



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Eidgenössisches Finanzdepartement (EFD)  
Nationales Zentrum für Cybersicherheit (NCSC)

# Herausforderungen für die Schweiz aus der Perspektive des Nationalen Zentrums für Cybersicherheit (NCSC)

**Pascal Lamia**

*24. November 2020*

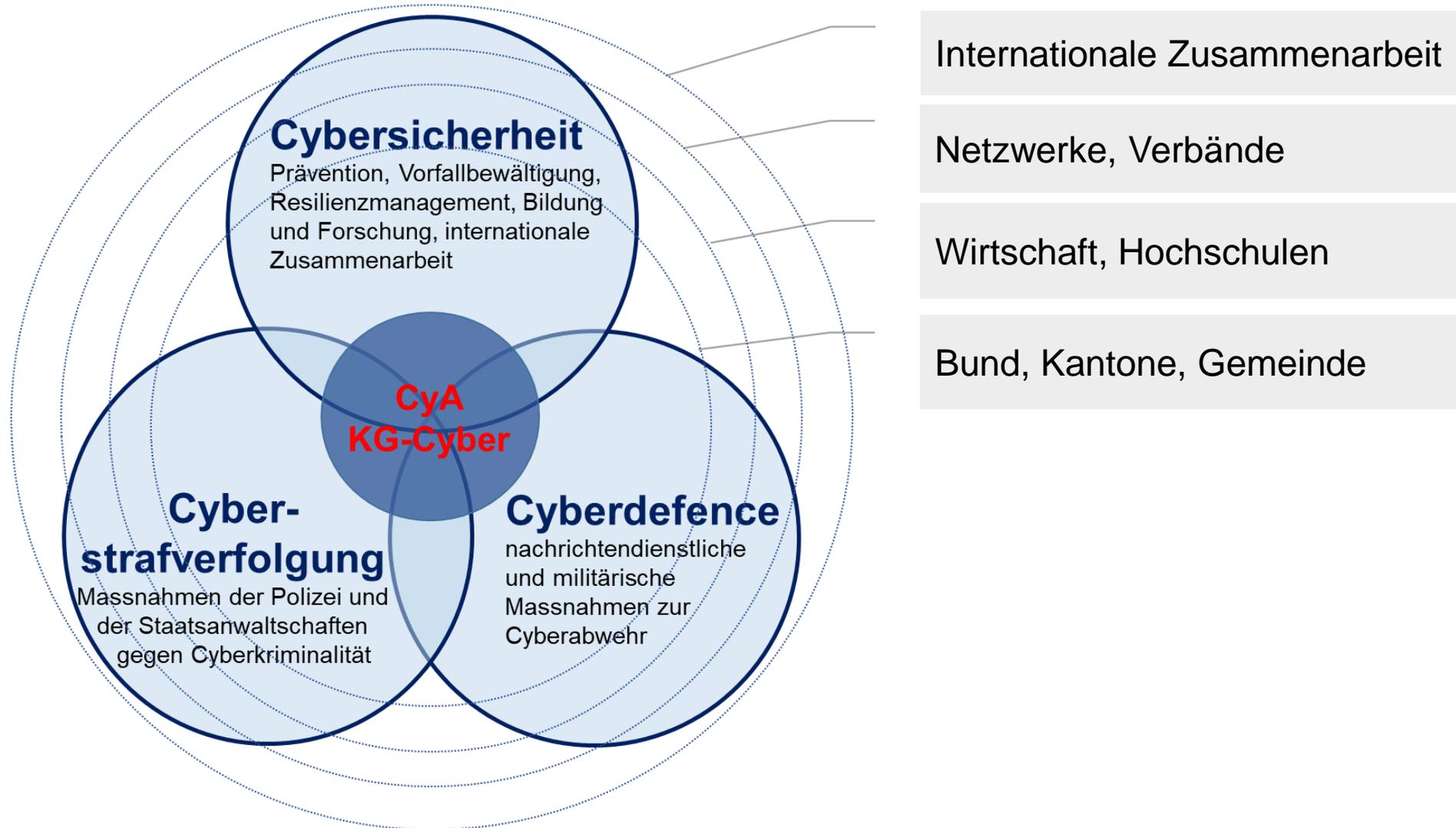


# Übersicht

1	Organisation des Bundes im Bereich Cyberrisiken
2	Stand Aufbau Nationales Zentrum für Cybersicherheit NCSC
3	Herausforderungen
4	Cyberrisiken im Gesamtkontext

