BREAKFAST-MEETING

Der Netzwerkanlass für Firmen

«Digitales Vertrauen – der Schlüssel zu moderner Informationssicherheit»

aarau regio

aarau standortförderung

Aarau

BREAKFAST-MEETING

Der Netzwerkanlass für Firmen

Hans-Peter Käser,
Senior Security-Experte beim
Bundesamt für Cybersicherheit
(BACS)

aarau regio

aarau standortförderung

Aarau

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Vertrauen in die Cybersicherheit – durch Resilienz und Transparenz

BREAKFAST-MEETING
Der Netzwerkanlass für Firmen

«Digitales Vertrauen – der Schlüssel zu moderner Informationssicherheit»

aarau regio
aarau standortförderung
Aarau

9. September 2026
Hans-Peter BACS Bundesamt für Cybersicherheit BACS

Das BACS – Aufgaben und Grundlagen

Das BACS ist das Kompetenzzentrum des Bundes für Cybersicherheit. Erste Anlaufstelle für Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen.

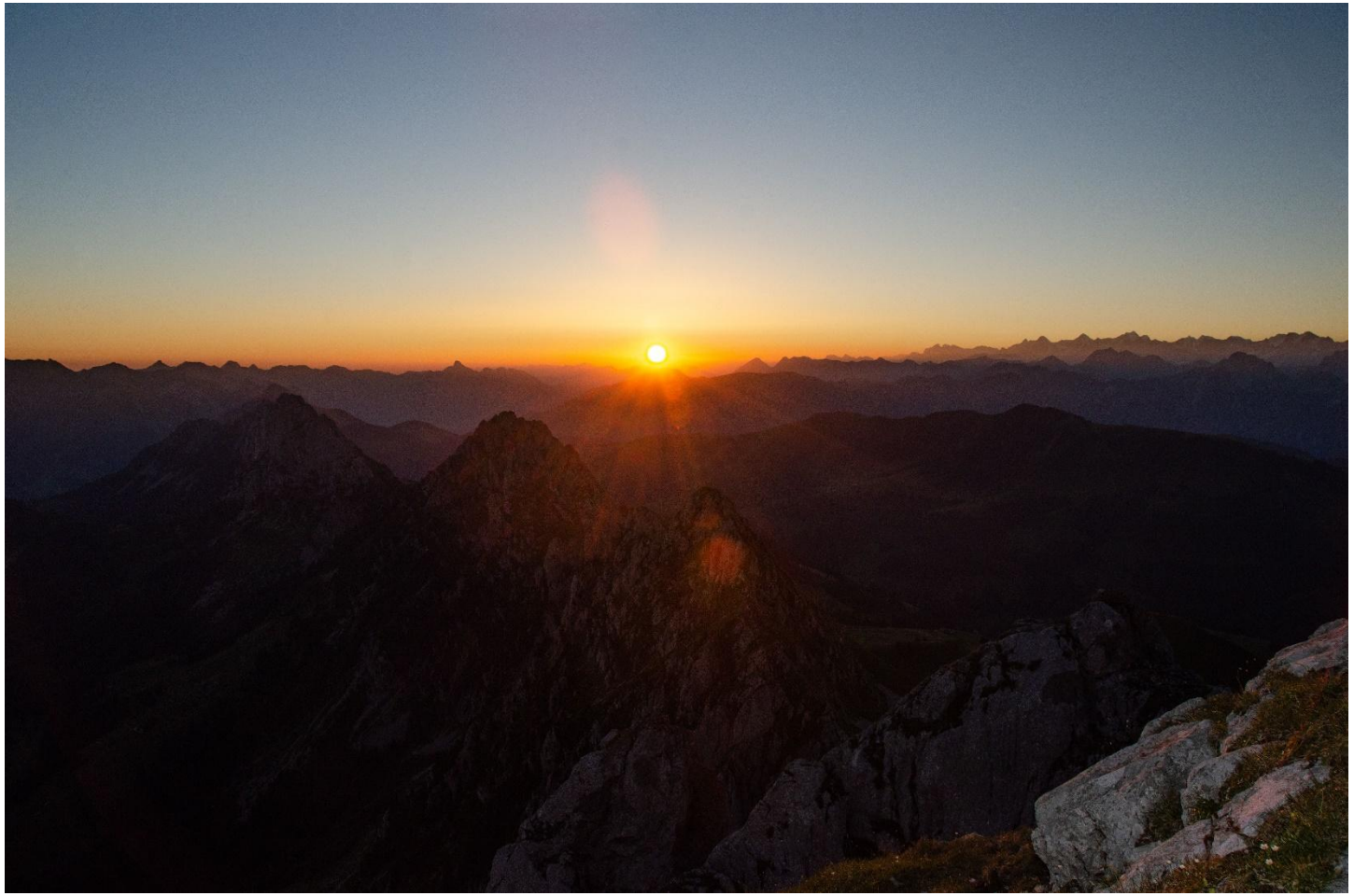
Ziele

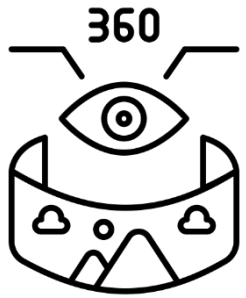
- Cyberbedrohungen verständlich machen
- Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen
- Schäden aus Cybervorfällen reduzieren
- Sicherheit von digitalen Produkten und Dienstleistungen erhöhen

Schwerpunkte

- Umsetzung der nationalen Cyberstrategie
- Cyber Security Hub und regelmässige Lageupdates
- Meldepflicht und Unterstützung kritischer Infrastrukturen bei Vorfällen
- Koordination Schwachstellen in der Schweiz und Anlaufstelle für die Bevölkerung
- Präventive Cybersicherheit zur Unterstützung von Behörden, Kritischen Infrastrukturen und der Wirtschaft / IKT-Minimalstandard

