Digital MasterClass

Kantonsrat Zürich

Cybersicherheit braucht mehr als nur Technologie

Zürich, 21. Oktober 2024

Dr. Ariane Trammell,
Leiterin der Information Security Research Group an der ZHAW

Dr. Melanie Knieps,
Forscherin für Cybersicherheit an der Universität Zürich

Eine Veranstaltung von:

Universität Zürich[UZH]
Digital Society Initiative

Partner:

Parldigi

Unterstützt durch:

DIZH

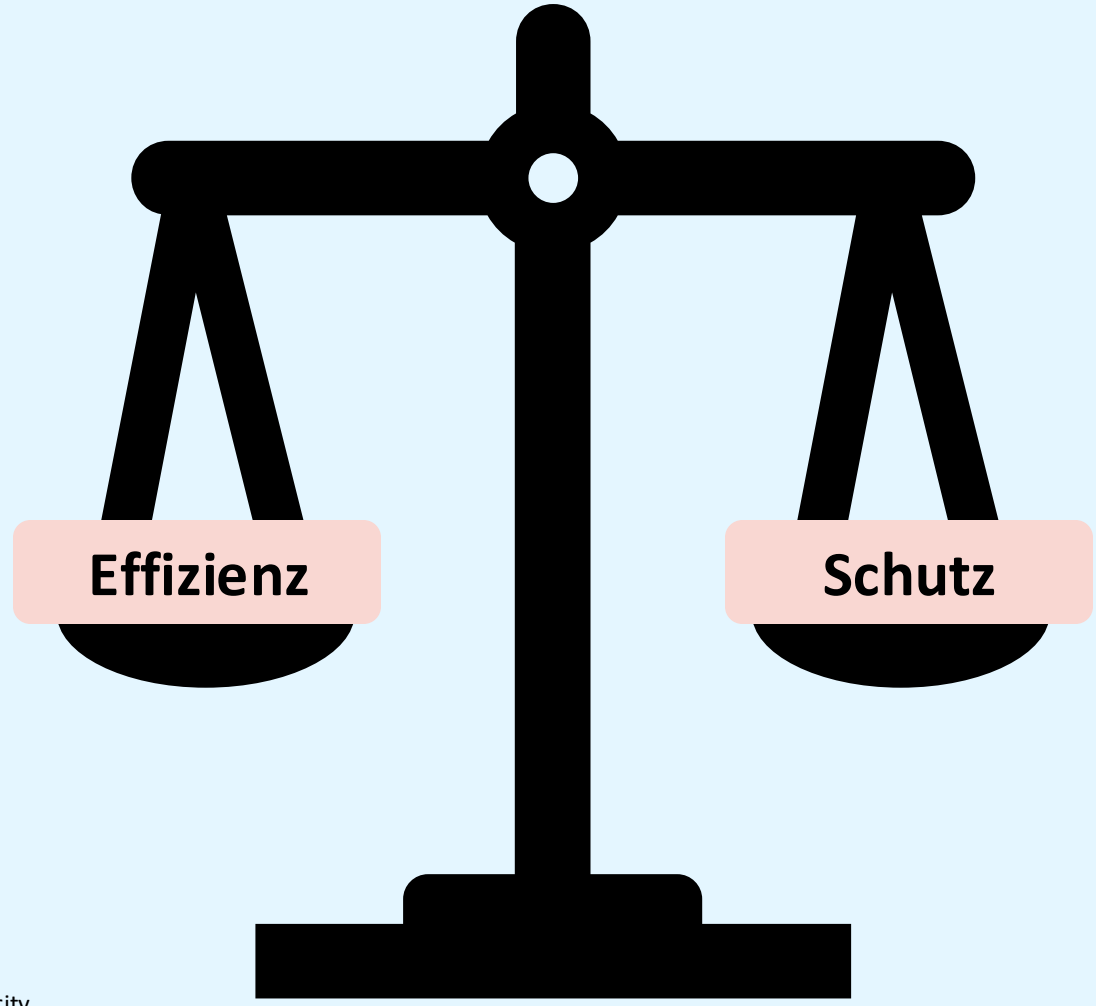
Stiftung Mercator Schweiz

Masterclass Cybersecurity

Gemeinsam für eine sichere Digitalisierung

Dr. Melanie Knieps und Dr. Ariane Trammell

Das Dilemma der digitalen Transformierung



Das Dilemma der digitalen Transformierung

Effizienz

Schutz

Agil

Das Dilemma der digitalen Transformierung

Effizienz

Schutz

Agil

Sicher

Abwägen

Wie finde ich einen guten Kompromiss?

Die Nationale Cyber Strategie (NCS)

Vision

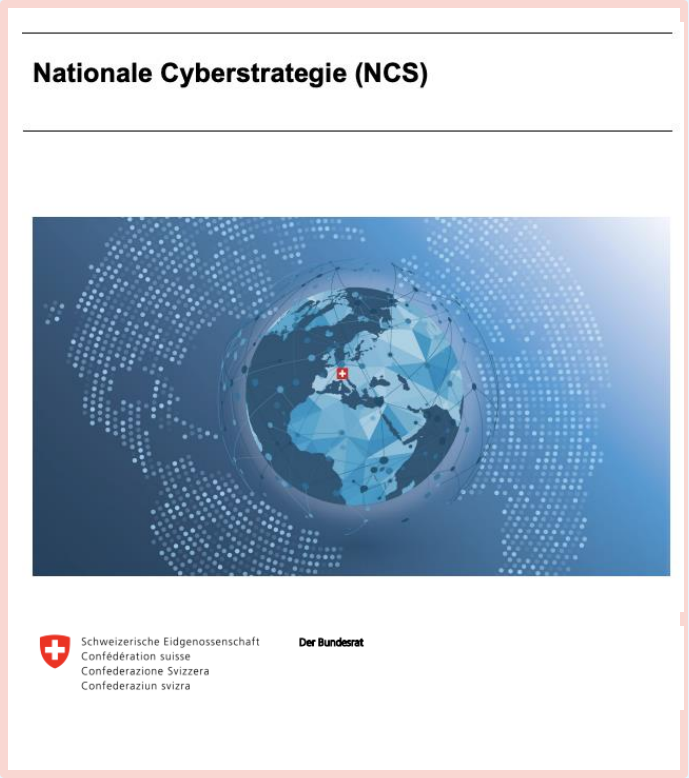
Effizienz

"Die Schweiz nutzt die **Chancen der Digitalisierung** und mindert Cyberbedrohungen und deren Auswirkungen durch geeignete **Schutzmassnahmen**."

Schutz

Herangehensweise

Die Schweiz befürwortet dabei einen **inklusiven Multi-Stakeholder-Ansatz**.



Die 1. Nationale Cyber Sicherheitskonferenz (NCSK)

26. September 2024:

280 Teilnehmende aus Wirtschaft, Wissenschaft, Kantonen und Verwaltung

Warum einen Multistakeholder Ansatz?

