

# KMU Day Langnau 2023

## AXA Versicherungen AG

Yves Kraft | Langnau, 7. Juni 2023

# Yves Kraft

Branch Manager Bern

Head of Security Academy



Der mathematische Nachweis, wann ein Angriff auf eine Anwendung durchgeführt wird (Clark + Davis 1995):

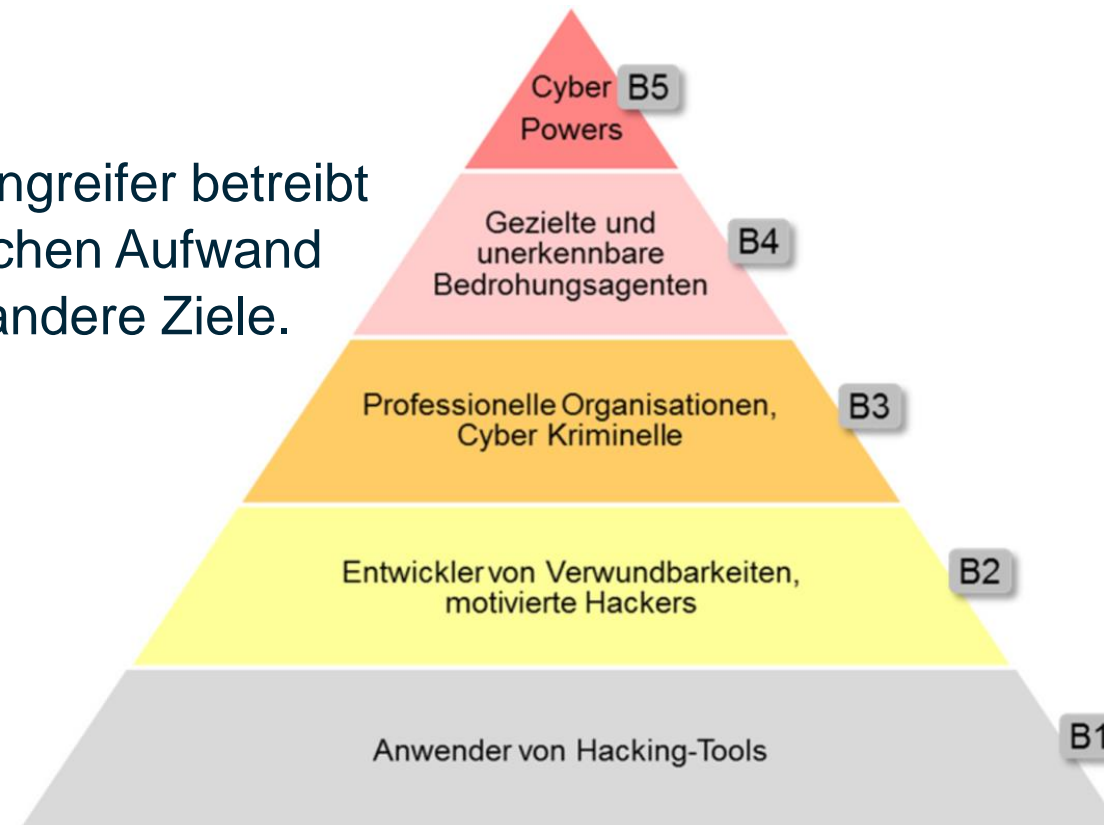
$$M_b + P_b > C_{cp} + C_{cm}P_aP_c$$

|          |                                       |
|----------|---------------------------------------|
| $M_b$    | Finanzieller Gewinn                   |
| $P_b$    | Psychologischer Gewinn                |
| $C_{cp}$ | Kosten für den Angriff                |
| $C_{cm}$ | Kosten für das Erwischen              |
| $P_a$    | Wahrscheinlichkeit für das Erwischen  |
| $P_c$    | Wahrscheinlichkeit einer Verurteilung |



Um eine wirkungsvolle Verteidigung aufzubauen, ist es notwendig zu wissen, wer der Angreifer ist.

Denn jeder Angreifer betreibt unterschiedlichen Aufwand und verfolgt andere Ziele.



Alle Arten von Angriffen haben immer Auswirkung auf mindestens einen der drei Grundwerte der IT-Sicherheit.