Einstieg ins Thema





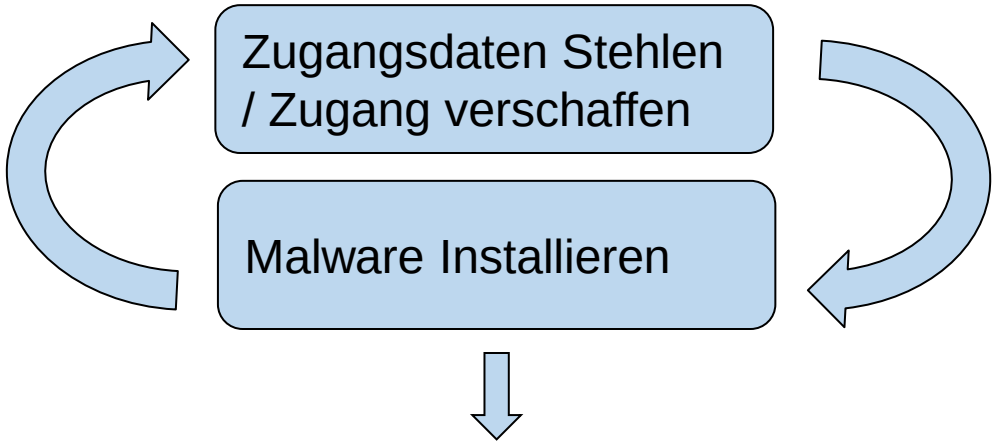
Digitalisierung als Treiber

Papstwahl 2005

Papstwahl 2013

http://www.spiegel.de/

Bedrohungen Auswirkungen auf Unternehmen oder Organisation

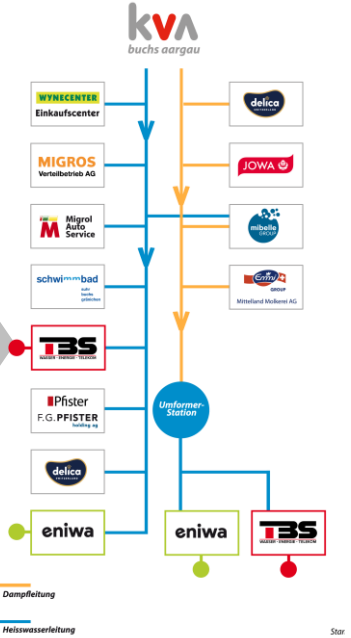


- Ransomware / Verschlüsselung
- Datenabfluss und Veröffentlichung von Daten
- Temporäre Zugangsverhinderung
- Spionage
- Sabotage
- Finanzielle Verluste

Anwendungsbeispiel KVA

Lieferkette – Betriebsmittel - Rohstoffe

Abfallberge
Seuchen
Gestank



Vernetzung verstärkt die Bedrohungen

Ein kompromittierter Partner in der Lieferkette kann als Einstiegspunkt für weitere Angriffe dienen

Deshalb: Cybersicherheit muss zu einem Qualitätsfaktor bei der Zusammenarbeit werden

Vernetzung benötigt Vertrauen

Wie kann ich der Cybersicherheit vertrauen?

1 **Vertrauen in sich selbst**

– dies erreichen wir mit **Resilienzmassnahmen**

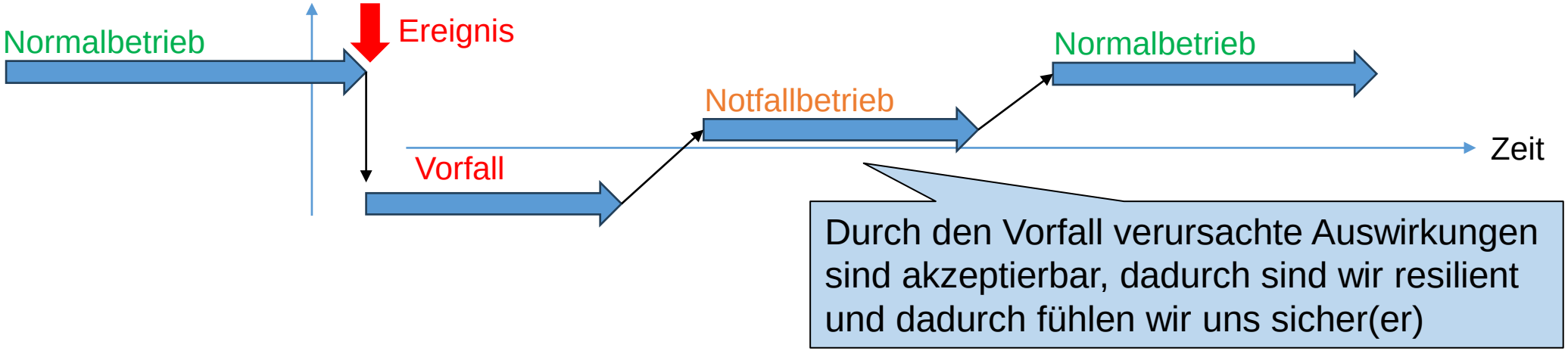
2 **Vertrauen in die Partner**

– dies erreichen wir durch gegenseitige **Transparenz**

1 Vertrauen in sich selbst – durch Resilienz

Wir sind resilient wenn wir nur akzeptierbare Auswirkungen erleiden können.
Wir müssen also

- Wissen was nicht akzeptierbar ist für unsere Organisation oder Firma
- Präventive Massnahmen ergreifen, um Vorfälle zu verhindern
- Bereit sein zu reagieren wenn es zu einem Vorfall kommt



Empfehlung #1: Einsatz eines Sicherheits- und Resilienzverfahrens

Ein mögliches, einfaches Verfahren:

1. Welches sind die geschäftskritischen Prozesse, welche Auswirkungen sind nicht akzeptierbar?
2. Welche digitalen Komponenten können einen Vorfall oder Störfall auslösen? Nur wenn es solche gibt, ist die Cybersicherheit für diese Prozesse wichtig.
3. Wie schütze ich diese Komponenten präventiv? Hierzu empfehlen wir sich an einem pragmatischen Grundschutz zu orientieren.
4. Wie erkenne ich, wenn diese Komponenten angegriffen werden oder der Schutz nicht mehr hält? Kann ich reagieren?

Empfehlung #2: Grundschutz Umsetzen

Anforderungen

- Für alle Aufgaben gibt es kompetente Verantwortliche
- Meine Systeme sind geschützt vor Fremdzugriffen
- Meine Systeme sind (wenn möglich) nicht direkt übers Internet zugreifbar und voneinander getrennt
- Meine Systeme sind aktuell/gehärtet – oder es existieren genügende Failsafe-Mechanismen, die einen Stör- oder Unfall verhindern
- Ein Ausfall der Systeme ist nicht das Ende, respektive führt nicht zum Störfall.
- Wenn etwas nicht ok ist, wird das sofort erkannt und behandelt.

Relevante Massnahmen

Mehr als nur Name / Passwort; Eingeschränkte Berechtigungen

Netzwerksegmentierung, kein Always-On Fernzugriff

Bei Systemen im Internet, sollte innerhalb von 24 Stunden gepatcht werden.