Weil arbeiten in Silos zu Problemen führt:

1. Mangelnde Kommunikation
2. Doppelaufwand
3. Nicht abgestimmte Zielsetzung
4. Weniger Innovation
5. Langsame Entscheidungsfindung
6. Geringere Motivation der MA
8. Ineffiziente Nutzung von Ressourcen
9. Widerstand gegen Veränderungen

Experteninput

Man muss unterschiedliche Perspektiven einbeziehen!

Kurzvorstellung

Psychologie

Melanie Knieps

Informationssicherheit

Ariane Trammell

Fakten

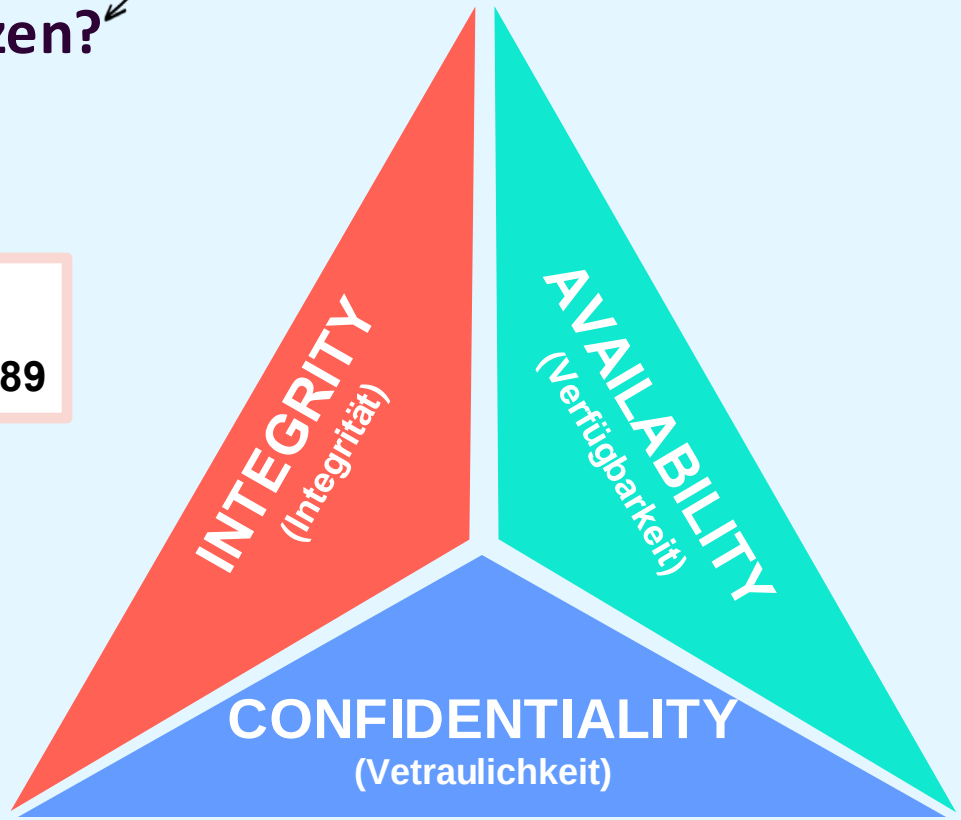
Was ist die Bedrohungslage in der Schweiz?

Allgemeine CIA Schutzziele

Was wollen wir schützen?

Kontostand

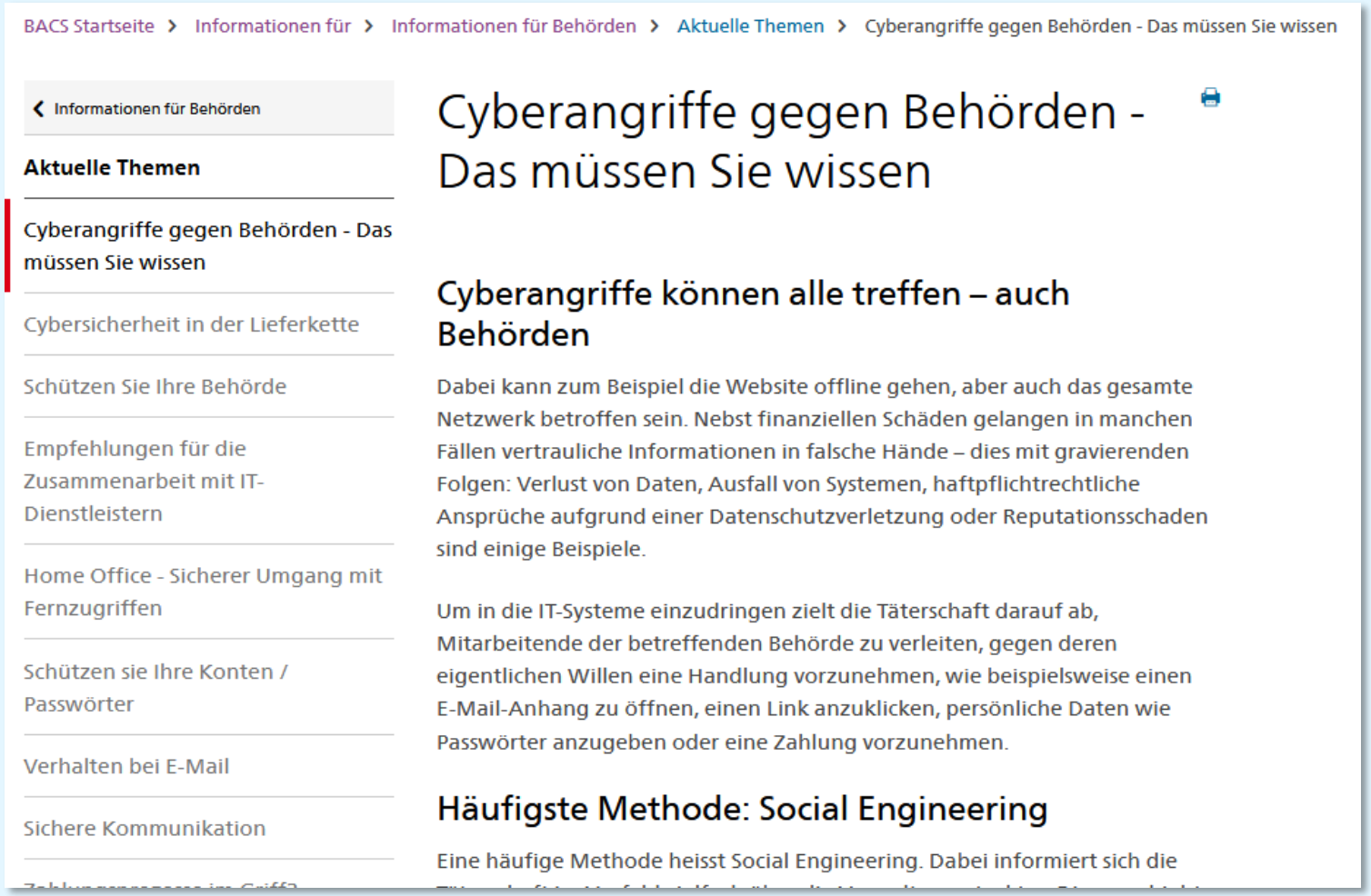
~~CHF 5.547~~ → CHF 1.789



Laut BACS

Bedrohungen gegen Behörden

- **Ransomware**
- **Datenabfluss**
- **Denial of Service**
- **Schadsoftware**
- **Phishing**
- **CEO Betrug**



