# Der kranke Patient

Sicherheit im Gesundheitswesen

# Preisliste der Chinesischen Hac r i-Soon – Organisiert als Unternehmen

| Medium | Leistung | | Preis |
|---|---|---|---|
| Priv Webseite | Zugang | | 15.000 Dollar |
| X (ehemals Twitter) | Flächendeckende Desinformation | | 100.000 Dollar |
| Priv. Mailaccounts, Messenger Dienste, Social Media Accounts | Zugang | | Preis auf Anfrage |

Ein neues Phänomen….

# CCaaS Cybercrime as a Service

Arbeitsteilung und neue Geschäftsmodelle
Kriminelle werden immer professioneller und nutzen disruptive Technologien

# Preise aus dem Darkweb

Kontoinformationen= 5$

Instagramm Account= 7$

Gesundheitsdaten= 1000$

# Leitfrage:

# Prozesse Gesundheitswesen versus Sicherheit

Prävention, Diagnostik, Behandlung, Impfung, Hygiene

Prävention, Detektion, Mitigation, Response, Hygiene Awareness, Pentests und Übungen

Systemimmanent stehen wir vor großen Herausforderungen
-die äußeren Ereignisse und Krisen wirken dabei wie Verstärker

*„In der gleichen Geschwindigkeit, in der wir digitalisieren, vernetzen, Komplexität steigern, können wir die labilen Systeme nicht ausreichend schützen.“*

(M. Schallbruch: ***Risiken der Cybergesellschaft beherrschen. Ein Auftrag an Staat und Politik :https://deutschland-und-die-welt-2030.de/de/beitrag/risiken-der-cybergesellschaft-beherrschen-ein-auftrag-an-staat-und-politik/)***

BSKI

Bundesverband für den Schutz Kritischer Infrastrukturen

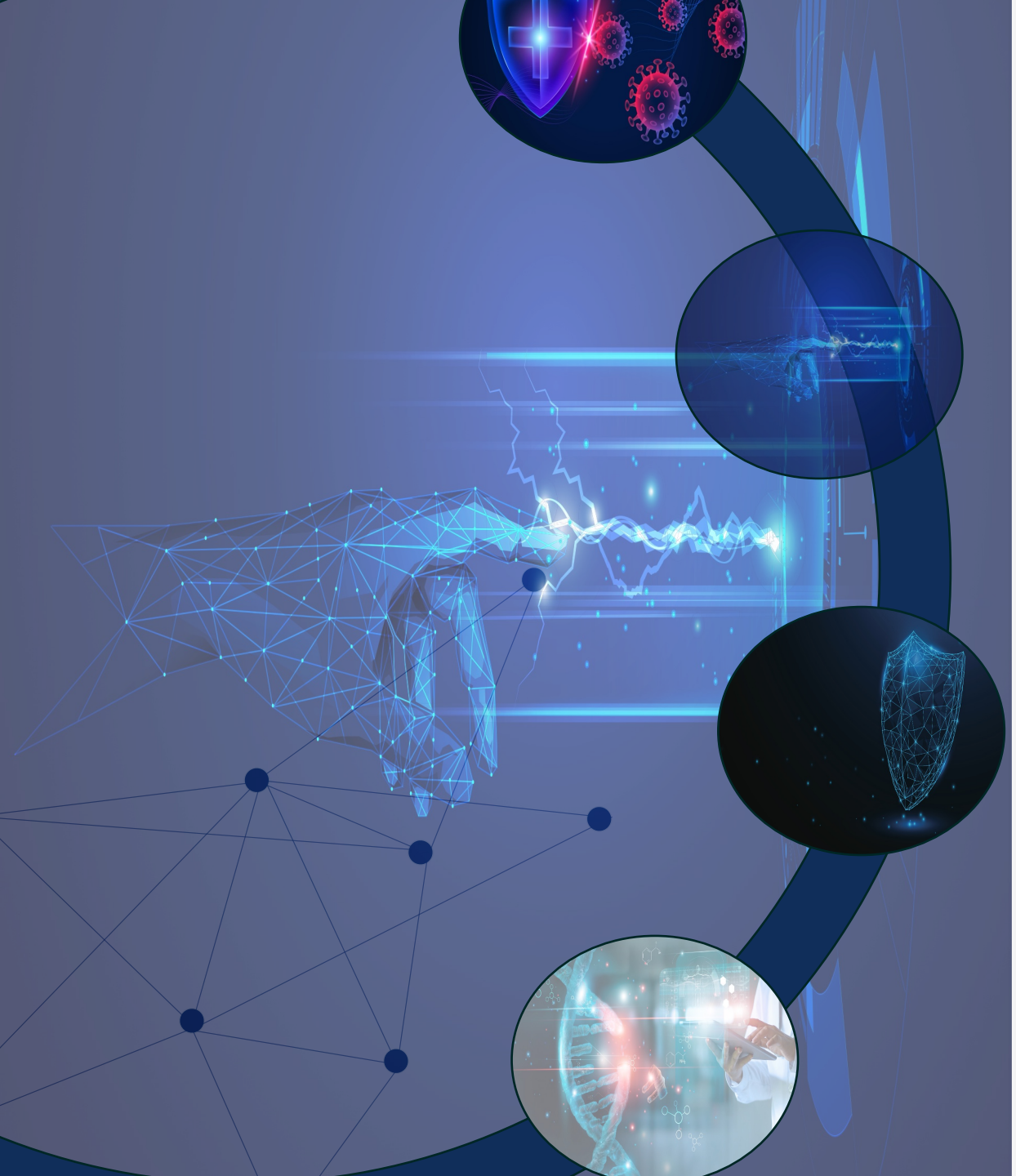
Die Aufgabe des Bundesverbandes für den Schutz Kritischer Infrastrukturen ist es, Sicherheitsrisiken für kritische Infrastrukturen und deren Zulieferer frühzeitig zu erkennen und durch gezielte Konzepte für Prävention, Reaktion und Postvention zu reduzieren. Dabei werden allerhöchste Schutzziele (technisch, organisatorisch, persönlich) für kritische Infrastrukturen verfolgt.

