Beyond Cybersecurity

Informationssicherheit am Wendepunkt

Andrea Tribelhorn
Angelo Mathis
ISSS Vorstandsmitglieder

20/06/2024

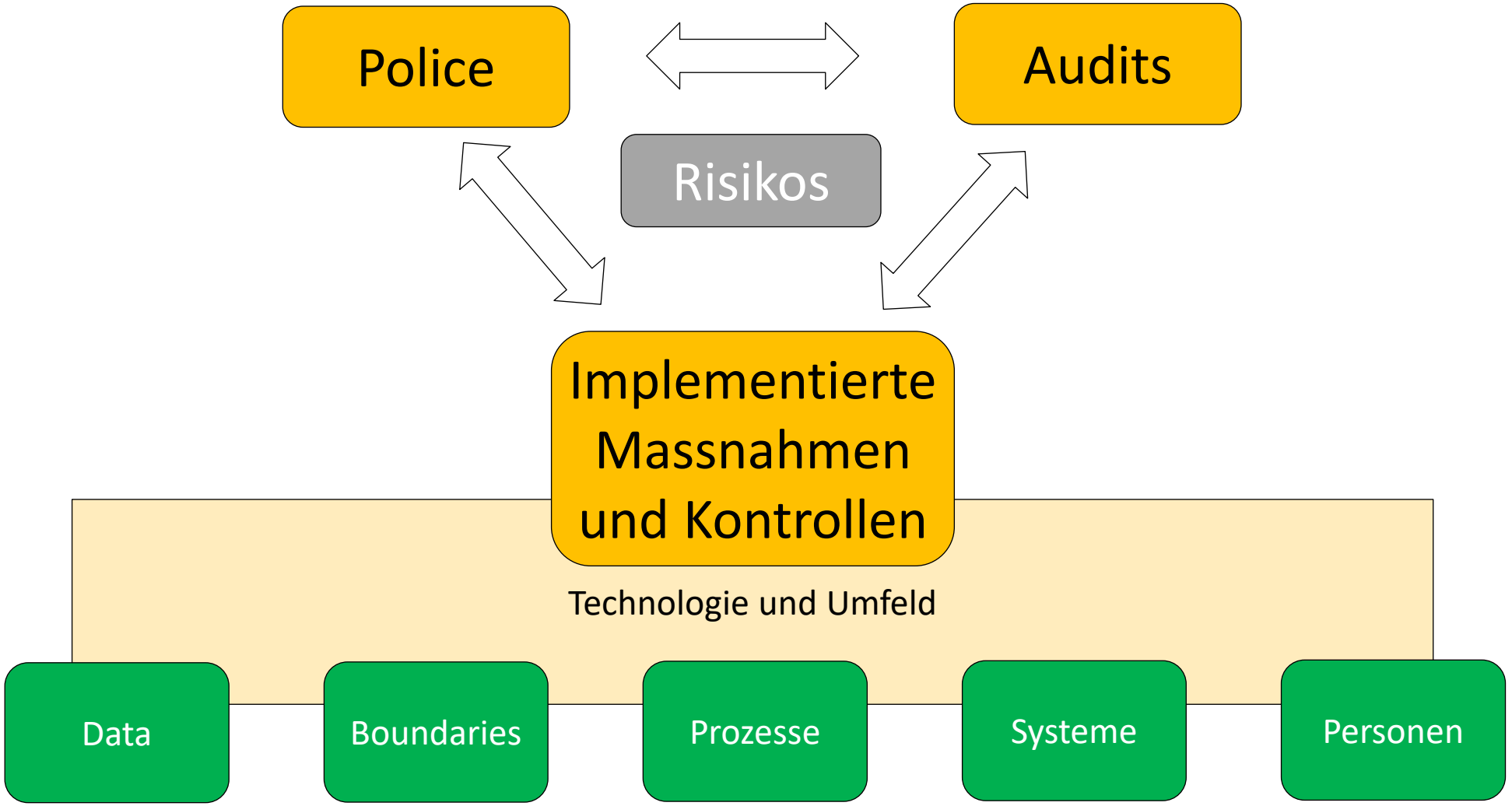
Beyond Cybersecurity – Informationssicherheit am Wendepunkt?