BACS Startseite › Informationen für › Informationen für Behörden › Aktuelle Themen › Cyberangriffe gegen Behörden - Das müssen Sie wissen

‹ Informationen für Behörden

Aktuelle Themen

- Cyberangriffe gegen Behörden - Das müssen Sie wissen
- Cybersicherheit in der Lieferkette
- Schützen Sie Ihre Behörde
- Empfehlungen für die Zusammenarbeit mit IT-Dienstleistern
- Home Office - Sicherer Umgang mit Fernzugriffen
- Schützen sie Ihre Konten / Passwörter
- Verhalten bei E-Mail
- Sichere Kommunikation

Cyberangriffe gegen Behörden - Das müssen Sie wissen

Cyberangriffe können alle treffen – auch Behörden

Dabei kann zum Beispiel die Website offline gehen, aber auch das gesamte Netzwerk betroffen sein. Nebst finanziellen Schäden gelangen in manchen Fällen vertrauliche Informationen in falsche Hände – dies mit gravierenden Folgen: Verlust von Daten, Ausfall von Systemen, haftpflichtrechtliche Ansprüche aufgrund einer Datenschutzverletzung oder Reputationsschaden sind einige Beispiele.

Um in die IT-Systeme einzudringen zielt die Täterschaft darauf ab, Mitarbeitende der betreffenden Behörde zu verleiten, gegen deren eigentlichen Willen eine Handlung vorzunehmen, wie beispielsweise einen E-Mail-Anhang zu öffnen, einen Link anzuklicken, persönliche Daten wie Passwörter anzugeben oder eine Zahlung vorzunehmen.

Häufigste Methode: Social Engineering

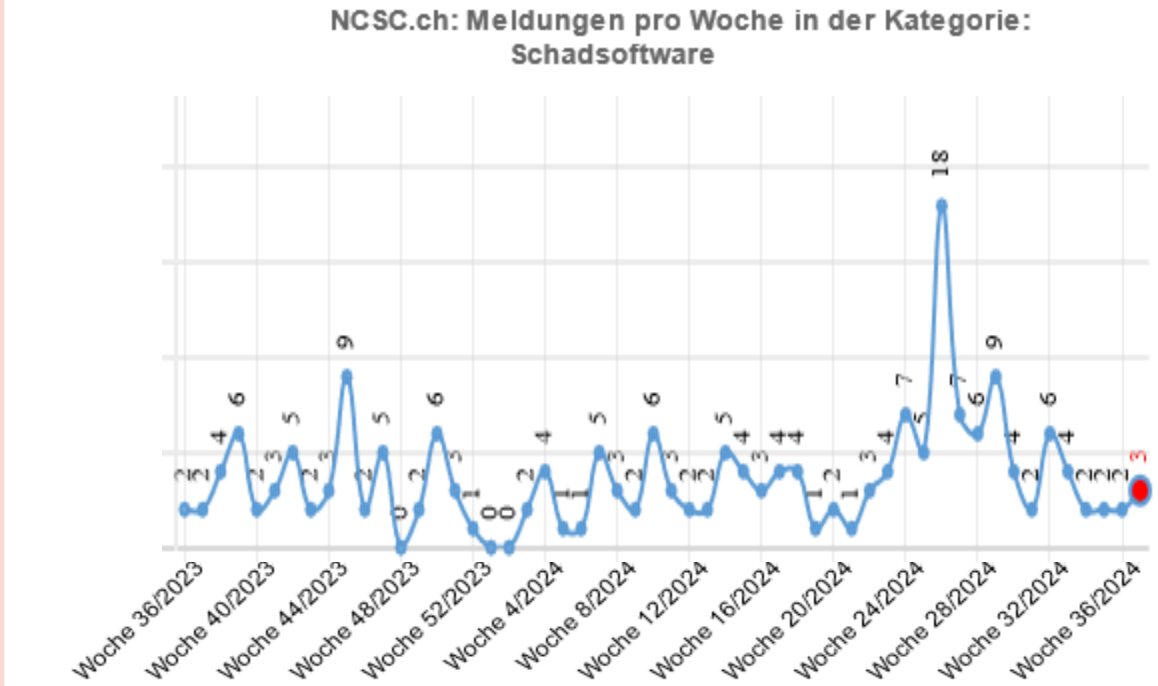
Eine häufige Methode heisst Social Engineering. Dabei informiert sich die

src: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden/aktuelle-themen/cyberangriffe-gegen-behoerden.html

Die Bedrohung in Zahlen

Pro Jahr werden dem BACS ca. 200 Fälle von Schadsoftware gemeldet.

Ungefähr die Hälfte davon ist Ransomware.



src: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html

Angriffe auf Schweizer Behörden

DDoS Angriff auf Bundesverwaltung

Wahrscheinlich als Demonstration gegen den Besuch von Wolodimir Selenski

DDos-Angriff

Hackerangriff auf Bundesverwaltung

Montag, 12.06.2023, 08:23 Uhr
Aktualisiert um 16:24 Uhr

TEILEN

- Mehrere Webseiten der Bundesverwaltung sind vorübergehend nicht mehr erreichbar gewesen.
- Grund war ein sogenannter DDoS-Angriff auf die Systeme der Bundesverwaltung.
- Ermittlungen der Bundesanwaltschaft sind im Gang.

Die Spezialisten der Bundesverwaltung hätten den Angriff rasch bemerkt und Massnahmen getroffen, um die Erreichbarkeit der Webseiten und Anwendungen so rasch wie möglich wieder herzustellen, teilte das Eidgenössische Finanzdepartement (EFD) mit.

Der Angriff habe offenbar der ganzen Bundesverwaltung gegolten, teilte das Nationale Zentrum für Cybersicherheit (NCSC) auf Anfrage mit. Zeitweise sei ein Grossteil der Webseiten der Bundesverwaltung und bundesnaher Betriebe sowie mehrere Anwendungen des Bundes nicht verfügbar gewesen.