# Miriam Schnürer

## Leitung der Geschäftsstelle NORD
## Vorstand BSKI

- 30 Jahre im Gesundheitswesen
- 17 Jahre exekutive Funktionen in globalen Konzernen in der Healthtech Branche

  Operations, Business Development, Vertrieb, Entwicklung, Produktmanagement, R&D
- 8 Jahre Erfahrung von internationalen Teams, in agiler Entwicklung R&D (Software, Technologie)
- Projekterfahrungen: Software & Apps, Digitalisierung, IoT, Blockchain, AI,
- Begleitung einer Pandemieübung in HH mit Krhs, öffentl. Sektor u Krisenstab. Aufbau einer Infektionsmgtmt Software, Vorschlag und Vorträge auf Konferenzen bezüglich eines öffentl Meldesystems (RKI, ECDC, Genf…)
- Beratung von Unternehmen, Start-up und Investoren im Bereich Healthcare und Healthtech.
- Head of Consulting Healthcare bei der BWI (100% Bundestochter/Militär/Behörden)



# Agenda

- Diagnostik: Die Bedrohung der Cyber Pandemie
- Die Impfung: Gesetzliche Vorschriften und Normen
- Prävention: Risikoanalyse für alle Bereiche
- Hygiene: Cyber Hygiene
- Behandlung: S.I.C.H.E.R Formel

# Agenda

- Diagnostik: Die Bedrohung der Cyber Pandemie
- Die Impfung: Gesetzliche Vorschriften und Normen
- Prävention: Risikoanalyse für alle Bereiche
- Hygiene: Cyber Hygiene
- Behandlung: S.I.C.H.E.R Formel

# Diagnostik: Die Bedrohung der Cyber Pandemie verstehen

# Attacken auf das Gesundheitswesen

# Diagnostik: Die Bedrohung der Cyber Pandemie verstehen

# Pro Sekunde


Lt. Microsoft

# OVERVIEW RECENT ATTACKS ON HOSPITALS

2.2.2024 DREIFALITGKEIT KRANKENHAUS ( DREI HÄUSER)
complete shut down of IT systems

31.1.2024 CARITAS KLINIK DOMINIKUS IN BERLIN
unclear effects and if data had been lost

28.01.2024 BEZIRKSKLINIKEN Mittelfranken
Encryption of data, ransomware

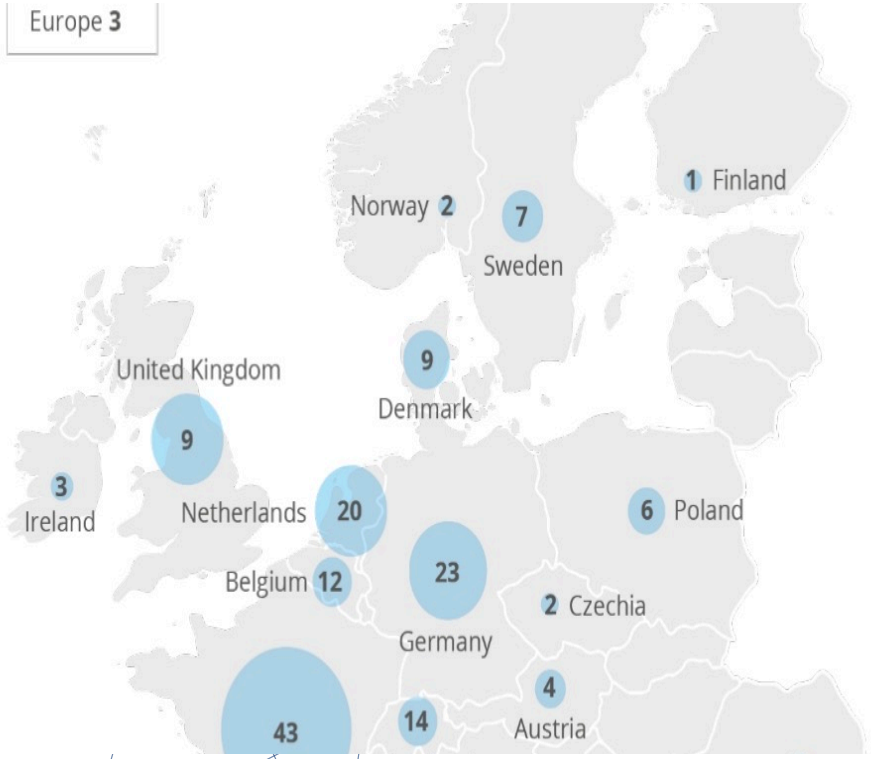
24.12.2023 KRANKENHÄUSER FRANZISKUS HOSPITAL BIELEFELD (DREI HÄUSER)
complete shut down, after one month still no access to most of the IT systems

