ParIdigi MasterClass
Grosser Rat Bern

Cybersecurity

Bern, 11. März 2024

Prof. Dr. Endre Bangerter, Co-Leiter Institute for Cybersecurity and Engineering, BFH

Dr. Melanie Knieps, Forscherin Digital Society Initiative, UZH

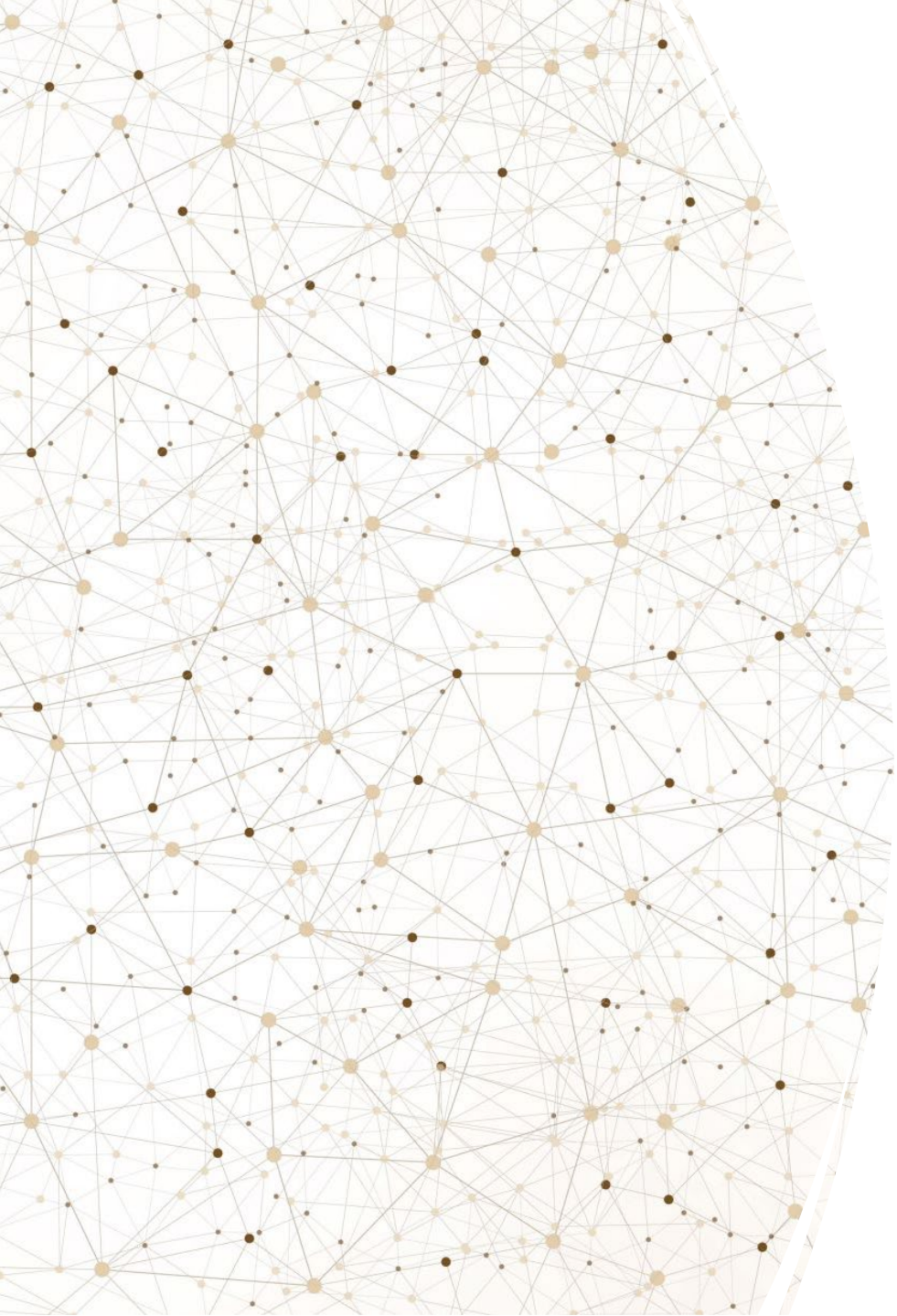
Eine Veranstaltung von:

Universität Zürich[UZH]
Digital Society Initiative

Parldigi

Unterstützt durch:

Stiftung Mercator Schweiz



Menschen in der Cybersicherheit

Wie man sie zum Scheitern verurteilen oder zur wertvollen Ressource befähigen kann.