- ▶ Vertraulichkeit (CONFIDENTIALITY)
- ▶ Integrität (INTEGRITY)
- ▶ Verfügbarkeit (AVAILABILITY)

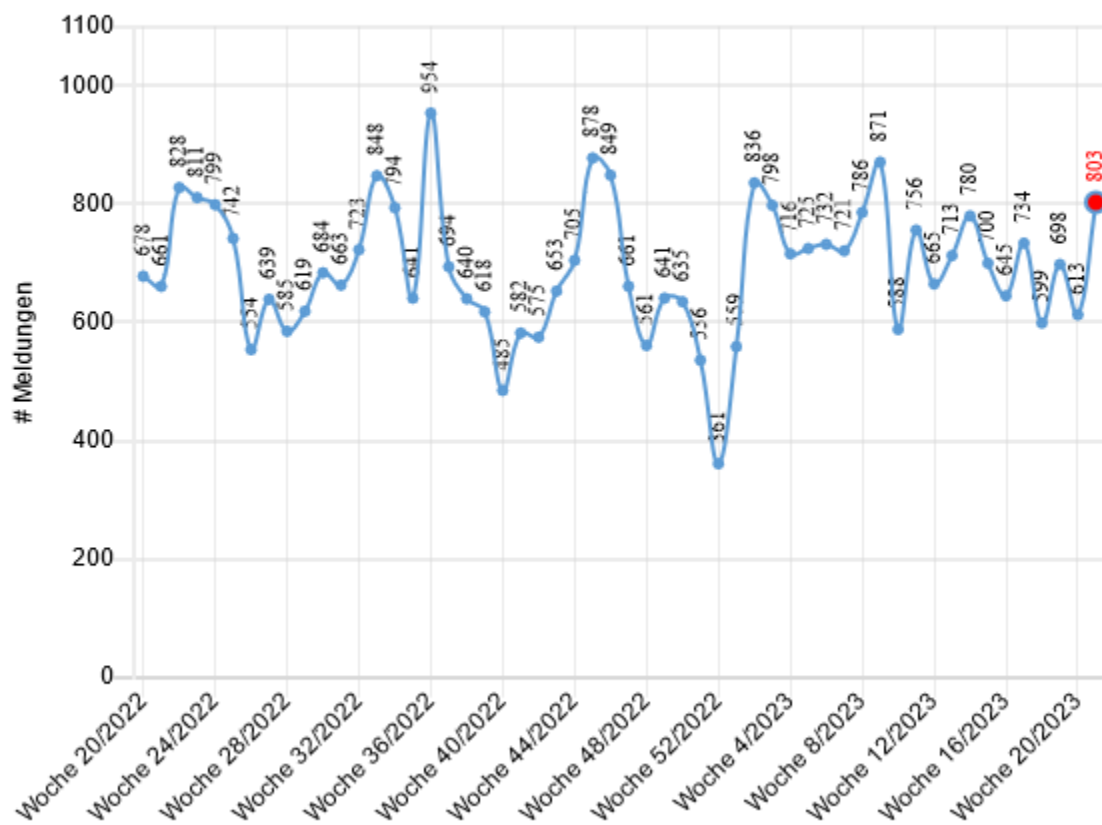


Weitere Schutzziele

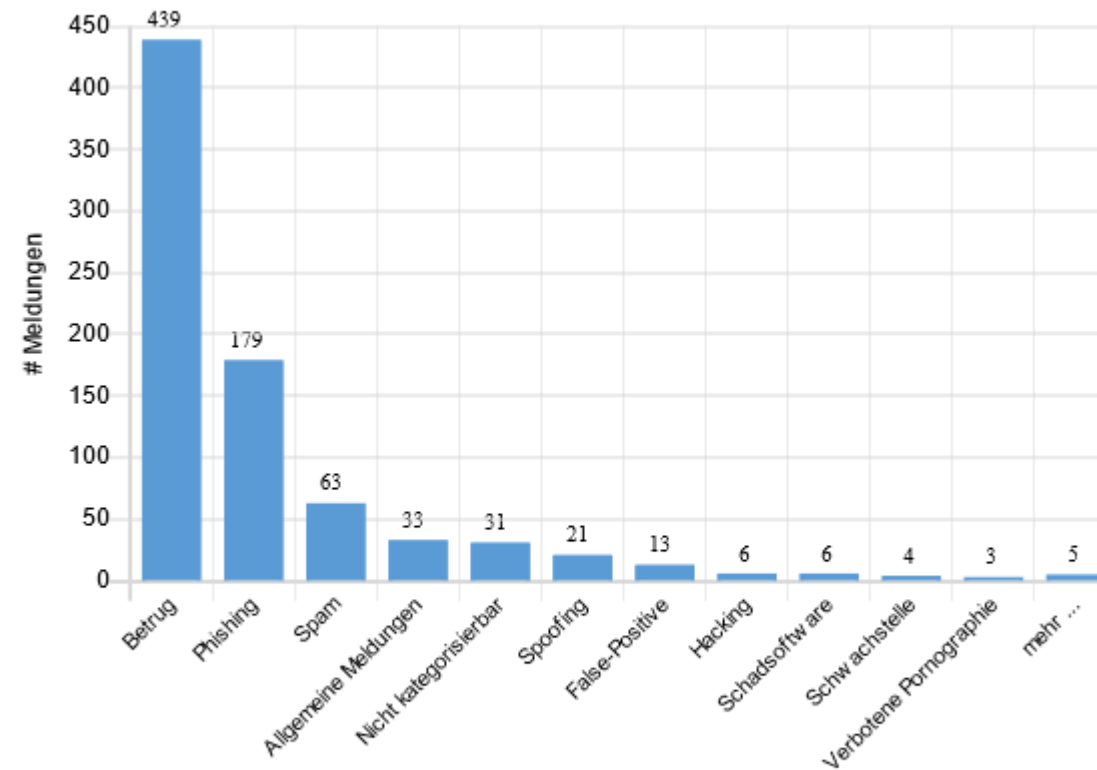
- ▶ Authentizität (AUTHENTICITY)
- ▶ Verbindlichkeit/Nichtabstreitbarkeit (NON REPUDIATION)
- ▶ Zurechenbarkeit (ACCOUNTABILITY)