Offline Backup, Vorfallmanagement, Redundanz resp. Ersatzhardware

Überwachung, Protokollierung, Notfallplan und Kommunikationsvorlagen

Empfehlung #2: Grundschutz Umsetzen

Anforderungen

- Für alle Aufgaben gibt es kompetente Verantwortliche
- Meine Systeme sind geschützt vor Fremdzugriffen
- Meine Systeme sind (wenn möglich) nicht direkt übers Internet zugreifbar und voneinander getrennt
- Meine Systeme sind aktuell/gehärtet – oder es existieren genügende Failsafe-Mechanismen, die einen Stör- oder Unfall verhindern
- Ein Ausfall der Systeme ist nicht das Ende, respektive führt nicht zum Störfall.
- Wenn etwas nicht ok ist, wird das sofort erkannt und behandelt.

Relevante Massnahmen beim Auslagern von IT-Diensten

Eigene Datensicherung aller wichtigen Daten

Möglichkeit auf alternative Lösungen zu wechseln

Überwachung, Notfallplan und Kommunikationsvorlagen

2 Vertrauen in den Partner – mit Transparenz

Proaktive und nachvollziehbar offenlegen aller für die Kunden wichtigen Sicherheits- und Resilienzmassnahmen.

Wichtige Sicherheits- und Resilienzmassnahmen

- **Exportierbarkeit**: Alle für die Resilienz des Kunden notwendigen Daten können von diesem auch exportiert werden für eine eigene Datensicherung
- **Produktsicherheit**: Es wird transparent aufgezeigt, welche Methoden für die sichere Entwicklung von IT-Produkten und Diensten verwendet wurden.
- **Zugriffstransparenz**: Es gibt eine Funktion, die es dem Kunden erlaubt, alle Zugriffe auf die Daten und deren Bearbeitung zu überwachen und nachzuvollziehen.
- **Transparenz der Sicherheitsfunktionen:** Der Einsatz von Kryptographie sowie wichtigen Sicherheitsfunktion ist verständlich dokumentiert.
- **Meldung von Vorfällen und Schwachstellen**: Es gibt einen klaren Prozess, welcher sicherstellt, dass Vorfälle und Schwachstellen gemeldet werden können und den Kunden weitergegeben werden.

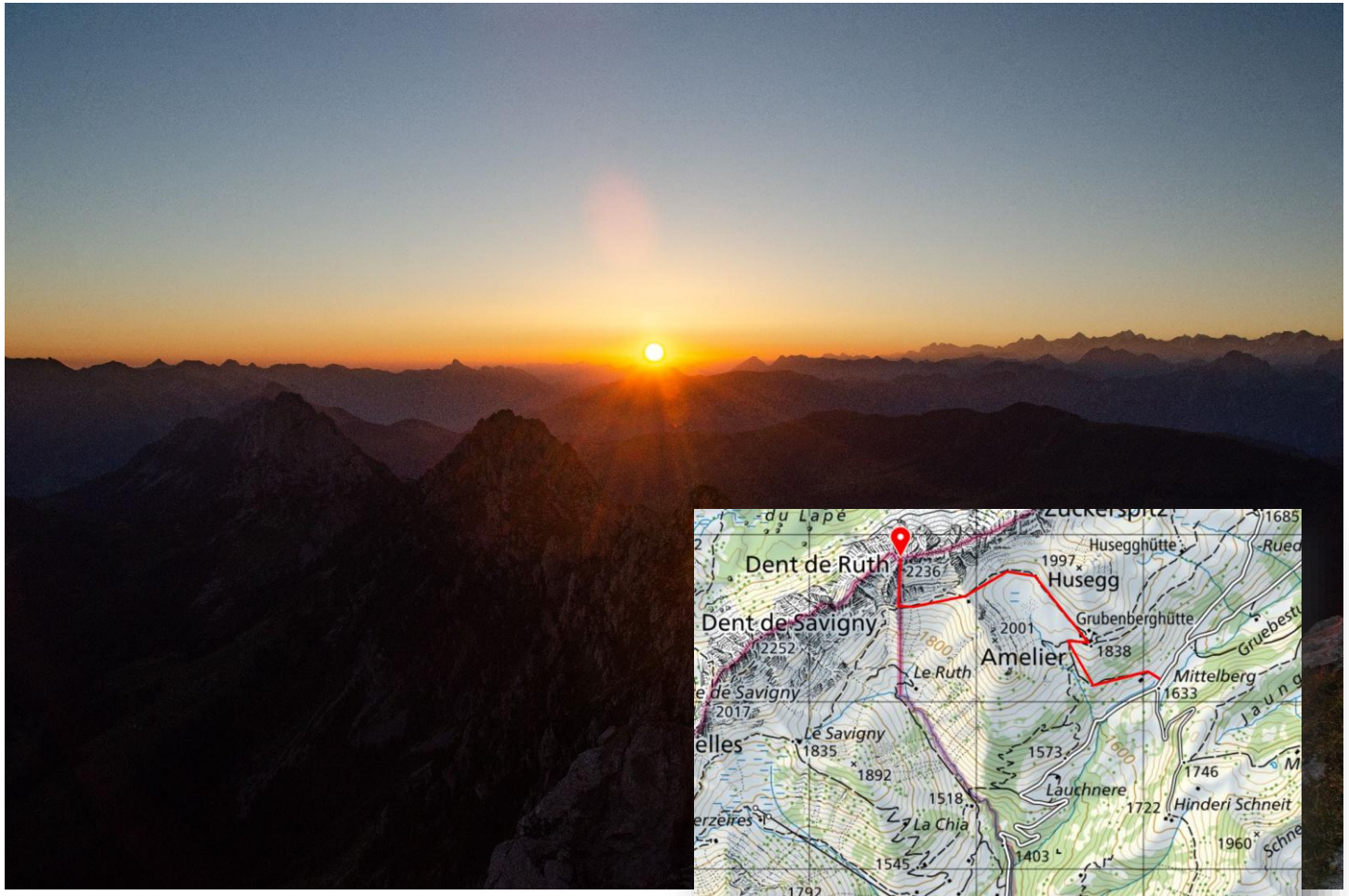
Konkret: Was sollte ich tun

Die eigenen geschäftskritischen Prozesse mit ihre IT-Abhängigkeiten verstehen.

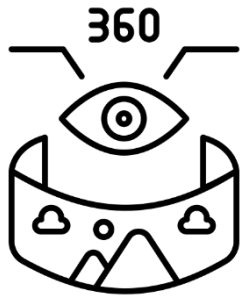
Einen IT-Grundschutz umsetzen und so (selbst)-Resilienz sicherstellen.

