



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cyberbedrohungen: Lage national und international



10. November 2023, BEA Bern Expo



Programm

Referent:

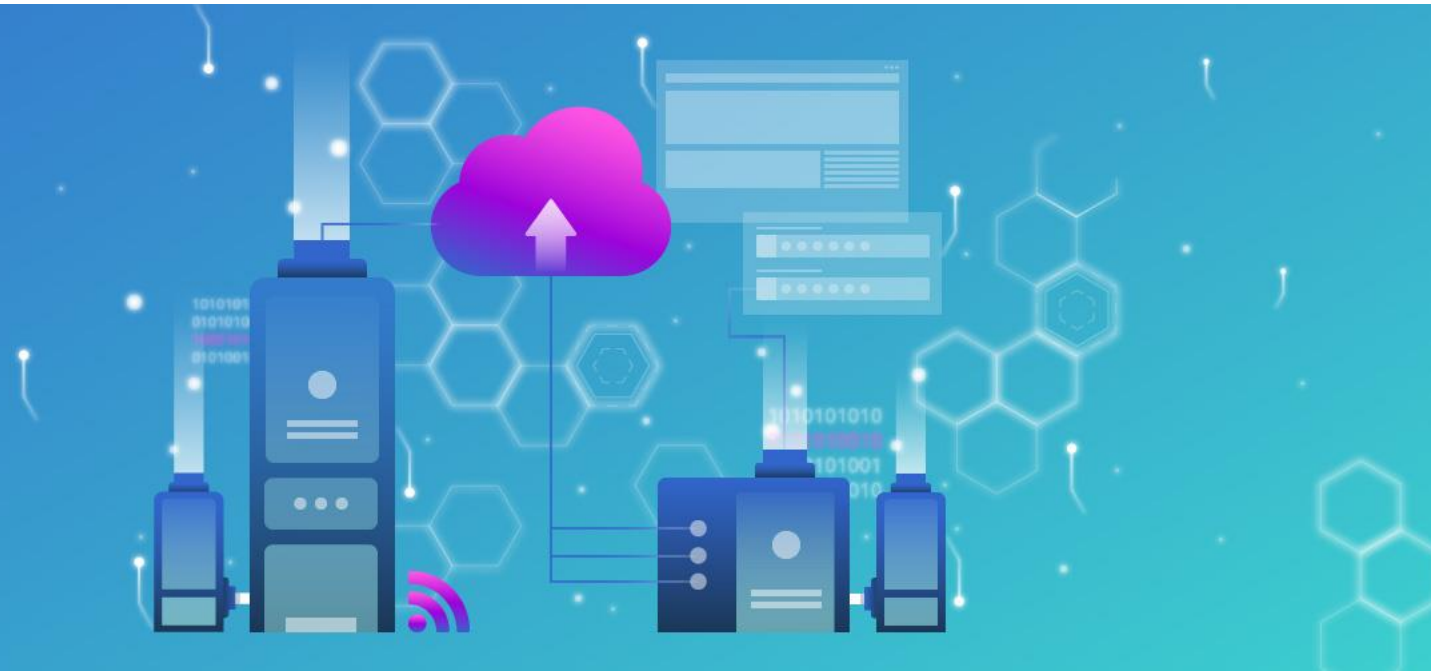
Max Klaus

stv. Leiter Operative Cybersicherheit OCS

Nationales Zentrum für Cybersicherheit NCSC



- 1. Das Nationale Zentrum für Cybersicherheit NCSC**
- 2. Lage national und international / Akteure**
- 3. Schlussfolgerungen / Empfehlungen**



1. Das Nationale Zentrum für Cybersicherheit NCSC



Wie alles begann

17.3508 MOTION

Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund

Eingereicht von:



EDER JOACHIM
FDP-Liberale Fraktion
FDP.Die Liberalen

Berichterstattung:

CLOTTU RAYMOND, GLÄTTLI BALTHASAR

Einreichungsdatum:


15.06.2017

Eingereicht im:

Ständerat

Stand der Beratungen:

Abgeschrieben

 ALLES ZUKLAPPEN

 EINGEREICHTER TEXT

Der Bundesrat wird beauftragt, im Zusammenhang mit der laufenden Überarbeitung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) ein Cybersecurity-Kompetenzzentrum auf Stufe Bund zu schaffen und dafür die notwendigen Massnahmen einzuleiten. Diese Organisationseinheit hat die Aufgabe, die zur Sicherstellung der Cybersecurity notwendigen Kompetenzen zu verstärken und bundesweit zu koordinieren. Sie soll departementsübergreifend wirksam sein, das heisst insbesondere, dass sie im Bereich Cybersecurity über Weisungsbefugnis gegenüber den Ämtern verfügen soll. Das Kompetenzzentrum arbeitet mit Vertretern der Wissenschaft (Hochschulen, Fachhochschulen), mit der IT-Industrie und mit den grösseren Infrastrukturbetreibern (insbesondere Energie, Verkehr) zusammen.