20.12.2023 MARIENHAUS GRUPPE
Phising Email. No access reported, still IT disruptions

28.11.223 KLINIKUM ESSLINGEN
Hackers got access and damages some servers (PACS) and administration

(Quelle: Henrik Nolte 11.2.2024)

# Diagnostik: Die Bedrohung der Cyber Pandemie verstehen




# Cyber Europe 2022: Testing the resilience of the european Healthcare Sector

40% of Health Organisations had no security awareness program
95% had difficulties do perform risk assessments
46% never performed risk assessment

https://www.enisa.europa.eu/publications/health-threat-landscape

# Die Pandemie trifft auf einen geschwächten Patienten

- Technologie und Digitalisierung
- Entwicklung Medizin und Medtech
- Paradigmenwechsel in der Medizin
- Gesellschaft  und Bevölkerung
- Klima, Natur und Versorgung
- Gesetzgebung und globale Strukturen

# Druckfaktoren auf das Gesundheitswesen

**GESELLSCHAFT**
Gesundheitskosten
Demographie
Chronische Krankheiten
Multimorbidität
Gesetze/Normen/politische Strategien
Qualitätsanforderungen
Geringere Fehlertoleranz,
Dr. Google
Globalisierung

**NEUE & sich verändernde PARADIGMEN**
Prädictive Medizin
Präventive Medizin
Personalisierte Medizin (precision)
Partizipatorische Medizin
Translationale Medizin


**TECHNOLOGIE**
Miniaturization (MEMS Micro electro mechanical systems)
Convergence, Web3
3. Generation Big Data (AI, Cloud, Hadoop, Predictive Analytics, Quantum)
Neue disruptive Technologien in Material, Herstellung
Sensorik, Robotik
(Bio)Print 3D,4D
Human machine interfaces, Digital Twin

**MEDIZIN und MED. TECH**
Komplexe Prozeduren Komplexe diagnostics
Near miss, adverse events, medical errors,
Resistenzen (HAI,MDR)
New emerging diseases
Konvergenzen Ernährung, Pharmacy, Chemie,..
Konvergenz der –ologies (Radio, cardio, onco, anesthesiology…)
AI (Imaging), Roboter, ..
Genomics, Proteomics, Immunotherapy

# Trifft auf einen geschwächten Patienten

# Weitere Bedrohungslagen & Druckfaktoren

Hacks
Stromausfall
Gasmangellage
Feuer/…. Pandemie, Infektionskrankheiten, Ausbrüche
Regulierung
Rechtsstreitrisiken
Wasserversorgung
Heizung
Investitionsstau

# Trifft auf einen geschwächten Patienten

# Weitere Bedrohungslagen & Druckfaktoren

Auswirkung auf:

Interne Parameter

- Qualität der Fachkräfte
- Diebstahl, Gewalt,
- Digitalisierung IOT
- Versorgung
- Kommunikation
- Externe Dienstleistungen
- Versicherungen
- Patientensicherheit
- Behandlungsqualität

# Trift auf einen geschwächten Patienten

# Beispiel: Finanzierung Krankenhaus

In den US werden weniger als 6% des Budgets in die Security gesteckt
In Deutschland ungefähr 2% des Gesamtbudgets in IT!

Stichpunkte: duale Finanzierung, Investitionsstau

# Exkurs Informationssicherheit versus Cyber Sicherheit, Datensicherheit

- Resilienz
  - Informationssicherheit
  - Cyber Sicherheit
  - Datensicherheit
  - IT Sicherheit
  - OT Sicherheit

# Agenda

- Diagnostik: Die Bedrohung der Cyber Pandemie
- Die Impfung: Gesetzliche Vorschriften und Normen
- Prävention: Risikoanalyse für alle Bereiche
- Hygiene: Cyber Hygiene
- Behandlung: S.I.C.H.E.R Formel

