



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Umsetzung der Nationalen Cyberstrategie (NCS) in der Schweiz



Romain Geiser- Bundesamt für Cybersicherheit, Schweiz
Programm Manager NCS



	5 strategische Ziele
	Selbstbefähigung
	Sichere und verfügbare Dienstleistungen und Infrastrukturen
	Wirksame Verhinderung, Bewältigung und Abwehr von Cyberangriffen
	Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität
	Führende Rolle in der internationalen Zusammenarbeit

April 2023 | www.ncsc.admin.ch

Nationale Cyberstrategie (NCS)

Die Strategie ist zeitlich nicht begrenzt.
Die Anpassungen werden je nach Bedarf vorgenommen.
Revision alle fünf Jahre.

17 Massnahmen

- M1** Bildung, Forschung und Innovation in der Cybersicherheit
- M2** Sensibilisierung
- M3** Bedrohungslage

von Trends, Risiken und Abhängigkeiten

stellen erkennen und verhindern
z, Standardisierung und Regulierung
der Zusammenarbeit zwischen den Behörden

management
ion
anagement
efence

der Zusammenarbeit der Strafverfolgungsbehörden
sicht

M14 Ausbildung der Strafverfolgungsbehörden

M15 Stärkung des digitalen internationalen Genfs

M16 Internationale Regeln im Cyberraum

M17 Bilaterale Zusammenarbeit zu strategischen Partnern und internationalen Kompetenzzentren