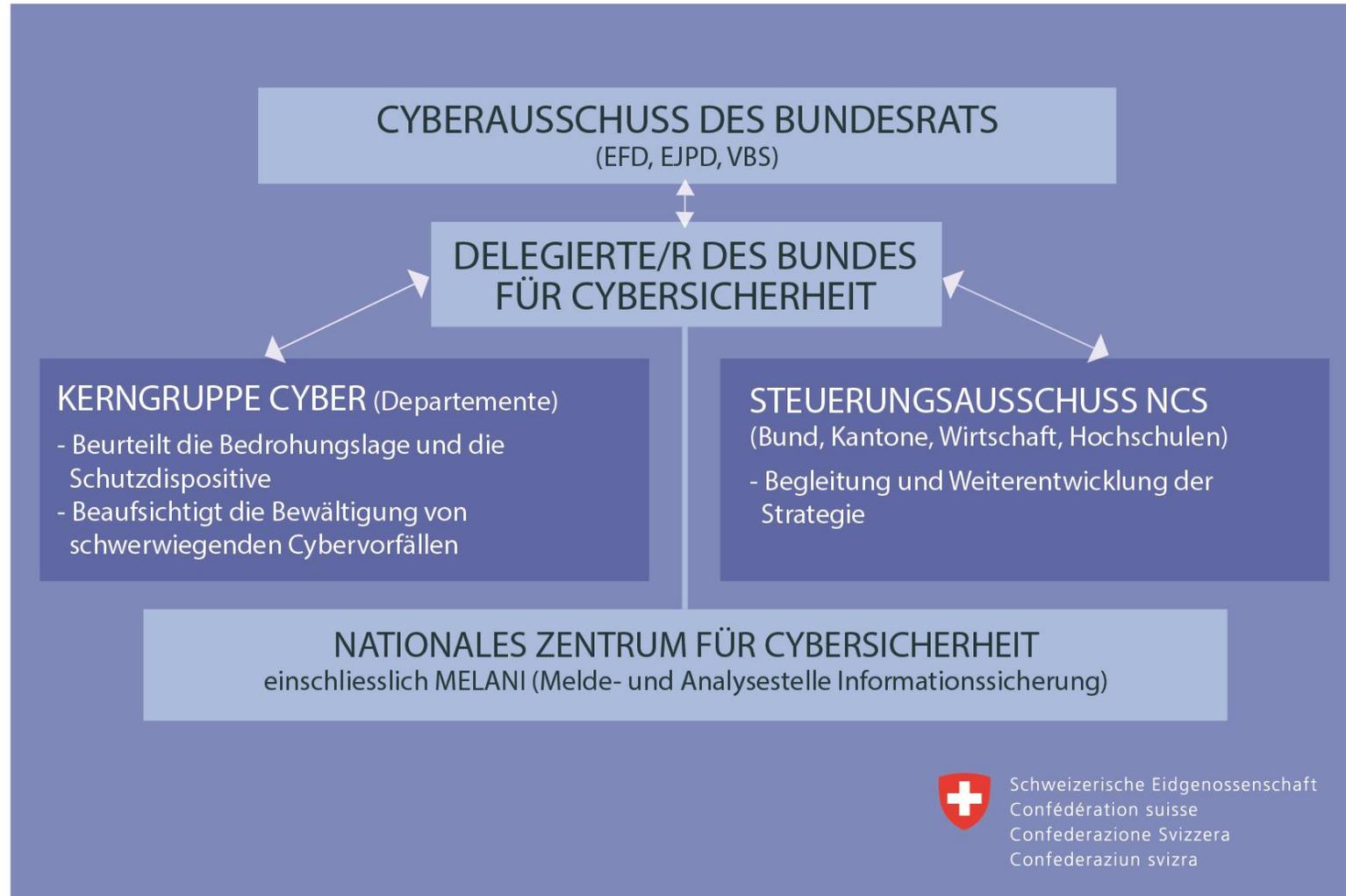


# Cyberrisikobereiche





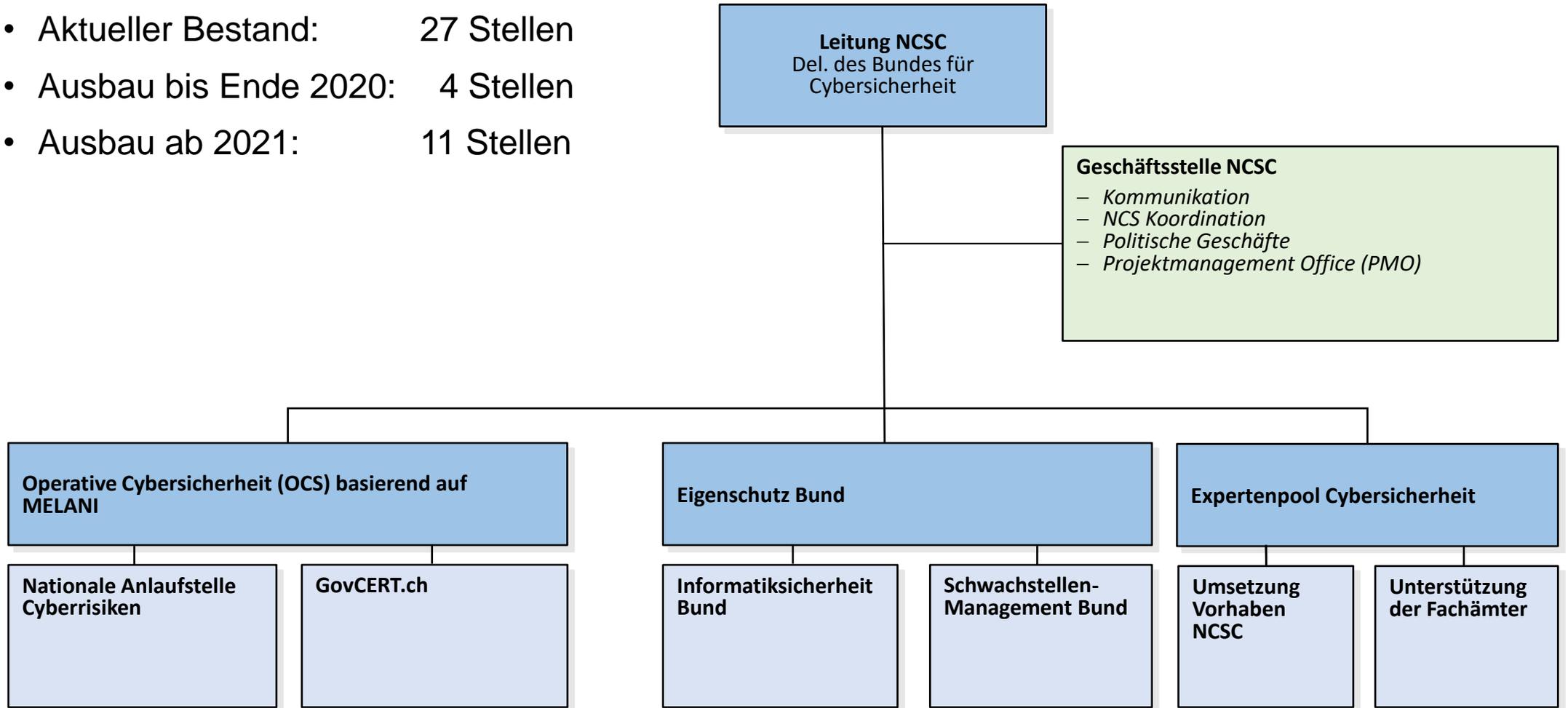
# Organisation des Bundes im Bereich Cyberrisiken





# Aufbau Nationales Zentrum für Cybersicherheit (NCSC)

- Aktueller Bestand: 27 Stellen
- Ausbau bis Ende 2020: 4 Stellen
- Ausbau ab 2021: 11 Stellen