# Aktuelle Beispiele (National)

Grafik 1 - NCSC.ch: Meldeeingang



Grafik 2 - NCSC.ch: Meldeeingang nach Hauptkategorien: Woche 21/2023



Total 803 Meldungen in der Woche 21/2023





# APT-Lifecycle

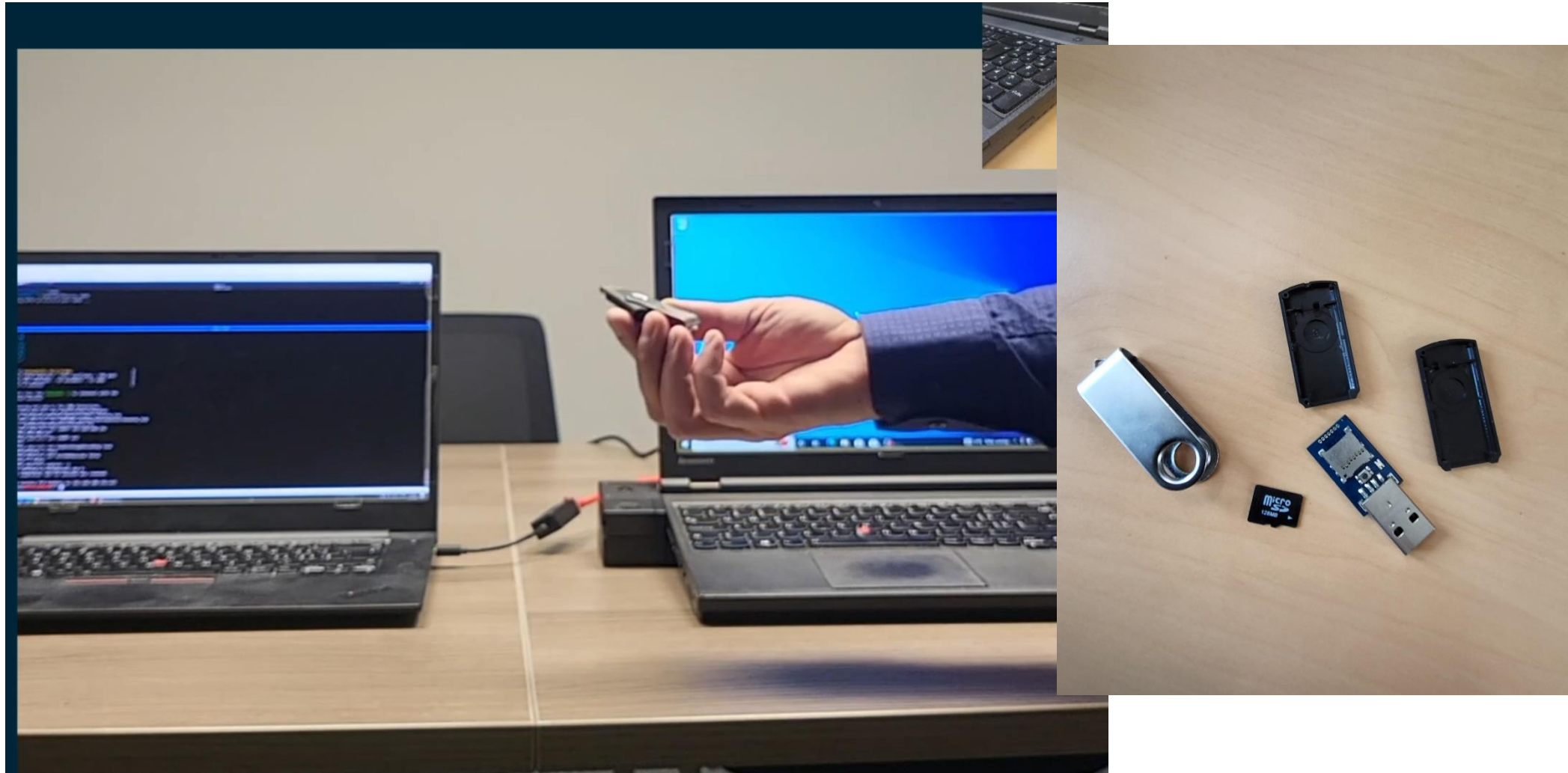




1. Kompromittierung
2. Diebstahl sensibler Daten
3. Daten verschlüsseln (1. Erpressung)
4. Mit Veröffentlichung der Daten drohen (2. Erpressung)
5. Öffentlich an den Pranger stellen
6. Optional: Androhung von Distributed-Denial-of-Service-Angriffen (3. Erpressung)
7. Optional: Kunden/Nutzer/Mitarbeiter drohen (4. Erpressung)
8. Optional: Business Email Compromise (BEC), Phishing etc.
9. Optional: Veröffentlichung gestohlener Daten



# Live Hacking Demo – BadUSB



# Aktuelle Beispiele aus dem Darknet CH Media (NZZ), Waadt, Kanton Basel, etc.

## CH Media

Switzerland  
chmedia.ch nzz.ch vsdruck.ch azmedien.ch  
views: 3764  
amount of data: ??? gb  
added: 2023-04-08  
publication date: 2023-05-03

information: CH Media is a Swiss media company which was founded in 2018 as a joint venture of the AZ Medien and the NZZ Media Group.

comment: Private and personal confidential data, projects, payroll, employee information and etc.

PLAY

5 DAYS BEFORE PUBLICATION

## BianLian

Home Companies Tags Contacts

### # Department of Education of the Canton of Basel-Stadt

<https://ed.bs.ch>