Offen und (proaktiv) transparent über Sicherheits- und Resilienzmassnahmen informieren (zum Beispiel auf der Webseite)

Fazit



Dent de Ruth
2236
Dent de Savigny
2252
Le Ruth
2017
Le Savigny
1835
1892
1518
La Chia
1545
1792
1464
1403
1363
Husegghütte
1997
Husegg
Grubenberghütte
2001
1838
Amelier
Mittelberg
1633
1573
1746
Lauchnere
1722
Hinderi Schneit
1960
1685
1800
1600


360

Hans-Peter Käser

- FEAM / Wirtschaftsinformatiker HF / Senior Security Expert
- Gastdozent an BFH, FHNW, HSLU, ICT Warrior
- Diverse Fachgremien ISSS, IOT/OT Forum CH

Bundesamt für Cybersicherheit (BACS)

Hans-Peter Käser
Senior Cybersecurity Expert
Experte Technologien & Security Engineering

Schwarztorstrasse 59, 3003 Bern
Tel. +41 58 464 79 51
Mobil +41 79 506 67 88
hans-peter.kaeser@ncsc.admin.ch
www.ncsc.admin.ch

Weiterführende Informationen

- Methode zur Prüfung und Behandlung von Risiken bei Lieferantenabhängigkeiten: https://www.ncsc.admin.ch/supply-chain-de
- Notfallkonzept-Vorlage: Ein Hilfsmittel für Unternehmen: https://www.bacs.admin.ch/de/notfallkonzept
- Kommunikationsvorlagen für den Fall, dass Prävention nicht ausgereicht hat und es bereits zu einem Vorfall gekommen ist: https://www.bacs.admin.ch/de/cyberangriff-wie-kommunizieren
- Sicherheitskontakt für externe – security-txt: https://www.bacs.admin.ch/de/security-txt-hinterlegen-sie-ihren-sicherheitskontakt-auf-ihrer-webseite
- Informationssystem zum Austausch von Informationen über Cyberbedrohungen, Cybervorfälle und Cybersicherheitspraktiken vom Bundesamt für Cybersicherheit: https://www.bacs.admin.ch/de/informationen-zum-csh
- Technologiebetrachtungen vom Bundesamt für Cybersicherheit: https://www.bacs.admin.ch/de/technologiebetrachtungen
- Entwurf für ein strukturiertes Vorgehen sowie IT-Grundschutz: BACS Cybersicherheits- und Resilienzmethode: https://www.bacs.admin.ch/de/cybersicherheits-und-resilienzmethode-csrm

BREAKFAST-MEETING

Der Netzwerkanlass für Firmen

Sebastian Svetel,
Verwaltungsrat Healthcare Cyber Security Center / Chief Information Security Officer (CISO)

aarau regio

aarau standortförderung

Aarau

H-CSC
Healthcare Cyber Security Center

UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH

Gemeinsam gegen Cyberbedrohungen – ein Schutzschild für Schweizer Gesundheitseinrichtungen

Sebastian Svetel

Aarau, 09. September 2026

KINDERSPITAL ZÜRICH

FÜR DIE GESUNDHEIT UNSERER KINDER.

Das Kinderspital Zürich ist das grösste universitäre Kinderspital der Schweiz und zählt zu den führenden Zentren für Kinder- und Jugendmedizin in Europa.

2'500
Mitarbeitende

100'000
Patientinnen und Patienten pro Jahr

Rund um die Uhr für Kinder und Jugendliche da

UNSER AUFTRAG

VERSORGUNG
Behandlung kranker und verletzter Kinder und Jugendlicher – von der Geburt bis zum 18. Lebensjahr.

FORSCHUNG
Entwicklung neuer Diagnose- und Behandlungsmethoden für die Medizin von morgen.

LEHRE
Aus-, Weiter- und Fortbildung von medizinischen und pflegerischen Fachpersonen.

ZUSAMMENARBEIT
Vernetzung mit Spitälern, Zuweisenden und Partnern in der ganzen Schweiz und international.

EINZIGARTIGE VERSORGUNGSKETTE

Akutspital Zürich Irchel

→

Rehabilitation Affoltern a. A.

→

Psychosomatik & Psychiatrie

→

Forschung & Lehre

KRITISCHE INFRASTRUKTUR – WENN ES UM LEBEN GEHT

EREIGNIS
Unfall, Krankheit oder Katastrophe (z. B. Crans-Montana)

↓

TRANSPORT
Rasche und sichere Verlegung in ein Zentrum mit höchster Spezialisierung

↓

KINDERSPITAL ZÜRICH
Sofort verfügbare, hochspezialisierte Behandlung rund um die Uhr – für Kinder und Jugendliche

↓

LEBEN RETTEN
Maximale Chancen für Heilung und Genesung

↓

VERTRAUEN SICHERN
Eine funktionierende Versorgung schafft Sicherheit und Vertrauen in unserer Gesellschaft

WARUM DAS KINDERSPITAL ZÜRICH ALS KRITISCHE INFRASTRUKTUR SO WICHTIG IST

H-CSC Healthcare Cyber Security Center

Am Beispiel der Brandkatastrophe in Crans-Montana – Silvesternacht 2025/2026

BRANDKATASTROPHE

Brand bricht aus
Während der Silvesterfeier in der Bar «Le Constellation» geraten Schaumstoffelemente an der Decke durch funkensprühende Partyfontänen in Brand.
Das Feuer breitet sich extrem schnell aus (Flashover).

Grossalarm
Der Brand wurde gemeldet; in kürzester Zeit trafen erste Einsatzkräfte ein. Die Dimension erforderte einen aussergewöhnlich grossen Rettungseinsatz.

Massenanfall von Schwerverletzten
Insgesamt standen 13 Helikopter, 42 Ambulanzen und mehr als 150 medizinische Rettungskräfte im Einsatz.

Extrem hohe medizinische Belastung
Viele Betroffene erlitten schwere Verbrennungen. Die Verletzten mussten triagiert, stabilisiert und auf zahlreiche Spitäler in der Schweiz verteilt werden. Die Schweiz benötigte dafür auch internationale Unterstützung.

41 Todesopfer – 115 Verletzte
Nach dem später aktualisierten Stand starben 41 Menschen, 115 wurden verletzt, viele davon schwer.

VON DER KATASTROPHE ZUR VERSORGUNG

Rettung & Erstversorgung vor Ort
Schnelle Alarmierung, Rettung und Erstbehandlung der Betroffenen.

↓

Triage & Verteilung
Schwerverletzte werden stabilisiert und auf zahlreiche Spitäler in der ganzen Schweiz verteilt – je nach Spezialisierung.

↓

Hochspezialisierte Spitalversorgung
Schwere Brandverletzungen benötigen spezialisierte Intensivmedizin, Chirurgie, Beatmung, Infektionsmanagement und Langzeitrehabilitation.

↓

Kinderspital Zürich
Auch Kinder und Jugendliche mit schwersten Brandverletzungen wurden ins Kinderspital Zürich verlegt und dort rund um die Uhr hochspezialisiert behandelt.