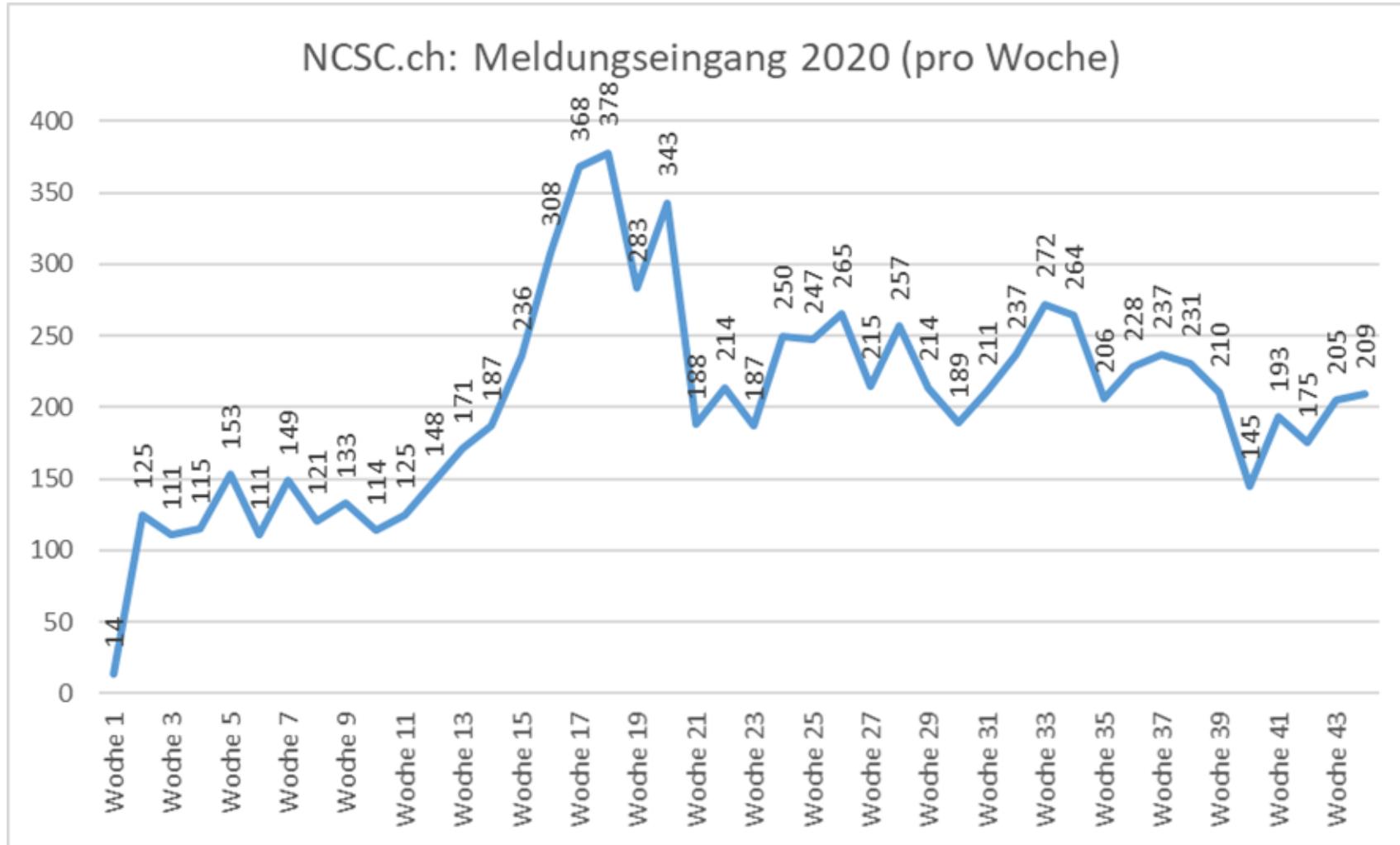


# Herausforderungen



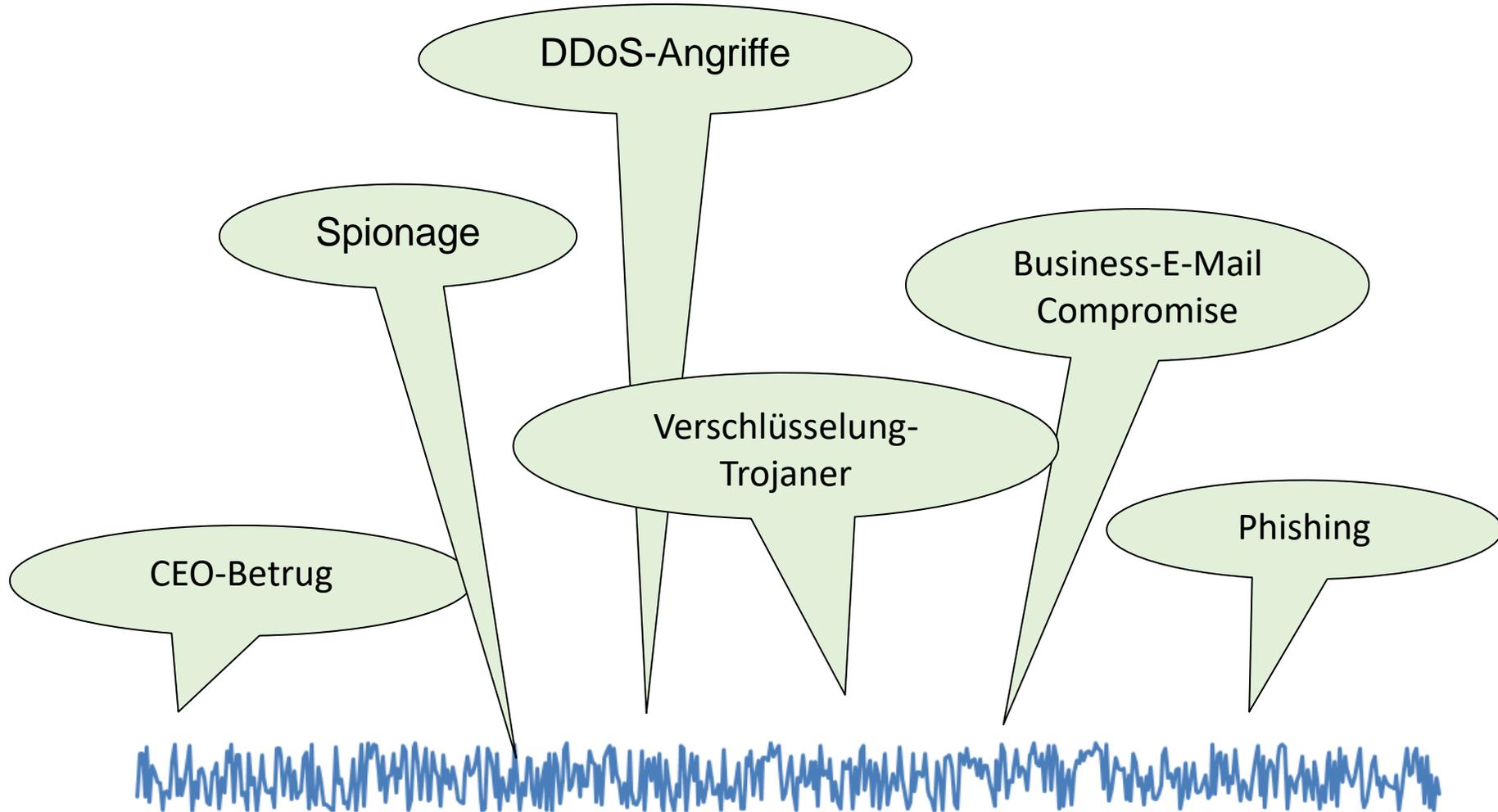


# Das NCSC in Zahlen – Anzahl Meldungen pro Woche





# Häufige Delikte



# Herausforderung KMU



Home » Tests & Ratgeber » Sicherheit » News

**SPECIAL** Special: Sicherheits-Center – Ransomware-Angriff auf Uniklinik Düsseldorf

## Ransomware legt Uniklinik Düsseldorf lahm

15.09.2020, 15:32 Uhr Ein Ransomware-Angriff hat die Uniklinik Düsseldorf komplett lahmgelegt. Nicht einmal Rettungswagen dürfen das Krankenhaus anfahren.



von Andy Voß



Grosse Konzerne wie Banken und Versicherungen wissen, dass sie sich gegen Hacker-Angriffe wehren müssen. Die Chefs vieler kleiner und mittlerer Unternehmen dagegen halten sich für zu wenig interessant für Angreifer aus dem Netz.

Eidgenössisches Finanzdepartement (EFD)  
Nationales Zentrum für Cybersicherheit (NCSC)

ERPRESSUNG

04.07.2020 12:55

## Universität bezahlt 1,14 Millionen Lösegeld an Hacker

Nach einem Hackerangriff verlangten Cyberkriminelle über eine Million Dollar von einer amerikanischen Universität. Diese bezahlte tatsächlich.

von Dominique Zeier



# Ransomware im Spital

## Hackerangriff auf Uniklinik Düsseldorf: Ermittlungen wegen fahrlässiger Tötung

Der IT-Ausfall an der Uniklinik geht tatsächlich auf einen Hackerangriff zurück. Die Erpresser zogen sich zurück. Es wird wegen eines Todesfalls ermittelt.

Lesezeit: 2 Min.  In Pocket speichern

   229



## Patientin starb nach verspäteter Behandlung

Gegen die Unbekannten wird jetzt auch wegen fahrlässiger Tötung ermittelt, da eine lebensbedrohlich erkrankte Patientin, die in der Nacht vom 11. auf den 12. September in die Uniklinik gebracht werden sollte, an ein Krankenhaus in Wuppertal verwiesen wurde. **Ihre Behandlung habe erst mit einstündiger** Verspätung stattfinden können. Sie starb kurze Zeit später, so der Justizminister in seinem Bericht.