# Die Impfung

# Gesetzliche Vorschriften und Normen als Schutzschild

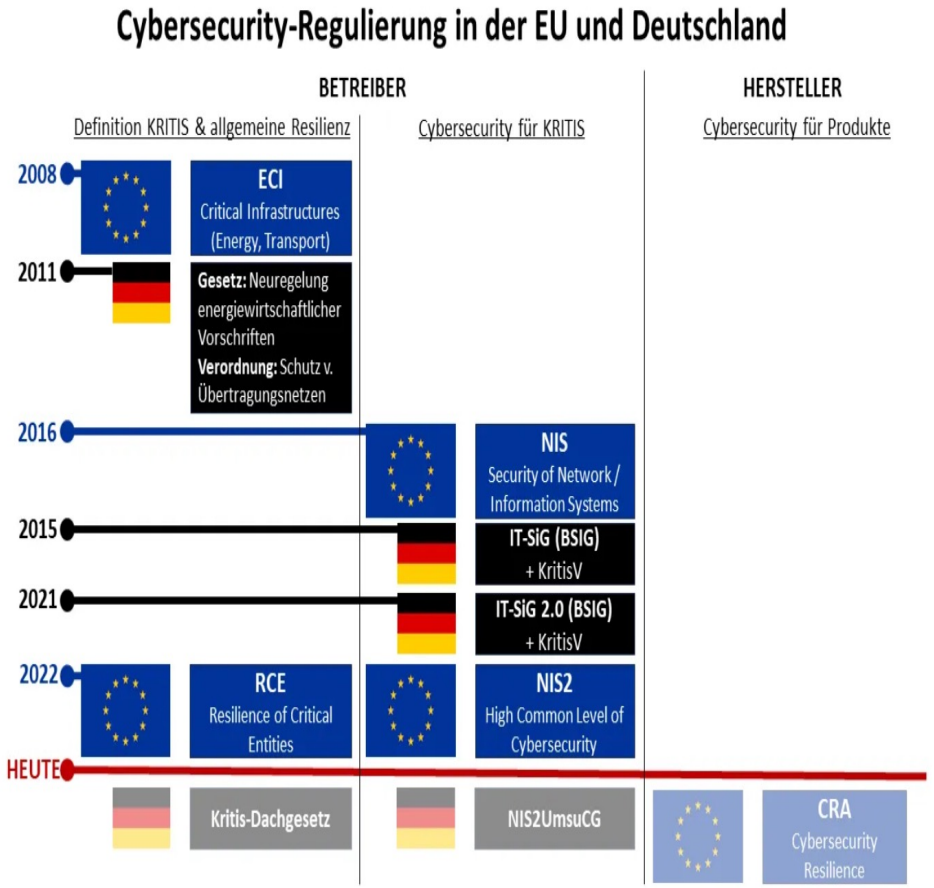
NIS2, RCE und ihre Bedeutung für die Informationssicherheit im Gesundheitswesen

# Die Impfung

| Gesetz | Jahr | Bedeutende Inhalte |
|---|---|---|
| IT-Sicherheitsgesetz | 2015 | • Änderungsgesetz für BSIG und weitere Gesetze<br>• Umfangreiche KRITIS-Definitionen und Sektoren<br>• Pflichten für Betreiber in §8a BSIG, Nachweise, Prüfungen<br>• Anlagenmethodik und Schwellenwerte (KritisV) |
| IT-Sicherheitsgesetz 2.0 | 2021 | • Änderungsgesetz für BSIG und weitere Gesetze<br>• Mehr KRITIS-Betreiber, neuer Sektor Entsorgung, zusätzlich UBI<br>• Mehr Pflichten für Betreiber, u.a. Angriffserkennung in §8a (1a) BSIG<br>• Höhere Sanktionen |
| NIS2-Umsetzung | 2024 | • Änderungsgesetz für BSIG und weitere Gesetze<br>• Neue »Einrichtungen«, mehr Sektoren, neue Gruppen<br>• Mehr Pflichten für Unternehmen, spezifisch Cybersecurity<br>• Viel höhere Sanktionen, engere Meldepflichten ans BSI |
| KRITIS-Dachgesetz | 2024 | • Eigenes Gesetz<br>• KRITIS-Sektoren und Betreiber, mit Ausnahmen<br>• Neue Pflichten für Betreiber: Resilienz, physische Sicherheit<br>• Sanktionen, Meldepflichten ans BBK |

Tabelle: *eigene Zusammenstellung IT-Sicherheitsgesetze seit 2015, Stand Januar 2024*

# Gesetzliche Vorschriften und Normen als Schutzschild



# Die Impfung

Und dann gibt es noch…
die Nationale Sicherheitsstrategie,
div, Strategien und Direktiven (Digitalisierung, KI, Patientensicherheit…)
Normen, Branchenspezifische Standards und Branchengesetzgebung

- Die Bundesregierung muss bis zum 17. Januar 2026 eine nationale Resilienzstrategie
- (Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen) verabschieden

# Die Impfung

# Kritis-Dachgesetz Risikoanalyse

erstmalig bis Januar 2026 durchzuführen von Bundes-und Landesministerien

- Risiken für die Wirtschaftsstabilität (hybride Angriffe, Terror, feindliche Bedrohungen
- Risiken für Binnenmarkt und Bevölkerung durch Abhängigkeiten
- Katastrophenschutzverfahren der Union (EU)
- Versorgungssicherheit (Hochwasser, Unfälle, Gasversorgung…)

# Die Impfung

# NIS2UmsuCG

**Zeitplan**

EU-Mitgliedsstaaten NIS2-Richtlinie bis spätes
dem **17.10.2**
Das G ichtlich
**v et** werden (6 Monate vor Inkrafttreten).