Strafverfahren gegen Hackergruppe

Online zum Angriff bekannt habe sich die Gruppierung «NoName». Diese

src: https://www.srf.ch/news/schweiz/ddos-angriff-hackerangriff-auf-bundesverwaltung

Angriffe auf Schweizer Behörden

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Polizei fedpol

Versorgungskette

Hackerangriff auf Firma Xplain: Auswirkungen auf fedpol und getroffene Massnahmen

Anfang Juni 2023 wurde öffentlich bekannt, dass die Schweizer Firma Xplain, eine Anbieterin von Software für Sicherheitsbehörden und Blaulichtorganisationen, Opfer eines Ransomware-Angriffs der Hackergruppe Play geworden ist. Da Xplain in Absprache mit den Strafverfolgungsbehörden und dem Bund nicht auf die Lösegeldforderungen einging, veröffentlichten die Hacker Mitte Juni 2023 das entwendete Datenpaket im Darknet. fedpol ist – neben anderen Verwaltungseinheiten von Bund und Kantonen – ebenfalls vom Datendiebstahl betroffen.
Die Firma Xplain informierte das Bundesamt für Cybersicherheit (BACS) über den Cybervorfall und erstattete Strafanzeige bei der Kantonspolizei Bern. fedpol wurde von Xplain am 23.05. 2023 über den Datendiebstahl informiert. Nach Bekanntwerden des Vorfalls reichte fedpol bei der Bundesanwaltschaft Strafanzeige gegen Unbekannt ein und informierte den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) über den Datenabfluss.

Wie ist fedpol betroffen

Vom gesamten heute bekannten gestohlenen und im Darknet publizierten Datenvolumen machen Daten mit fedpol-Bezug gemäss aktuellem Kenntnisstand (Stand September 2023) weniger als 10% aus. fedpol hat dank eigener Analysen bereits frühzeitig festgestellt, dass darunter auch operative

Fakten

Von wem geht die Bedrohungslage aus?


Staatlich Finanziert
Organisierte Kriminalität
Opportunistische Angreifer
Massenangriffe / Hintergrundrauschen
Raffinesse
Verfügbare Ressourcen
Möglicher Schaden
Anzahl Akteure
Anzahl Angriffe
Anzahl Opfer

Fakten

Die Bedrohungslandschaft ist vielfältig und professionell.

Experteneinschätzung

Wie bestimmt man das Risiko?

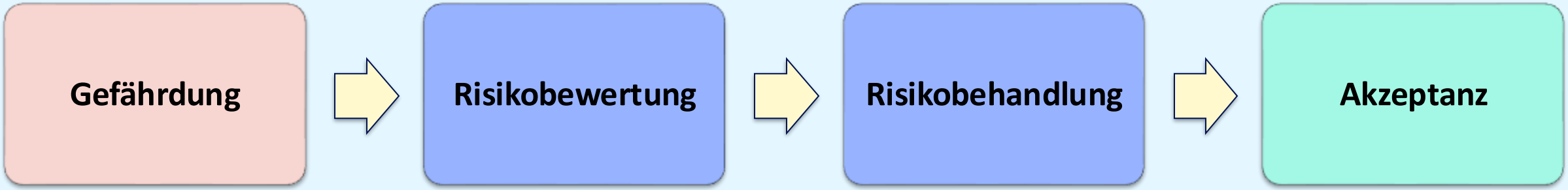
Was bestimmt das Risiko eines Cyberangriffs?

Motivation → Fähigkeiten → Möglichkeiten → Risiko

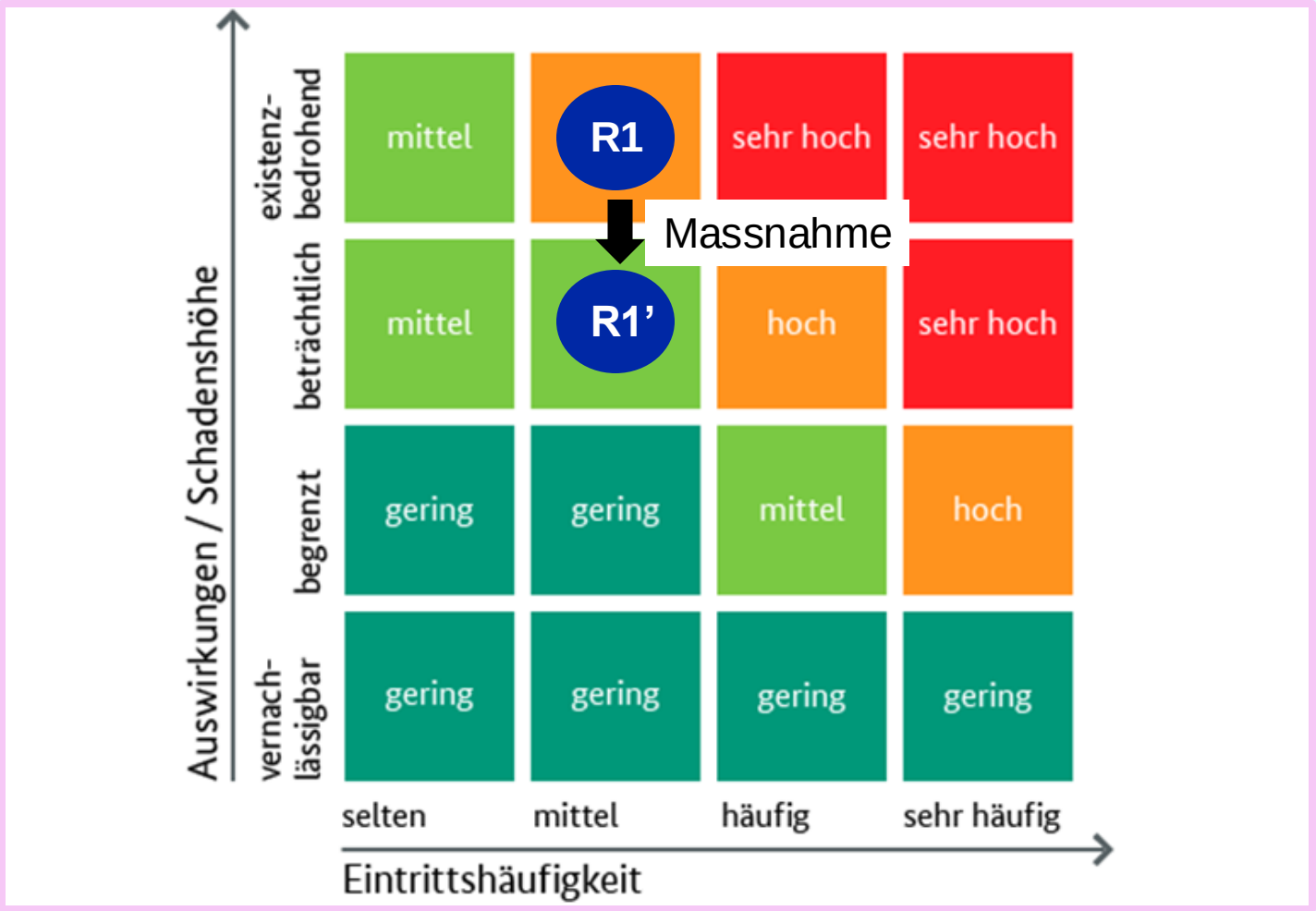
Experteneinschätzung

Wie managt man das Risiko?

