KANTON
LUZERN


# Cybersicherheit in der Verwaltung

## *Bedrohungen, Akteure & Schutzmassnahmen*

*VSLG-Seminar*
*S. Frank, Cyberkoordinator Kanton Luzern*

*Luzern, 30.11.2023*

KANTON
LUZERN

# Cybervorfälle «Gemeinden» Okt-Nov 2023

## CYBER-ANGRIFF AUF ICT-SYSTEME DER GEMEINDE ZOLLIKOFEN

23. November 2023

**Aufgrund eines Cyber-Angriffs in der Nacht auf den 22. November 2023 stehen die ICT-Systeme der Gemeindeverwaltung Zollikofen zur Zeit nicht zur Verfügung. Die notwendigen Massnahmen zum Schutz von Daten und ICT-Infrastruktur wurden eingeleitet.**

Auf die ICT-Systeme der Gemeinde Zollikofen ist ein Cyber-Angriff verübt worden. In der Nacht auf den 22. November 2023 haben die Überwachungssysteme einen externen Angriff festgestellt. Sämtliche ICT-Systeme wurden heruntergefahren und vom Internet getrennt.

Mit externen Cybersecurity-Spezialisten werden zurzeit die ICT-Systeme vertieft untersucht, damit diese möglichst zeitnah wieder hochgefahren werden können. Die Gemeinde Zollikofen verfügt über externe Backup-Systeme, die nach derzeitigem Kenntnisstand nicht vom Angriff betroffen sind.

Aktuell sind die Mitarbeitenden der Gemeindeverwaltung weder per E-Mail noch per Telefon zu erreichen. Auch Mitteilungen/Bestellungen via Internetseite der Gemeinde Zollikofen www.zollikofen.ch erreichen die Gemeindeverwaltung momentan nicht. Kundinnen und Kunden sind gebeten, die Gemeindeverwaltung persönlich am Schalter zu kontaktieren, wobei nur beschränkte Dienstleistungen erbracht werden können. Für Notfälle ist eine Hotline eingerichtet worden. Die Hotline ist während der üblichen Öffnungszeiten unter der Nummer +41 79 102 63 67 erreichbar.

**Schweiz**

**Deutschland**

MEHRE STÄDTE UND KREISE BETROFFEN

## Hackerangriff sorgt für Verwaltungsausfall in NRW

Aktuell sind mehrere Städte und Kommunen in Nordrhein-Westfalen offline. Grund dafür ist eine Cyberattacke auf einen kommunalen IT-Dienstleister.

31. Oktober 2023

**Davon betroffen sind demnach 72 Mitgliedskommunen in Südwestfalen, darunter die Landkreise Hochsauerlandkreis, Märkischer Kreis, Olpe, Siegen-Wittgenstein, Soest sowie mehrere Kommunen im Rheinisch-Bergischen Kreis und einige externe Kunden im Bundesgebiet. Wie die Regionalzeitung Sauerland Kurier berichtet, geht man im Hochsauerlandkreis davon aus, dass der IT-Ausfall mehrere Tage dauert. Die meisten Verwaltungen seien nur noch telefonisch erreichbar, da auch der E-Mail-Verkehr betroffen ist, heißt es im Bericht.**

KANTON
LUZERN

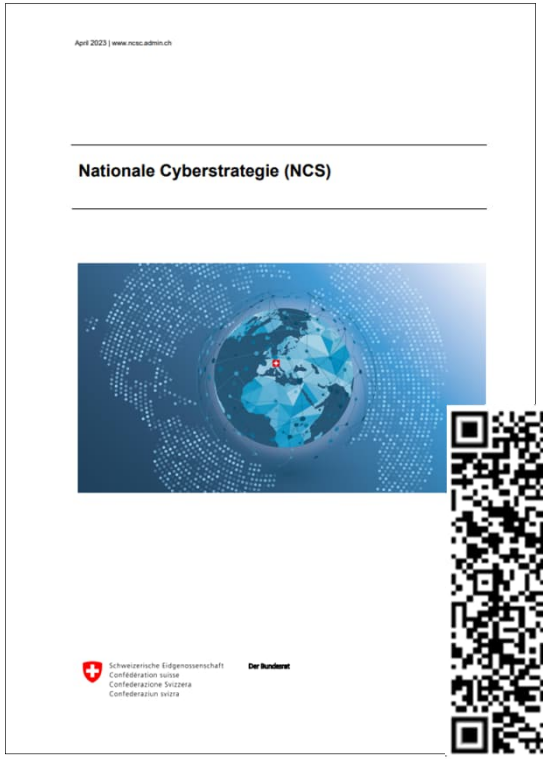
# Agenda

- Akteure und Bedrohungen aus dem Cyberraum
- Wie werden Cyberangriffe durchgeführt?
- Best Practice: Wie können Sie sich schützen?
- Fragen – was Sie schon immer mal fragen wollten!

Aber zuerst möchte ich mich und meine Funktion vorstellen….

KANTON
LUZERN

# Cyberkoordinator




**Download-Link:**


**Download-Link:**

KANTON
LUZERN

# Cyberkoordinator: Aufgaben


- Ansprechperson für alle Cyberbelange des Kantons
- Ist SPoC für die Bundesbehörden (z.B. NCSC, NDB, BABS)
- Vernetzung der Akteure (staatliche und private)
- Beurteilt/Erhöht das kantonale Sicherheitsdispositiv
  - 80 Gemeinden
  - ~ 60 Unternehmen und Institutionen
- Verfolgt die Cyber-Entwicklung auf strategischer Ebene

KANTON
LUZERN

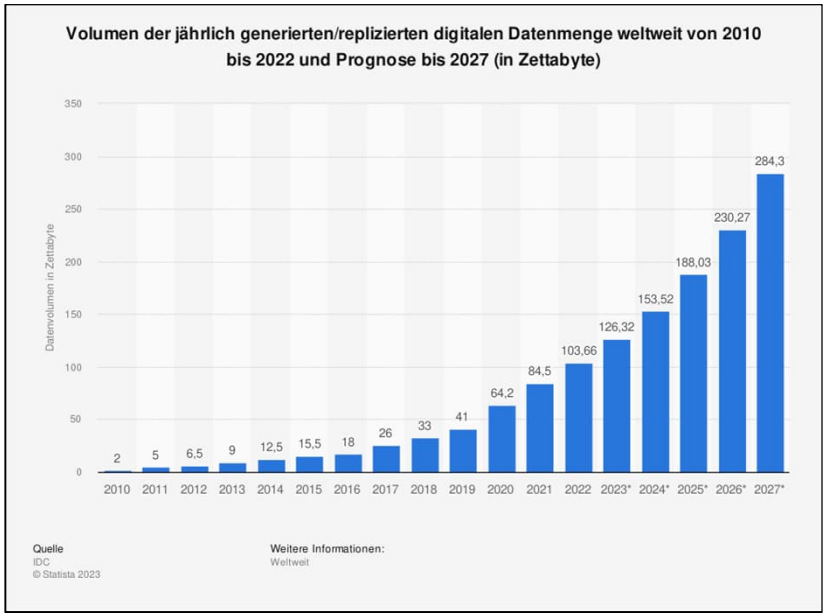
# 01 - Cyberbedrohung

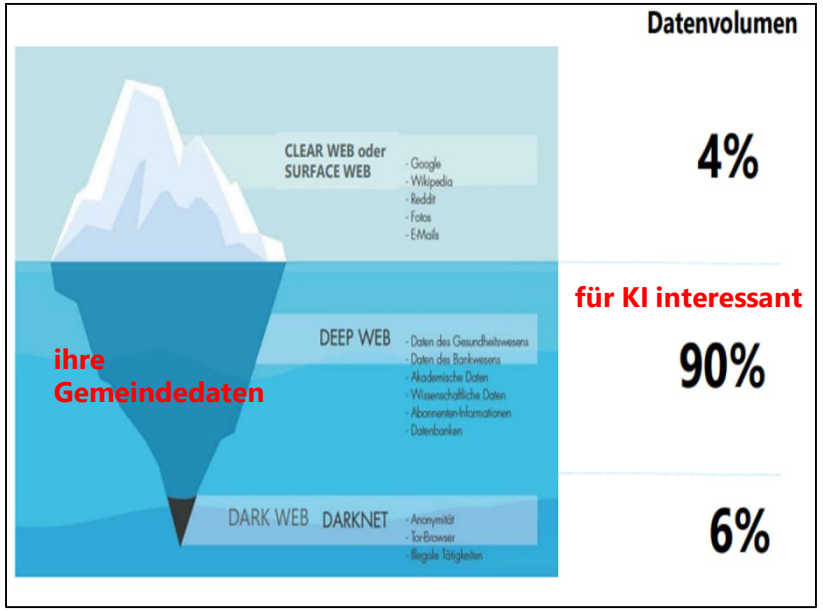
Welche Cyberakteure und Cyberbedrohungen gibt es?