Schon gerissen

# Die Impfung

# Es hängt alles mit allem zusammen….

**Ein Hack gegen eine andere Infrastruktur kann Sie ebenso treffen.**

**Ebenso sind Lieferanten oder Mitarbeiter ohne es zu wollen der „ Vektor“ für eine Infektion**

# Agenda

- Diagnostik: Die Bedrohung der Cyber Pandemie
- Die Impfung: Gesetzliche Vorschriften und Normen
- Prävention: Risikoanalyse für alle Bereiche
- Hygiene: Cyber Hygiene
- Behandlung: S.I.C.H.E.R Formel

# Prävention

# Risikoanalyse und Risikomanagement im Gesundheitswesen

Warum ist das Risikomanagement ein zentrales Element?

> Hoping for the best, prepared for the worst, and unsurprised by anything in between.
>
> — Maya Angelou —

# Prävention

## Risikoanalyse und Risikomanagement im Gesundheitswesen

- Risiko identifizieren
- Risiko bewerten
- Risiken steuern
- Risiko Überwachung und Steuerung

# Prävention

Risikomatrix (nach Nohl)

| Wahrscheinlichkeit W | Mögliche Schadensschwere S: Leichte Verletzungen oder Erkrankungen | Mittelschwere Verletzungen oder Erkrankungen | Schwere Verletzungen oder Erkrankungen | Möglicher Tod, Katastrophe |
|---|---|---|---|---|
| sehr gering | 1 | 2 | 3 | 4 |
| gering | 2 | 3 | 4 | 5 |
| mittel | 3 | 4 | 5 | 6 |
| hoch | 4 | 5 | 6 | 7 |

www.maschinen-sicherheit.net

- 1-2: keine Risikoreduzierung nötig
- 3-4: Risikoreduzierung notwendig
- 5-7: Risikoreduzierung dringend notwendig

Risikomatrix nach Nohl

Besuchen

# Prävention: Stromausfall

- Überwachung - Automatisierung insbesondere autarke automatisierte strombezogene Sicherheitssysteme
- Analoge Szenarien und Übungen (inkl. Checklisten)
- Redundante Systeme
- Autarkie !
- Wartung

# Prävention -> Vorgehen

Checklisten
Asset und Risikomanagement
Emergency Response plans: Protokolle und Pläne inkl aller mögliche und unmögliche Risiken
Bevorratung und Lieferketten stabilisieren

Denken an!

Psychologische Effekte
Interessen der Stakeholder!
Wie wird Kommunikation und Versorgung gewährleistet
Evakuierungspläne
IT nicht vergessen!

# Agenda

- Diagnostik: Die Bedrohung der Cyber Pandemie
- Die Impfung: Gesetzliche Vorschriften und Normen
- Prävention: Risikoanalyse für alle Bereiche
- **Hygiene: Cyber Hygiene**
- Behandlung: S.I.C.H.E.R Formel

# Hygiene ist das halbe Leben:

# Cyber-Hygiene

Saubere Cyberhygiene beinhaltet –wie jede gute Hygiene – Schaffung von Routinen um die Gesundheit des Systems zu erhalten.

Richtlinien aufstellen und aktuell halten

- Dokumentieren und Inventarisieren aller Soft-und Hardware sowie ihre Verwaltung
- Nicht genutzte oder veraltete Hard- und Software sollte entfernt werden (Updates,Patches)
- Schutzmechanismen (zB Antimalwarerprodukte oder Firewalls überprüfen.
- Segmentierung
- Lieferanten und Hersteller prüfen
- Notfallpäne  (IRP Incident Response Plan)
- Off Site Back up
- BCM

# Hygiene ist das halbe Leben:

# Cyber -Hygiene

- Passwortmanagement und n-Faktorauthentification
- Logging und Montiroing
- Usermanagement  (für Daten und Anwendungen)
- Schulungen
- Stabstelle
- Üben üben üben

Wissen die Mitarbeiter was sie tun müssen?
Wissen die Mitarbeiter an wen sie sich wenden können?
Werden die Mitarbeiter im Notffall zu ihrer Familie müssen?