Management von Cyberrisiken



Management von Cyberrisiken



Src:https://www.bsi.bund.de

Reduktion der Risiken durch Technische und Organisatorische Massnahmen (TOM)

- Firewalls
- Patch Management
- MFA
- Backups
- Verschlüsselung
- Etc.

Technische Massnahmen

ZUSAMMENSPIEL

- Schulungen
- Prozesse
- Vorgaben
- Arbeitsklima
- Konzepte
- Etc.

Organisatorische Massnahmen

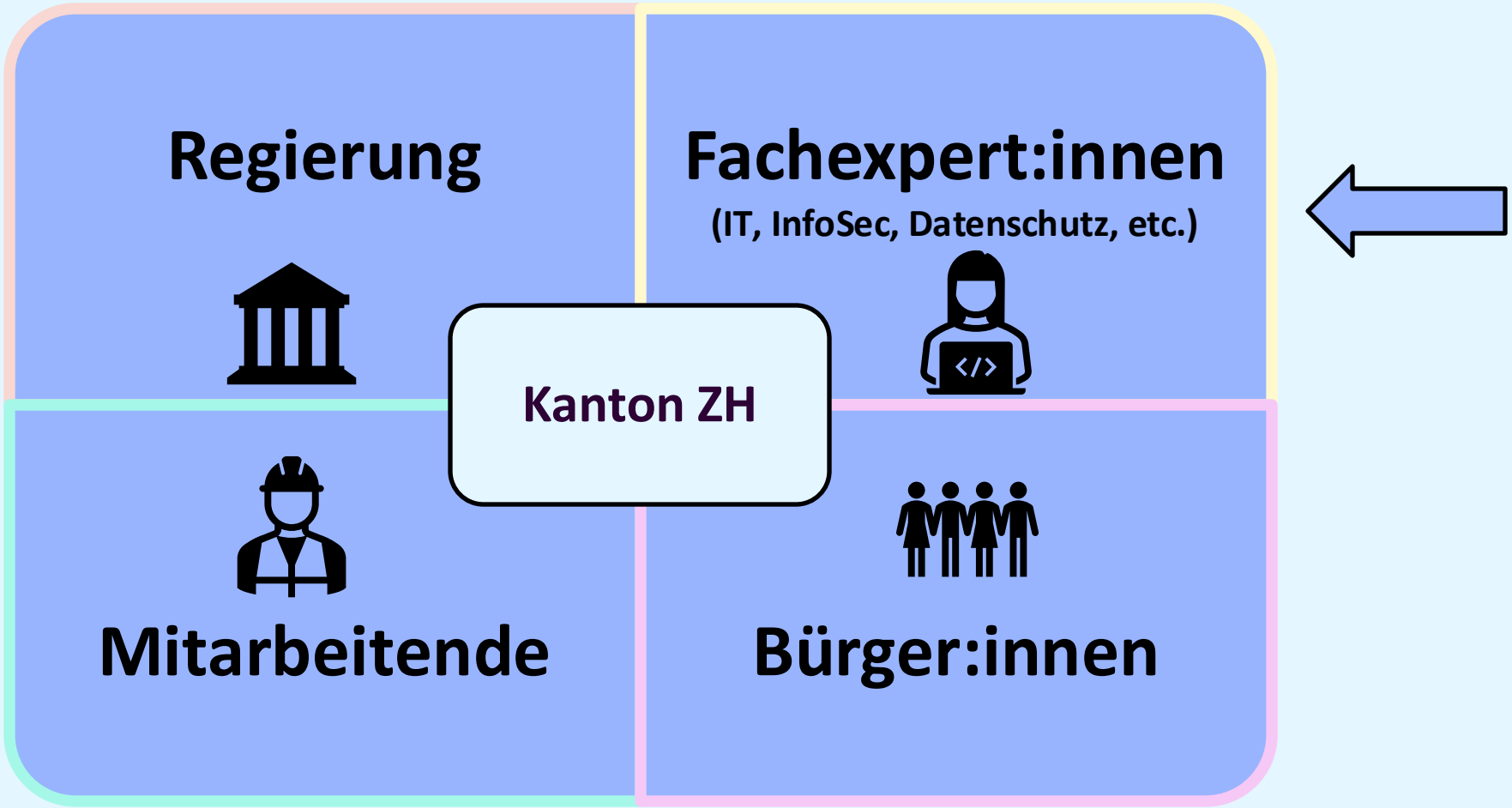
Risiko-Analyse

Risiken und Massnahmen sind organisations-spezifisch.

Verantwortung

Wer schützt den Kanton?

Cybersecurity funktioniert nur dann, wenn alle mitmachen!