Rahmenbedingungen für das NCSC



Keine Meldepflicht für Cybervorfälle



Subsidiarität



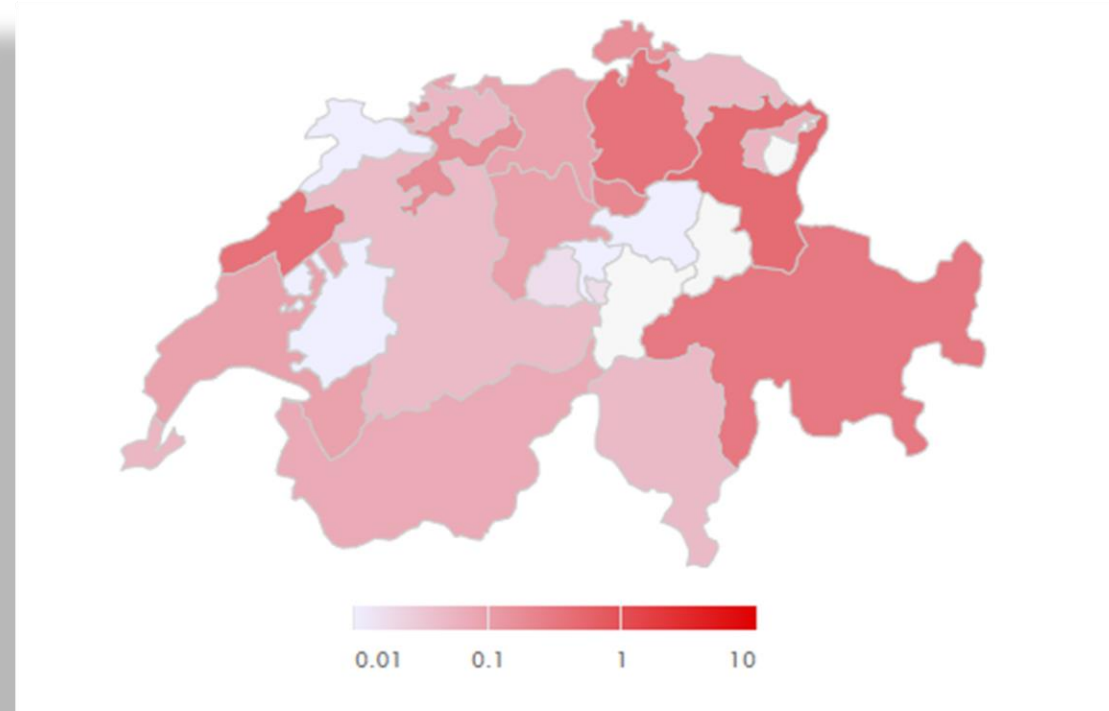
Keine Weisungsbefugnis ausserhalb der Bundesverwaltung



