oneconsult
together against cyberattacks

KMU Day Langnau 2023
AXA Versicherungen AG

Yves Kraft | Langnau, 7. Juni 2023

Yves Kraft

Branch Manager Bern

Head of Security Academy

Mathematische Basis

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

$$M_b + P_b > C_{cp} + C_{cm} P_a P_c$$

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

Know Your Enemy

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

Denn jeder Angreifer betreibt unterschiedlichen Aufwand und verfolgt andere Ziele.

CIA-Prinzip

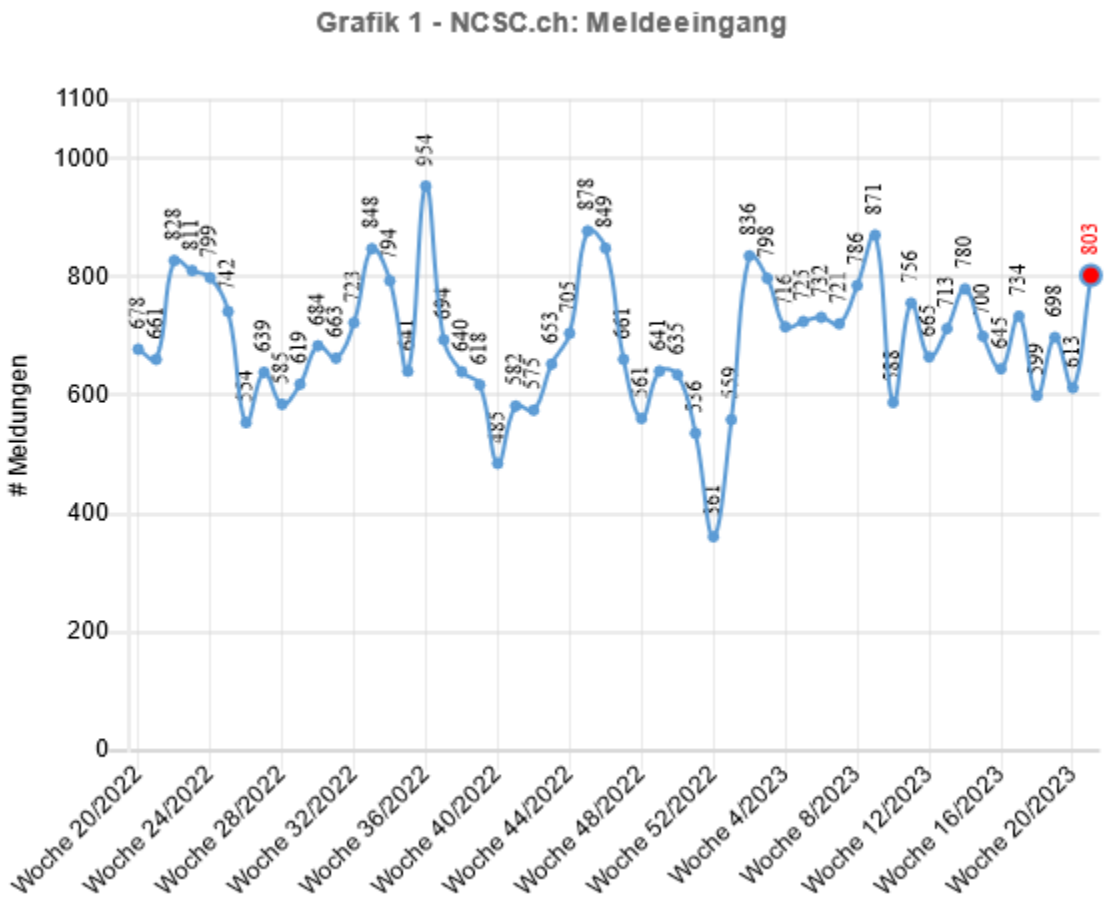
Alle Arten von Angriffen haben immer Auswirkung auf mindestens einen der drei Grundwerte der IT-Sicherheit.

