Sie die **Krisenkommunikation** vor

CYBERSICHERHEIT – AUCH EIN DATENSCHUTZ-THEMA

- Bei jedem Cyber-Incident, bei dem **personenbezogene Daten** betroffen sind, greift die Datenschutz-Grundverordnung (DSGVO)
  - **Meldepflicht gem. Art. 33 DSGVO** regelt die Meldung an die **Aufsichtsbehörde**
    - 72 Stunden-Frist ab Bekanntwerden
  - **Benachrichtigungspflicht gem. Art. 34 DSGVO** regelt die Benachrichtigung **betroffener Personen**
    - *Beachte: Die DSGVO sieht eine höhere Schwelle für die Benachrichtigung der betroffenen Personen vor als für die aufsichtsbehördliche Meldung***.**
  - Auch **Auftragsdatenverarbeiter** können betroffen sein

- Klare interne Governance und Incident Response Plan

KRISENKOMMUNIKATION BEI CYBERSICHERHEITSVORFÄLLEN

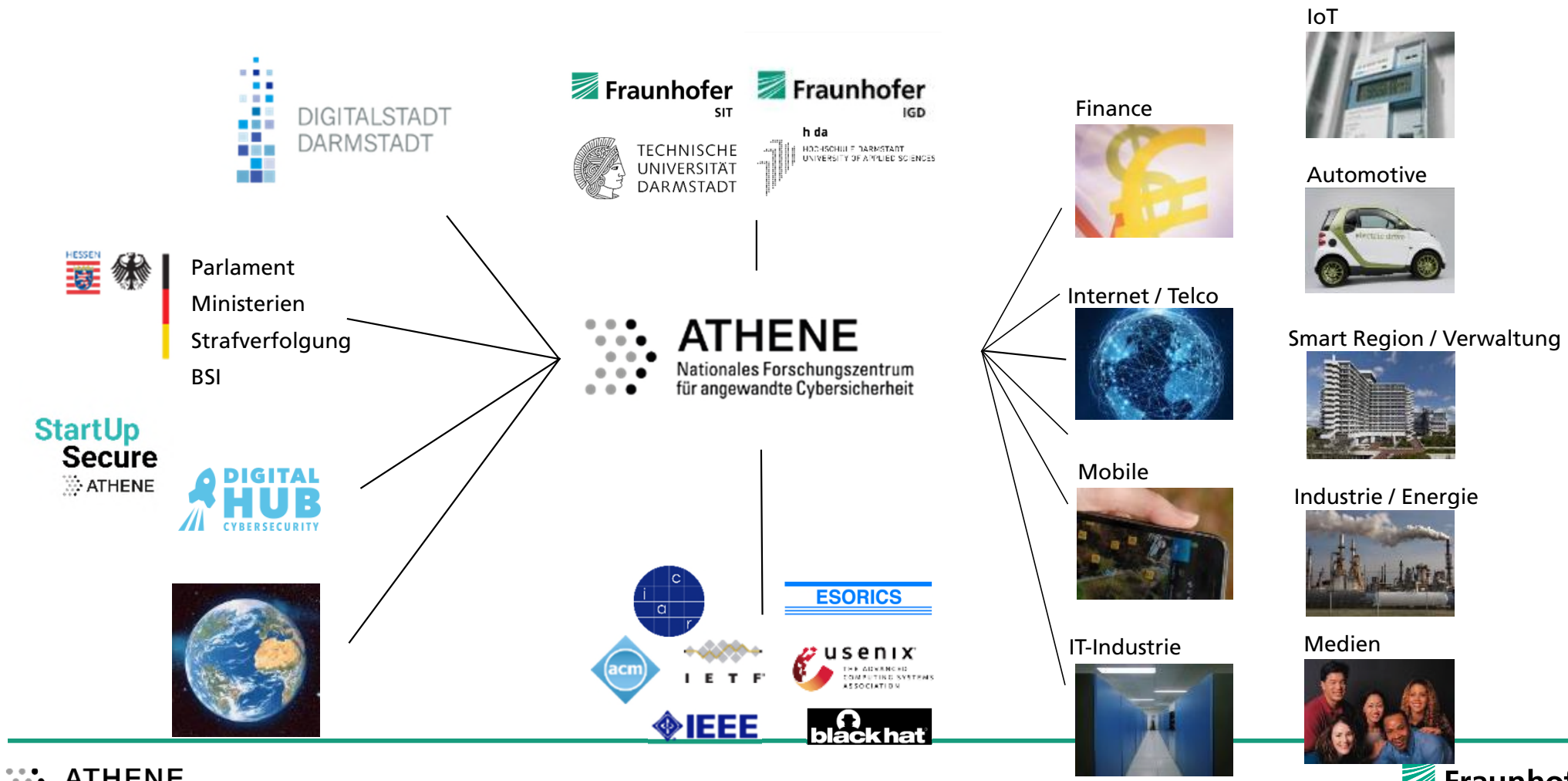
- Intern abgestimmte **Kommunikationswege** und **multidisziplinäre Teams**, die ein gemeinsames Verständnis der Lage haben
  - nicht zu früh in die Kommunikation:
    - wissen, was passiert ist – und ggf. die Angreifer nicht vorwarnen
- **Nur einer spricht**
- **Klare, abgesicherte Aussagen** – keine Wortklauberei oder Verschleierung
  - Transparent, aber nicht notwendigerweise vollständig
  - Nur Fakten kommunizieren
  - Falls möglich: Handlungsempfehlungen für Stakeholder

ATHENE – FORSCHUNG MIT IMPACT
FORSCHUNGSZENTRUM DER FRAUNHOFER-GESELLSCHAFT UNTER MITWIRKUNG VON HOCHSCHULEN

Fraunhofer SIT
Fraunhofer IGD
TECHNISCHE UNIVERSITÄT DARMSTADT
h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES
GOETHE UNIVERSITÄT FRANKFURT AM MAIN
UNIKASSEL VERSITÄT

- Gegründet 2019
- Exzellente Forschung zum Wohle von Gesellschaft, Staat und Wirtschaft
- Dauerhaft gefördert von BMBF und HMWK
- Mit über 550 Forschenden – etwa 50:50 Fraunhofer und Hochschulen – das größte Cyber-Zentrum in Europa

ANWENDUNGSBEREICHE UND ÖKOSYSTEM



HERZLICHEN DANK
FÜR IHRE AUFMERKSAMKEIT!

Kirstin Scheel
Fraunhofer-Institut für Sichere Informationstechnologie SIT |
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
Rheinstr. 75, 64295 Darmstadt, Germany
Telefon: +49 6151 869-268
E-Mail: kirstin.scheel@sit.fraunhofer.de
Web: www.sit.fraunhofer.de