Dr. Melanie Knieps (UZH, CYRENzh)

Wie funktioniert effiziente Cybersicherheit?

PPT Framework

P	**People**
P	**Process** (Tasks & Structure)
T	**Technology**

Ausgewogenheit ist alles

Physische Sicherheit: Eine Analogie

People	• **Einhaltung bewährter Praktiken** • **Melden von Problemen**
Process	• **Instruktionen/Training zu gängigen Angriffsszenarien (z.B. Tailgating, phishing)** • **Bereitstellung von Feedback Möglichkeiten (klare Ansprechspartner/-wege)**
Technology	• **Keypad mit Karte/Passwort** • **Funktionierendes Türschloss** • **Alarm**

Wer/was ist verantwortlich bei einem Breach?

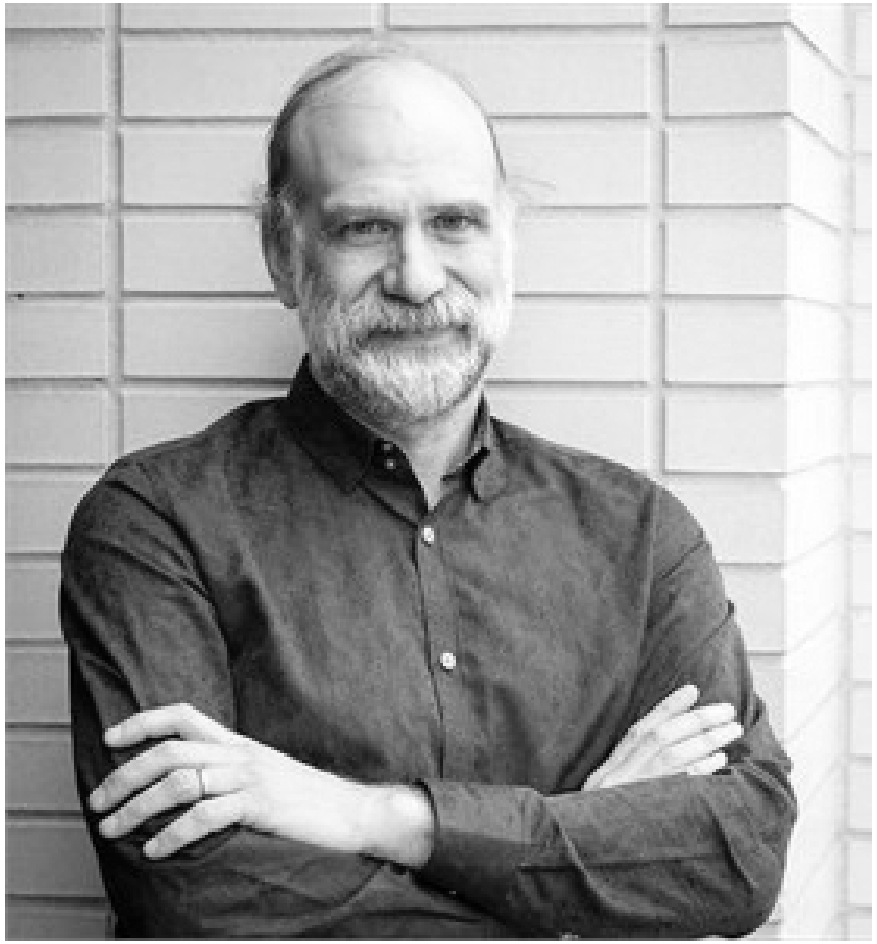
Beispiel Tailgating bei Gebäude-Sicherheit