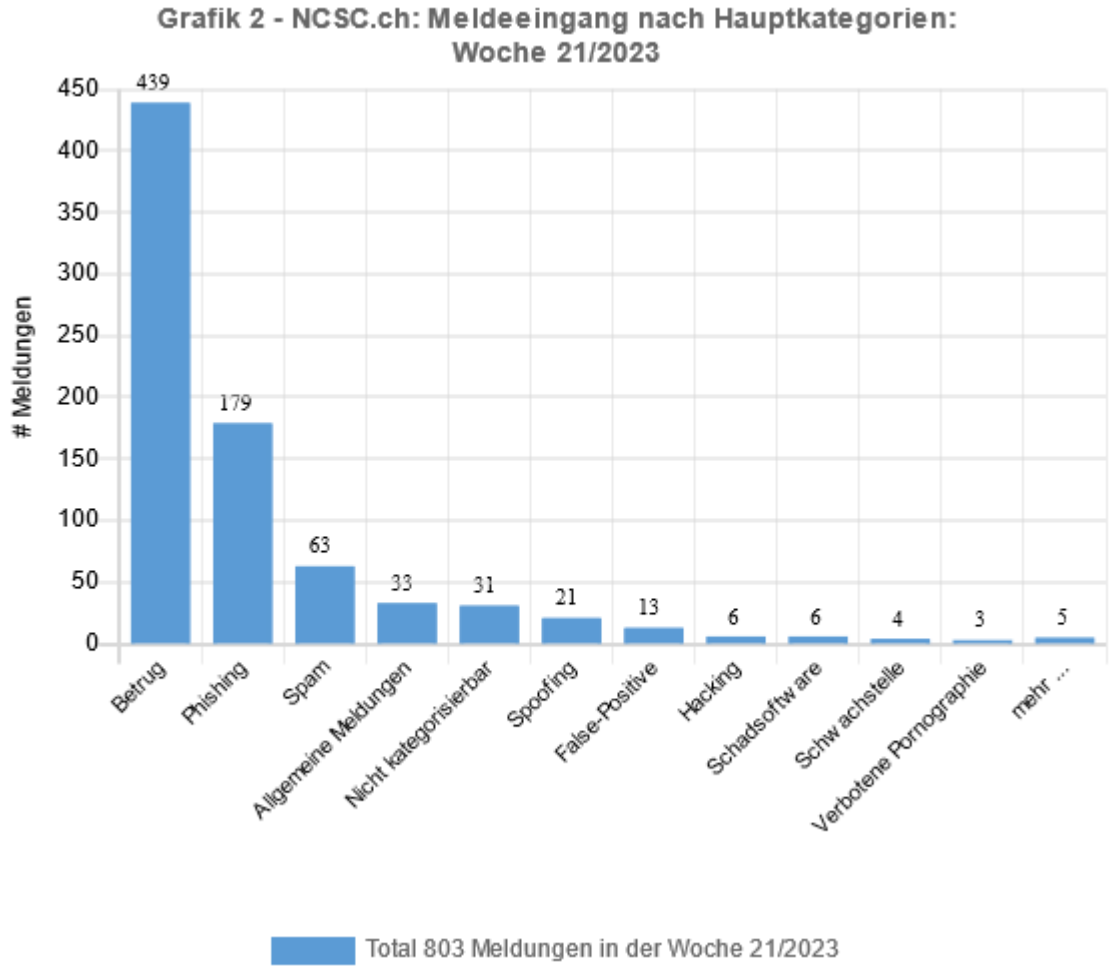
- Vertraulichkeit (CONFIDENTIALITY)
- Integrität (INTEGRITY)
- Verfügbarkeit (AVAILABILITY)

Weitere Schutzziele

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

Aktuelle Beispiele (National)