KANTON
LUZERN

# Informationsgesellschaft

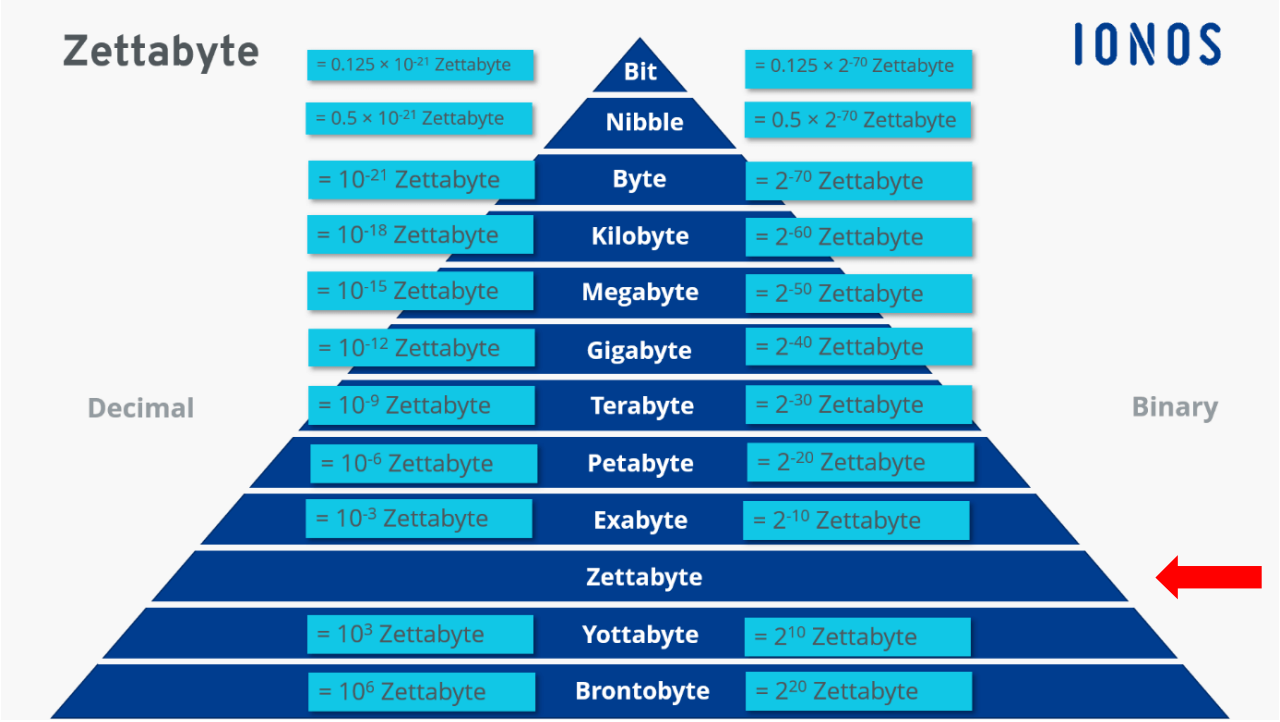
## Daten sind das neue Öl, Informationen das neue Gold