Beispiel Phishing bei Netzwerk-Sicherheit

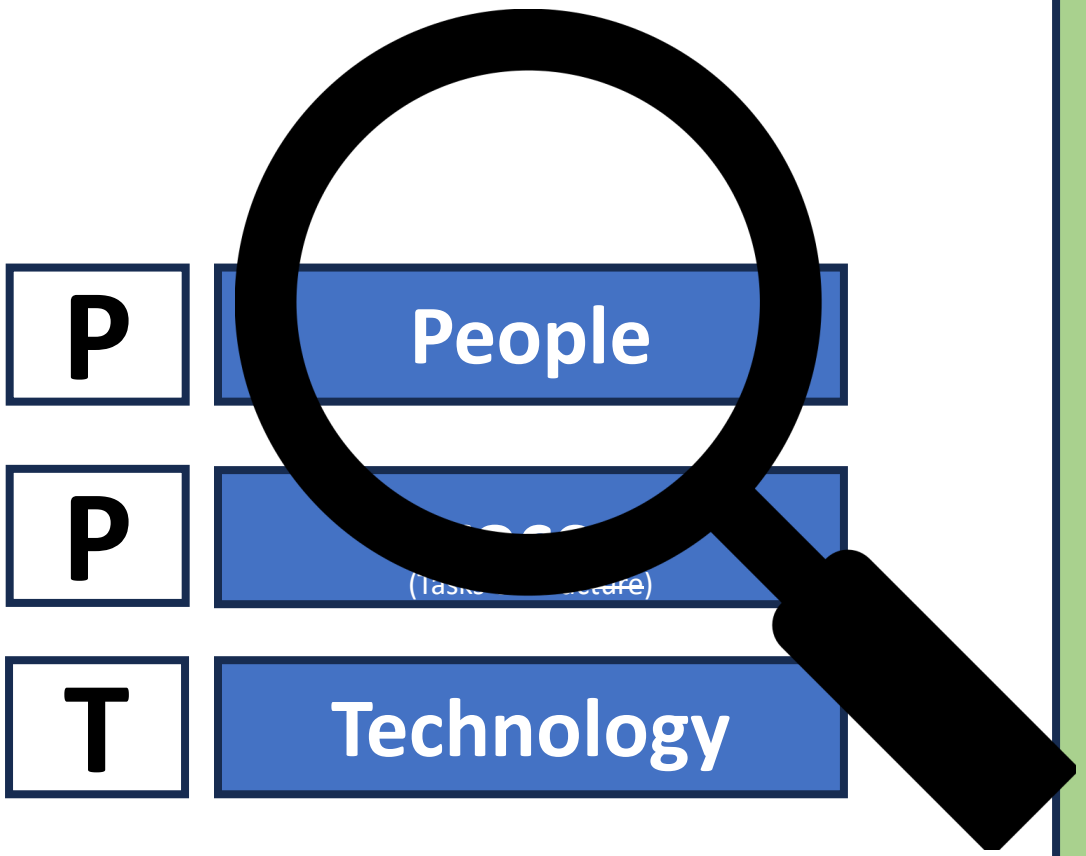
Der Mensch als Sündenbock

"Der Mensch ist oft das schwächste Glied in der Sicherheitskette und ist hauptverantwortlich für das Versagen von Sicherheitssystemen".

(Schneier, 2000, p. 149)

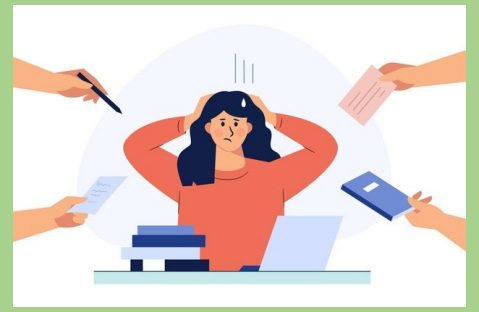


Sind es wirklich die Angestellten?



O **Organisation**

Arbeits-bedingungen



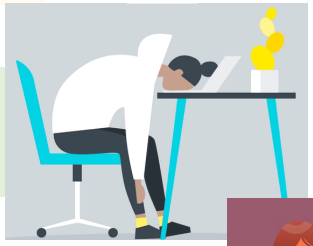
Prioritäten der Geschäftsleitung

Arbeitsbedingungen unter der Lupe

Erfüllen Vorgesetzte ihre Vorbildfunktion?

