# CETRATUS

Risk Based Cyber Security

CETRATUS

# Warum sollten Cyber-Kriminelle mich angreifen? Ich bin doch kein Ziel, oder?

# Bedrohungslage
## Cyber Angriffe

**Ransomware warning: Cyber criminals are mailing out USB drives that install malware**

Don't insert USB drives from unknown sources, even if they're addressed to you in the post.

CYBERKRIMINALITÄT

**Cyber-Angriffe auf Firmen nehmen in der Schw**

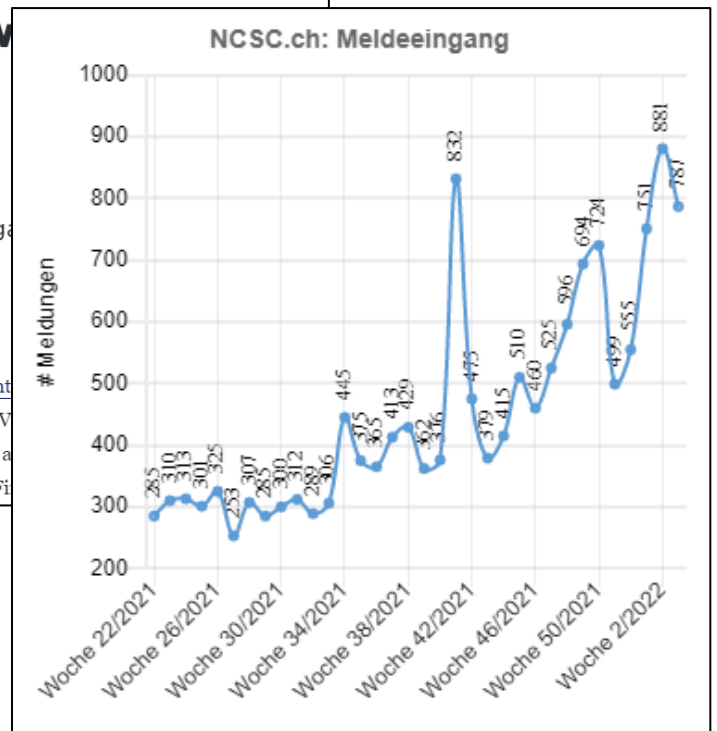
Lesezeit: 1 Minute

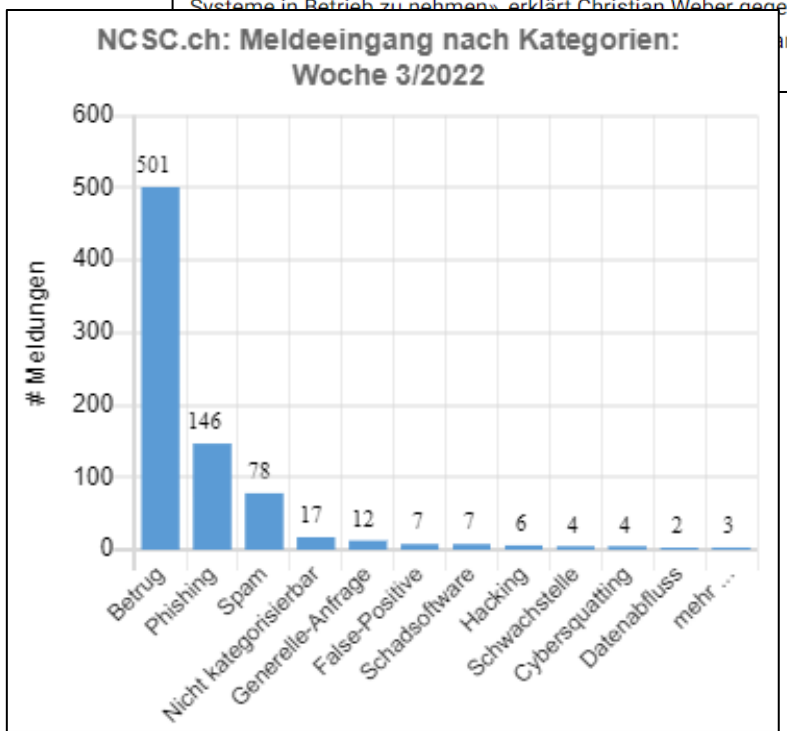
Teilen Merken Drucken Kommentare

Die Internetkriminalität hat im verga
nochmals deutlich zugenommen.

**Veröffentlicht** am 11.01.2022 - 07:37 Uhr

aut einer Untersuchung von Check Point
Attacken auf Firmen im Vergleich zum V
Experten stellten fest, dass die Angriffe a
geworden sind. In der Schweiz seien vor allem Fi




Weiterhin **kein Zeitungspapier** wegen Hacker-Attacke

Coya Vallejo Hägi
Zürich, am 11.01.2022

Die Luzerner Papierfabrik der CPH Chemie & Papier Holding steht seit fünf Tagen still. Das, weil das Unternehmen Opfer eines Hacker-Angriffs wurde.

Die einzige Schweizer Zeitungspapierfabrik ist stillgelegt. Die Betreiberin, die CPH Chemie & Papier Holding, wurde vergangenen Freitag Opfer einer Hacker-Attacke. Als Folge wurden alle IT-Systeme der Fabrik heruntergefahren und die Papierproduktion gestoppt.