# Agenda

- Diagnostik: Die Bedrohung der Cyber Pandemie
- Die Impfung: Gesetzliche Vorschriften und Normen
- Prävention: Risikoanalyse für alle Bereiche
- Hygiene: Cyber Hygiene
- Behandlung: S.I.C.H.E.R Formel

# Die Behandlung

# Sicherheit mit der S.I.C.H.E.R Formel

S: Starke Passwörter verwenden
I: Infrastruktur regelmäßig überprüfen und aktualisieren
C: Continuous Monitoring für frühzeitige Erkennung von Anomalien
H: Human Factors berücksichtigen (z.B. Sensibilisierung für Phishing-Angriffe)
E: Encyption: Verschlüsselung für sensible Daten
R: Regelmäßige Überprüfung der Sicherheitsrichtlinien und -maßnahmen

# Widerstand, Erholung, Transformation

Hoping for the best, prepared for the worst, and unsurprised by anything in between.

— Maya Angelou —

# Mein Kontakt:

Ihr dürft mich gerne jederzeit kontaktieren!

Miriam Schnürer
GreenTEC Campus
Leckerstr. 7
25917 Enge-Sande
017647951418
miriam.schnuerer@bski.de

## Ist mein Krankenhaus eine Kritische Infrastruktur?

Krankenhäuser sind aufgrund ihrer herausragenden Bedeutung für die Bevölkerung eine zentrale Kritische Infrastruktur.

Die *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)* definiert im Hinblick auf die Sicherheit in der Informationstechnik Krankenhäuser mit mehr als 30.000 vollstationären Behandlungsfällen pro Jahr als kritische Anlagen im Bereich der stationären Versorgung. Dieser Schwellenwert spiegelt bewusst nur die Sicht des Bundes wider, regionale Versorgungsstrukturen werden dabei nicht berücksichtigt.

Eine flächendeckende medizinische Versorgung der Bevölkerung kann allein durch die Einrichtungen, die unter die BSI-KritisV fallen, besonders in weitläufigen Gebieten mit nur einem oder wenigen Krankenhäusern, jedoch nicht sichergestellt werden. So kann auch der Ausfall von Krankenhäusern mit niedrigeren Versorgungskennzahlen Kreise und Kommunen vor erhebliche Versorgungsprobleme stellen. Somit sind auch Krankenhäuser, die nicht unter das IT-Sicherheitsgesetz fallen Kritische Infrastrukturen im Hinblick auf die Versorgung der Bevölkerung.

Ausfall oder
itte.

nd ihrer

esellschaft.

Beschleunigung und Bruchstellen

Kritische Infrastrukturen sind Systeme und Einrichtungen, deren Ausfall oder Beeinträchtigung schwerwiegende Folgen für die Gesellschaft hätte.

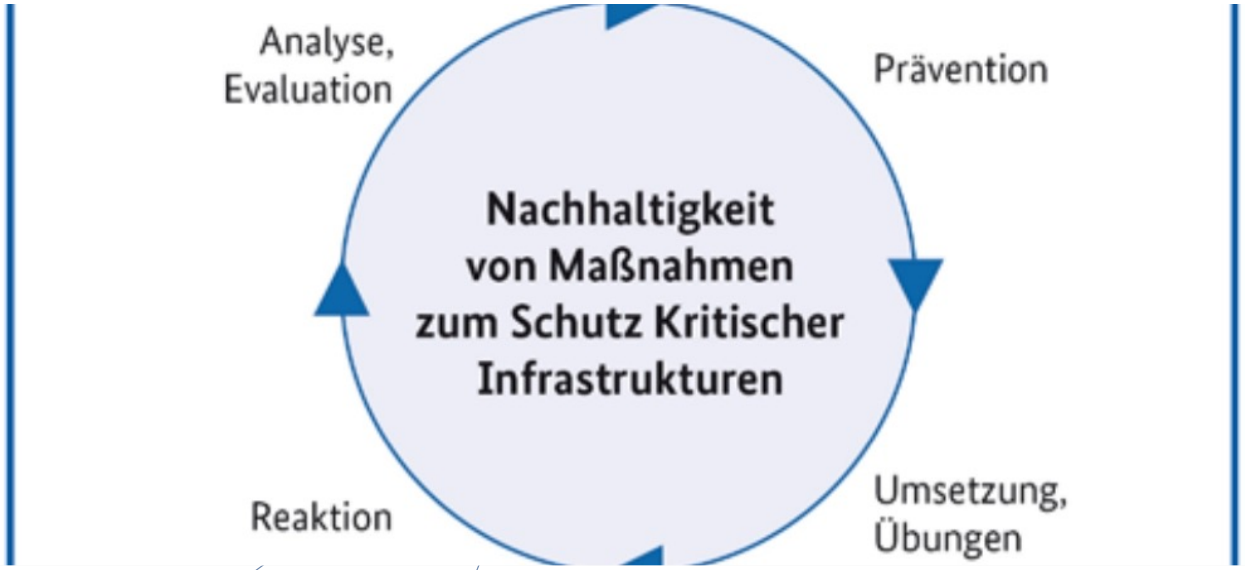
Krankenhäuser gehören zu den Kritischen Infrastrukturen aufgrund ihrer lebenswichtigen Rolle in der Gesundheitsversorgung.

Sie spielen eine unverzichtbare Rolle für das Funktionieren der Gesellschaft.

# ENISA EUROPA

- The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.