Gibt es zwischen Vorgesetzten und Belegschaft einen regelmässigen Austausch zu Sicherheitsfragen?

Sind die Produktivitätsziele zu unrealistisch?



Wie reagieren Kollegen und Vorgesetzte auf gutes Sicherheitsverhalten?

Gibt es zu viele Ablenkungen am Arbeitsplatz?

Gagné, M. (2014). *The Oxford Handbook of Work Engagement, Motivation, and Self-Determination Theory*. Oxford University Press.

Prioritäten der GL unter der Lupe

Wirtschaftlicher Vorteil durch Cybersicherheit

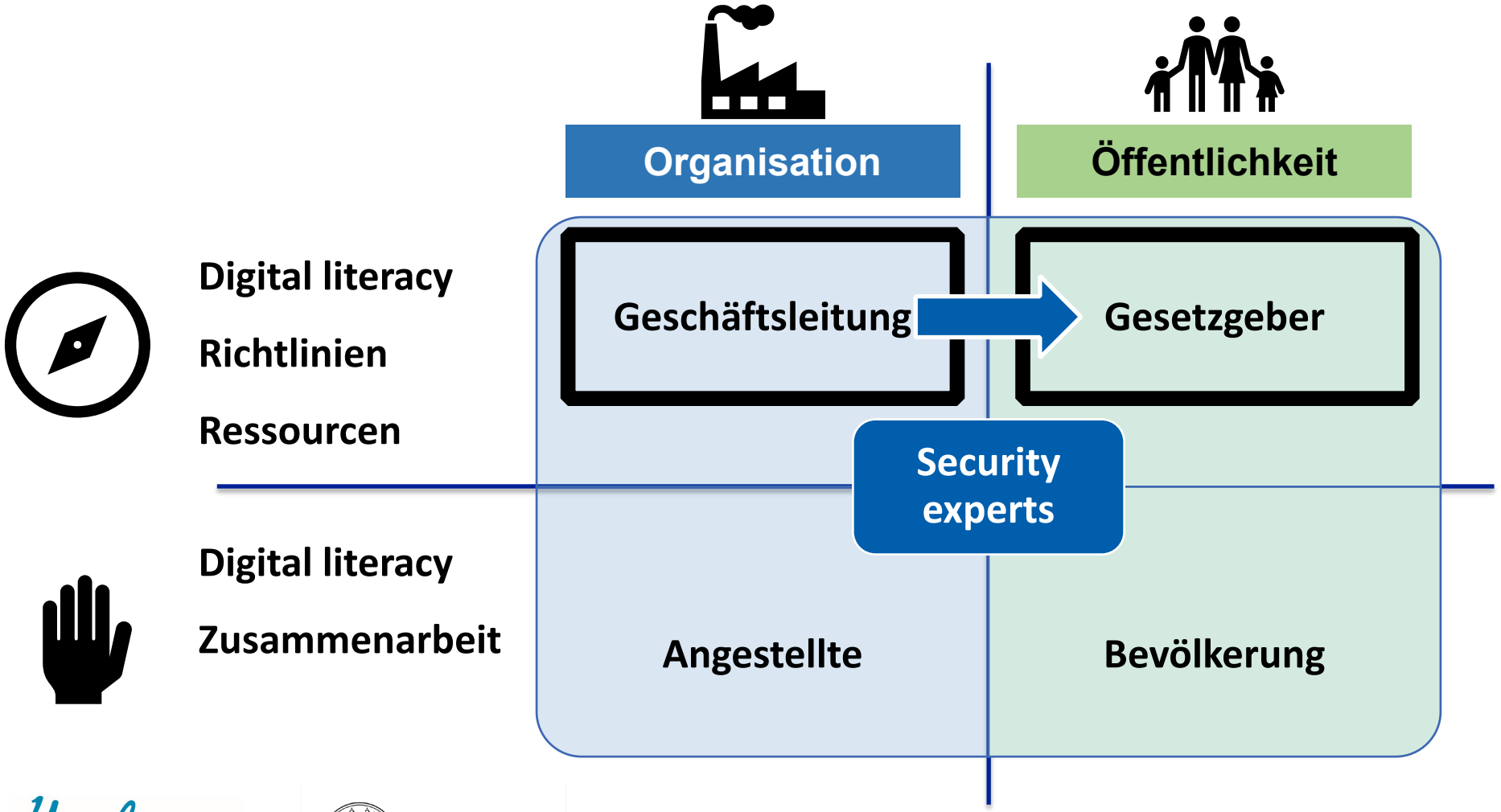
- **96%** sehen CS als entscheidend für das **Unternehmenswachstum**
- **90%** sehen CS als einen **Differenzierungsfaktor**