- **Cybersecurity** Challenges **im Gesundheitswesen**
- Technologischer Wandel als **Chance oder Risiko?**
- Regulatorische **Anforderungen**
- Cybersecurity **Fähigkeiten der Zukunft**

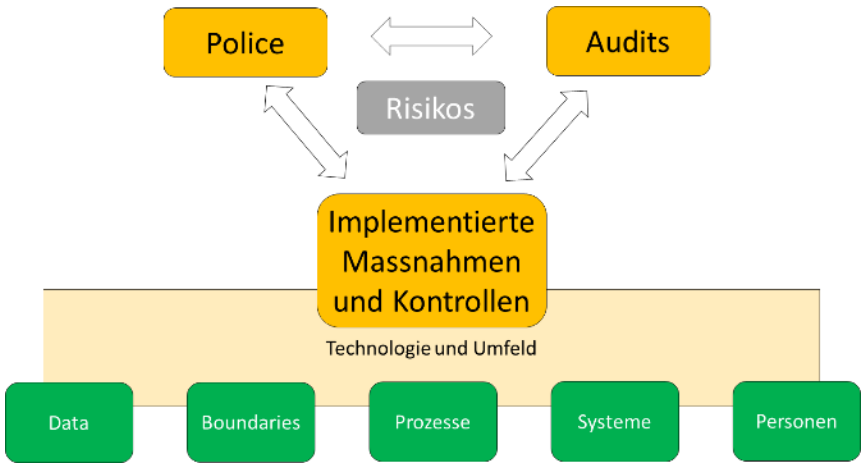
Beyond Cybersecurity – Informationssicherheit am Wendepunkt?

- **Cybersecurity** Challenges **im Gesundheitswesen**
- Technologischer Wandel als **Chance oder Risiko?**
- Regulatorische **Anforderungen**
- Cybersecurity **Fähigkeiten der Zukunft**

Was ist Sicherheit



Die Welt verändert sich massiv



Data: dezentralisiert / Cloud

Boudaries: Integrationen in Ecosysteme, international

Technologische Wendepunkte

- Künstliche Intelligenz (AI)
- Robots
- Digitale Medizin

Personen: Zunehmendes 'digitales Leben' beeinflusst Prozesse und Kontrollen

- Digitale ID
- Digitale Twins (Patienten) und digitale Spitäler (zB BIM)
- Neue Arbeitsweise (Home Office, nicht Vollzeit)
- Persönliche Technologie und Wearables
- Metaverse

Systeme und Prozesse:

- Digitalisierung
- Anything as a service
- APIs
- Vertikale und horizontale Prozessintegrationen
- Agile Entwicklungen
- Digital unterstützte administrative Prozesse und medizinische Entscheidungen

Umfeld:

- Bedrohungen von statlichen feindlichen Institutionen mit unvergleichlichen Ressourcen
- Überwachung und Manipulation von Informationsflüssen

Challenges / Implikationen für das Gesundheitswesen

- Resilienz der Systeme und der Prozesse
  - Operative Sicherheit
  - Prozessuale Sicherheit
  - Medizinische Sicherheit
- Sicherung der Data Privacy
  - Dezentrale Daten
- Sichere AI Integration
  - AI für Sicherheit
  - Schutz von AI
  - Zuverlässige AI

Beyond Cybersecurity – Informationssicherheit am Wendepunkt?

- **Cybersecurity** Challenges **im Gesundheitswesen**
- Technologischer Wandel als **Chance oder Risiko?**
- Regulatorische **Anforderungen**
- Cybersecurity **Fähigkeiten der Zukunft**

KI und Sicherheit

KI kann zur Verbesserung der Sicherheit eingesetzt werden

- Analysieren
- Muster erkennen
- Ausnahmen identifizieren"

Angreifer können KI nutzen, um Angriffe zu verbessern

- Gezielte Angriffe leichter durchzuführen
- Automatisierung
- Neue Schwachstellen leichter entdecken
- Beachten Sie, dass es in diesem 'neuen' Bereich eine Asymmetrie zugunsten des Angreifers gibt

KI ist Ziel des Angriffs

KI zu hacken ist überraschend einfach!

Chance und Massnahmen

Chancen:

- Der technologische Wandel ist am entstehen und verspricht immense Vorteile für das Gesundheitswesen medizinisch und prozessual / administrativ
- Neue Technologien bringen Vorteile für Resilienz, Data Privacy und Sicherheit.

Massnahmen:

- Risikostrategien neu gestalten
- Security by design verfolgen
- Neue Governance einführen (z.B. für KI)
- Nicht in Silos denken
- Im Ecosystemen denken und agieren
- Neue Skills in die Organisationen integrieren

Beyond Cybersecurity – Informationssicherheit am Wendepunkt?