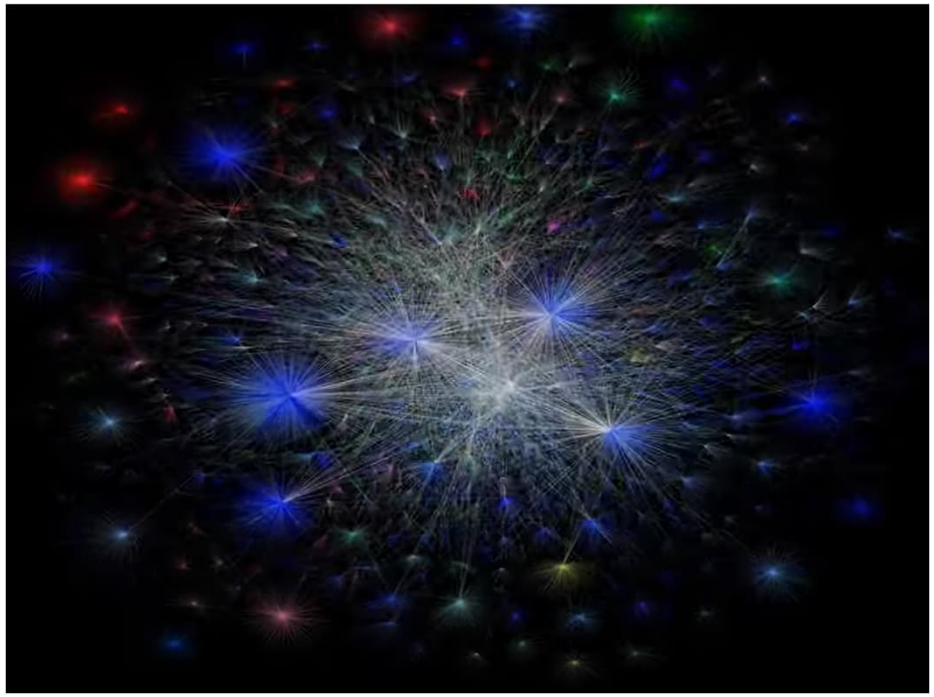
KANTON
LUZERN

# Zettabyte-Ära

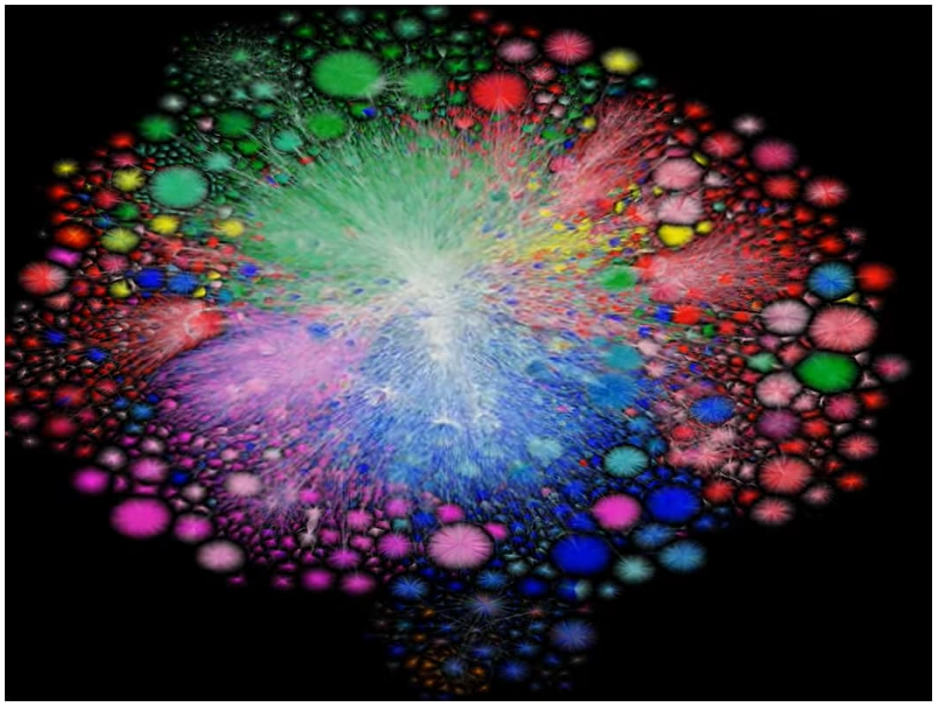


KANTON
LUZERN

# Wertschöpfungsraum «Internet»



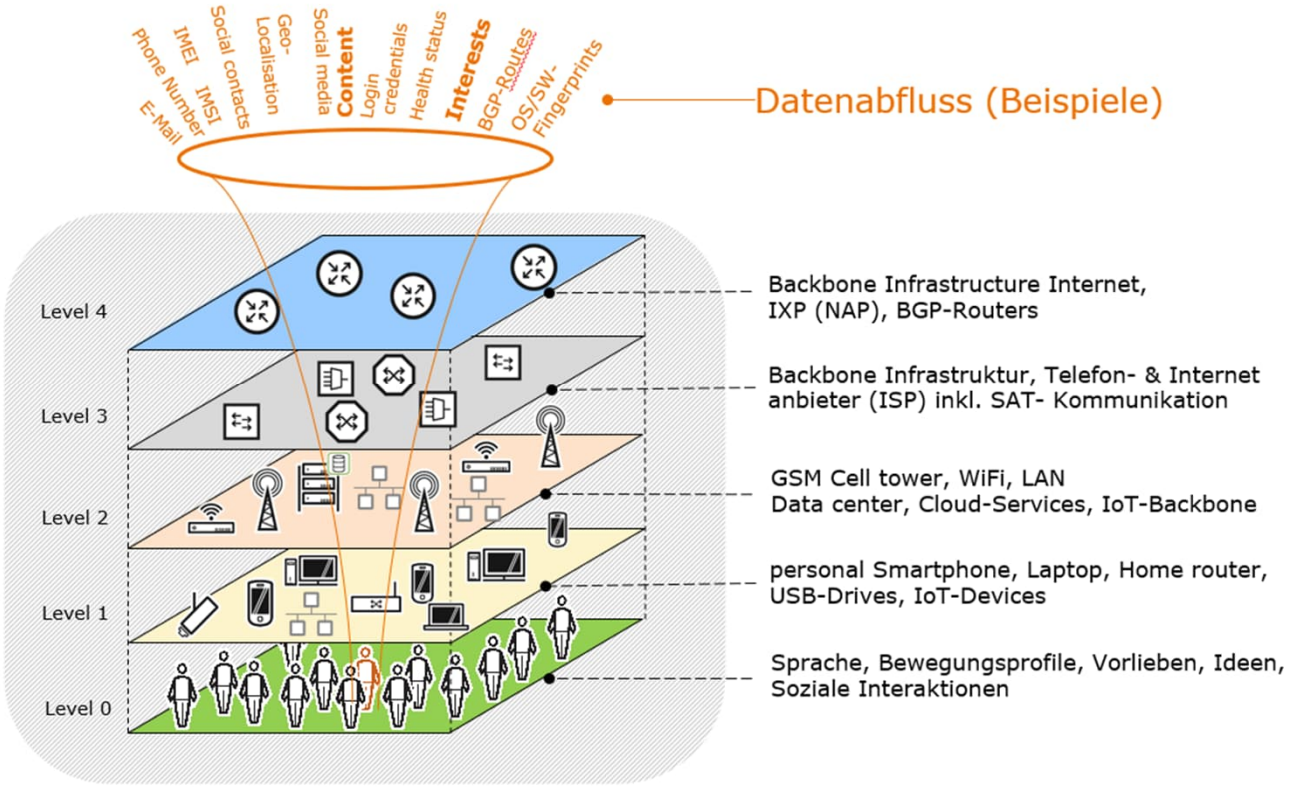
Internet 1997



Internet 2021

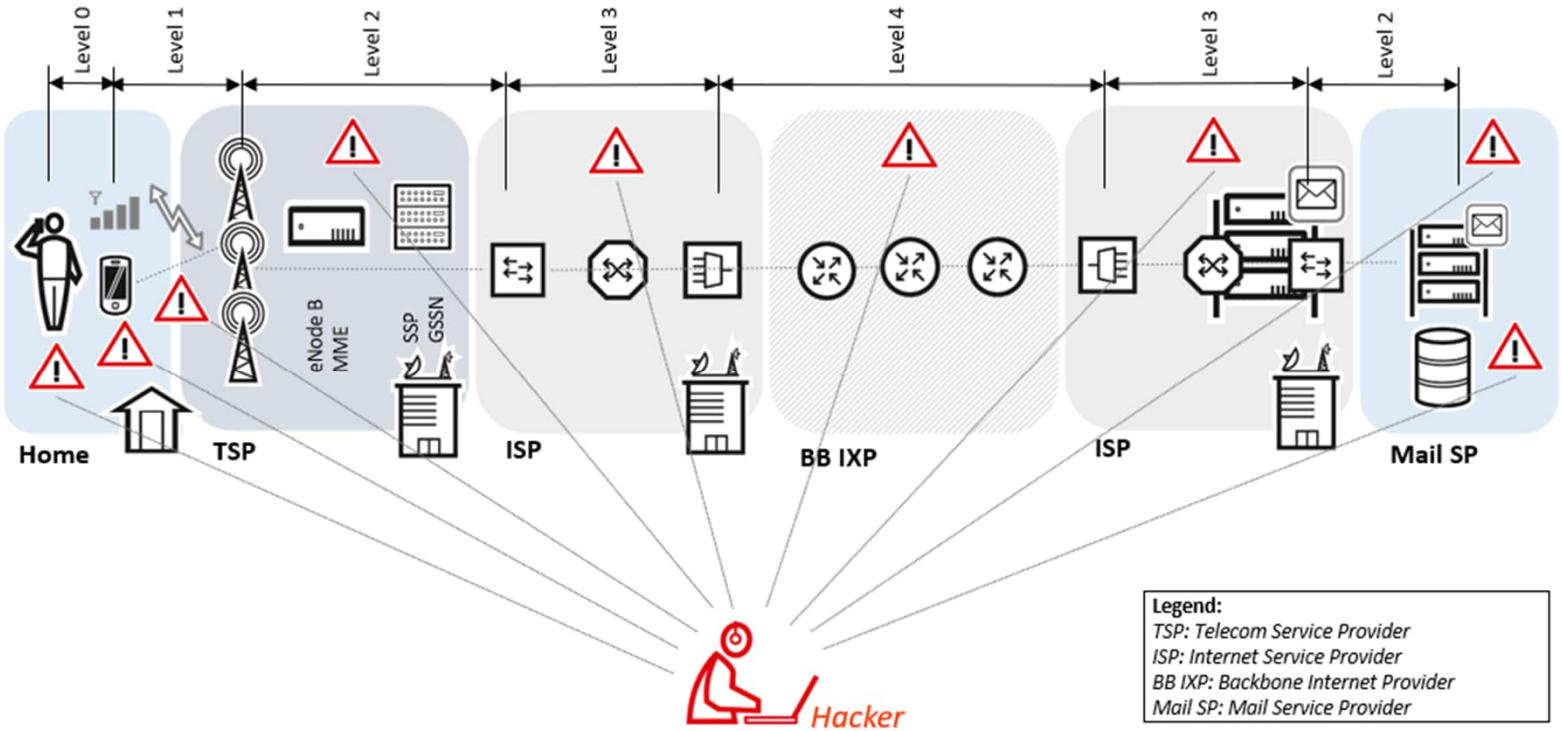
KANTON
LUZERN

# Angriffsflächen «Internet»



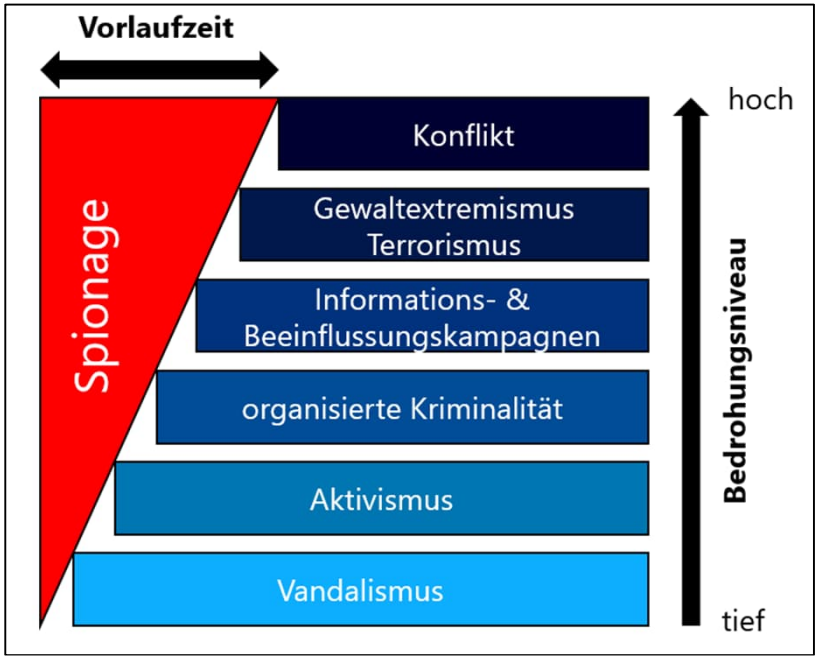
KANTON
LUZERN

# Beispiel: E-Mail versenden



KANTON
LUZERN

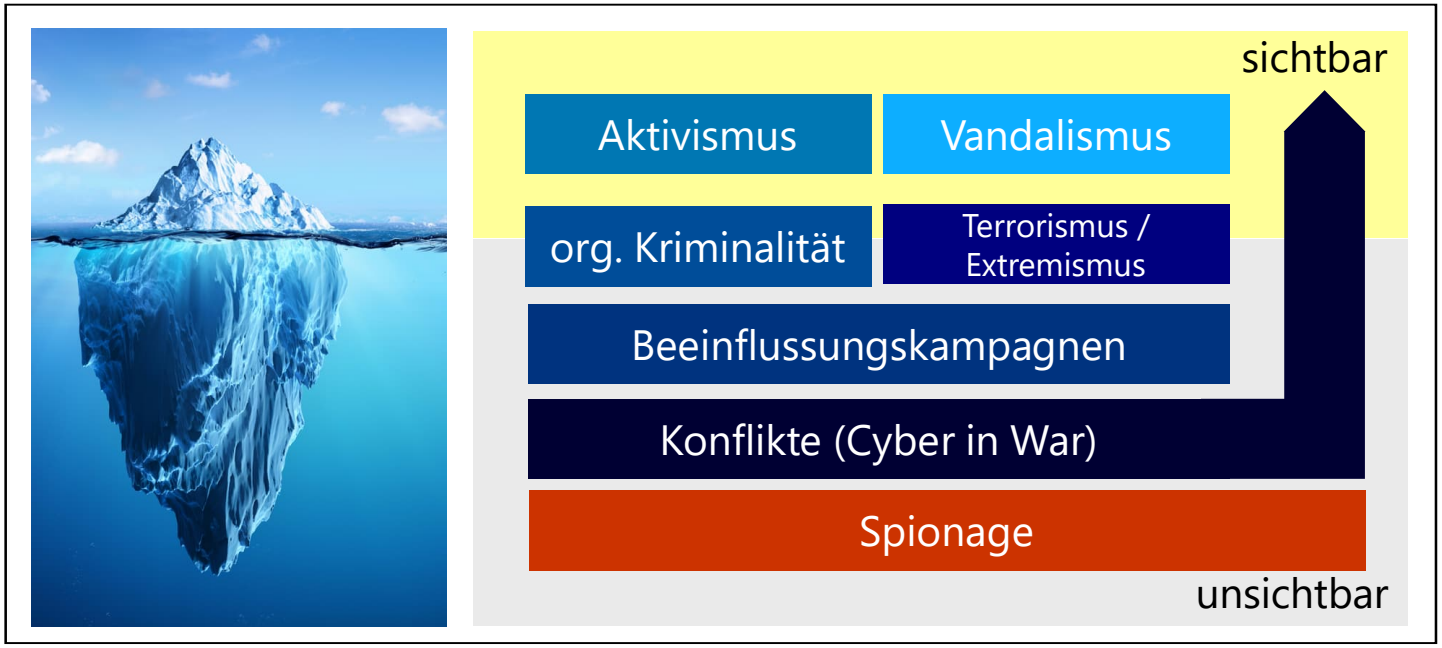