ABER:

- **46%** sind "**Cyber-Hinterherhinker**"
- **60%** ziehen CS nicht von Anfang an in ihre **Geschäftsstrategien**, **Dienstleistungen** oder **Produkte** ein.
- **Nur 15%** diskutieren Fragen der Cybersicherheit in spezifischen **Vorstandssitzungen**.
- **91%** betrachtet Cybersicherheit als eine rein **technische Funktion**

https://www.inside-it.ch/ceo-umfrage-zu-security-lieber-reagieren-als-agieren-20231023

Wie sehen Sicherheitsexperten das Problem?



Verknüpfung zw. Sicherheit und Business

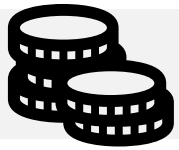
Sensibilisierung / digital literacy erhöhen.

Mehr Regulierung zu präventiven Massnahmen

Was sich ändern muss

Cybersicherheit ist eine Teamaufgabe.

Cybersicherheit ist nicht kostenlos.



Wir müssen unsere Expert:innen befähigen.

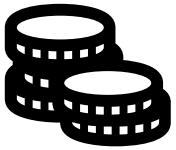
Wie schafft man nachhaltigen Wandel?

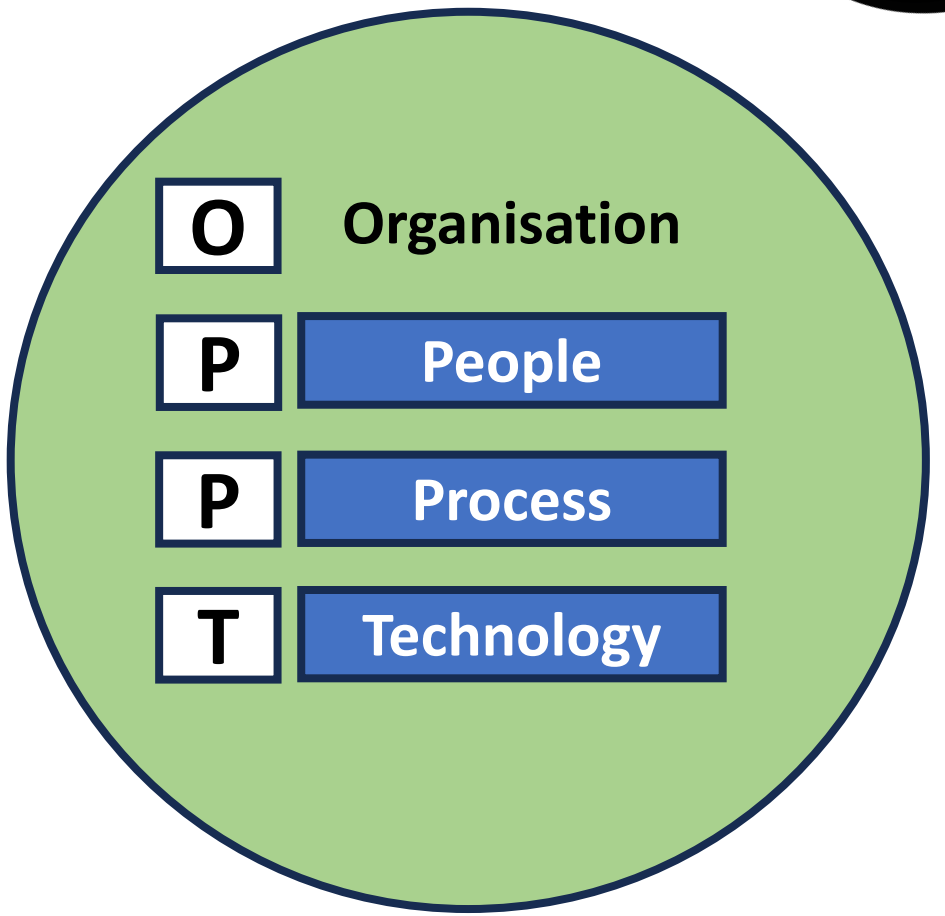
Sicherheitskultur:

Es braucht ein austariertes Miteinander zwischen PPT und Organisation

Sicherheit und Business müssen mehr miteinander verknüpft werden.