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

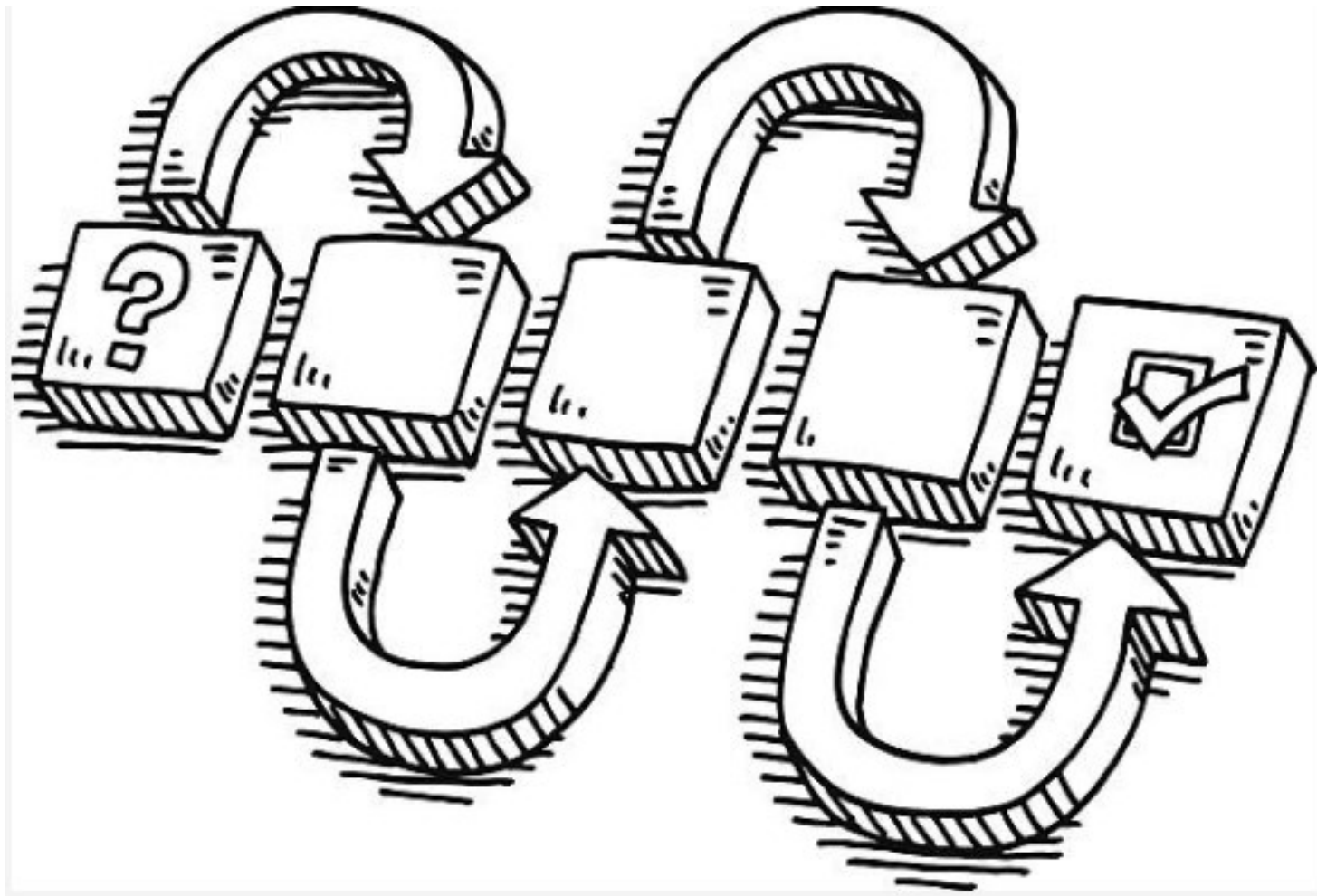


Was sind die Herausforderungen?

- Diversität der Umsetzungspartner