# Arten von Cyberbedrohungen




- Unterschiedliche Vorlaufzeiten für Vorbereitung bei Bedrohungsformen.
- Spionage ist omnipräsent und wird dauernd ausgeübt.

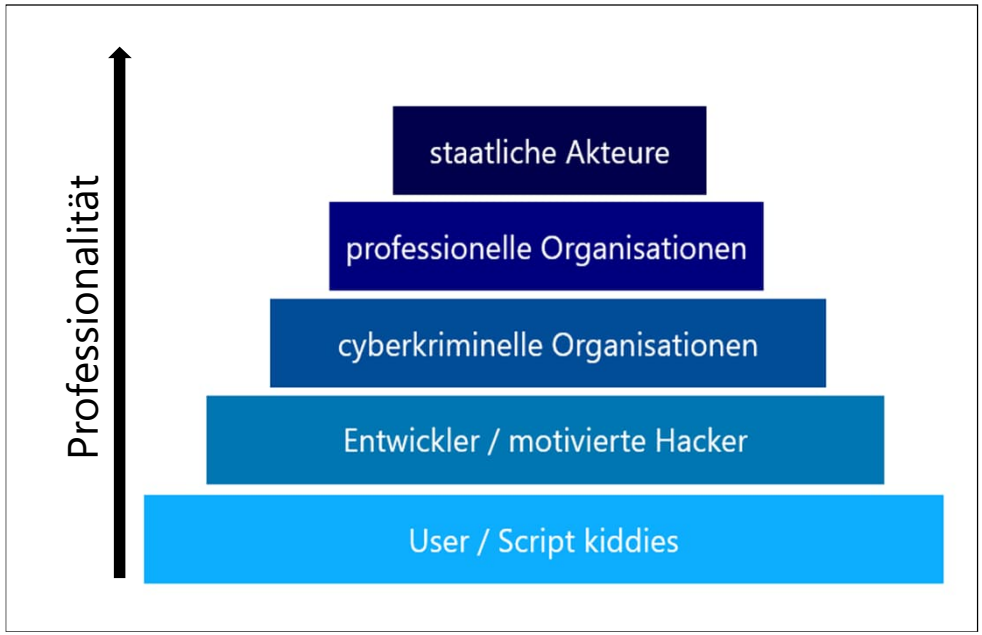
KANTON
LUZERN

# Herausforderung: Sichtbarkeit



KANTON
LUZERN

# Pyramide der Cyberakteure



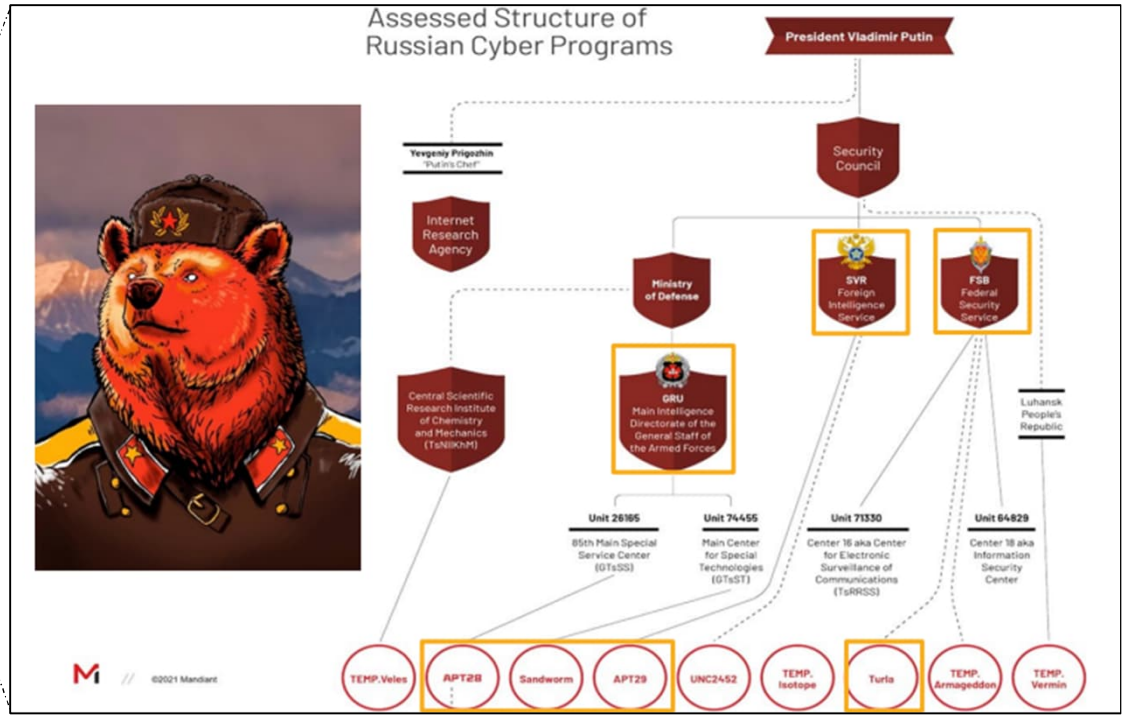

- Übergänge zwischen den Einteilungen sind fliessend
- Zusammenarbeit zwischen den Akteuren horizontal und vertikal
- Zuordnung nicht immer klar