- In Geschäftsstrategien, Dienstleistungen oder Produkten berücksichtigen
- Als Differenzierungsfaktor nutzen





Wie schafft man nachhaltigen Wandel?

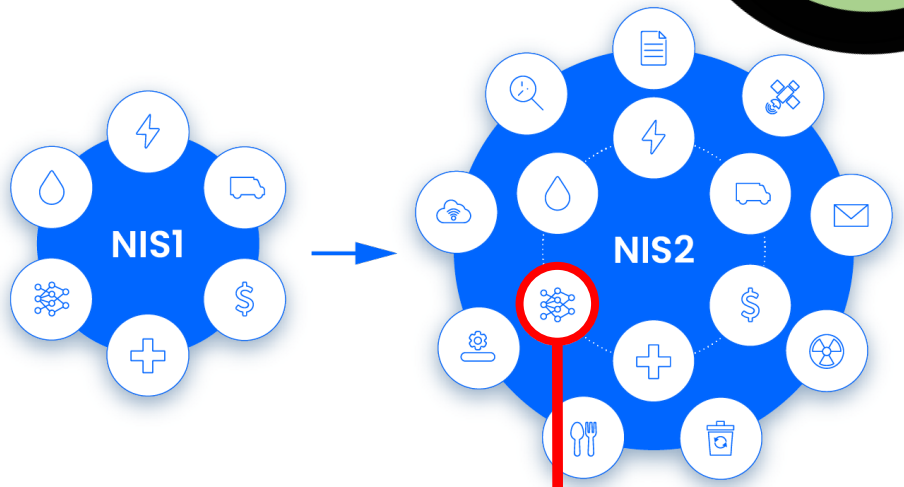
Mehr Regulierung für präventive Massnahmen

- Zum Schutz der Schweizer Kritischen Infrastrukturen für Gesellschaft und Wirtschaft
- Zum Schutz der Schweizer Wettbewerbsfähigkeit (z.B. NIS2)

Was der Gesetzgeber tun kann:

77 NRP

- Klärung des Begriffs der kritischen Infrastrukturen und Ausweitung des Anwendungsbereichs
- Verschärfung von Mindestanforderungen
- Auferlegung zusätzlicher Anforderungen für IT-Dienste



Xplain
homeland security. digital end-to-end

Gesetzesempfehlung

Gesetzes-empfehlung

Ein Vorschlag zur Verbesserung der Cybersicherheit kritischer Infrastrukturen in der Schweiz

Warum diese Gesetzesempfehlung?

Auch wenn in der Schweiz allmählich ein rechtlicher Rahmen für die Cybersicherheit entwickelt wird, bestehen immer noch erhebliche rechtliche Lücken. Das neue Informationssicherheitsgesetz (ISG) ist ein notwendiger, aber kein hinreichender Schritt, um die Widerstandsfähigkeit des Landes gegenüber Cyber-Bedrohungen zu verbessern.

Dieses Dokument zeigt die wichtigsten rechtlichen Lücken auf, wobei der Fokus auf kritische Infrastrukturen liegt. Es skizziert einen Vorschlag, wie durch gesetzgeberische Massnahmen Anreize geschaffen werden können, um verbindliche Mindestanforderungen an die Cybersicherheit für kritische Infrastrukturen einzuführen.

Dieser Vorschlag ist das Ergebnis des Forschungsprojekts «Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland», das im Rahmen des Nationalen Forschungsprogramms 77 «Digitale Transformation» von Forschern der Universität Zürich und der Universität Lausanne mit Unterstützung des Schweizerischen Nationalen Zentrums für Cybersicherheit durchgeführt wurde.