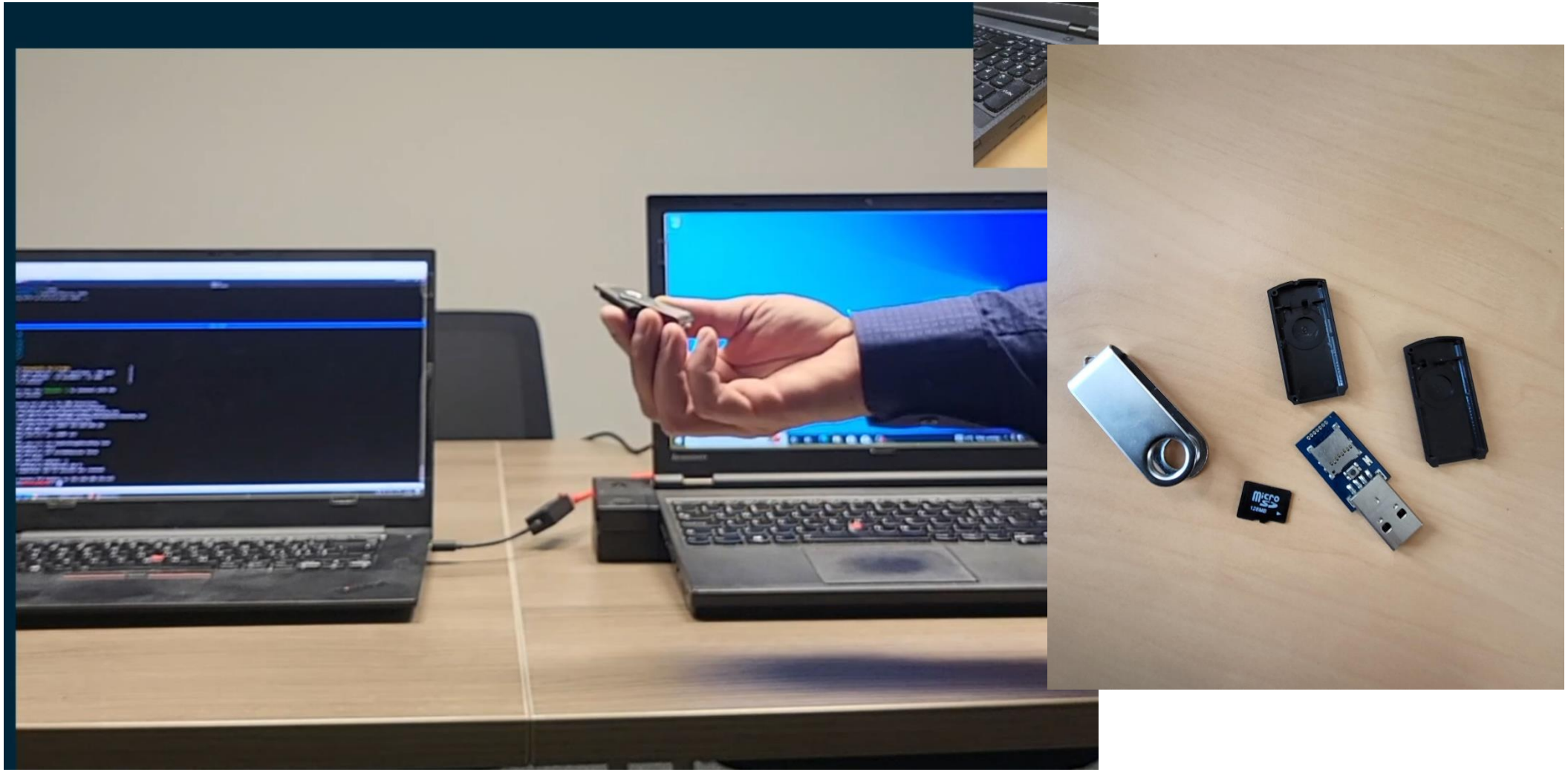


APT-Lifecycle

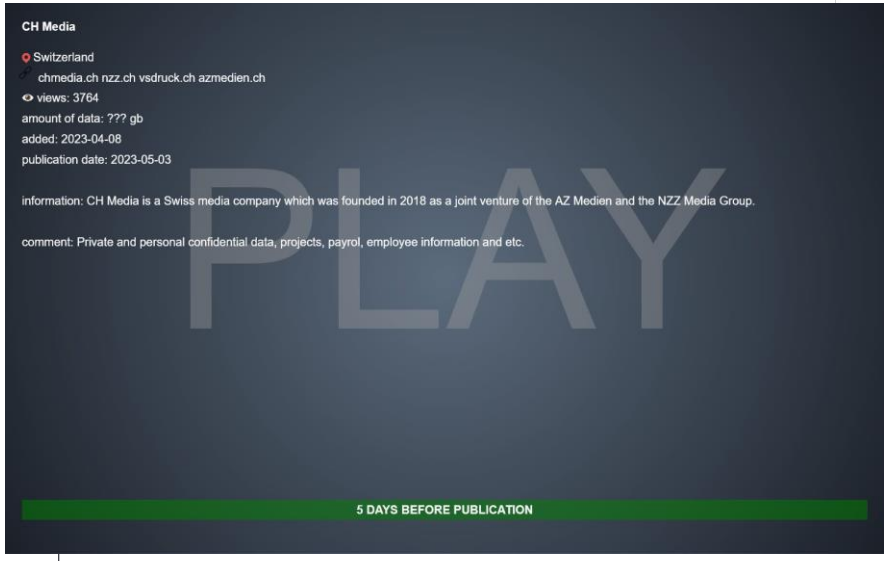
Ransomware heute

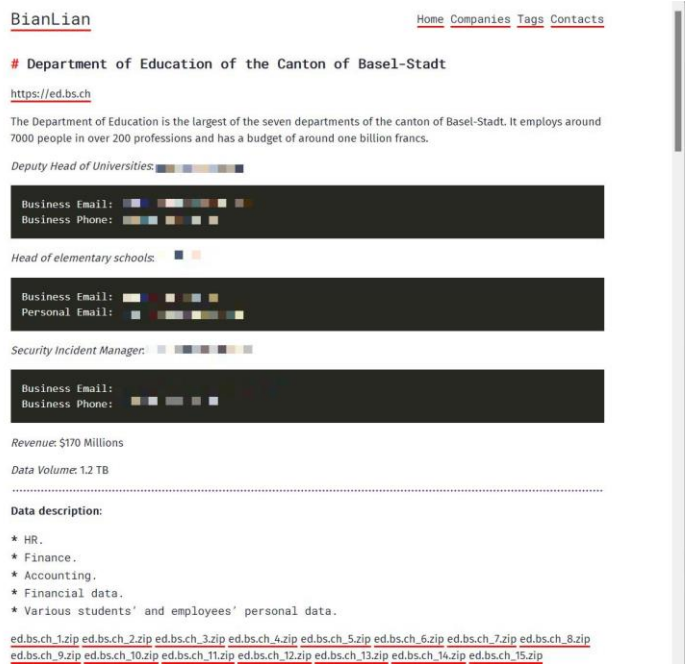
1. Kompromittierung
2. Diebstahl sensibler Daten
3. Daten verschlüsseln (1. Erpressung)
4. Mit Veröffentlichung der Daten drohen (2. Erpressung)
5. Öffentlich an den Pranger stellen
6. Optional: Androhung von Distributed-Denial-of-Service-Angriffen (3. Erpressung)
7. Optional: Kunden/Nutzer/Mitarbeiter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