KANTON
LUZERN

# Beispiel: Strukturen staatlicher Akteure

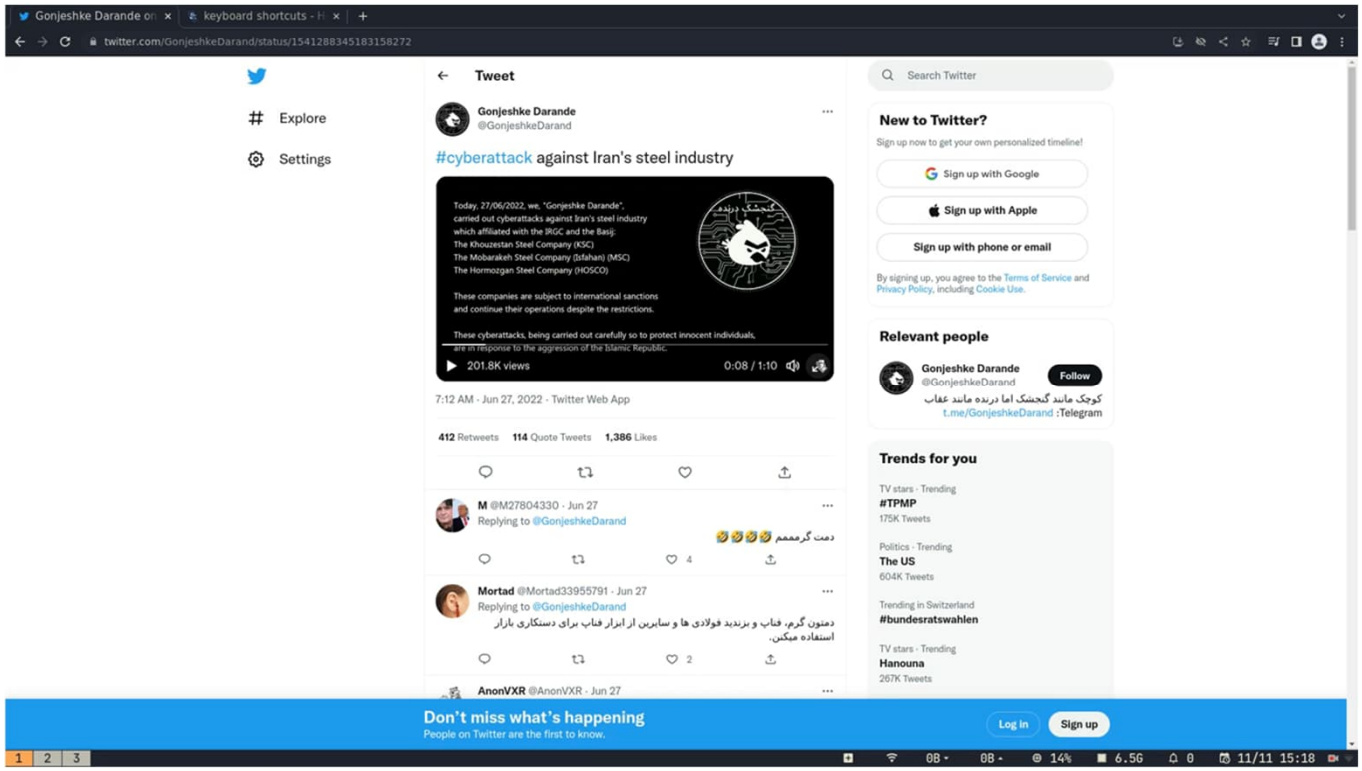
**oberer Teil der «Pyramide»**


involvierte Cyberakteure



KANTON
LUZERN

# Beispiel: Cyberangriff staatlicher Akteur



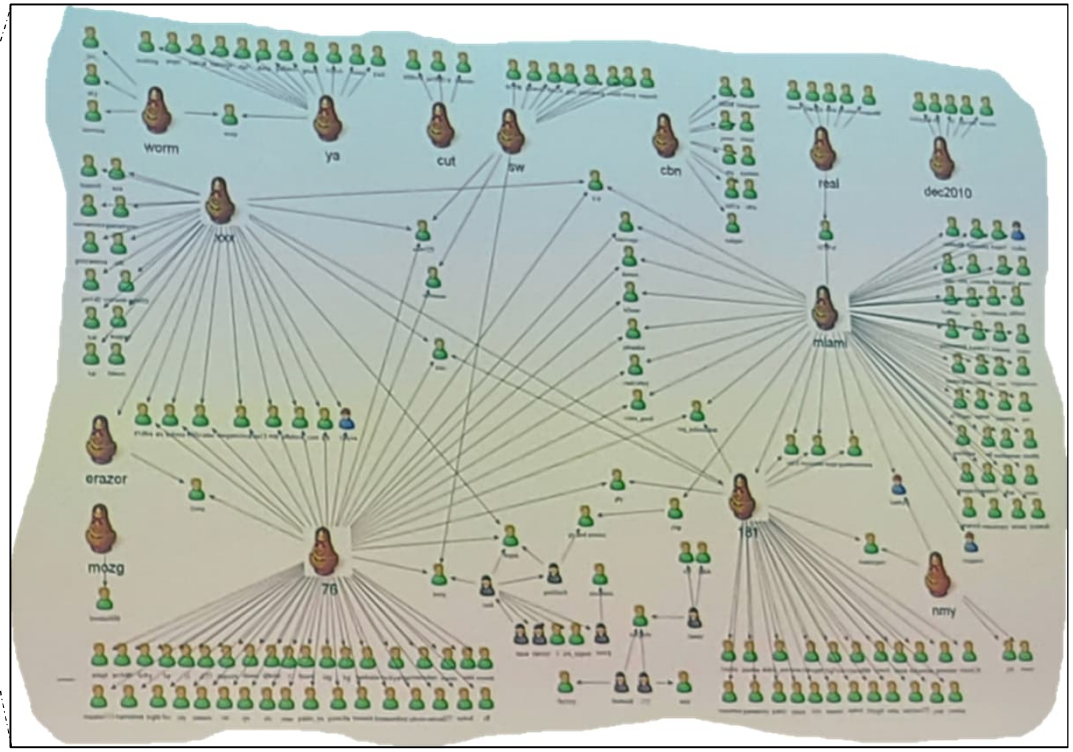

Angriff auf iranisches Stahlwerk (Juni 2022)

KANTON
LUZERN

# Beispiel: Strukturen cyberkrimineller Akteure

**unterer Teil der «Pyramide»**

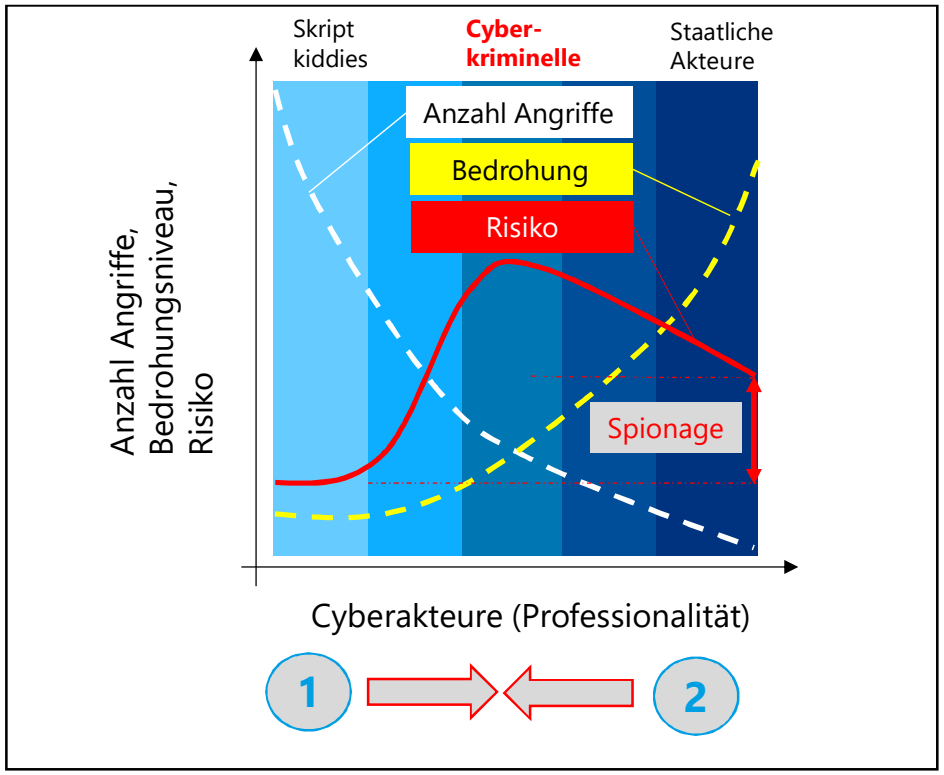

involvierte Cyberakteure




*Quelle: NCSC / EFD*

KANTON
LUZERN

# Risikobetrachtung




1. Monetäre Anreize ziehen immer mehr Softwareentwickler in cyberkriminelle Gruppierungen.
2. Immer mehr professionelle Tools sind Cyberkriminellen verfügbar.