Zentrale Begriffe und Grundproblem

Was ist Cybersicherheit?

Cybersicherheit kann definiert werden als die Gesamtheit aller Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen[1].

Der Begriff der Cybersicherheit kann von jenem der «Informationssicherheit» und der «IT-Sicherheit» unterschieden werden. Allerdings ähneln Massnahmen der Cybersicherheit weitgehend den Massnahmen zur Gewährleistung der Informationssicherheit und der IT-Sicherheit und können daher mit diesen kombiniert werden. Die drei Begriffe sind eng miteinander verknüpft.

Cybersicherheit ist eine globale Herausforderung und kann nicht als ein Problem verstanden werden, das mit rein technischen Mitteln gelöst wird. Vielmehr umfasst sie verschiedene Dimensionen, einschliesslich Gesetzgebung und Regulierung.

In der Vergangenheit wurden verschiedene Rechtsbereiche unter Berücksichtigung von Erwägungen, die an die Cybersicherheit grenzen, geregelt: Das Strafrecht befasst sich beispielsweise mit Cyberkriminalität; Fragen der Cyberverteidigung fallen in den militärischen

1 Bundesrat, Nationale Cyber-Strategie (NCS), 2023, S. 9. Die NCS wurde 2023 verabschiedet, Sie ist die Strategie zum Schutz der Schweiz vor Cyberbedrohungen und ersetzt die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken von 2018–2022.

77 NFP Digitale Transformation Nationales Forschungsprogramm · Universität Zürich · UNIL | Université de Lausanne

Recommandation législative

Une proposition pour améliorer la cybersécurité des infrastructures critiques en Suisse

Pourquoi cette recommandation législative ?

Il y a d'importantes lacunes en Suisse en matière de cybersécurité, même si un cadre légal est en développement. L'adoption, puis la révision, de la nouvelle Loi sur la sécurité de l'information (LSI) sont des pas importants, mais ce n'est pas suffisant pour assurer un niveau approprié de cyberrésilience en Suisse.

Ce document relève les lacunes légales les plus importantes en matière de cybersécurité des infrastructures critiques. Il propose des mesures législatives pouvant créer des incitations, plus précisément par l'introduction d'exigences minimales de cybersécurité pour les infrastructures critiques.

Ce document est le fruit d'un projet de recherche intitulé « Improving trust in cybersecurity through ethics and law » qui a été réalisé dans le cadre du programme national de recherche 77 « Transformation numérique » par des chercheurs de l'Université de Zurich et de l'Université de Lausanne avec le soutien du Centre national suisse pour la cybersécurité (NCSC).

Notions centrales et problématique

Qu'est-ce que la cybersécurité ?

La cybersécurité peut être définie comme l'ensemble des mesures visant à prévenir et gérer les cyberincidents ainsi qu'à améliorer la cyberrésilience[1].

La notion de cybersécurité peut être distinguée de la « sécurité de l'information » et de la « sécurité informatique ». Cela étant, les mesures de cybersécurité sont dans une large mesure similaires aux mesures permettant d'assurer la sécurité de l'information et la sécurité des moyens informatiques et peuvent donc être combinées avec celles-ci. Les trois notions sont étroitement liées.

La cybersécurité est un défi global qui ne peut être limité à des questions techniques. Elle implique au contraire différentes dimensions, dont la législation et la réglementation.

Historiquement, différents domaines juridiques ont été réglementés en tenant compte de considérations avoisinant la cybersécurité : le droit pénal vise par exemple la cybercriminalité, la cyberdéfense porte

1 Conseil fédéral, Cyberstratégie nationale (CSN), 2023, p. 9. La CSN a été adoptée en 2023, est la stratégie de protection de la Suisse contre les cybermenaces et remplace la Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC) 2018–2022.

77 PNR Transformation numérique Programme national de recherche · Universität Zürich · UNIL | Université de Lausanne

SCAN ME

ParIdigi MasterClass

Grosser Rat Bern

Eine Veranstaltung von:

Universität Zürich[UZH]

Digital Society Initiative

Parldigi

Unterstützt durch:

Stiftung Mercator Schweiz