- **Cybersecurity** Challenges **im Gesundheitswesen**
- Technologischer Wandel als **Chance oder Risiko?**
- Regulatorische **Anforderungen**
- Cybersecurity **Fähigkeiten der Zukunft**

National, EU & International

de facto Standards

Zunehmende Regulierung

Branchenspezifisch (bspw. GDK)

Technologie-spezifisch (bspw. EU AI Act)

Datenschutz

Informations-Sicherheits-Management (ISMS)

ICT-Risiko-Management

Meldepflichten

Nachweis-pflicht / Zertifizierungen

Cyber & Krisen Resilienz

3rd Party Risk Management

GDK = Gesundheitsirektorenkonferenz
AI = Artificial Intelligence

Beispiel: Informationssicherheitsgesetz (ISG) – seit Jan. 2024 in Kraft

Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen ab Januar 2025

ZIEL:

- **Frühwarnung und Übersicht zur Bedrohungslage:** Warnungen durch NCSC & Übersicht Bedrohungslage
- **Rechtssicherheit und -gleichheit:** Alle profitieren von den geteilten Informationen aber nicht alle sind bereit dazu, Informationen über Cyberangriffe zu teilen.
- **Internationaler Kontext**: Die Meldepflicht entspricht zu einem grossen Teil der Umsetzung der NIS2-Richtline.

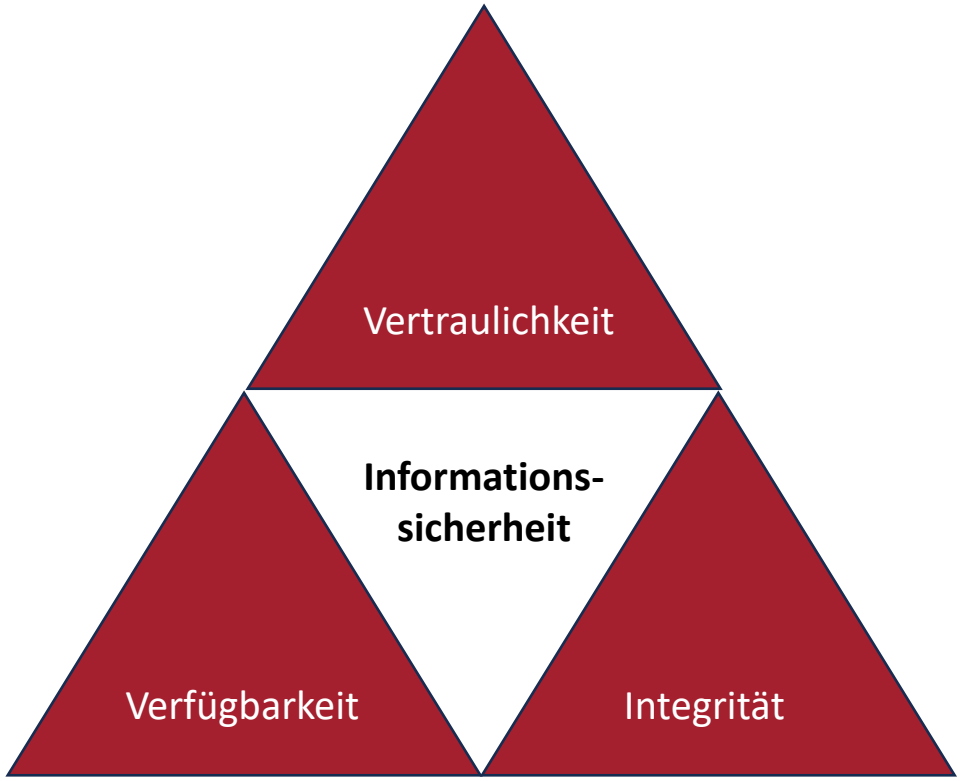
WER muss melden – Betreiberinnen kritischer Infrastrukturen (Art. 74b):

- f) **Gesundheitseinrichtungen** gemäss der kantonalen Spitalliste nach Art. 39 des Bundesgesetzes vom 18. März 1994
  g) **medizinische Laboratorien** mit einer Bewilligung nach Art.16 des Epidemiengesetzes vom 28. September 2012

FRIST der Meldung:

- Die Meldung muss **innert 24 Stunden** nach der Entdeckung des Cyberangriffs erfolgen.