2. Lage national und international / Akteure



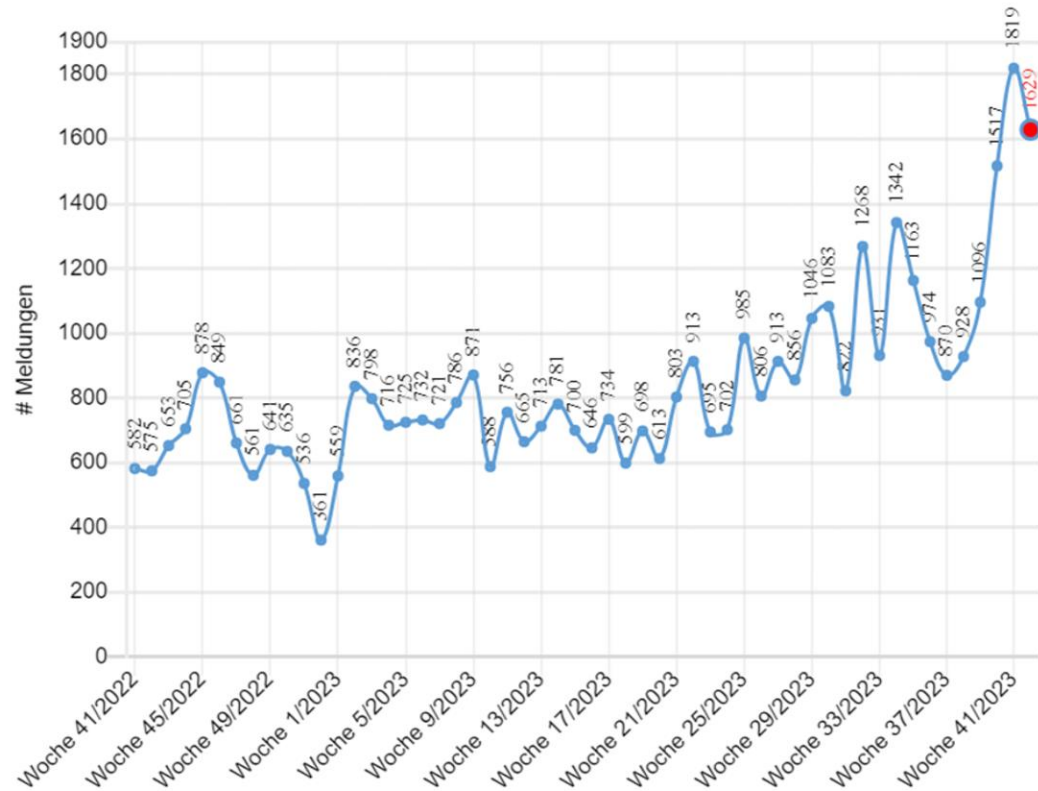
Aktuelle Bedrohungslage



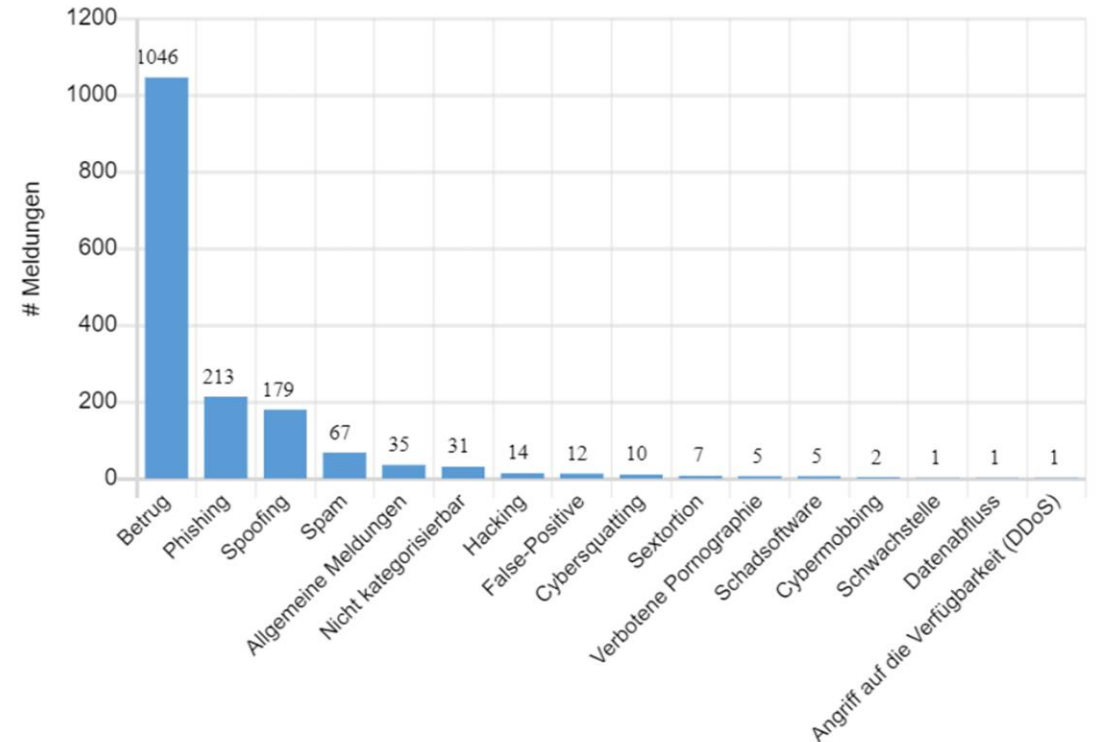


Kennzahlen NCSC (Woche 42/2023)

Grafik 1 - NCSC.ch: Meldeeingang



Grafik 2 - NCSC.ch: Meldeeingang nach Hauptkategorien: Woche 42/2023





3. Schlussfolgerungen / Empfehlungen



Schlussfolgerungen

- Die Bedrohungslage verändert sich laufend
- KMU sind in der Regel stärker gefährdet als Grossunternehmen
- Meistens Angriffe nach dem Giesskannenprinzip, gezielte Angriffe selten
- Alle können Opfer eines Cyber-Angriffs werden. Es gibt kaum branchenspezifische Unterschiede
- Finanzieller Gewinn als Hauptmotivation
- Gesunder Menschenverstand als «Grundschutz» im privaten Bereich



Empfehlungen: proaktiv (1/3)

Besuchen Sie unsere Website:
www.ncsc.admin.ch:

Informationen für:

- Privatpersonen
- Unternehmen
- Behörden
- IT-Spezialisten

Zahlreiche **kostenlose** Anleitungen,
Checklisten, Whitepapers.