**Für Unternehmen (KMU) und Gemeinden gehen von professionellen cyberkriminellen Organisationen die größte Gefahr aus!**

KANTON
LUZERN

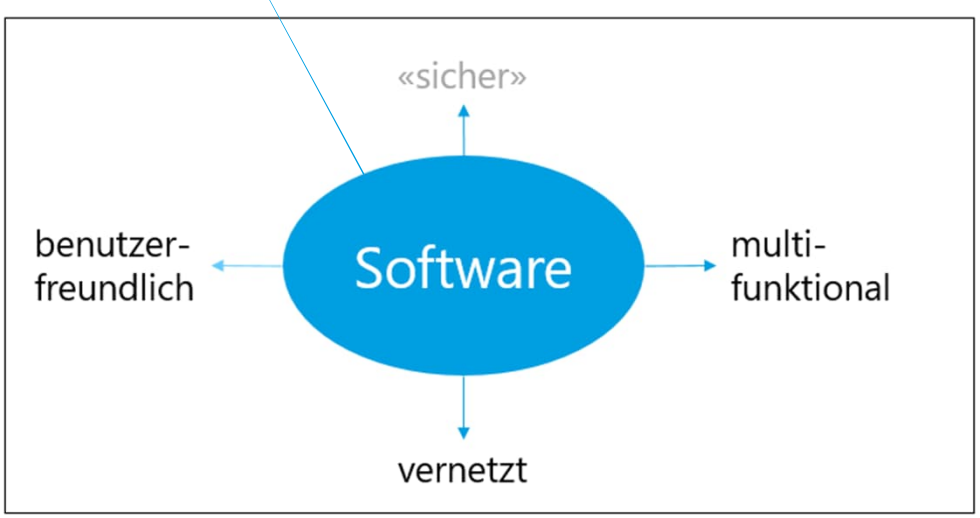
# 02 – Cyberangriff

Wie wird ein Cyberangriff durchgeführt?

KANTON
LUZERN

# Hauptauslöser: Anforderungen an Software

**«Eierlegendwollmilchsau»**

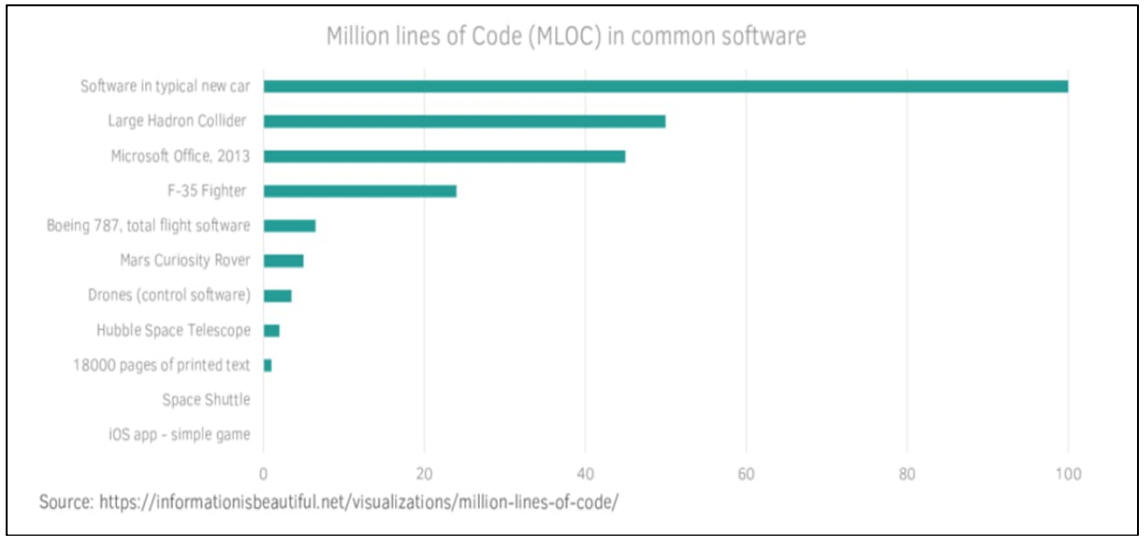



- Grössere Anzahl von Codezeilen
- Hohe Abhängigkeiten von anderen Softwarekomponenten
- Entwickler kennt «seine» Software nicht mehr vollständig

KANTON
LUZERN

# Übersicht: Anzahl Codezeilen

**Anzahl Programmcodezeilen**

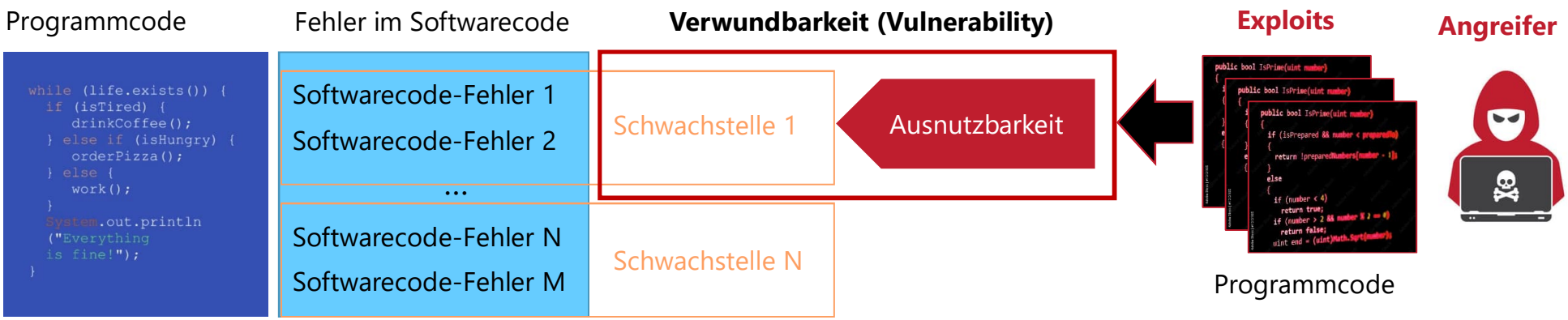



- 15 Fehler pro 1'000 Linien Softwarecode
- Behebung eines Softwarecode-Fehlers benötigt 30 mal länger als eine Linie Softwarecode zu schreiben.
- Behebung dadurch für Softwareunternehmen unattraktiv

**Aus Softwarecodefehler entstehen Schwachstellen!**

KANTON
LUZERN

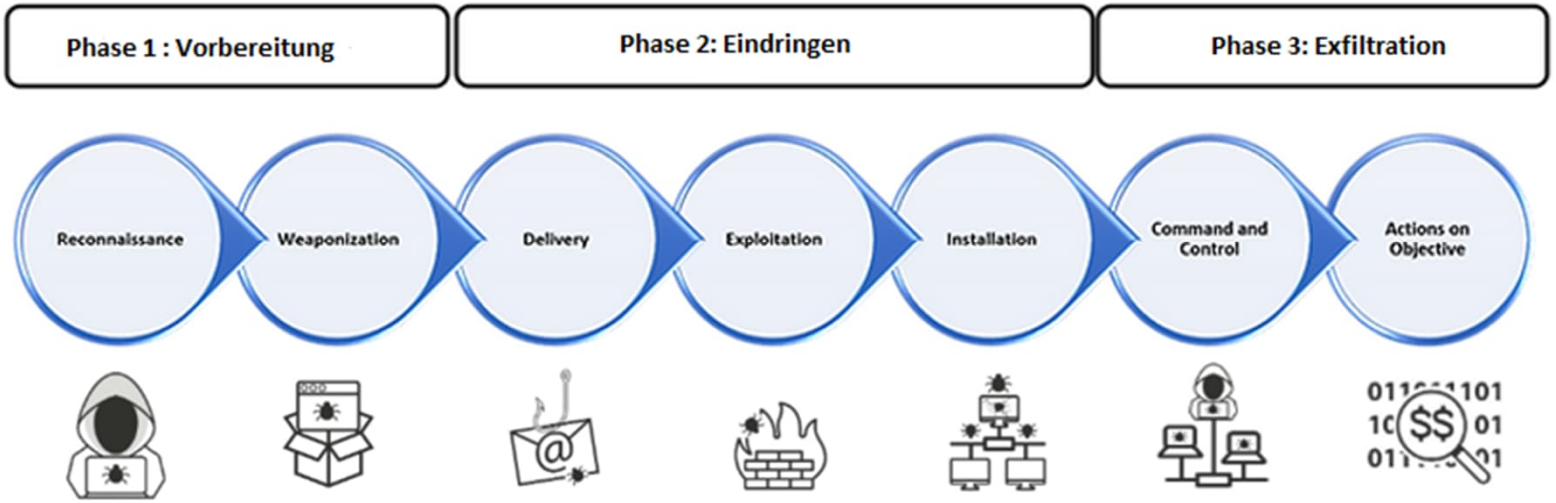
# Schwachstelle, Verwundbarkeit und Exploits