The Department of Education is the largest of the seven departments of the canton of Basel-Stadt. It employs around 7000 people in over 200 professions and has a budget of around one billion francs.

Deputy Head of Universities:

Business Email: [redacted]  
Business Phone: [redacted]

Head of elementary schools:

Business Email: [redacted]  
Personal Email: [redacted]

Security Incident Manager:

Business Email: [redacted]  
Business Phone: [redacted]

Revenue: \$170 Millions

Data Volume: 1.2 TB

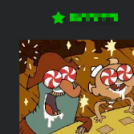
#### Data description:

- \* HR.
- \* Finance.
- \* Accounting.
- \* Financial data.
- \* Various students' and employees' personal data.

[ed.bs.ch\\_1.zip](#) [ed.bs.ch\\_2.zip](#) [ed.bs.ch\\_3.zip](#) [ed.bs.ch\\_4.zip](#) [ed.bs.ch\\_5.zip](#) [ed.bs.ch\\_6.zip](#) [ed.bs.ch\\_7.zip](#) [ed.bs.ch\\_8.zip](#) [ed.bs.ch\\_9.zip](#) [ed.bs.ch\\_10.zip](#) [ed.bs.ch\\_11.zip](#) [ed.bs.ch\\_12.zip](#) [ed.bs.ch\\_13.zip](#) [ed.bs.ch\\_14.zip](#) [ed.bs.ch\\_15.zip](#)

## Chuv.ch - Switzerland - CHUV Vaud University Hospital Center

by [redacted] - Tuesday January 24, 2023 at 02:40 PM



V.I.P User

VIP

Posts: 7  
Threads: 6  
Joined: Mar 2022  
Reputation: 1

4 hours ago (This post was last modified: 4 hours ago by [redacted])

+2M - No Password

```
"identifiant_pp": "10005267843", "prenom_dexercice": "M", "nom_dexercice": "M", "code_civilite": "M", "code_civilite_dexercice": "M", "code_profession": "70", "1
...
https://t.me/[redacted]
```