Organisationsstruktur zur Umsetzung von Cybersecurity
3 Lines of Defense

IT-Betrieb

Ausführung von Prozessen

1. Line of Defense

Risiko Management

Definition von Vorgaben

2. Line of Defense

Interner Audit

Externer Audit

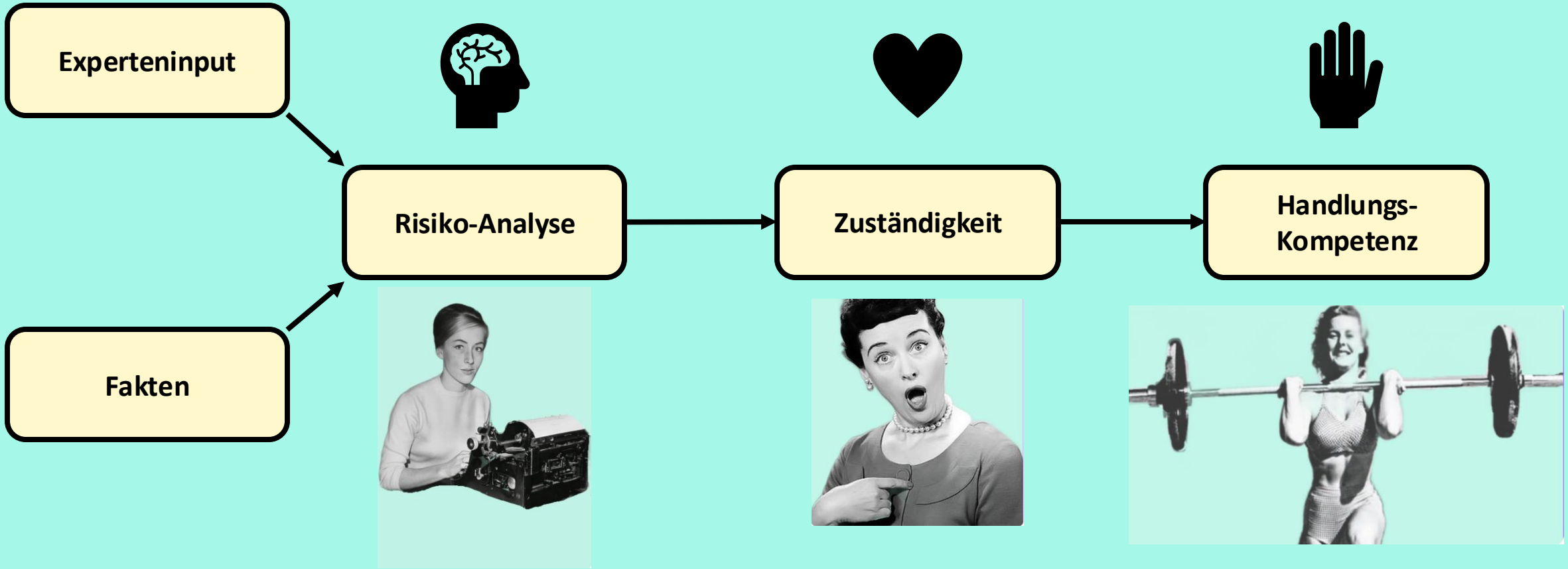
3. Line of Defense

Teamwork

Zuständigkeit

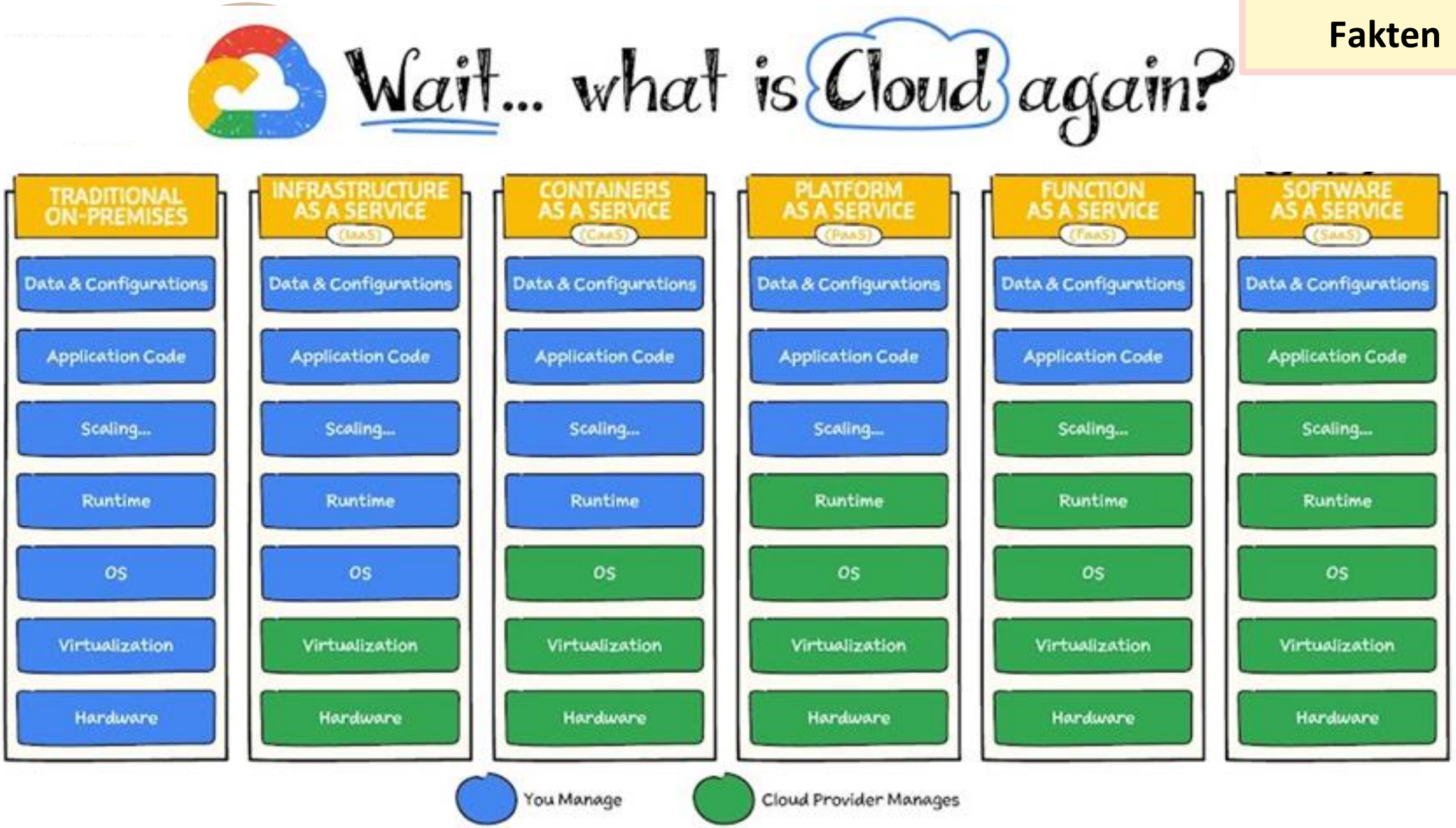
Cybesicherheit ist eine Teamaufgabe.