Berücksichtigung der drei Schutzziele als Basis für Security Compliance



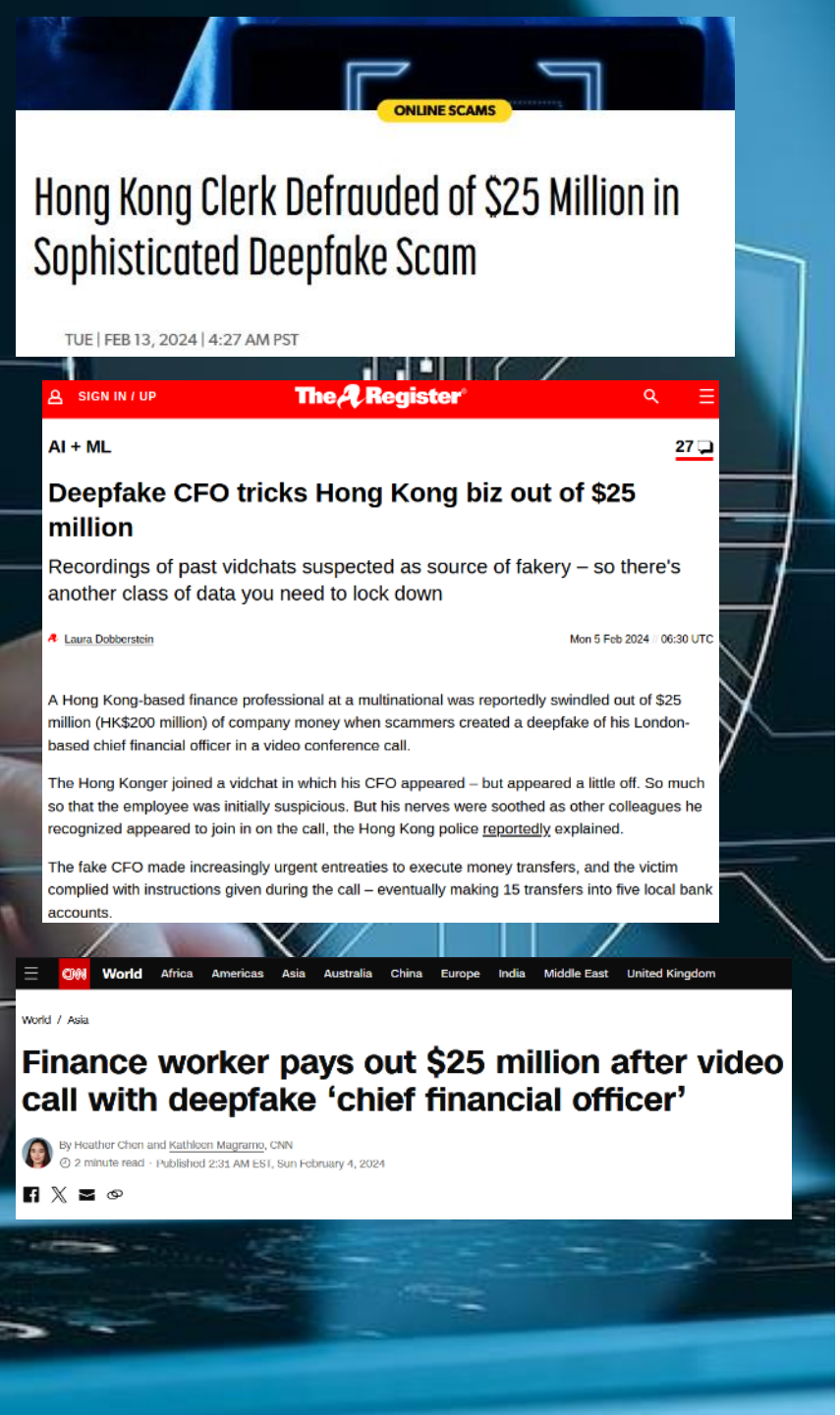
Hilfestellung für Umsetzung

ISSS Cyber-Navi
https://cybernavi.ch

Vortrag zum „Cyber-Navi for Healthcare“ um 14:25 hier in Raum Rigisaal

„Cyber Hygiene“ hilft auch die Compliance Anforderungen zu erfüllen

- **Ganzheitliche und wiederkehrende Auseinandersetzung mit dem Thema Informationssicherheit,** Steuerung des strategischen Unternehmensrisikos, Informationssicherheits-Management «Ich weiss, was für unsere Organisation wichtig ist in Bezug auf Informationen und IT»
- **Umsetzung grundlegender Massnahmen («IT Grundschutz»):** Patchen von Systemen, regelmässige Backups, Mehrfaktor-Authentifizierung (MFA), Accounts sind vor Fremdzugriffen geschützt, Monitoring
- **Wie reagieren wir im Notfall?** Sind wir vorbereitet? Haben wir einen Notfallplan, ein Krisenkommunikationskonzept, eine Krisenorganisation und Notfallkontakte?
- **Umsichtiges Verhalten aller Mitarbeitenden** zum Schutz vor Informationssicherheits-Risiken. Aufmerksamkeit für mögliche Risiken, Hilfe zur Selbsthilfe, eigenverantwortliches Handeln
- **Integration der Sicherheit** in Betrieb und Unternehmenskultur