# Vorgehen Szenarien/Risiken durchspielen




Gefahren:

Naturkatastrophen/Klimawandel
CBRN (chemisch, biologisch, radiologisch, nuklear)
Kriminalität/Terror/Sabotage
Menschliches/technisches Versagen

# Schadenslagen Deutschland 2000-2023





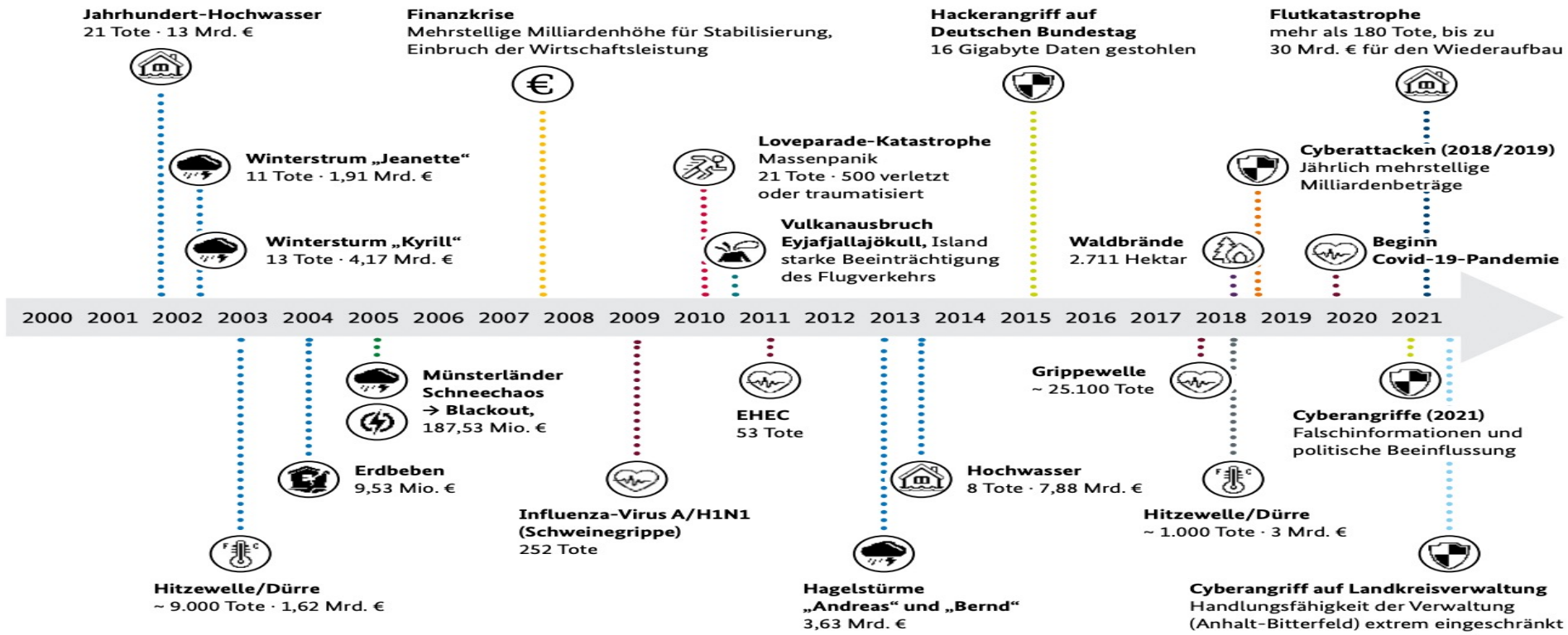



***Abbildung 1: Ausgewählte Schadenslagen in Deutschland zwischen 2000 und 2021 (Quelle Icons: Getty Images / diverse Künstler).***

# Neue und alte Herausforderungen

## Die BANI Welt

**Brittle (spröde, brüchig), anxious (verunsichtert), non linear, incomprehensible (unverständlich)**

| | | | |
|---|---|---|---|
| Brüchigkeit | Angst (Entscheidungsunwillen usw) | Nichtlineares, schlecht vorhersehbar | Incomprehensble (nicht nur komplexe sondern chaotische Probleme) |
| Belastbarkeit/Lockerheit/Flexibilität | Achtsamkeit/Empathie | Kontext/Flexibilität | Transparenz/Intuition |

# Schlüsselfaktoren für die Resilienz

- einen bewussten Umgang mit Risiken und deren frühzeitige Wahrnehmung
- eine verbesserte Planung und Etablierung von Steuerungsmaßnahmen
- ein stärkeres Verständnis für seine Stakeholder, Assets und Stakeholder
- Unternehmenskultur
- Simple Organisationsstrukturen