KINDERSPITAL ZÜRICH ALS KRITISCHE INFRASTRUKTUR

Einzigartige Versorgung für Kinder und Jugendliche
Über 52'000 stationäre und mehr als 370'000 ambulante Behandlungen jährlich – aus der ganzen Schweiz.

Zentrum für hochspezialisierte Medizin
Intensivmedizin, Neonatologie, Verbrennungsbehandlung, komplexe Chirurgie – auf höchstem Niveau.

Systemrelevante Funktion
Teil der nationalen Versorgungsstruktur und eine zentrale Drehscheibe in Krisen – und Katastrophensituationen.

Vertrauen der Bevölkerung
Eltern müssen wissen, dass ihre Kinder jederzeit bestmöglich und sicher versorgt sind – auch in einer Krise.

VOR WELCHEN CYBERBEDROHUNGEN HABEN SICH SPITÄLER IN DER SCHWEIZ ZU SCHÜTZEN?

H-CSC Healthcare Cyber Security Center

Spitäler sind auf digitale Systeme angewiesen – von der Patientenaufnahme bis zur Intensivmedizin. Cyberangriffe können die Versorgung gefährden, Daten gefährden und Vertrauen zerstören.

PHISHING & SOCIAL ENGINEERING

Täuschung von Mitarbeitenden, um an Zugangsdaten, Informationen oder Zahlungsanweisungen zu gelangen.

GESTOHLENE IDENTITÄTEN & KONTENÜBERNAHME

Angreifer erlangen gültige Zugangsdaten und übernehmen Benutzerkonten – auch mit hohen Rechten.

SCHWACHSTELLEN IN SYSTEMEN & ANWENDUNGEN

Ungepatchte Systeme, Fehlkonfigurationen oder bekannte Schwachstellen werden ausgenutzt, um Angriffe durchzuführen.

RANSOMWARE & ERPRESSUNG

Schadsoftware verschlüsselt Systeme und Daten und fordert ein Lösegeld für die Freigabe.

DDOS-ANGRIFFE

Überlastung von Netzwerken, Websites oder Online-Diensten durch massenhaften Datenverkehr – Dienste und Systeme sind nicht mehr verfügbar.

ANGRIFFE AUF MEDIZINTECHNIK & IOT

Vernetzte Medizinprodukte und IoT-Geräte werden kompromittiert oder manipuliert und können die Patientensicherheit gefährden.

INSIDER-BEDROHUNGEN

Vorsätzliche oder unbeabsichtigte Handlungen von Mitarbeitenden verursachen Schäden – durch Missbrauch, Fehler oder Nachlässigkeit.

SUPPLY-CHAIN-ANGRIFFE

Angreifer kompromittieren Dienstleister, Softwareanbieter oder Lieferanten und gelangen dadurch ins Spital.

DATENABFLUSS & DATENDIEBSTAHL

Unbefugtes Kopieren oder Abziehen sensibler Patienten-, Personal- oder Forschungsdaten.

SPITAL VON HEUTE

ALTE PROZESSE. SILOS. REAKTIV.

PAPIERBASIERT
- Formulare und Berichte
- Manuelle Dokumentation

SILO-DENKEN
- Abteilungen arbeiten isoliert
- Daten nicht vernetzt

REAKTIV STATT PROAKTIV
- Behandlung nach Auftreten
- Wenig Vorhersagefähigkeit

PERSONALMANGEL & HOHE BELASTUNG
- Hoher administrativer Aufwand
- Überlastete Teams

EINGESCHRÄNKTE DATENNUTZUNG
- Daten liegen unstrukturiert vor
- Kaum Echtzeit-Analysen

INEFFIZIENZ & HOHE KOSTEN
- Doppeluntersuchungen
- Lange Wartezeiten

VS.

SPITAL DER ZUKUNFT

INTELLIGENT. VERNETZT. MENSCHLICH.

KI & DATENINTELLIGENZ
- KI-gestützte Diagnostik
- Prädiktive Analysen

VERNETZTE SYSTEME
- Nahtloser Datenaustausch
- Interoperable Plattformen

PROAKTIVE & PERSONALISIERT
- Prävention & Frühwarnsysteme
- Personalisierte Behandlungspläne

ENTLASTETES PERSONAL
- Automatisierung von Routinen
- Mehr Zeit für Patienten

ECHTZEIT-DATENNUTZUNG
- Live-Dashboards & Insights
- Datenbasierte Entscheidungen

EFFIZIENZ & NACHHALTIGKEIT
- Optimierte Abläufe
- Ressourcenschonend & kosteneffizient

ERGEBNIS HEUTE

LANGE WARTEZEITEN | UNZUFRIEDENE PATIENTEN | ÜBERLASTETES PERSONAL | HOHE KOSTEN | GERINGE EFFIZIENZ

ERGEBNIS ZUKUNFT

KURZE WARTEZEITEN | ZUFRIEDENE PATIENTEN | MOTIVIERTES PERSONAL | GERINGERE KOSTEN | HOHE EFFIZIENZ

FÜR EINE BESSERE VERSORGUNG. HEUTE UND MORGEN.

CYBERVORFÄLLE IM GESUNDHEITSWESEN IN EUROPA

Die Zahl der gemeldeten Cybervorfälle im Gesundheitswesen ist in den letzten Jahren deutlich und kontinuierlich gestiegen.

+309%

Zunahme der gemeldeten Cybervorfälle im europäischen Gesundheitswesen zwischen 2018 und 2024

GEMELDETE CYBERVORFÄLLE IM GESUNDHEITSWESEN IN EUROPA (2018–2024)

Von 466 Vorfällen im Jahr 2018 auf 1.907 Vorfälle im Jahr 2024 – ein Anstieg um über das 4-Fache in nur 6 Jahren.

ANTEIL DER CYBERVORFÄLLE IM GESUNDHEITSWESEN AN ALLEN GEMELDETEN VORFÄLLEN IN EUROPA

Der Anteil hat sich in 6 Jahren mehr als verdoppelt.

HÄUFIGSTE ARTEN VON CYBERVORFÄLLEN IM GESUNDHEITSWESEN (2024)

Phishing / Social Engineering	32%
Ransomware / Erpressung	25%
Malware / Schadsoftware	17%
Unbefugter Zugriff	13%
Datenleck / Datenabfluss	7%
Sonstige	6%

Ransomware bleibt die bedrohlichste und teuerste Gefahr für Gesundheitseinrichtungen.

Kernaussage: Cyberangriffe auf das Gesundheitswesen nehmen in Europa kontinuierlich zu – sowohl in absoluten Zahlen als auch im Anteil an allen Vorfällen.