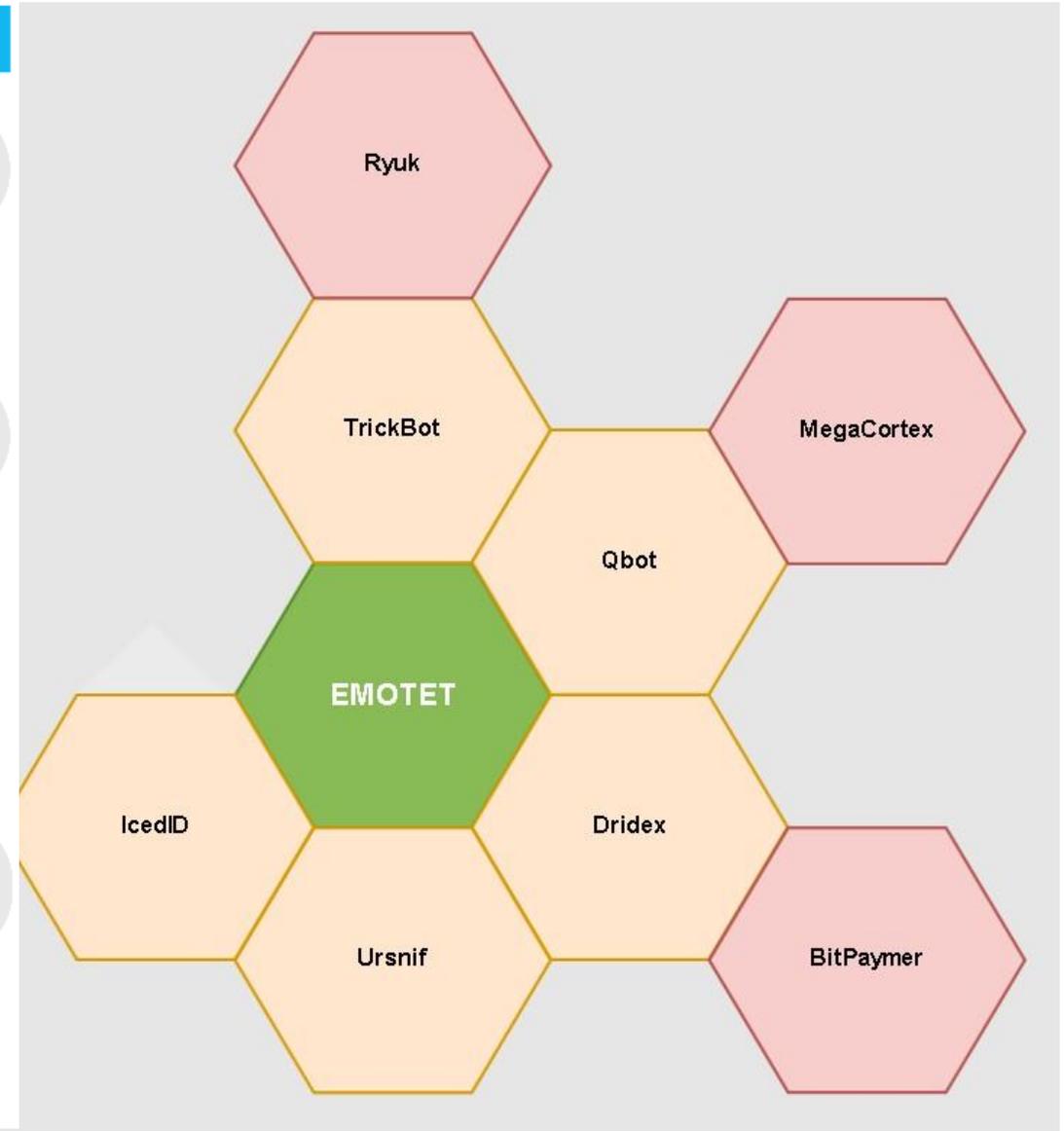
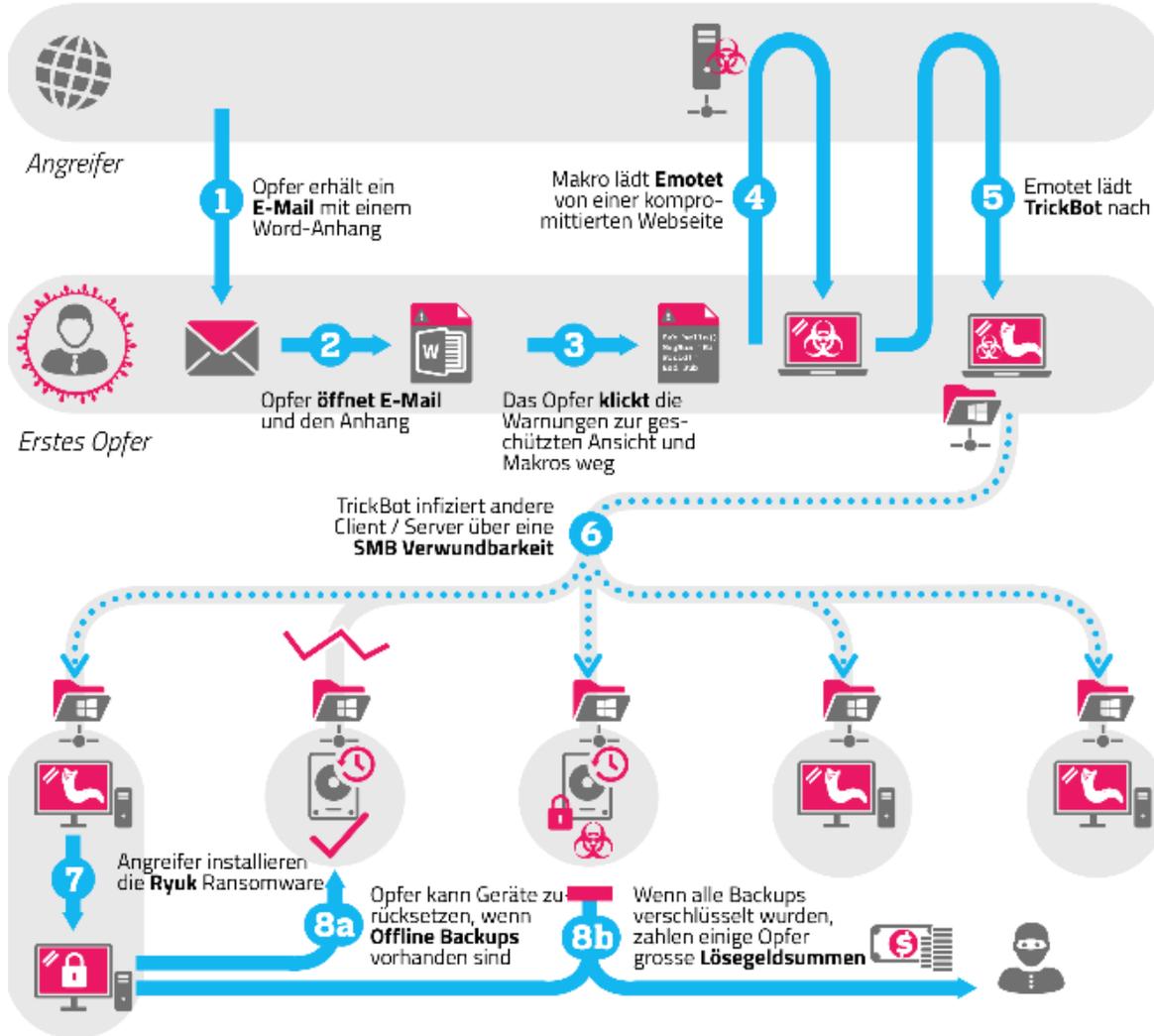
Bei dem Hackerangriff sind nach bisherigen Erkenntnissen keine Daten gestohlen oder unwiederbringlich gelöscht worden. Das hätten Untersuchungen von IT-Experten ergeben, teilte die Klinik mit.