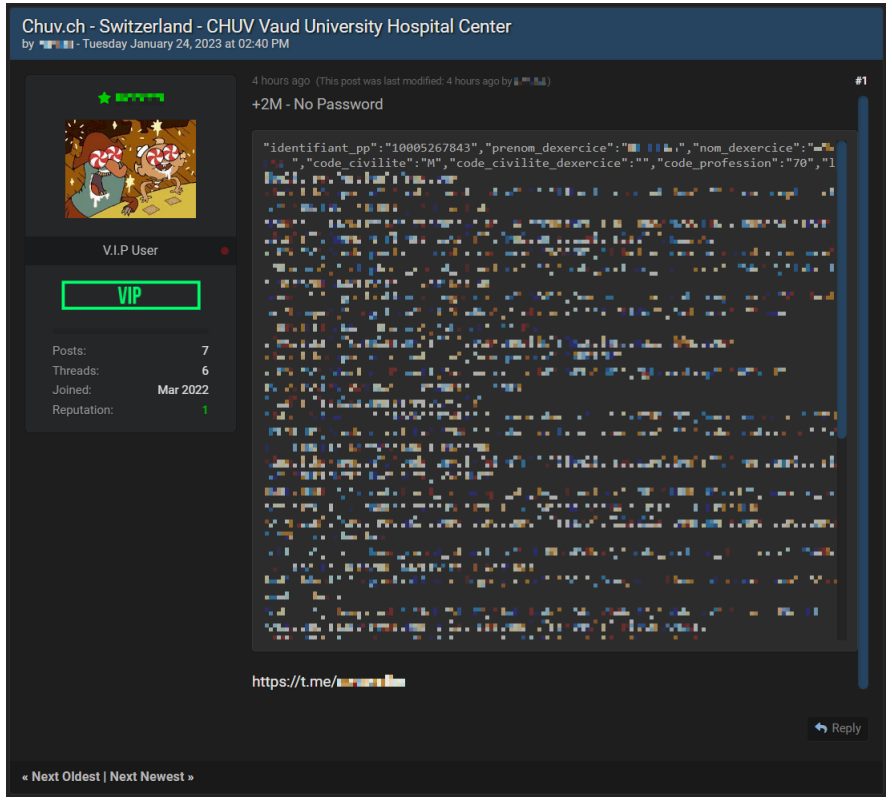
Live Hacking Demo – BadUSB

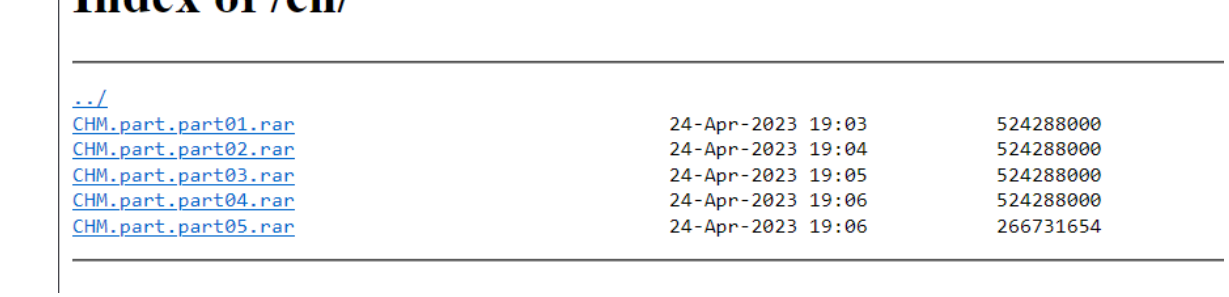


Aktuelle Beispiele aus dem Darknet
CH Media (NZZ), Waadt, Kanton Basel, etc.









Aktuelle Beispiele aus dem Darknet
Supply Chain Angriff auf Fedpol

CYBERANGRIFF

Publiziert 3. Juni 2023, 12:15

Daten des Fedpol im Darknet veröffentlicht

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

1 / 2

Hacker haben Daten ...
Getty Images

Die Server
Bundesamt
Hackerangr
«Blick»

BZ SCHWEIZ

1 Monat gratis lesen

Login Menü

Abstimmungen Bundeshaus

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

Cyberkriminalität in der Schweiz

Hacker veröffentlichen 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 Bundesrätinnen Karin Keller Sutter (r.) 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

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.