- Wirkungsmessung
- Dynamische Lage
- Ressourcen



NCS-Umsetzung heute





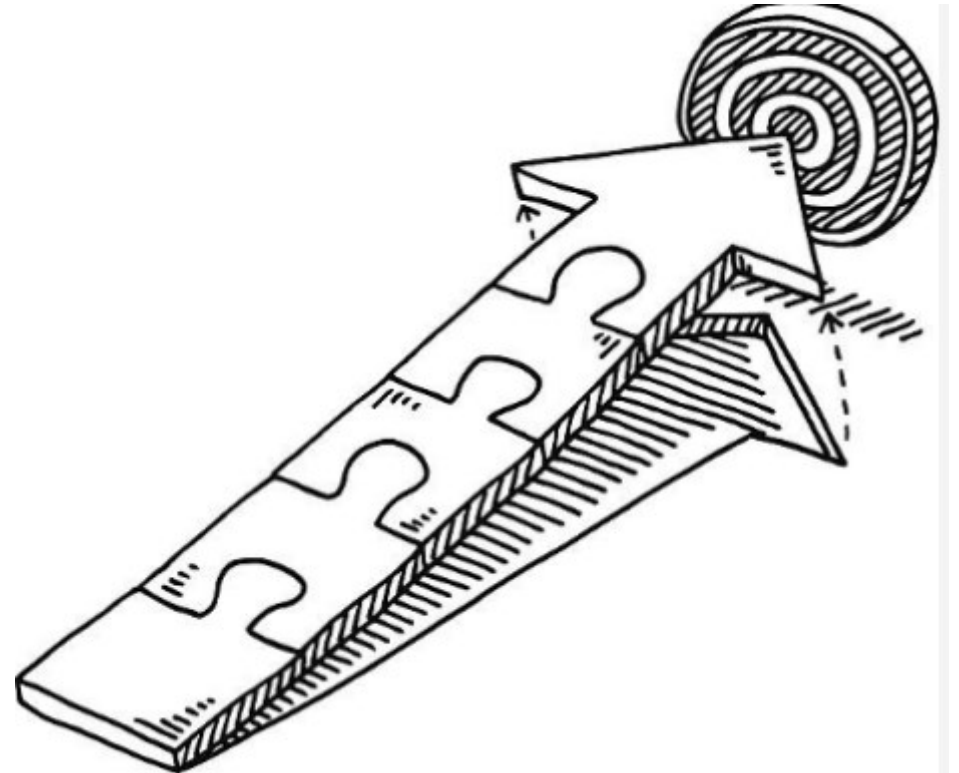
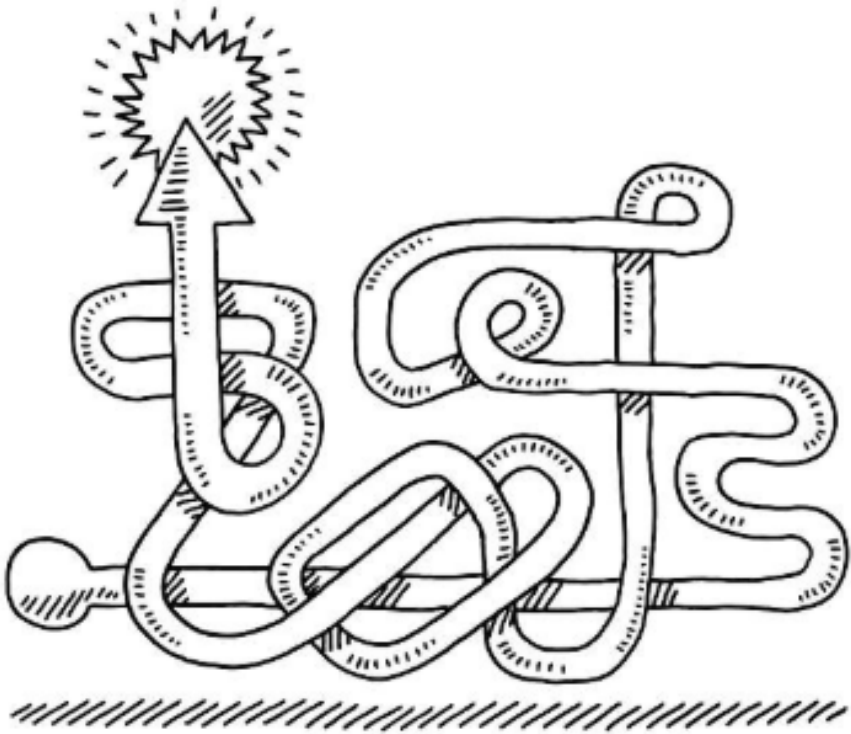
≈ 90 Vorhaben