**Vulnerability**: Schwachstelle mit einer Ausnutzbarkeit
**Exploit**: Technik oder Programmcode der eine Verwundbarkeit ausnutzen kann

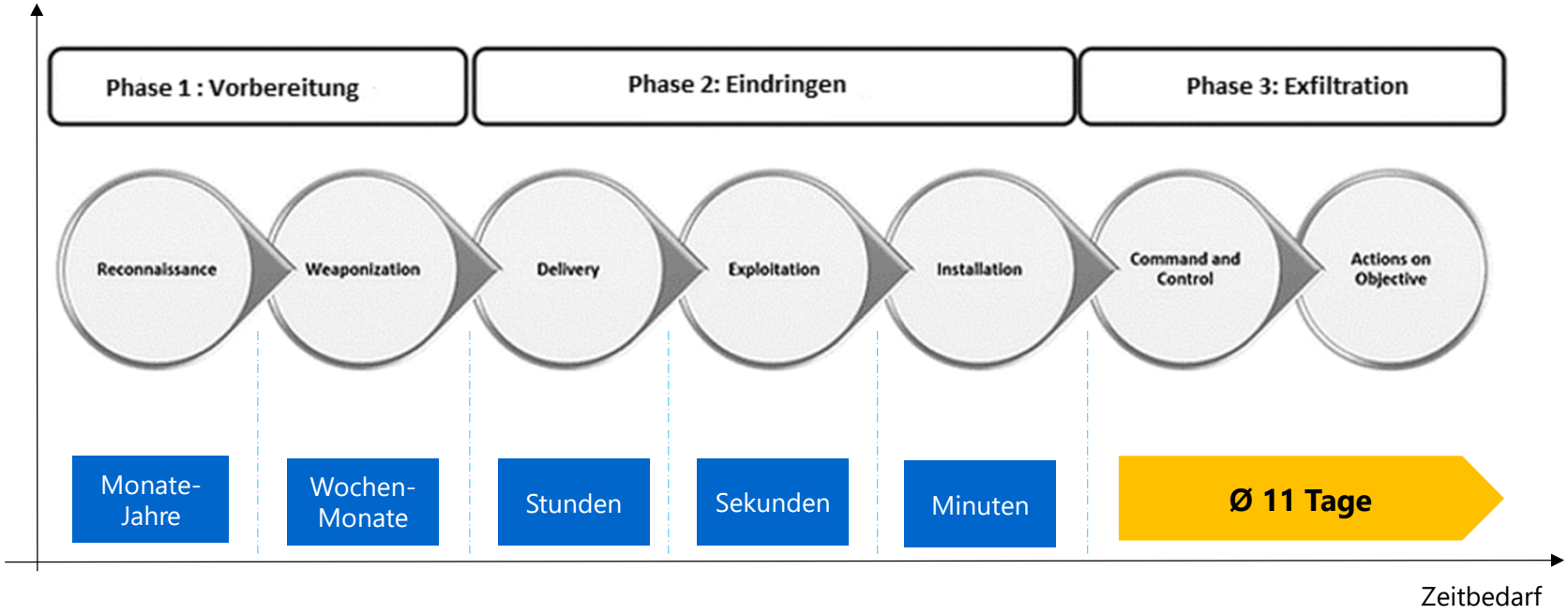
KANTON
LUZERN

# Ablauf eines Cyberangriffes



KANTON
LUZERN

# Cyberangriff: zeitliche Verhältnis



KANTON
LUZERN

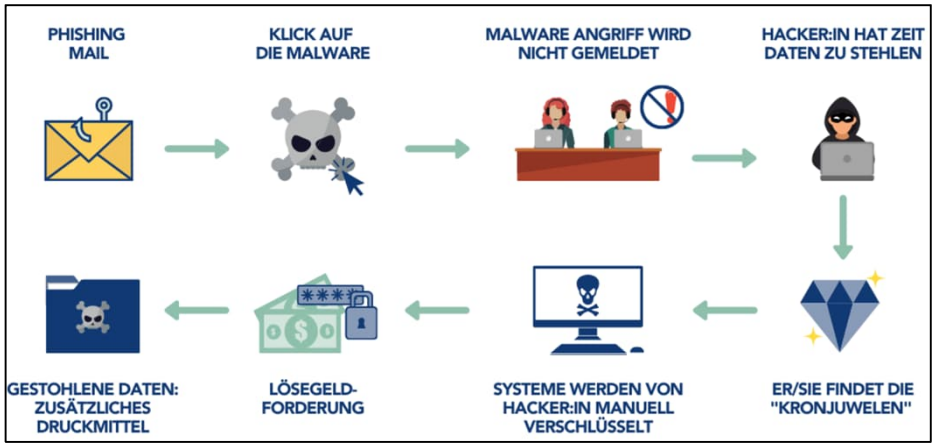
# Arten von Cyberangriffen


… die heute häufigsten Angriffe

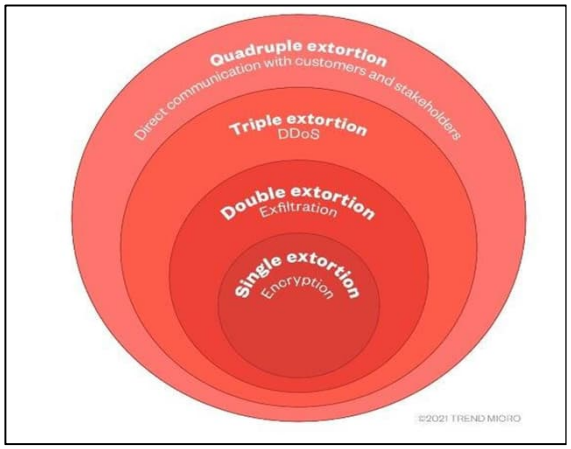
KANTON
LUZERN

# Beispiel: Ransomware

**typischer Ablauf (double extortion)**




**mögliche Ausprägungen:**




**Neu:** Einsatz von intermittierende Verschlüsselung

KANTON
LUZERN

# 03 - Schutzmassnahmen

Wie können Sie sich schützen?

KANTON
LUZERN

# Empfehlung 1:
## Sensibilisierung der Gemeindemitarbeitenden


- 46% der erfolgreichen Cyberangriffe sind infolge von Unachtsamkeit oder mangelnde Schulung der Mitarbeitenden möglich.
- Fehlendes Verständnis für die Gefahren und die Auswirkungen
- Melden Sie in jeden Fall Sicherheitsvorfälle ihrem IT-Administrator (Fehlerkultur)

KANTON
LUZERN

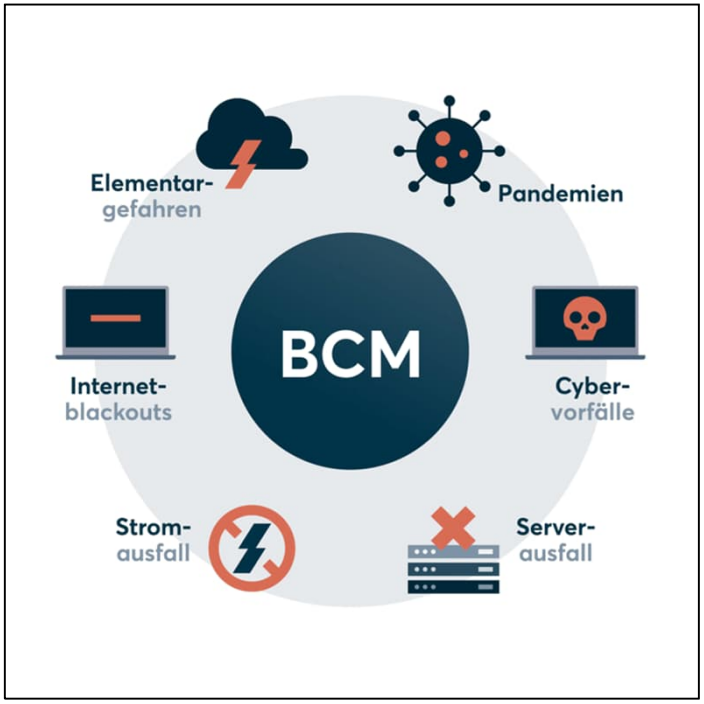
# Angebot Kanton: E-Learning KKJPD/SVS


Link: Swiss Government Training Portal (elearningcyber.ch)