< Next Oldest | Next Newest >

## Index of /ch/

| File Name                           | Date        | Time  | Size      |
|-------------------------------------|-------------|-------|-----------|
| <a href="#">CHM.part.part01.rar</a> | 24-Apr-2023 | 19:03 | 524288000 |
| <a href="#">CHM.part.part02.rar</a> | 24-Apr-2023 | 19:04 | 524288000 |
| <a href="#">CHM.part.part03.rar</a> | 24-Apr-2023 | 19:05 | 524288000 |
| <a href="#">CHM.part.part04.rar</a> | 24-Apr-2023 | 19:06 | 524288000 |
| <a href="#">CHM.part.part05.rar</a> | 24-Apr-2023 | 19:06 | 266731654 |

# Aktuelle Beispiele aus dem Darknet Supply Chain Angriff auf Fedpol

CYBERANGRIFF Publiziert 3. Juni 2023, 12:35

## Daten des Fedpol im Darknet veröffentlicht

Hacker haben Server angegriffen, die Daten des Fedpol und des Bundesamts für Polizei beherbergen.



1/2

BZ SCHWEIZ 1 Monat gratis lesen Login Menü

Abstimmungen Bundeshaus

Startseite | Schweiz | Cyberangriff in der Schweiz: Hacker veröffentlichten Daten des Fedpol im Darknet

Cyberkriminalität in der Schweiz

### Hacker veröffentlichten Daten des Fedpol im Darknet

Bei einem Cyberangriff wurden Server attackiert, die Daten des Fedpol und des Bundesamts für Polizei beherbergen. Die Behörden bestätigen die Veröffentlichung der Daten.

Publiziert: 03.06.2023, 12:35



Die Bundesstinnen Karin Keller Sutter (l.) und Viola Amherd besuchen die Alarmzentrale des Bundesamt für Polizei (Fedpol). (Archivbild)  
Foto: Peter Schneider (Keystone)

Hacker haben Daten vom Bundesamt für Polizei (Fedpol) und dem Bundesamt für Zoll und Grenzsicherheit (BAZG) im Darknet veröffentlicht. Sie nutzten eine Schwachstelle auf den Servern der deutschsprachigen Firma aus, die diese Daten beherbergte.

xplain

xplain

#### Anwendungsbereiche

- Polizei
- Migrations-, Arbeits- und Wirtschaftsämter
- Vollzugsbehörden und Bewährungshilfe
- Staats- und Jugendanwaltschaften
- Grenzverwaltung
- Gerichte
- Private & weitere Sicherheitsdienste

#### Xplain

Switzerland  
www.xplain.ch  
views: 2239  
amount of data: ??? gb  
added: 2023-05-23  
publication date: 2023-06-01

information: Xplain AG is a company that operates in the Consumer Services industry.

comment: Private and personal confidential data, finance, taxes, clients private information. For now partially published compressed 5gb. If there no reaction full dump will be uploaded.

## Index of /xp/

|                     |             |
|---------------------|-------------|
| XPL part.part01.rar | 29-May-2023 |
| XPL part.part02.rar | 29-May-2023 |
| XPL part.part03.rar | 29-May-2023 |
| XPL part.part04.rar | 29-May-2023 |
| XPL part.part05.rar | 29-May-2023 |
| XPL part.part06.rar | 29-May-2023 |