[illegible]

- Bund
- Kantone
- Wirtschaft
- Hochschulen
- Zivilgesellschaft

Vom «kleinen» Sensibilisierungsprojekt bis zum Aufbau der zentralen Fähigkeiten für Cyberdefence

Koordination & Kontrolle





NCS Steuerungsausschuss

Vertretungen

- aus der Wirtschaft
- aus der Zivilgesellschaft
- aus der Wissenschaft
- Alle Departemente des Bundes

Er erfüllt folgende Kernfunktionen:

- Regelmässige Überprüfung und Strategieentwicklung
- Vorschlag von zusätzlichen Massnahmen und Prioritäten
- Jährliche Berichterstattung



Dr. Maya Bundt, Präsidium



Das BACS agiert als Drehscheibe in der Koordination der NCS Umsetzung

Zentralisierte Koordination/ Governance

- Umsetzungspartner und Stakeholder sind eng in die NCS eingebunden; Synergien fördern
- Die Fortschritte/ Risiken der Vorhaben sind regelmässig überprüft.
- Wirkungsmessung mit KPI's



Sichtbarkeit der NCS stärken

Umsetzung der NCS ist aktiv kommuniziert, online und live.

Neue Vorhaben werden lanciert

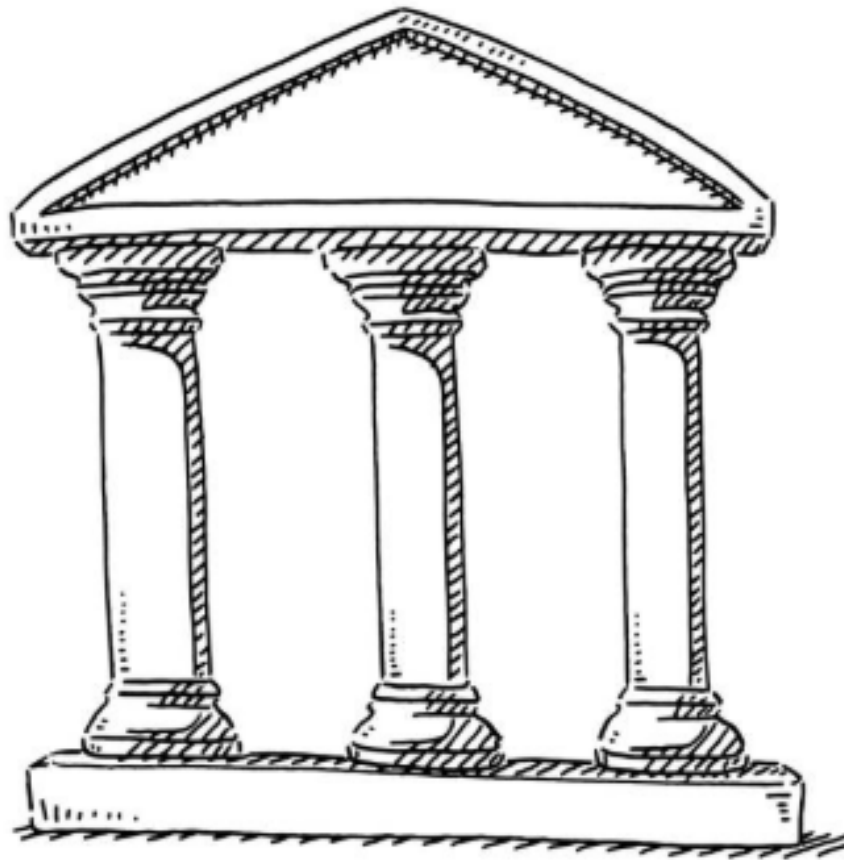
- NCS passt sich den Anforderungen der Cybersicherheit an.