Quelle: ENISA Threat Landscape 2024 – Healthcare Sector (Datenbasis: 2018–2024)

DAS HEALTHCARE CYBER SECURITY CENTER

H-CSC Healthcare Cyber Security Center

WAS IST DAS H-CSC?

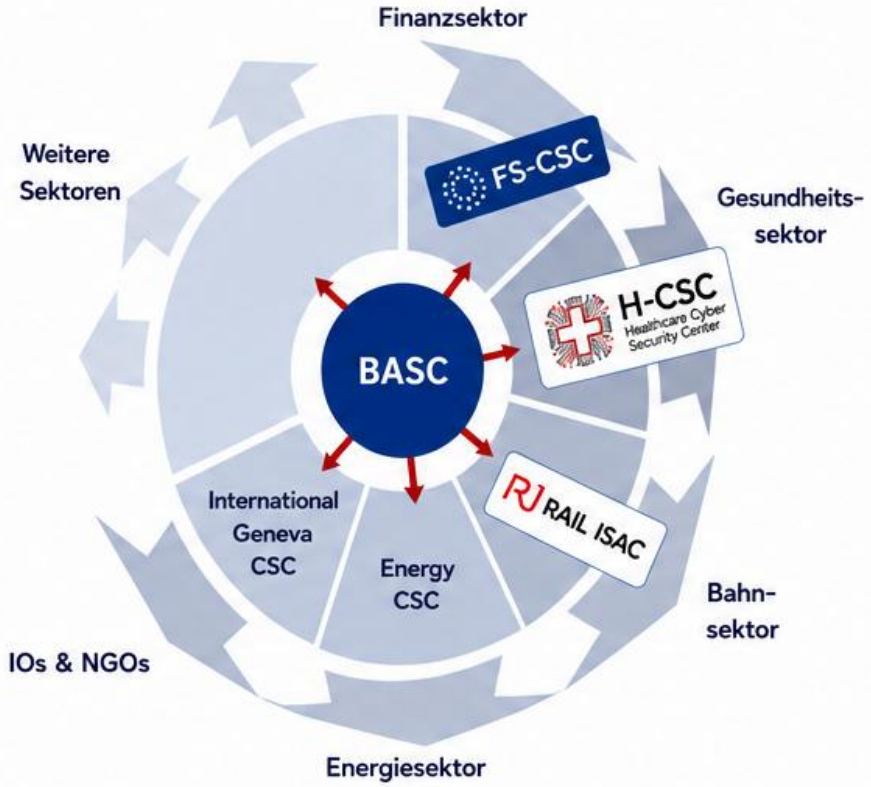
Gemeinnütziger Verein, gegründet am 28. August 2025 von 18 Schweizer Spitälern.

Förderung der Cybersicherheits-fähigkeiten durch branchenspezifische Sicherheitsdienstleistungen.

Stärkung der Prävention, Erkennung und Eindämmung von Cybervorfällen durch aktive Zusammenarbeit der Mitglieder.

VISION

Vision: Ein resilientes, vertrauenswürdiges und vernetztes Schweizer Gesundheitswesen, das Cyberbedrohungen frühzeitig erkennt, wirksam abwehrt und den sicheren Betrieb kritischer medizinischer Leistungen jederzeit gewährleistet.



ZIELE

Ausbau bestehender Fähigkeiten und Schaffung von Synergien zur nachhaltigen Stärkung von Prävention, Erkennung und Eindämmung von Cybervorfällen.

Unabhängige, vertrauensbasierte und praxisorientierte Ergänzung bestehender nationaler Cybersicherheitsstrukturen.

Langfristige Positionierung als zentrales Kompetenz- und Koordinationszentrum für Cybersicherheit im Schweizer Gesundheitswesen.

TECHNISCHE, GOVERNANCE – UND COMMUNITY SERVICES

HERSTELLER-AUSTAUSCHKANÄLE:

Plattform zum gezielten Austausch zu Herstellern, Produkten und Best Practices im Bereich Cybersicherheit.

BESCHAFFUNGSRICHTLINIEN:

Dokumentation für Sicherheitsanforderungen zur stärkeren Verankerung von Informationssicherheit in Beschaffungsprozessen.

AWARENESS-KAMPAGNEN UND ELEARNING:

Zentrale Sammlung bewährter Awareness-Kampagnen und branchenspezifischer eLearning-Lektionen zur einfachen Wiederverwendung.

THREAT INTELLIGENCE SHARING:

Sicherer Austausch von Informationen zu Bedrohungen, IoCs und Schwachstellen zur Stärkung von Prävention und Angriffserkennung.

KONFERENZEN & MONATLICHE WEBINARE:

Vernetzung und Austausch von Erfahrungen und Ergebnissen sowie Weiterbildung anhand von Beiträgen von Fachexperten.

ERFA-GRUPPE INFORMATIONSSICHERHEIT:

Praxisnaher Erfahrungsaustausch für CISOs und IT-Sicherheitsverantwortlichen (auch für nicht H-CSC Mitglieder).

DARKNET MONITORING:

Überwachung relevanter Darknet-Quellen zur frühzeitigen Erkennung kompromittierter Zugangsdaten und sensibler Informationen.

TECHNOLOGIERADAR (IN ARBEIT):

Verzeichnis, der bei den Mitgliedern eingesetzten Lösungen mit Erfahrungen aus Gesundheitseinrichtungen.

BIBLIOTHEK:

Strukturierte Dokumentensammlung zu Themen wie ISMS, Incident Response Playbooks, usw. in vier Sprachen.

DIE MITGLIEDER

Aktuell 43 Gesundheitseinrichtungen aus allen Sprachregionen der Schweiz

H-CSC Healthcare Cyber Security Center

HFR Hôpital fribourgeois Freiburger Spital
Psychiatrische Universitätsklinik Zürich
Hôpital du Jura
ipw Integrierte Psychiatrie Winterthur
spitalSTSAG
Inselgruppe
Spital Männedorf
KSW Kantonsspital Winterthur
Kantonsspital Baselland
Gruppo Ospedaliero Moncucco
Società anonima senza scopo di lucro
PDAG Für Ihre psychische Gesundheit
USZ Universitäts Spital Zürich
Spital Schwyz
solothurner spitäler soH
schulthess klinik
GHOL Groupement hospitalier de l'Ouest lémanique
Klinik Schloss Mammern Führende Rehabilitation am See
Hôpital du Valais Spital Wallis
Lindenhofgruppe
hoch Health Ostschweiz
Kantonsspital Graubünden
Spital Thurgau
Schweizer Paraplegiker Zentrum
fmi Spitäler fmi AG
luksgruppe
Psychiatrische Dienste Graubünden
Balgrist Universitätsklinik
Spitaluster
Gesundheit Mittelbünden
Spital Emmental
Spital Muri
spitäler schaffhausen
Spitalzentrum Centre hospitalier Biel-Bienne
Hirslanden
Universitätsspital Basel
Stiftung Gesundheitsförderung Bad Zurzach + Baden
eoc
Universitäts-Kinderspital Zürich
Zuger Kantonsspital
ksu Kantonsspital Uri
KS_B