Teamwork und Eigenverantwortung ermöglichen Cybersicherheit



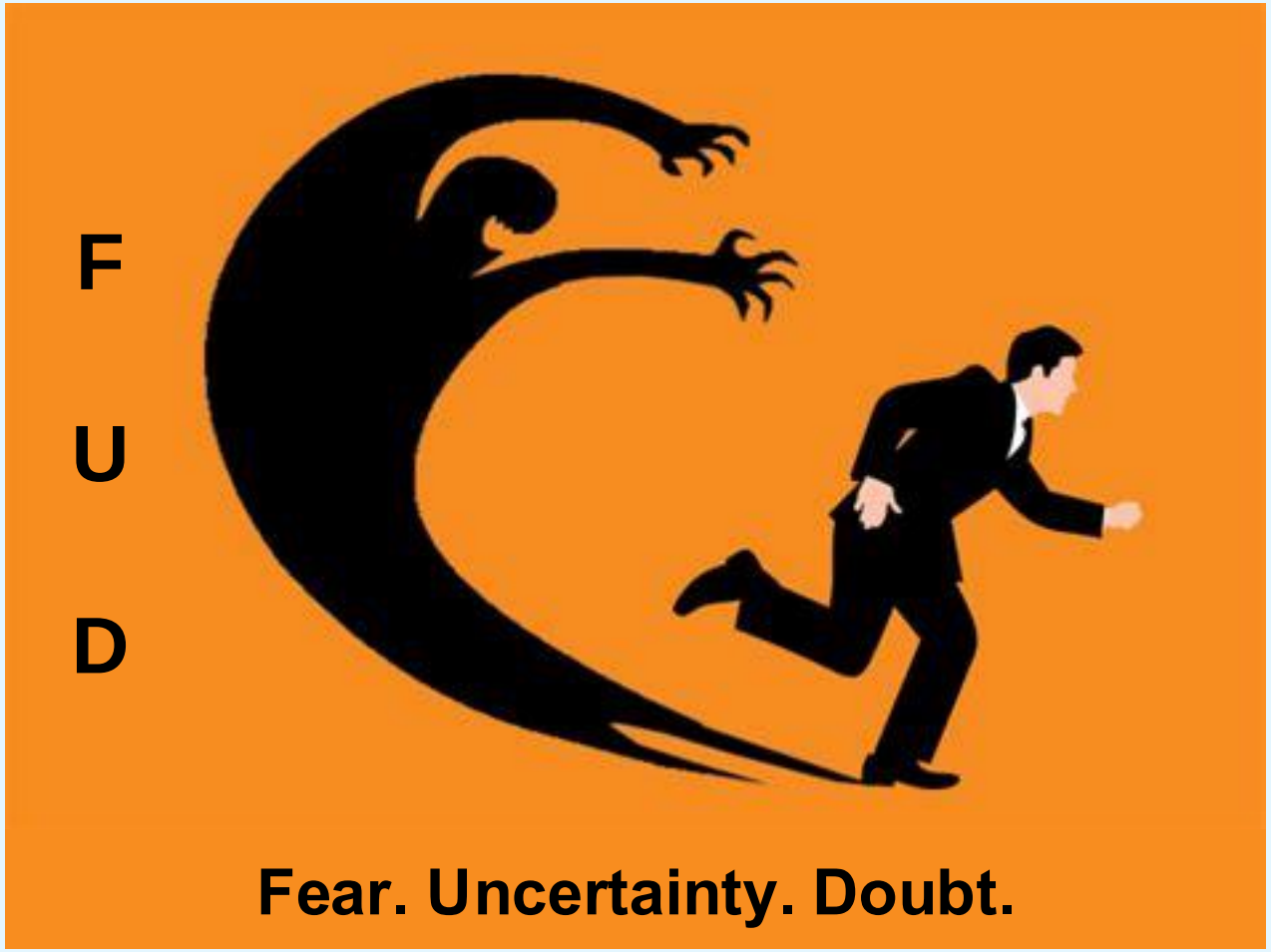
Beispiel

Was bedeutet das für die Nutzung der Cloud?



https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=de

Vorsicht mit Emotionen



Emotionen wie Bauchgefühl oder Intuition sind eine gute Entscheidungshilfe bei Menschen mit langjähriger Expertise.

ABER: Fachfremde sollten ihre Emotionen kritisch betrachten.

Was sind Emotionen?
Was sind Fakten?

Vertrauen hilft bei FUD

Service-Provider

Kompetenz	+
Benevolenz	= / +
Integrität	+

Microsoft 365

End-to-end Verschlüsselung?

Judikative

Kompetenz	+
Benevolenz	= / +
Integrität	+

Geheimdienste Exekutive

Kompetenz	?
Benevolenz	?
Integrität	?

Fakten? Emotionen?

Zu Bedenken

Zertifizierte Clouds verwenden

Es gibt viele Zertifizierungen für Cloud Provider welche vor Vertragsabschluss geprüft werden müssen!

Beispiel:
ISO 27001, 27017, 27018
SSAE18 SOC 1, SOC 2, SOC 3
etc.

Vertrag abschliessen

Verträge definieren Zuständigkeiten, Service Level Agreements (SLAs), Kosten, etc.

Compliance beachten

Vor allem im Hinblick auf den Datenschutz.
Wo werden Daten gespeichert?
Wie werden Daten gelöscht?

Technik verstehen

Grosse Cloud-Anbieter bieten Ausbildungen und Zertifizierungen für ihre Cloud Infrastruktur (allgemein und Security)

Beispiel:
Google Cloud Certified Security Engineer
AWS Certified Security Specialist
Microsoft SC-900