Entwicklung und Unterstützung der Schlüsselgremien

- Steuerungsausschuss, Round Table zur NCS, andere..
- Berichte



Die 3 Säulen der Umsetzung





Round table zur Nationalen Cyberstrategie



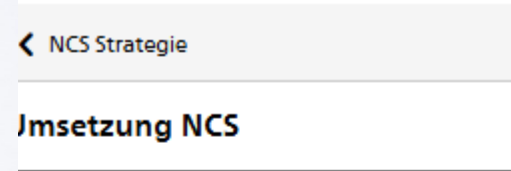


bilaterale Zusammenarbeit und Umsetzungsforen





Information – Austausch - Beratung



M6: Resilienz, Standardisierung und Regulierung

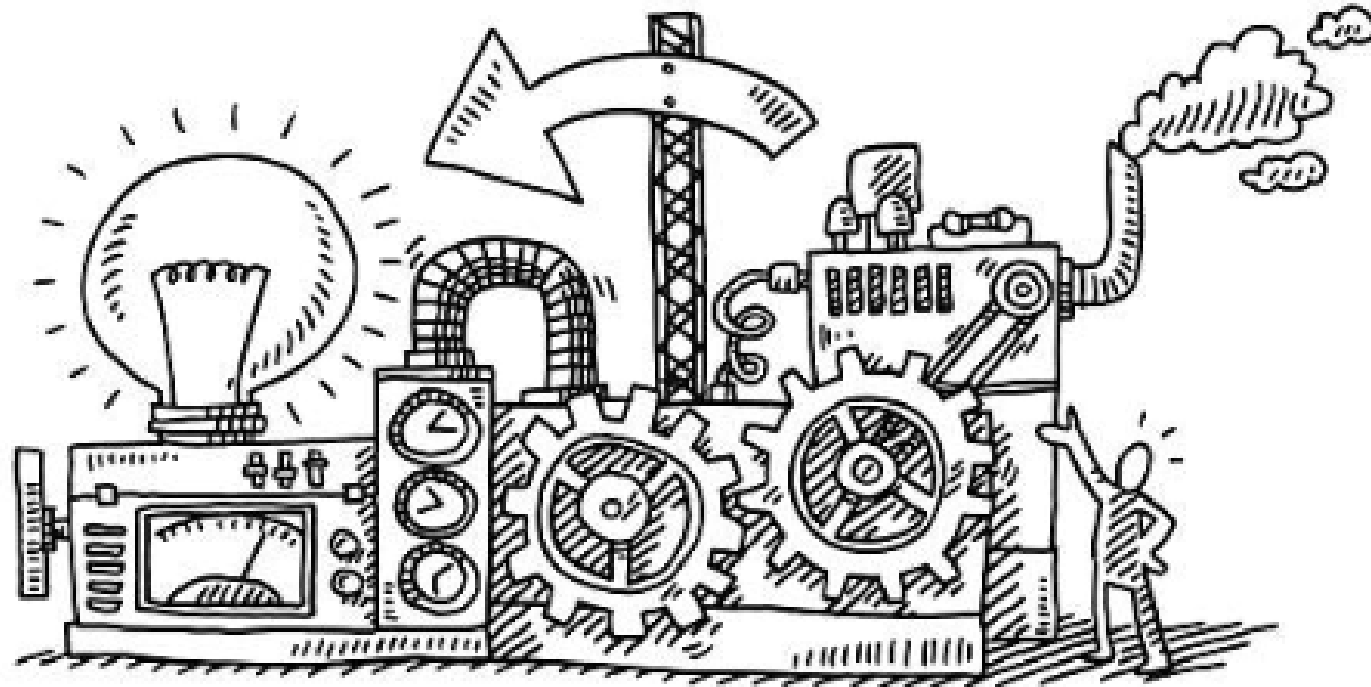
Vorhaben

- › M6-6.1: Swiss FS-CSC
 - › M6-6.2: SWICYBA - Swiss Industry Cybersecurity Association
 - › M6-6.3: Rail ISAC (Information Sharing and Analysis Center)
 - › M6-6.4: Health CSC
 - › M6-6.5: NCSC - Markant Cyber Conference Lebensmittelbranche 202
 - › M6-6.6: Minimalstandard 2.0 «Methode BACS»
 - › M6-6.7: Meldepflicht für Cyberangriffe auf kritische Infrastrukturen
 - › M6-6.8: Cyber-Safe - Label
 - › M6-6.9: Resilienzüberprüfungen (Risiko- und Verwundbarkeitsanaly
- Teilsektoren
- › M6-6.12: Cyberkrisen Bewältigung in Finanzzentren: ein internation
 - › M6-6.13: CyberSeal - Label
 - › M6-6.14: Cyber Community Management





Wirkungsbewertung





Inputs

«Was gemacht wird» : Controlling

Outputs

Ergebnisse

Wirkung

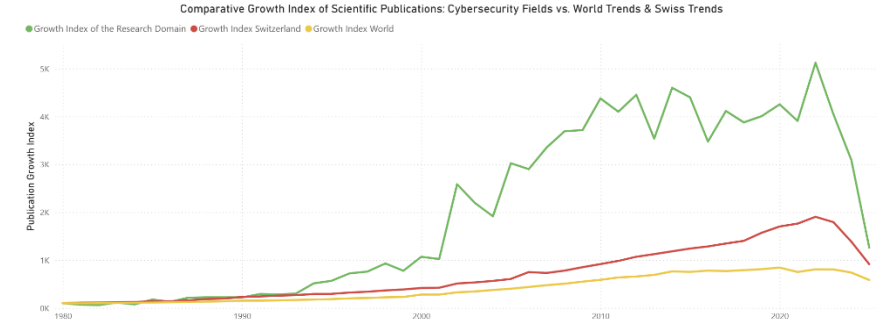
«Funktioniert es?»:
Leistungskennzahl (KPIs)