Künstliche Intelligenz in der Cybersicherheit

- **Präventive Massnahmen**: Wichtig sind fortlaufende Schulungen, Zero Trust-Architekturen und KI-gestützte Sicherheitstools.
- **Zweischneidiges Schwert**: KI wird sowohl von Cyberexperten zur Abwehr von Angriffen als auch von Hackern für die Verbesserung ihrer Angriffsmethoden genutzt.

Fallbeispiel: Betrugsfall durch den Einsatz von Deepfake-Technologie in der Finanzbranche in Hong Kong

Problem

Ein Finanzmitarbeiter eines multinationalen Unternehmens wurde durch **Deepfake-Technologie** betrogen und überwies irrtümlich **25 Millionen** US-Dollar an Betrüger, die sich als sein CFO und Kollegen ausgaben.

Fazit

De… …e
be…
Sic…

Prozesse definieren & implementieren

Nicht alle (technischen) Herausforderungen erfordern eine **technische Lösung**

Beyond Cybersecurity – Informationssicherheit am Wendepunkt?

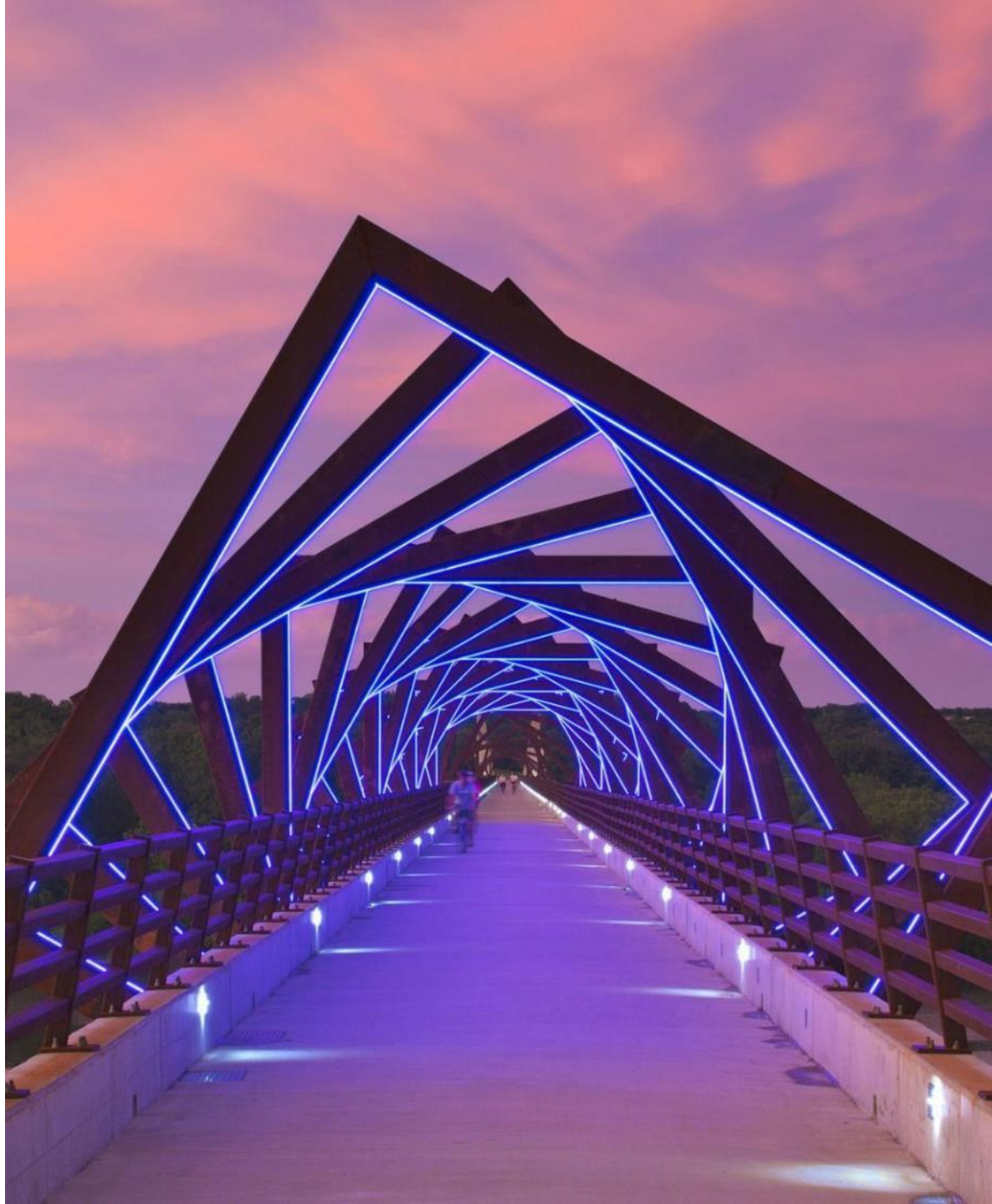
- **Cybersecurity** Challenges **im Gesundheitswesen**
- Technologischer Wandel als **Chance oder Risiko?**
- Regulatorische **Anforderungen**
- Cybersecurity **Fähigkeiten der Zukunft**