PLAY

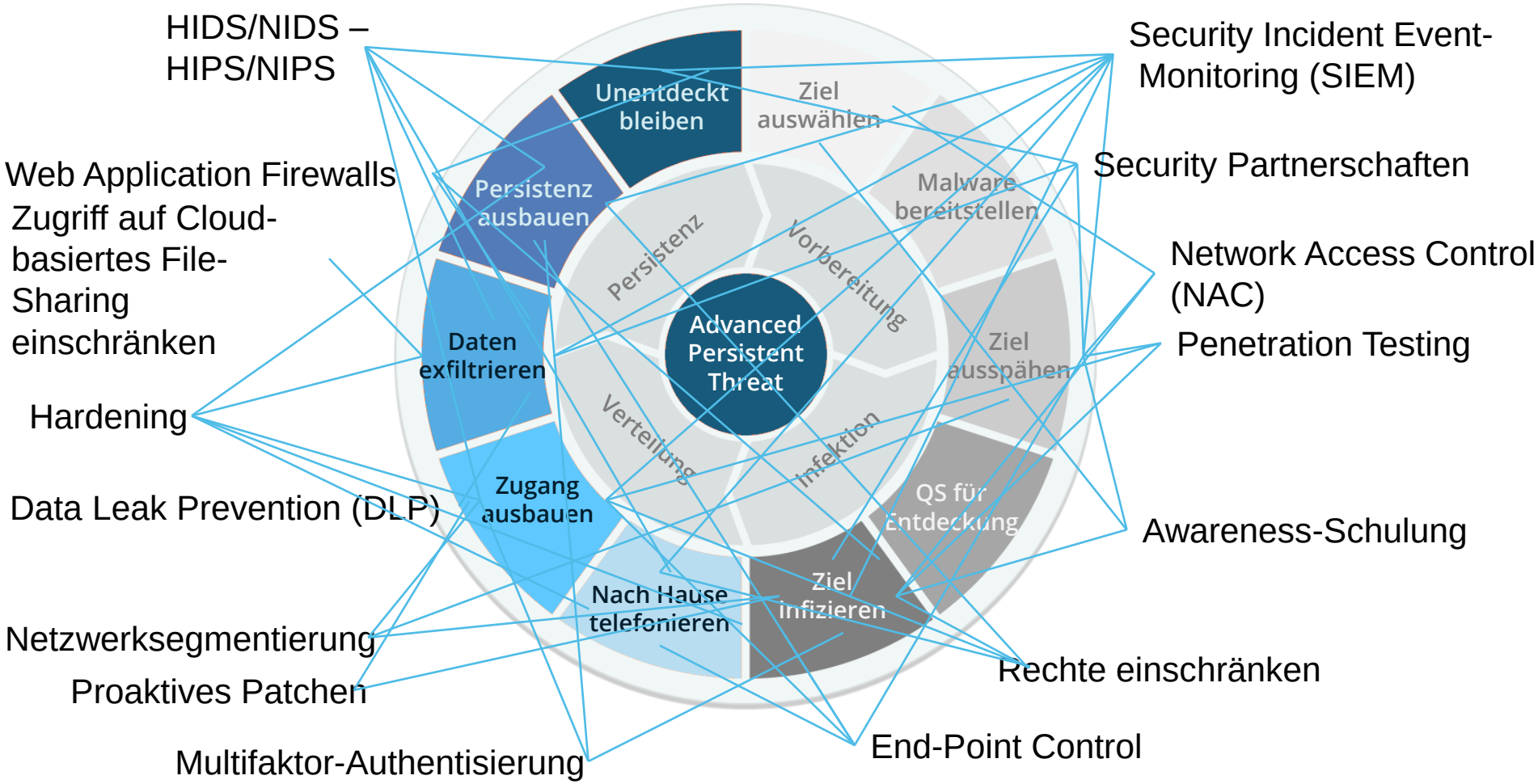
Index of /xp/

../	
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

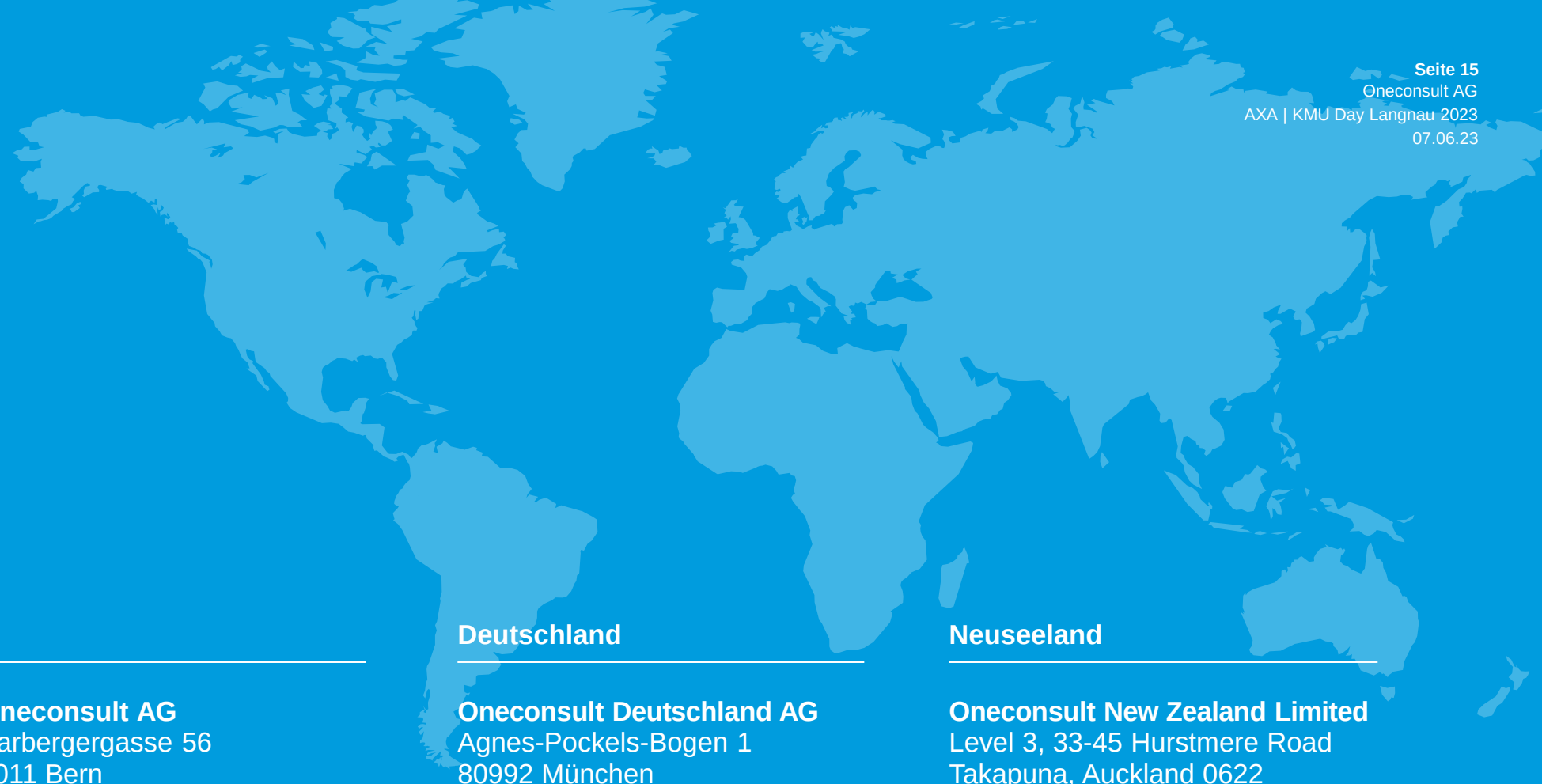
Backup, Backup, Backup!

- 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



Kontakt



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
Aarbergergasse 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