method by Bertelsmann Stiftung

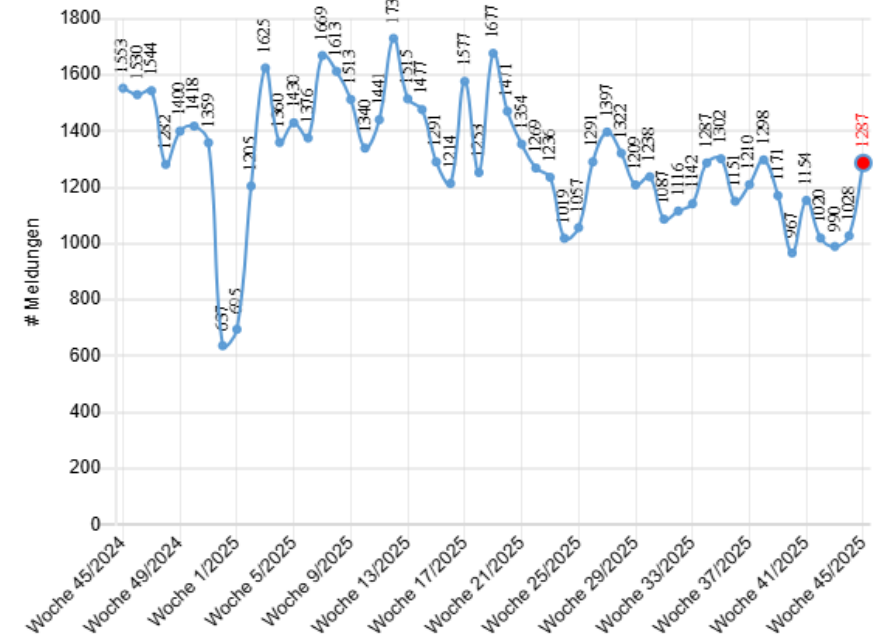


Wirkung NCS – Leistungskennzahlen (KPIs)

Publication Matrix by Institution and Research Topic											
Topic	École Polytechnique Fédérale de Lausanne	ETH Zurich	European Organization for Nuclear Research	FHNW University of Applied Sciences and Arts	IBM Research - Zurich	Università della Svizzera italiana	University of Bern	University of Geneva	University of St.Gallen	University of Zurich	Total
Access Control and Trust	33	73	8		25	10	10	20	7	14	194
Advanced Authentication Protocols Security	47	133		2	29		4	3		3	216
Advanced Software Engineering Methodologies	85	60	5	7	13	86	86	11	7	36	388
Advanced Steganography and Watermarking Techniques	55	9			6			92			161
Advanced Wireless Network Optimization	36	9			3	1	2			1	50
Cryptographic Implementations and Security	216	91		110	18	51	2	1	1	3	444
Cryptography and Data Security	221	415	4	2	302	17	12	10	10	15	970
Cryptography and Residue Arithmetic	51	15	6		13					10	89
Cybercrime and Law Enforcement Studies		5				4	1	1	1	3	14
Cybersecurity and Cyber Warfare Studies	8	61	1	1	2	4	3	13	3	27	117
Data Privacy and Cybersecurity						1				1	1
Digital and Cyber Forensics	4	6		1		2		3		2	17
Digital literacy in education	7	2	1	7		1	1	5	6	16	45
Digitalization, Law, and Regulation	2	11		1			11	2	17	46	87
Distributed and Parallel Computing Systems	153	185	1503	2	40	24	36	87	15	76	2038
Embedded Systems Design Techniques	340	155	26	2	7	50	15	10		4	579
Information and Cyber Security	9	68	5	15	12	3	7	8	25	24	169
Information Technology Governance and Strategy	16	5		17	2	2	24	5	172	4	245
Network Security and Intrusion Detection	45	106	9	1	41	6	6	10	1	46	260
Network Traffic and Congestion Control	154	94	12		34	6	26	3	1	12	329
Physical Unclonable Functions (PUFs) and Hardware Security	36	19	1	1	5	16	1	9	1	4	89
Privacy, Security, and Data Protection	34	61		5	20	34	17	22	52	89	315
Security and Verification in Computing	72	178	2	1	48	21	4	8	4	7	336
Security, Politics, and Digital Transformation		3				1				2	6
Software Engineering Research	68	107	13	10	9	345	243	19	9	357	1115
Software Engineering Techniques and Practices	13	54	2	54	5	19	13	23	30	74	271
Software Reliability and Analysis Research	19	23	6		2	15	4		2	7	76
Software Testing and Debugging Techniques	106	103	9	5	10	192	29	12	6	47	578
User Authentication and Security Systems	25	46		2	19	5	2	6	7	12	119
Wireless Communication Security Techniques	211	153			4	2	1	13		378	
Wireless Networks and Protocols	48	28	2		11	2	4	5	1	101	
Total	2114	2358	1612	246	680	920	564	401	386	941	9797