... und weitere Mitglieder

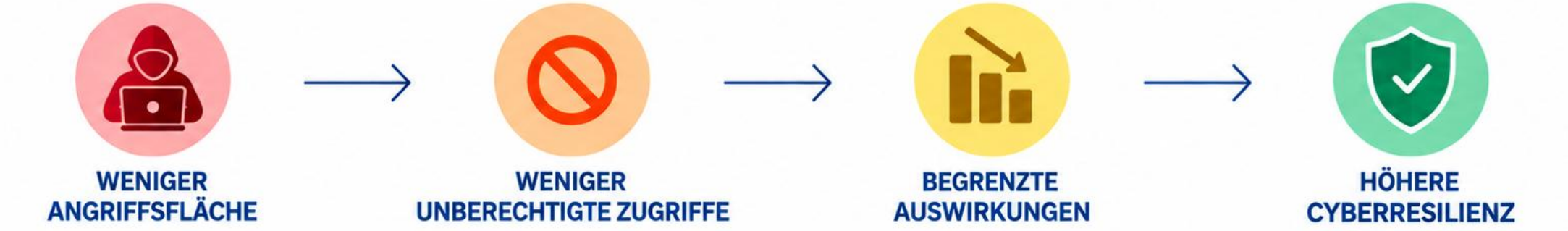
Healthcare Cyber Security Center (H-CSC), 3000 Bern

info@h-csc.ch

IDENTITÄT IST DER NEUE SICHERHEITSPERIMETER

H-CSC Healthcare Cyber Security Center

IAM stellt sicher, dass **die richtige Person** zur **richtigen Zeit, aus dem richtigen Kontext und mit den richtigen Berechtigungen** auf die **richtigen Ressourcen** zugreift.



IAM SCHAFFT VERTRAUEN UND SICHERHEIT

Healthcare Cyber Security Center (H-CSC), 3000 Bern
info@h-csc.ch

Universitäts-Kinderspital Zürich

Sebastian Svetel
Chief Information Security Officer
Data Protection Officer

Lenggstrasse 30, 8008 Zürich
Tel. +41 44 249 24 07
sebastian.svetel@kispi.uzh.ch
http://www.kispi.uzh.ch/

BREAKFAST-MEETING

Der Netzwerkanlass für Firmen

Sarah Burkhard,
Gründerin & Chief Corporate Development, ITSENSE AG

aarau regio

aarau standortförderung

Aarau

BREAKFAST MEETING AARAU · 9. SEPTEMBER 2026

Vertrauen.

Das Fundament auf dem wir bauen.

Sarah Burkhard

FOUNDER · CHIEF CORPORATE DEVELOPMENT · ITSENSE AG

ITSENSE

Der Moment, in dem Vertrauen sichtbar wurde.

Das Projektteam nach dem erfolgreichen Go-live für die Axpo Holding.

Kritische Infrastruktur bedeutet: Es darf nicht einfach irgendwie funktionieren. Es muss belastbar funktionieren.

Vertrauen, das gewachsen ist.

NETCLOUD
ICT PROFESSIONALS

Bundesanwaltschaft
Ministère public de la Confédération
Ministero pubblico della Confederazione
Procura publica federala

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Medizinischer Dienst
Bayern

swisscom

Thurgau

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

SPITALUSTER

Spitalzentrum
Centre hospitalier
Biel-Bienne

Energie Wasser Bern
ewb

Stadt Bern

Kanton Zug

edelweiss

Universitätsspital
Basel

Deutsche
Sporthochschule Köln
German Sport University Cologne

Stadt
Luzern

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

ITSENSE

Rot

Die richtigen Menschen zur richtigen Zeit in der richtigen Rolle das Richtige tun können.

Digitale Identität entscheidet, was wir tun dürfen. Und damit, was wir tun können.

ITSENSE

Diese Fragen beantwortet heute kein Mensch mehr.

Tausendfach pro Sekunde. Von digitalen Systemen.

Und genau hier beginnt Identity & Access Management.

IAM

Zugriff ist Verantwortung.

Begründen.

Warum braucht diese Rolle diesen Zugriff?

Begrenzen.

Nur so viel wie nötig. Nur so lange wie nötig.

Überwachen.

Wird der Zugriff korrekt genutzt?

Entziehen.

Was passiert bei Rollenwechsel oder Austritt?

COREONE

Wer auf IAM verzichtet, verzichtet auf eine strukturierte Verwaltung und Überwachung.

Risiko mit möglichen verheerenden Folgen.

Unklare Berechtigungen

Niemand weiss mehr sauber, wer worauf zugreifen darf.

Wachsende Angriffsfläche

Alte Konten, zu viele Rechte, vergessene Ausnahmen.

Fehlende Nachvollziehbarkeit

Zugriff ist vorhanden — aber warum und woher, ist nicht belegbar.

Schwache Resilienz

Bei einem Vorfall ist unklar, was wo warum.

Verlust digitaler Souveränität

Kritische Befähigung liegt dort, wo die Organisation sie nicht mehr selbst führen kann.

Ohne IAM wird Vertrauen unkontrolliert verteilt.

Drei Wege, wie wir gemeinsam Verantwortung wirksam machen.

COREONE

CoreOne.

Swiss made IAM Software.

ITSENSE

IAM Projekte & Services.

Strategie, Rollenmodelle, Prozesse, Umsetzung.

COMMUNITY

Swiss IAM Circle.

Wissen, Community, Austausch, Verantwortung.

Nicht theoretisch. Aus Überzeugung und Praxis.

24
Jahre Swiss made IAM

1 Mio.+
Verwaltete Identitäten

250+
IAM Kundenprojekte

2×
Best of Swiss Software

Zuhause in Aarau.

Zweifach Silber bei den Best of Swiss Software Awards 2025.