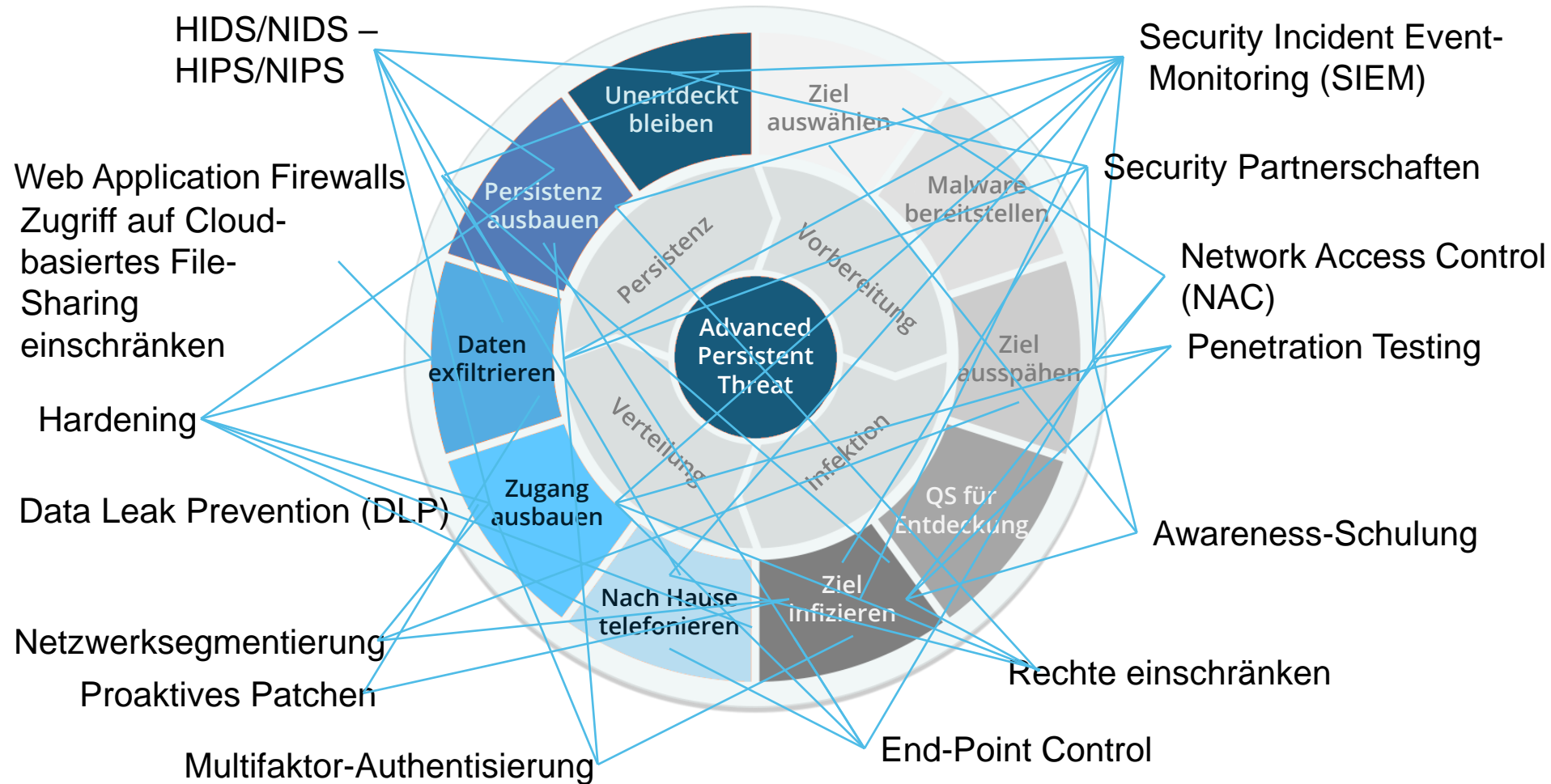


# Backup, Backup, Backup!

- ▶ Prozess für die regelmässige Datensicherung (Backup) definieren
- ▶ Einhaltung konsequent durchsetzen
- ▶ Datensicherung und weitere technische Massnahmen können auch an eine spezialisierte IT-Dienstleistungsfirma ausgelagert werden
- ▶ Datensicherung regelmässig auf ihre Funktionsfähigkeit überprüfen!
- ▶ Von Zeit zu Zeit das Einspielen von Backups üben
- ▶ Sicherungskopie sollte offline gespeichert werden
- ▶ Ältere Backups immer über einen bestimmten Zeitraum aufbewahren



# Wirkung im APT-Lifecycle



## Holding

---

**Oneconsult International AG**  
Giesshübelstrasse 45  
8045 Zürich  
Schweiz

+41 43 377 22 22  
info@oneconsult.com

## Schweiz

---

**Oneconsult AG**  
Giesshübelstrasse 45  
8045 Zürich  
Schweiz

+41 43 377 22 22  
info@oneconsult.com

**Oneconsult AG**  
Aarberggasse 56  
3011 Bern  
Schweiz

+41 31 327 15 15  
info@oneconsult.com

## Deutschland

---

**Oneconsult Deutschland AG**  
Agnes-Pockels-Bogen 1  
80992 München  
Deutschland

+49 89 248820 600  
info@oneconsult.com

## Neuseeland

---

**Oneconsult New Zealand Limited**  
Level 3, 33-45 Hurstmere Road  
Takapuna, Auckland 0622  
New Zealand

+64 27 325 4299  
info@oneconsult.com