- Das JSD wird das E-Learning KKJPD/SVS interessierten Gemeinden kostenlos zur Verfügung stellen: https://elearning.luzerner-gemeinden.ch
- Alle Gemeinden erhalten dazu ein Infoschreiben (ab dem 08.12.2023)
- Boarding der Gemeinde Mitarbeitenden ab Januar 2024 durch Cyberkoordinator
- Auswertung dezidiert für jede Gemeinde mit Plattform möglich

KANTON
LUZERN

# Empfehlung 2:
## Kennen der kritischen Prozesse (BCM)

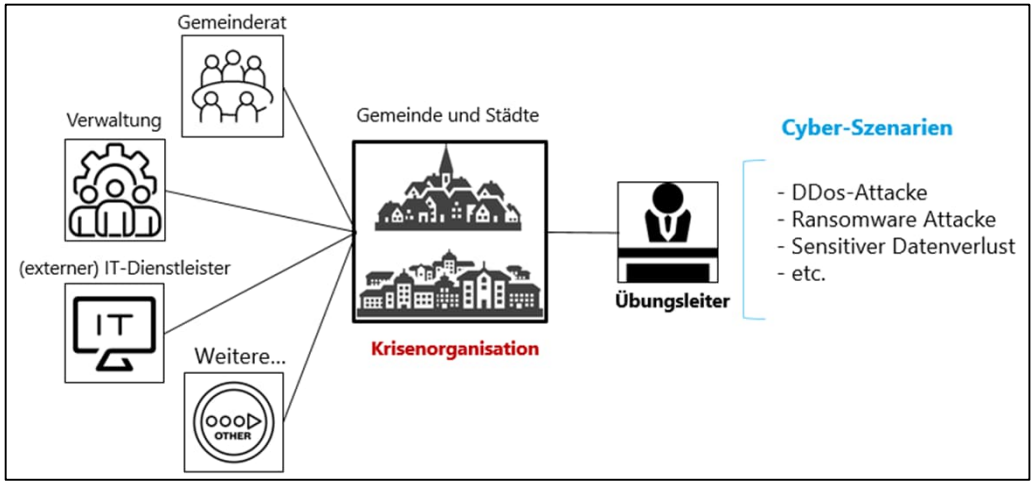



- Auswirkungen mannigfaltig
- Evaluieren Sie die kritischen Prozesse in ihrem Arbeitsumfeld
- Prüfen Sie die Abhängigkeit von der IT dieser kritischen Prozesse
- Definieren Sie Notbetriebsprozesse (ohne IT)
- Planen Sie die max. Ausfallzeit mit ihrem IT-Dienstleister

KANTON
LUZERN

# Empfehlung 3:
## Üben von Cybervorfällen in der Krisenorganisation

**Table Top Excercise (TTX)**




**Mehrwert:**

- Notfallpläne optimieren
- Zusammenarbeit stärken
- Schwachstellen erkennen
- Wirksamkeit erhöhen
- Rollen / Verantwortlichkeiten
- Train as you fight

KANTON
LUZERN

# Empfehlung 4:
# Passwortsicherheit

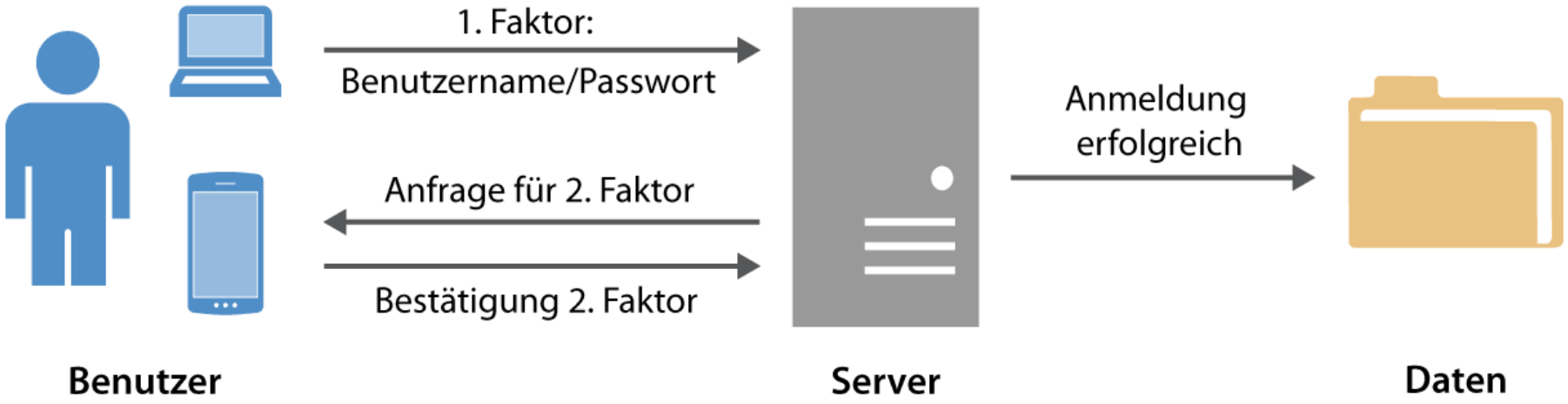
**Übersicht Passwortmanager**


- Verwenden Sie komplexe Passwörter (min. 8 besser 12 Zeichen)
- *Beispiel:*
  **I**mmer **a**m **M**ontag **u**m **8** **U**hr **t**reffe **i**ch **m**ich **m**it **C**ybie **a**uf **e**ine n **K**affee **– d**azu **g**ibt **e**s **1** **G**ipfeli

  Passwort: **IaMu8UtimmCaeK–dge1G**
- Verwenden Sie niemals gleiche Passwörter für unterschiedliche Dienste
- Wechseln Sie Passwörter regelmässig (max. 90 Tage)
- **Einsatz von Passwortmanager für sichere Aufbewahrung**
- **Evaluieren Sie ein gutes und sicheres Produkt für Ihre Gemeinde**

KANTON
LUZERN

# Empfehlung 5:
## Einsatz von zweiten Faktor für Anmeldung (2FA)

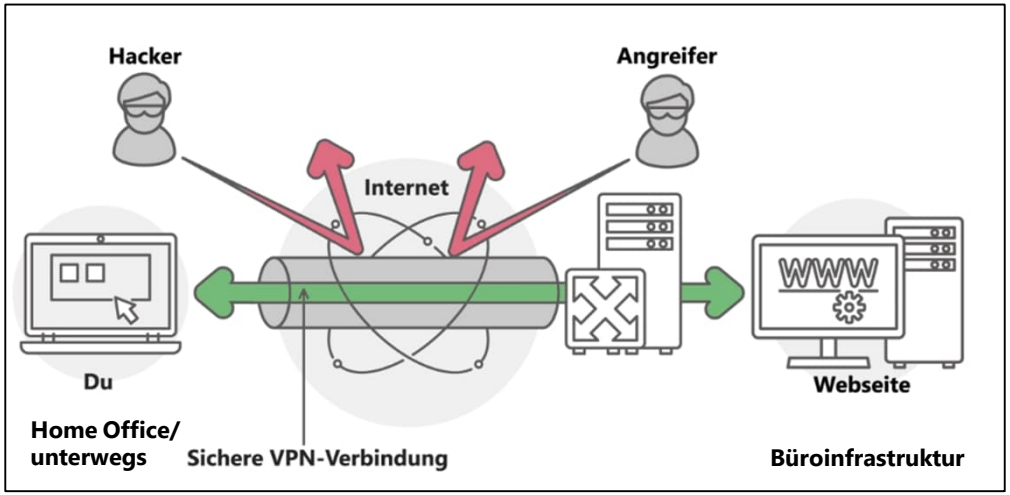



**Wenn immer möglichen setzen Sie diesen zweiten Faktor ein!**

KANTON
LUZERN

# Empfehlung 6:
## Einsatz von VPN im Home Office, aktuelle Systeme

**Einsatz von VPN**




- Halten Sie ihre Endgeräte-, Serverbetriebssysteme und Antivirenprogramme aktuell
- Home Office: Greifen Sie ausschliesslich über eine geschützte Verbindung (VPN) auf ihre Bürodaten zu
- Home Office: Surfen Sie nie direkt mit ihrem Bürogerät im Internet

KANTON
**LUZERN**

Justiz und Sicherheitsdepartemente
**Departementssekretariat**
Bahnhofstrasse 15
6002 Luzern

*Vielen Dank!*