ITSENSE COREONE

www.itsense.ch
www.coreone.ch

KONTAKT

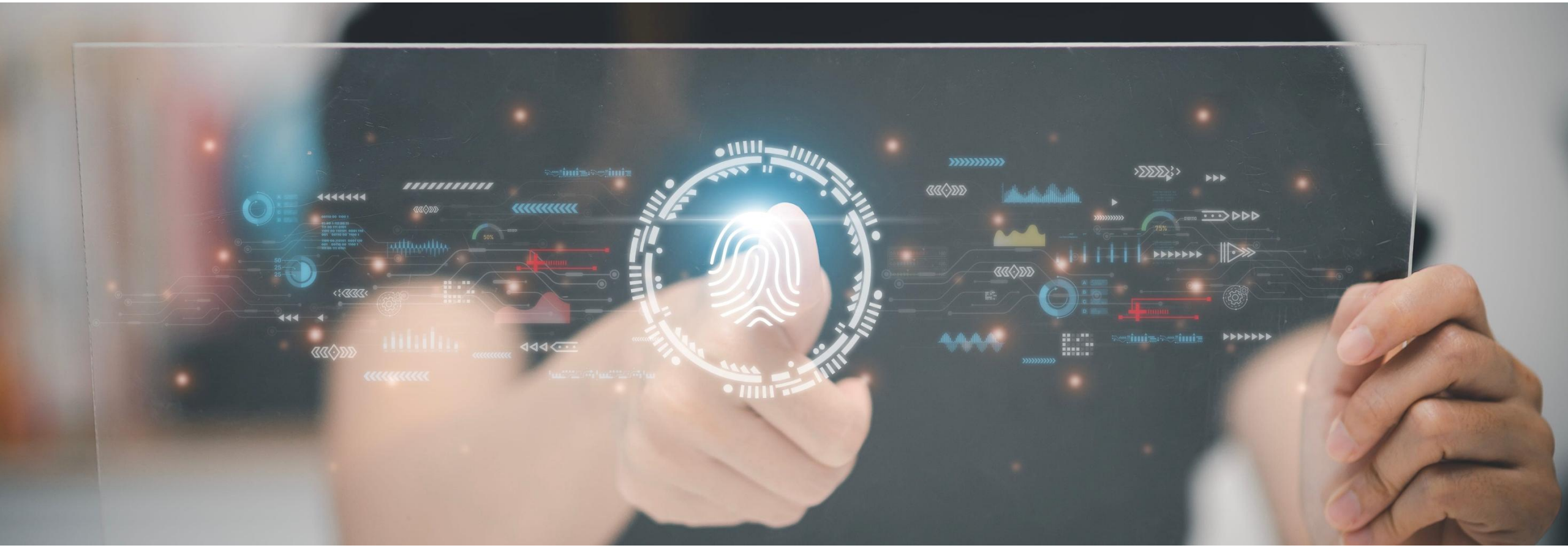
Zäme für Souveränität.

Folge Sarah auf LinkedIn

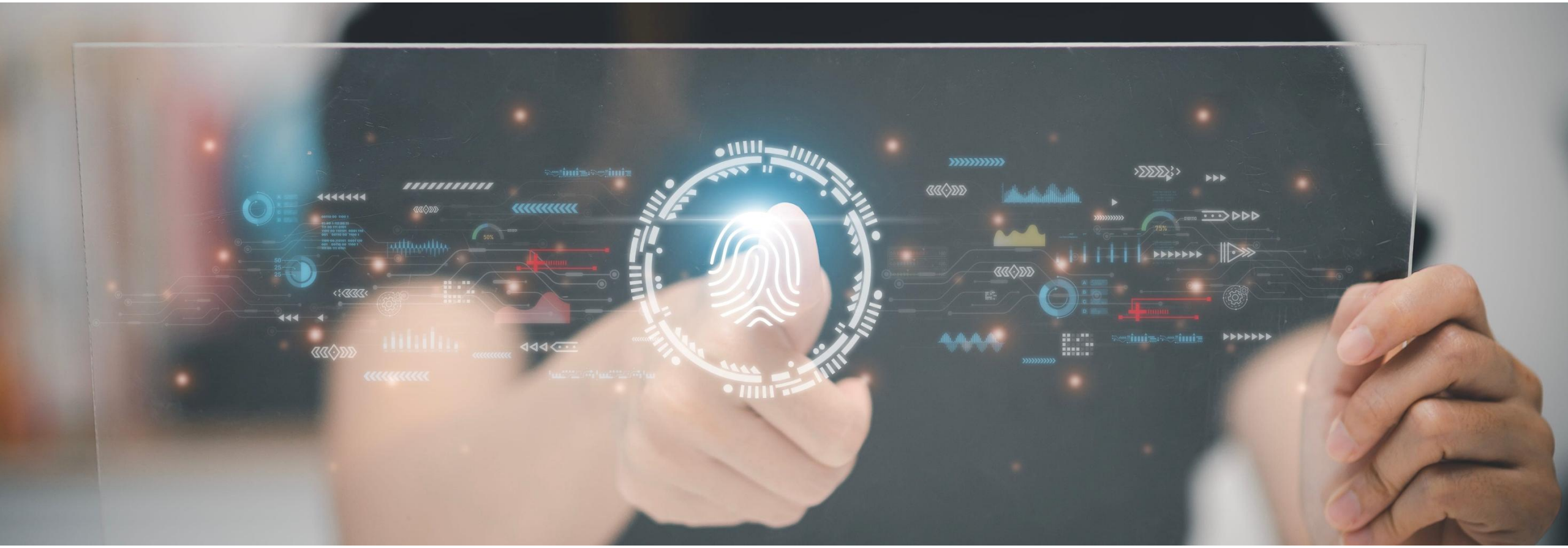
Folge ITSENSE auf LinkedIn

Kontakt speichern

Podiumsdiskussion



Ihre Fragen aus dem Publikum



Im Namen unserer Partner danken wir Ihnen für Ihre Teilnahme am Breakfast-Meeting.

Partner dieser Veranstaltung:

Fachhochschule Nordwestschweiz

aarau regio

AIHK Aargauische Industrie- und Handelskammer

HIVA Handels- und Industrieverein der Region Aarau

Aarau

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

H-CSC Healthcare Cyber Security Center

ITSENSE

Ausblick Veranstaltungen 2027

Wirtschaftsförderung:

- **Mittwoch, 26. Mai 2027: 1. Breakfast-Meeting 2027, (kostenlos, mit Anmeldung), Aarau (AHA)**
- **Mittwoch, 22. September 2027: 2. Breakfast-Meeting 2027, (kostenlos, mit Anmeldung), Aarau (AHA)**

BREAKFAST-MEETING

Partner dieser Veranstaltung:

aarau standortförderung

Aarau

aarau regio

Fachhochschule Nordwestschweiz

AIHK Aargauische Industrie- und Handelskammer

HIVA
Handels- und Industrieverein der Region Aarau

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

H-CSC Healthcare Cyber Security Center

ITSENSE

Vielen Dank für Ihre Aufmerksamkeit

«Aarau überrascht»

vielfältig

visionär

naturnah

Stay connected

https://www.asf-aarau.ch

aarau standortförderung