Die Hacker hätten eine Schwachstelle in einer Anwendung ausgenutzt. "Die Sicherheitslücke befand sich in einer marktüblichen und weltweit verbreiteten kommerziellen Zusatzsoftware. Bis zur endgültigen Schließung dieser Lücke durch die Softwarefirma war ein ausreichendes Zeitfenster gegeben, um in die Systeme einzudringen", teilte die Klinik mit. Die Angreifer hätten dafür gesorgt, dass nach und nach Systeme ausfielen und ein Zugriff auf gespeicherte Daten nicht mehr möglich war.



# Emotet Infektionsablauf

Attribution  
CC BY-SA/CS/PL/IT





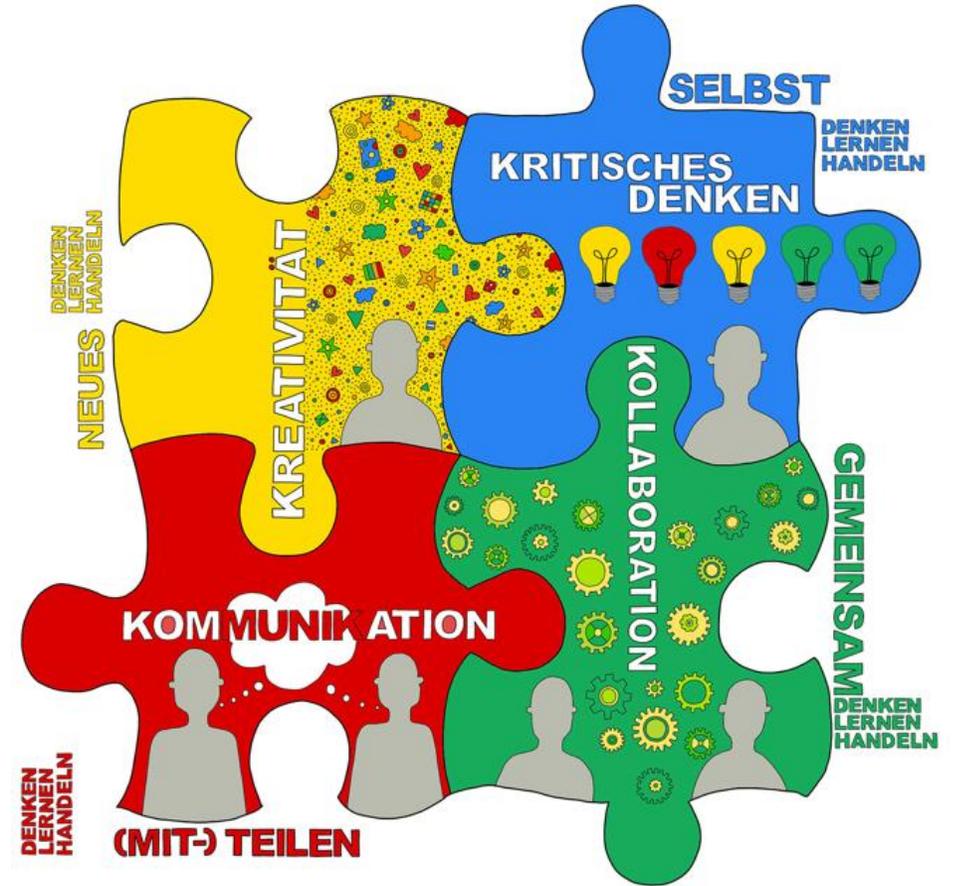
# Herausforderungen

- Koordination NCSC intern
- Übersicht über die aktuelle Cyberlage
- Übersicht aller 'Cyber' Player in der Schweiz und International
- Koordination mit allen Partnern
- Stufengerechte Informationen an die Öffentlichkeit
- Ausbau NCSC