Hypothese

Das Security-Team wird durch künstliche Intelligenz ersetzt.

Wandel der Paradigmen

- Partizipative Sicherheit - Von Mauern zu **Brücken**
- **Flexibilität** statt statischer Ansätze
- Cybervorfälle zur **Vertrauensbildung**
- **Communities** einbeziehen - wie bspw. ethische Hacker
- Cybersicherheit ist Psychologie, Technologie, Kommunikation und Soziokultur



Exkurs: Cybervorfälle sind nicht das Ende der Welt
ISSS Courage Award Winners 2024

- Vertrauensbildung
- Mutig sein
- Proaktiv sein
- Hilfe herbeiziehen
- Werden Sie nicht zur Geisel!

Unico Data AG, Fondation de Verdeil, FedPol Switzerland

Der CISO von morgen

- Stratege und Teamplayer
- Interaktion mit Metaverse Strafverfolgungsbehörden
- Agiler Risikogestalter
- Vertrauensbildner für Menschen und Maschinen
- Partner in Vorständen und Gremien

Cybersecurity wird interdisziplinärer

Technisches Verständnis
Standards & Regularien
Innovation
Leadership
Mgmt. von Komplexität
Branchen-Kenntnisse
Risiko-Management
Ethik & Werte
Kommuni-kation
Projekt-leiter
Mitarbei-tende
Verwaltungs-rat
Juristen
Datenschutz
Fachbereiche
IT-Expert/innen
Infrastruktur / OT-Expert/innen
Einkauf
Risiko-Manager
Lieferant-/innen
Kund/innen

Das Security Team wird nicht (vollständig) durch künstliche Intelligenz ersetzt.

Take-Aways

- **Cyberangriffe** werden weiterhin **stark zunehmen** inkl. Fehlinformation und Desinformation.
- **Neue Technologien verbreiten sich rasant**. Zukünftig wird u.a. der **Umgang mit KI-Systemen** ein elementares Thema für Organisationen.
- **Compliance** ist ein zunehmend wichtiges Thema in der Cybersicherheit. Neue Regulierungen und Standards schaffen einen **Rahmen für den Schutz von Informationen**.
- Durch die **zunehmende Vernetzung** und Abhängigkeit von technischen Lösungen wird **Cybersecurity** ein wichtiger Bestandteil der **Unternehmensstrategie** und im strategischen **Risikomanagement** (VR-Ebene).
- **Kollaboration** über Unternehmensgrenzen hinweg wird immer wichtiger.
- Nicht alle (technischen) **Probleme** bedürfen einer technischen **Lösung**.
- Informationssicherheit ist
  1) **Chefsache** und 2) ein **kontinuierlicher Prozess**

Vielen Dank für Ihre Aufmerksamkeit!

/SSS information security society switzerland

Email: info@isss.ch
Telefon: +41 31 311 53 00
Webseite: www.isss.ch

Andrea Tribelhorn
Mitglied der Geschäftsleitung
Detecon (Schweiz) AG

Mobile: +41 (0)79 798 82 95
Email: Andrea.Tribelhorn@detecon.com

Angelo Mathis
Digital Assurance @ PWC

Mobile: +41 (0)79 795 01 11
Email: angelo.mathis@pwc.ch