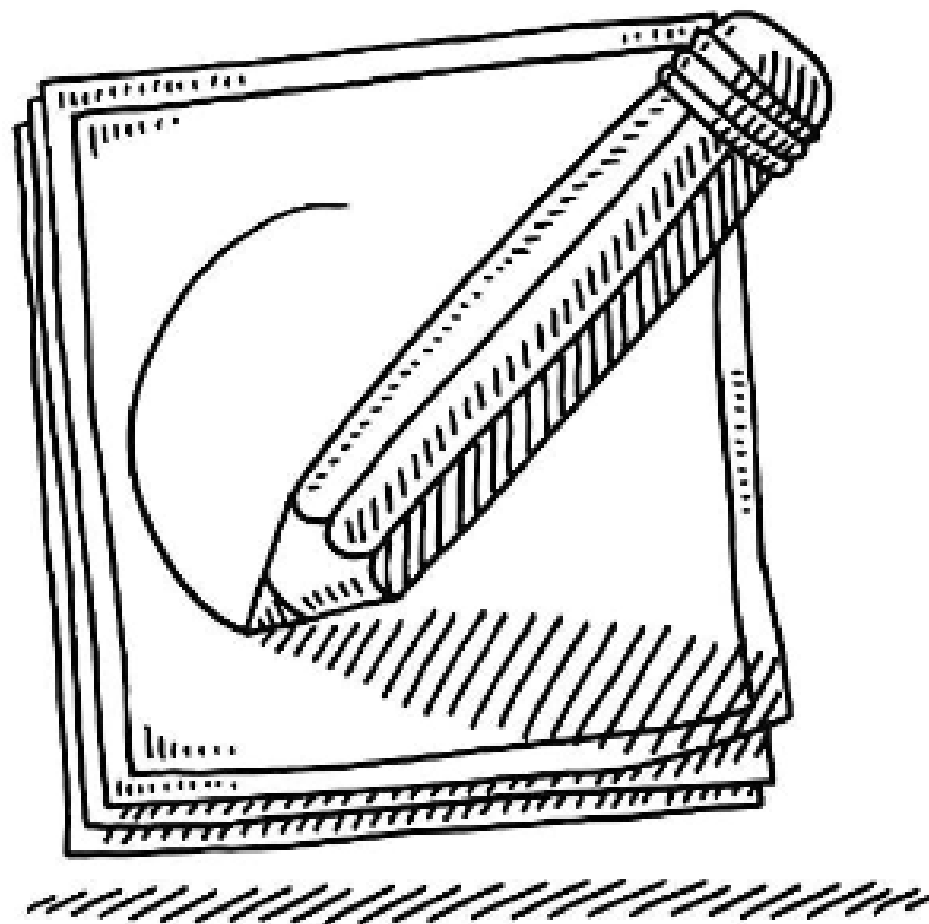


Grafik 1 - NCSC.ch: Meldeeingang



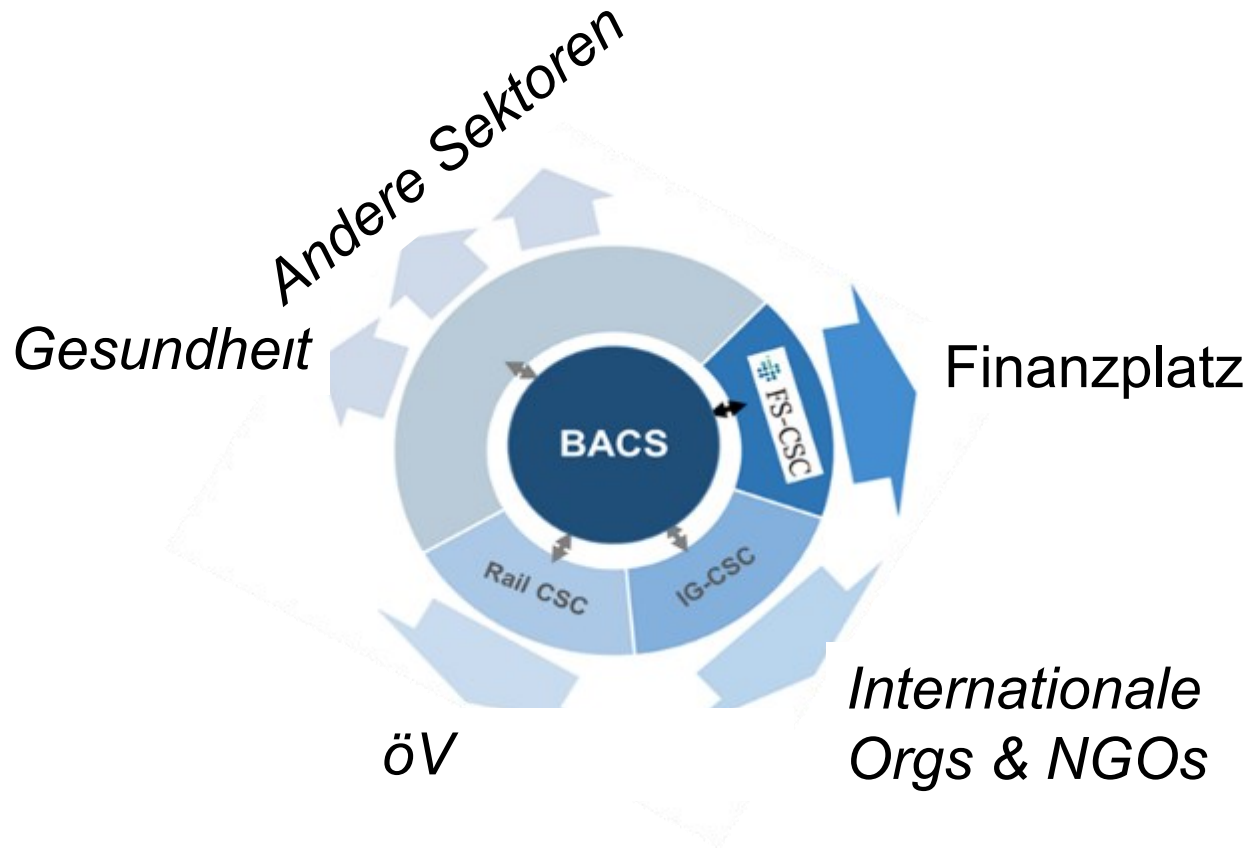


Ein Beispiel aus der Umsetzung





Cybersecurity Centers (CSC)



CSCs sind sektorspezifische Zentren für präventive Cybersicherheitsmassnahmen.

Die CSCs können gezielt auf branchenspezifische Risiken eingehen und den Austausch sowie die Reaktionsfähigkeit stärken.

- Cyber Threat Intelligence und Monitoring (sektorspezifisch)
- Best Practices und Leitfäden
- Operative Unterstützung und fachliche Beratung
- Sektorspezifische Sensibilisierung (z. B. Schulungsmaterialien)

vielen Dank



romain.geiser@ncsc.admin.ch

LinkedIn