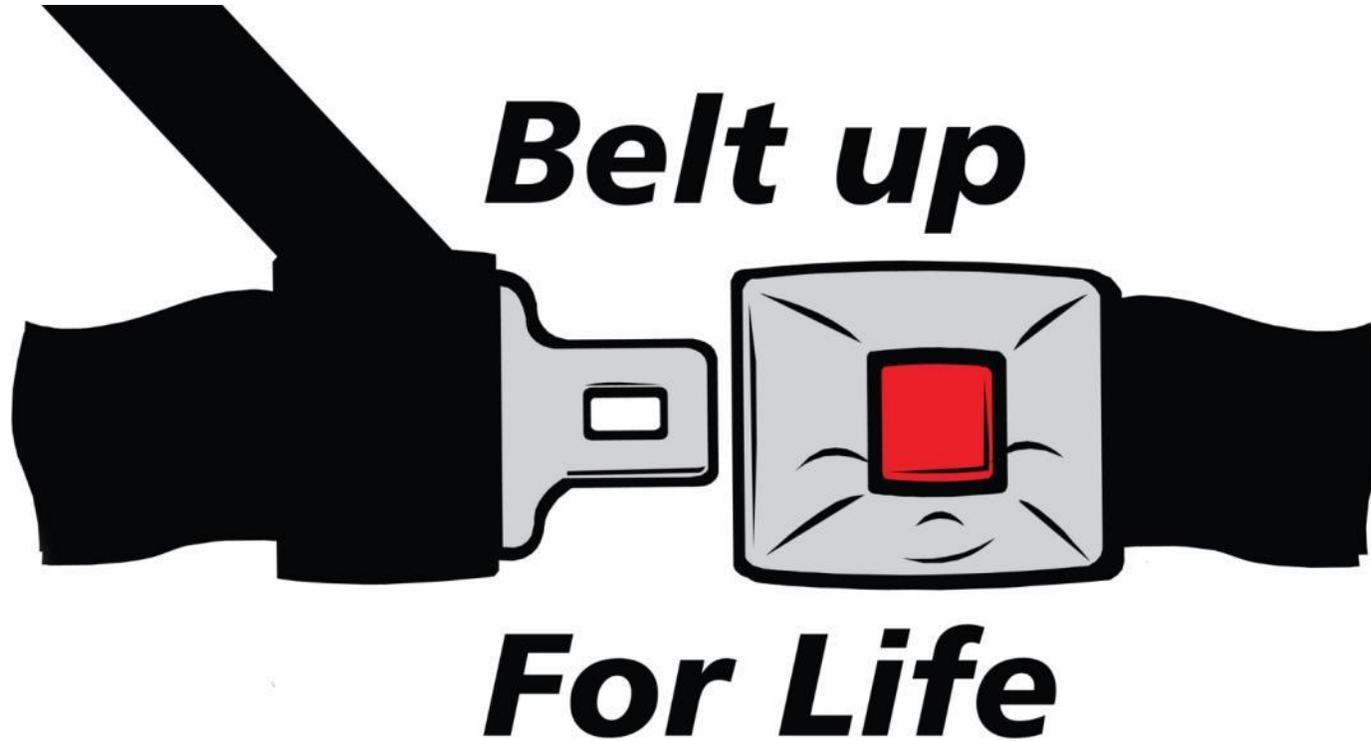


# Klare und verständliche Kommunikation





# Sicherheit vs. Risiko





# Cyber Risiken im Gesamtkontext

- Informationssicherheit ist nicht gleich IT-Sicherheit. Nur ein **integraler, Risikomanagement basierter Prozess** kann zu einem besseren Informationsschutz führen.
- **Risikomanagement ist Aufgabe der Geschäftsleitung!**
  - Fragen Sie die richtigen Fragen und vertrauen sie nicht auf eine rein technische Lösung. Diese mag als Sicherheitsmassnahme Sinn machen, aber sie sind nur Teil des Risikomanagements.
- **Nehmen Sie Ihre Eigenverantwortung wahr!**
  - Prinzipiell gilt: Chancen sind zu ergreifen, aber die inhärenten Risiken zu erkennen (Datenschutz, Komponentensicherheit, Abhängigkeiten etc...)
  - Es empfiehlt sich Risiken früh genug zu erkennen und wo nötig geeignete Massnahmen zu ergreifen



# Vielen Dank für Eure Aufmerksamkeit



## **Pascal Lamia**

Stv. des Delegierten für Cybersicherheit  
Leiter Operative Cybersicherheit und MELANI  
Nationales Zentrum für Cybersicherheit (NCSC)

[pascal.lamia@gs-efd.admin.ch](mailto:pascal.lamia@gs-efd.admin.ch)

Eidgenössisches Finanzdepartement (EFD)  
**Nationales Zentrum für Cybersicherheit (NCSC)**