The screenshot shows the homepage of the National Center for Cyber Security (NCSC). At the top, there is a navigation bar with the Swiss flag, the text 'Bundesverwaltung', 'EFD', and 'NCSC'. Below this is a search bar and a menu with categories like 'Aktuell', 'Cyberbedrohungen', 'Informationen für', 'NCS Strategie', 'Dokumentation', and 'Über NCSC'. The main content area features a large blue banner with the text 'Herzlich Willkommen im Nationalen Zentrum für Cybersicherheit NCSC'. Below the banner are two columns of icons: 'Informationen für' (targeting Privatpersonen, Unternehmen, Behörden, IT-Spezialisten) and 'Melden Sie uns' (for a Cyber incident or a Weakness). The lower section is divided into three columns: 'Aktuelle Vorfälle' with a text-based news item about a phishing SMS; 'Statistik' with two line charts showing 'NC SC.ch: Meldeingang' and 'NC SC.ch: Meldeingang nach Kategorien' for the week of 10.05.2022; and 'Im Fokus' with a news item about a security measure for infrastructure and a photo of a person working on a laptop. At the bottom, there is a 'Medienmitteilungen' section with an 'abonnieren' button.



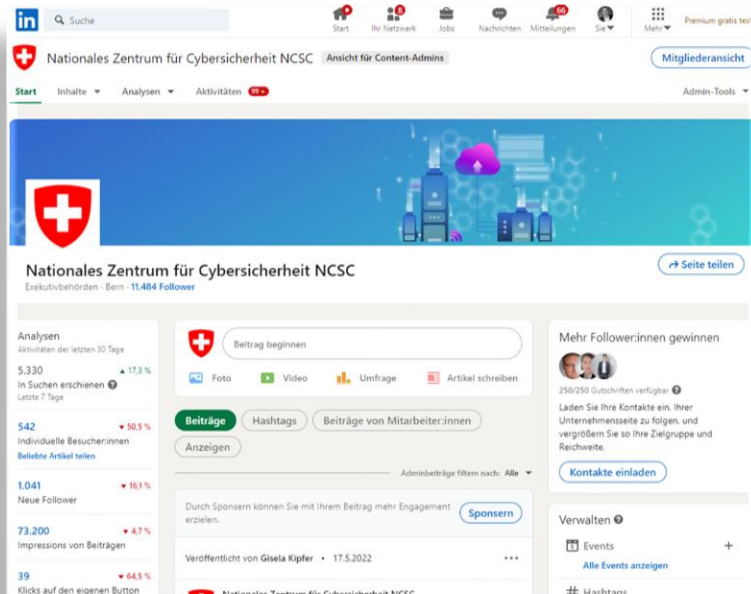
Empfehlungen: proaktiv (2/3)

Folgen Sie uns auf LinkedIn:

<https://www.linkedin.com/company/70430924/admin/>

Folgen Sie uns auf X (Twitter)

https://twitter.com/GovCERT_CH





Empfehlungen: proaktiv (3/3)

Das Übliche zuerst:

- Starke Passwörter / regelmässiger PW-Wechsel / 2FA
- Virenschutz
- Firewall (blacklist usw.)
- Updates
- Backups
- ...

Aber:

- Technische Massnahmen allein genügen nicht!
- Organisatorische Massnahmen wie BCM, Krisenkommunikation usw. berücksichtigen!

Empfehlungen: reaktiv

Meldeformular NCSC:

<https://www.report.ncsc.admin.ch/de/>

Das NCSC garantiert:

- Anonyme Meldungen
- 100% Vertraulichkeit
- Keine Sanktionen (evtl. DSGVO der EU beachten!)
- In der Regel Erstantwort innerhalb von 24 Stunden.

Strafverfolgung:

- Privatpersonen: Kantonspolizei am Wohnsitz
- Unternehmen: Kantonspolizei am Geschäftssitz



Vielen Dank für Ihre Aufmerksamkeit