# Alles was schief gehen kann, wird schief gehen…zum ungünstigsten Zeitpunkt

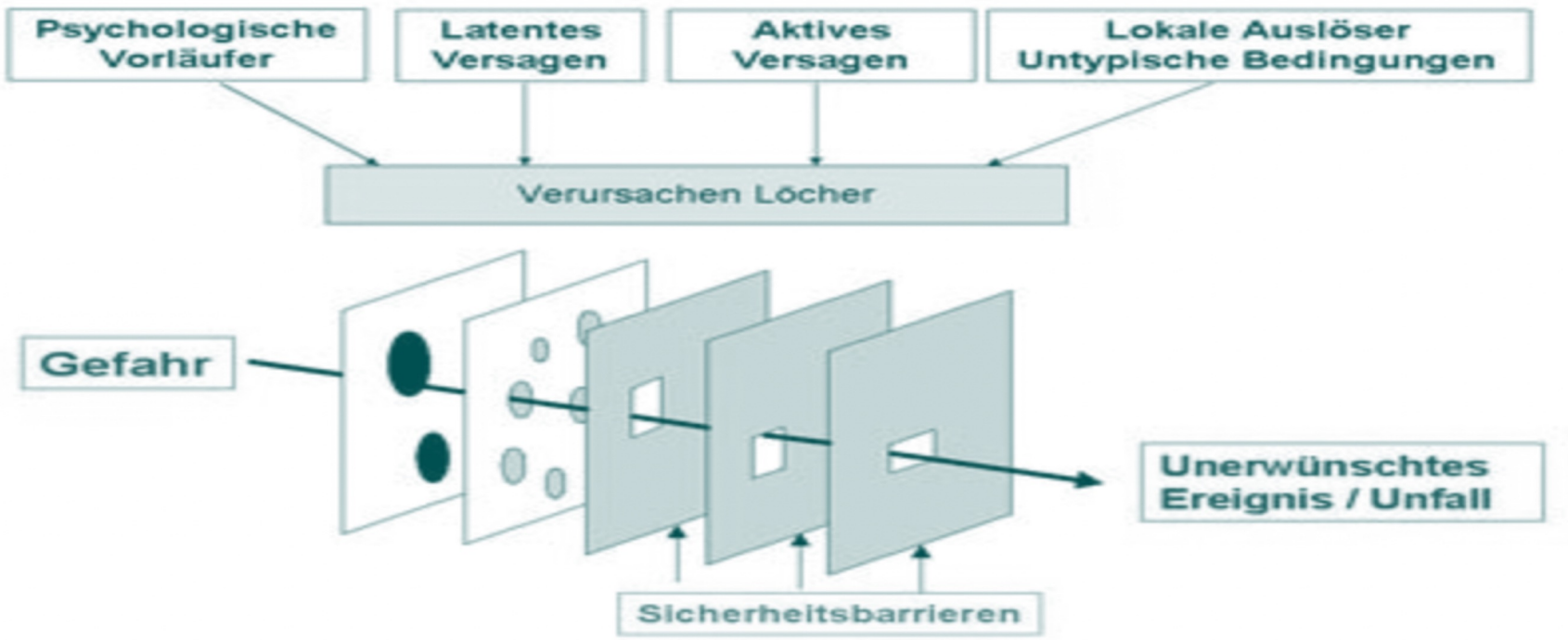



*Abb.: Swiss Cheese Model of System Accidents (nach Reason)*


# Wichtige Elemente für resiliente Organisationsformen

- Analyse des eigenen Hauses
- Risikomanagement und Vorausschau(Identifikation und Maßnahmen)
- Flexibilität und Anpassungsfähigkeit (Entscheidungsfindung, Kommunikation, Verantwortung/agile Methoden, Vertrauen)
- Führung in der Krise -> stark und koordiniert
- Lernende Organisation
- Kooperation und Netzwerke
- Psychologische Aspekte

ÜBEN ÜBEN ÜBEN

# Schutz

Prävention,
Detektion,
Mitigation,
Response/Awareness

PEN Tests und ÜBEN; ÜBEN; ÜBEN

1.Sensibilisierung und Schulung des Personals
2.Implementierung von Krisenplänen und Notfallmaßnahmen
3.Aufbau von Kooperationen und Netzwerken

# Schutz

## Normen und Vorschriften

Für die Steigerung der Resilienz in Unternehmen stehen eine Reihe von Normen und Rechtsvorschriften zur Verfügung:

- DIN EN ISO 22301:2020-06 Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (ISO 22301:2019); Deutsche Fassung EN ISO 22301:2019
- ISO 22316:2017-03 Sicherheit und Resilienz – Resilienz von Organisationen – Grundsätze und Attribute
- DIN ISO 22320:2019-07 Sicherheit und Resilienz – Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen (ISO 22320:2018)
- ISO 37301:2021-04 Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung
- ISO 31000:2018-02 Risikomanagement – Leitlinien

# Schutz

Proaktiv mit den Bundeskriminalämtern (IT-Sicherheit) oder benannten Stellen Kontakt aufnehmen

Proaktiv mit Landräten, Feuerwehr usw sprechen und gemeinsam Szenarien durchsprechen und entwickeln

ISO 27001
BCM! (Business Continuity Management einziehen)

BBK = Checklisten -> Achtung: diese sind nicht wirklich vollständig und umfassend