Nutzen und Risiken in der Cloud

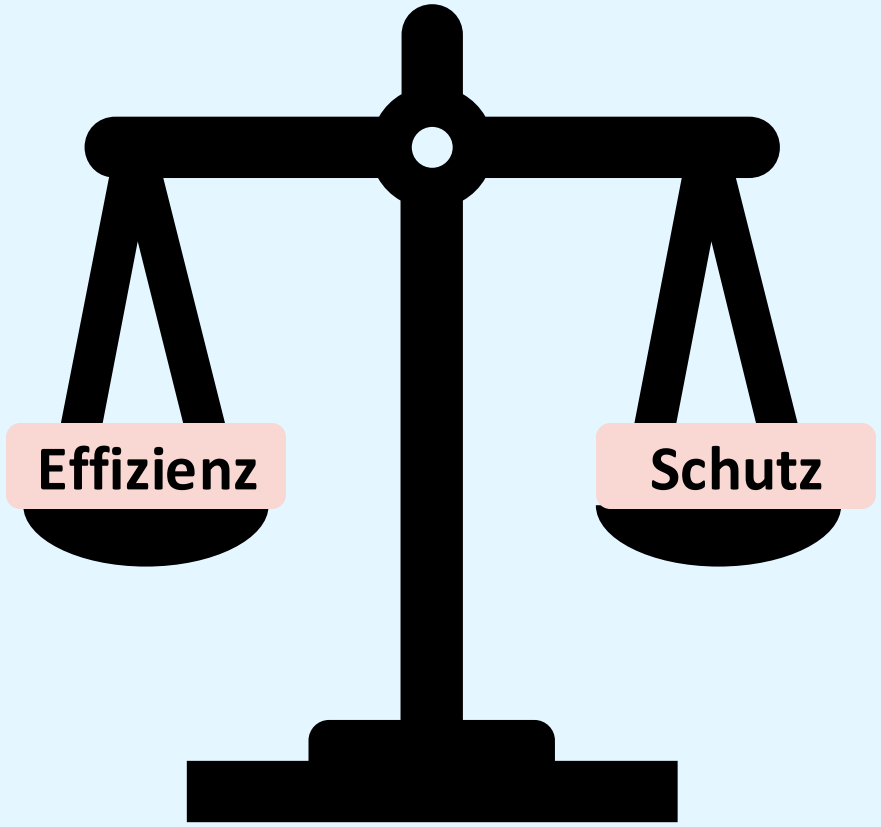
Nutzen

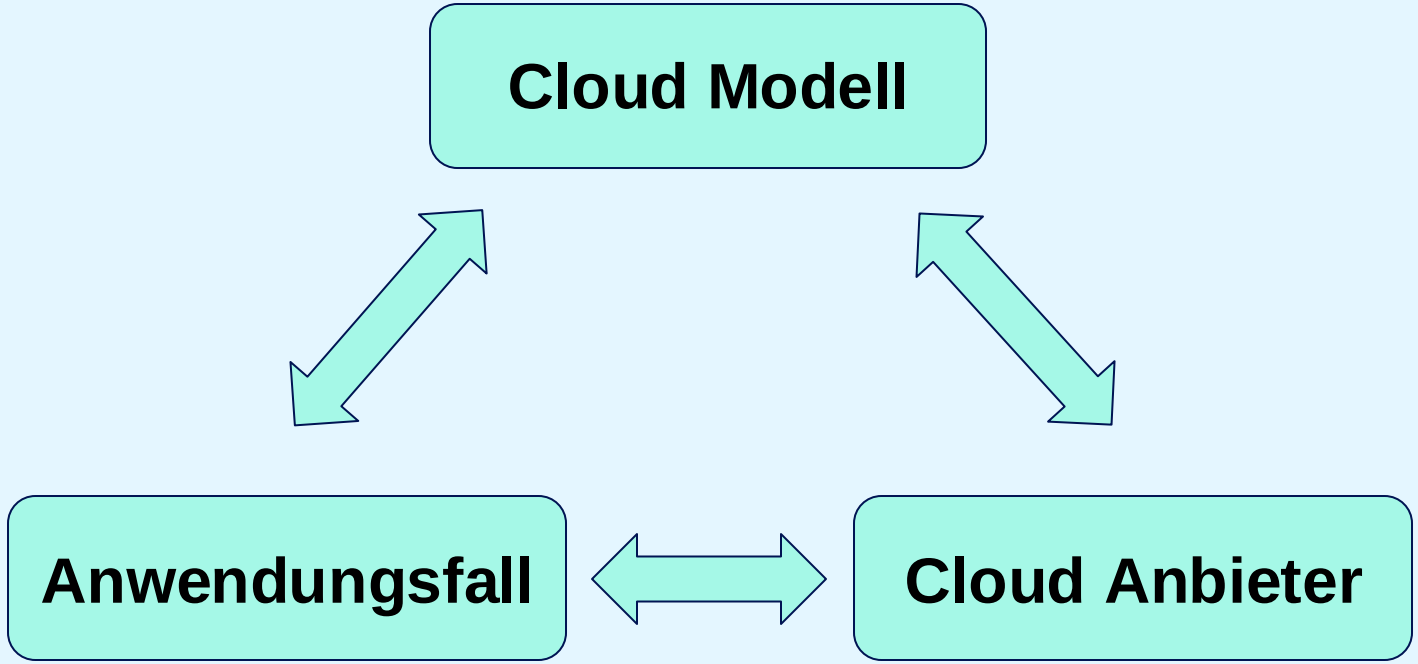
- Skalierbarkeit und Flexibilität
- Einfachere Zusammenarbeit
- Zeitgewinn durch Auslagerung von Tätigkeiten
- Einfacher Zugang

Risiken

- Anbieterabhängigkeit
- Weniger Kontrolle über Prozesse und Infrastruktur
- Datensouverenität

Risikoanalyse in der Cloud





Verantwortlichkeiten

Die Verantwortung für die «Cloud-Sicherheit» ist geteilt zwischen dem Cloud-Provider und dem Cloud-Kunden und hängt vom gewählten Modell ab.

**Es ist wichtig zu verstehen,
wer für was verantwortlich ist.**

Handlungskompetenz

Was kann ich konkret tun?

Handlungskompetenzen aufbauen:
Cyberresilienz durch Wissen und Teamwork!

Lehrangebot für Behörden
https://elearningcyber.ch/de

Infos für Behörden
https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden.html

Teilnahme an CYREN^{ZH}
https://cyrenzh.ch/events/

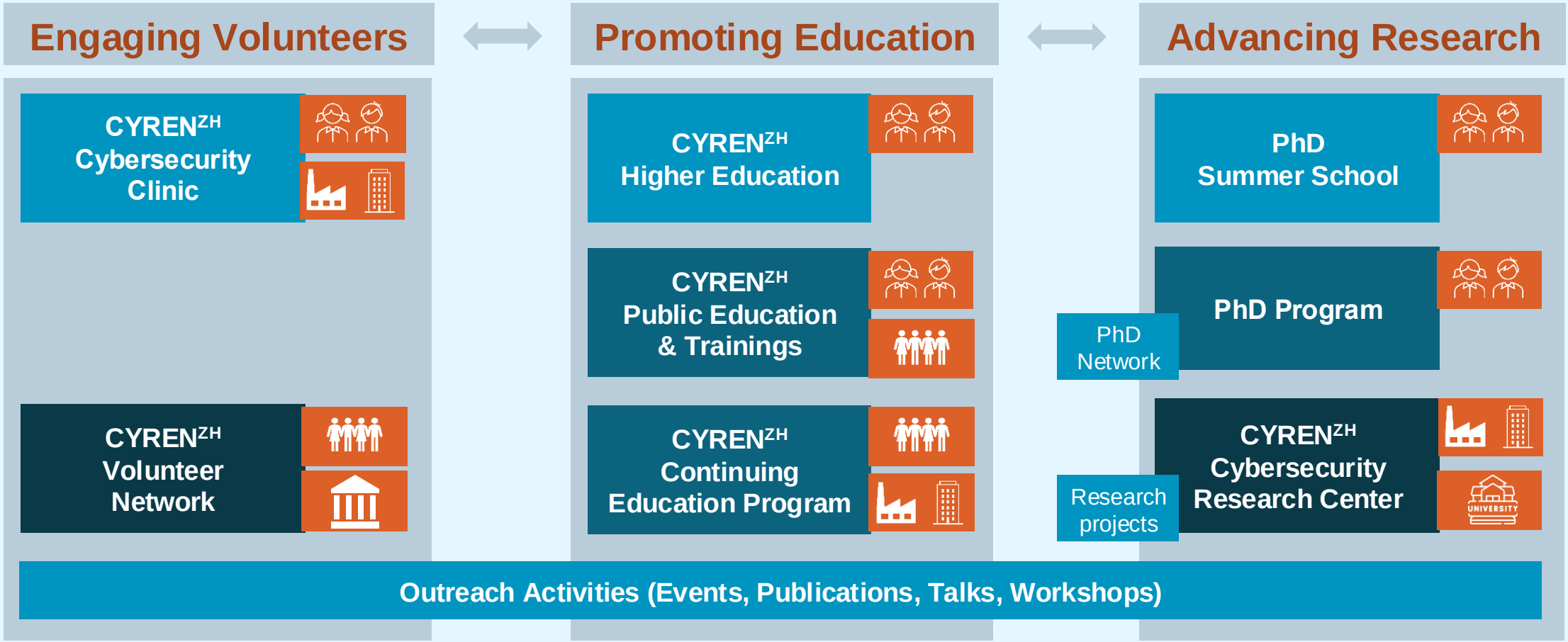
Persönlich

Unterstützung von Initiativen für Awareness / Ausbildung

Verankerung von Cybersicherheit in der Schule

Kanton

Three pillars of CYREN ZH



Digital MasterClass

Kantonsrat Zürich

nächste Veranstaltung: **20. Januar 2025**

Die digitale Verwaltung: Was kann sie, was darf sie?

Eine Veranstaltung von:

Universität Zürich[UZH]
Digital Society Initiative

Partner:

Parldigi

Unterstützt durch:

DIZH

Stiftung Mercator Schweiz