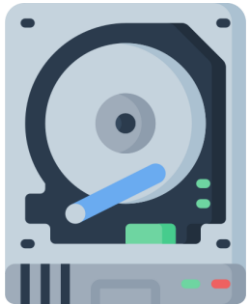
Diese konnte bis heute nicht wieder aufgenommen werden. «Wir sind immer noch dran, die IT-Systeme in Betrieb zu nehmen», erklärt Christian Weber gegenüber digitec. Das sei ein sehr
an Daten, die wir wiederherstellen

CETRATUS

# Wie kann ich Daten verlieren?

Was sind häufige Formen von Datenverlusten?

- Menschliches Versagen
- Festplattenschäden
- Computer Diebstahl
- Katastrophen



Schwachstelle mittlerweile behoben

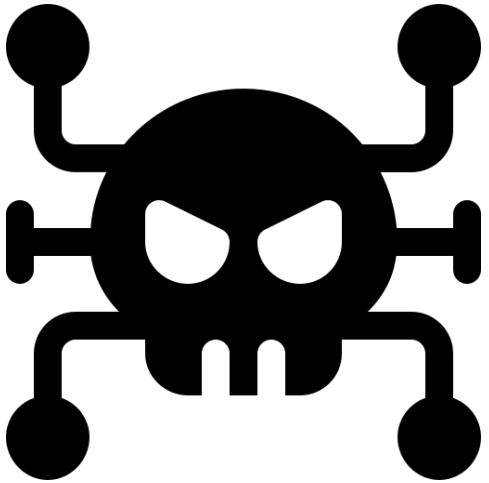
**Sicherheitslücke im SBB-System ermöglicht massiven Zugriff auf sensible Kundendaten**

Mo 24.01.2022 - 15:37 Uhr
von René Jaun und nba

# Wie kann ich Daten verlieren?

Und dann gibt es noch die Arten von Datenverlusten, die mit "Cyber" zu tun haben

- Viren & Malware
- Hacker und Insider

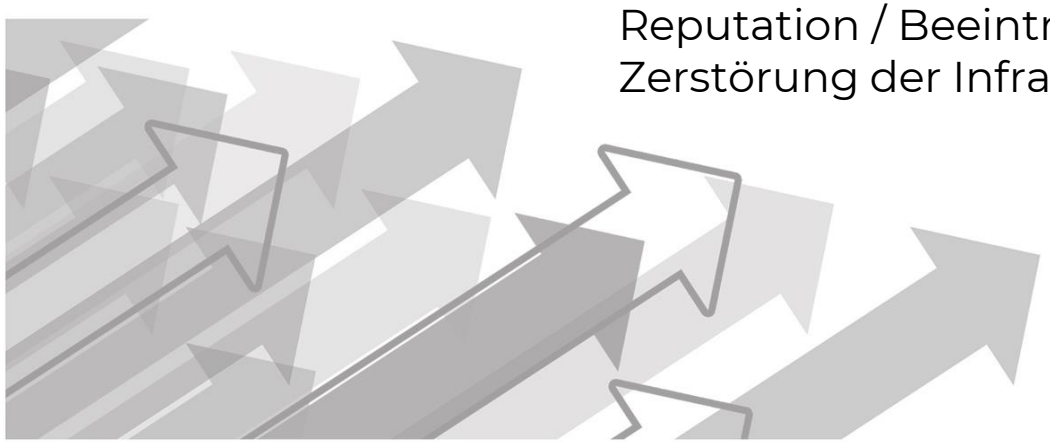


# Cybersicherheit
## Wie funktionieren Cyberangriffe?

Wer steckt hinter all diesen Anschlägen, was sind die Ziele und welche Methoden verwenden sie?

**Angreifer**
Cyber Kriminelle
Hacktivists
Länder
Insider

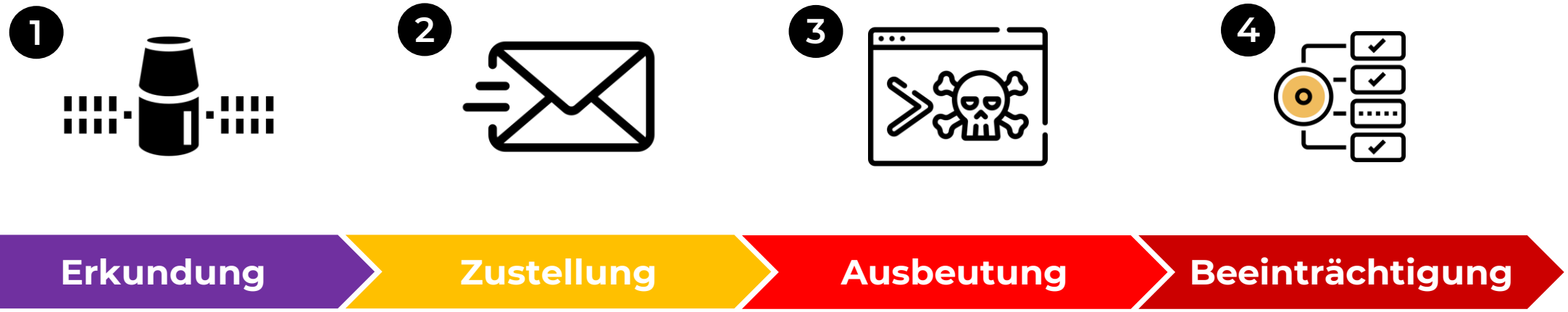
**Ziele**
Geld
Vertrauliche Informationen (Account Informationen/IP)
Reputation / Beeinträchtigung des Rufes
Zerstörung der Infrastruktur



**Methode**
Malware
Social Engineering
Vulnerabilities
Supply Chain Attacks

# Cybersicherheit
## Wie funktionieren Cyberangriffe?

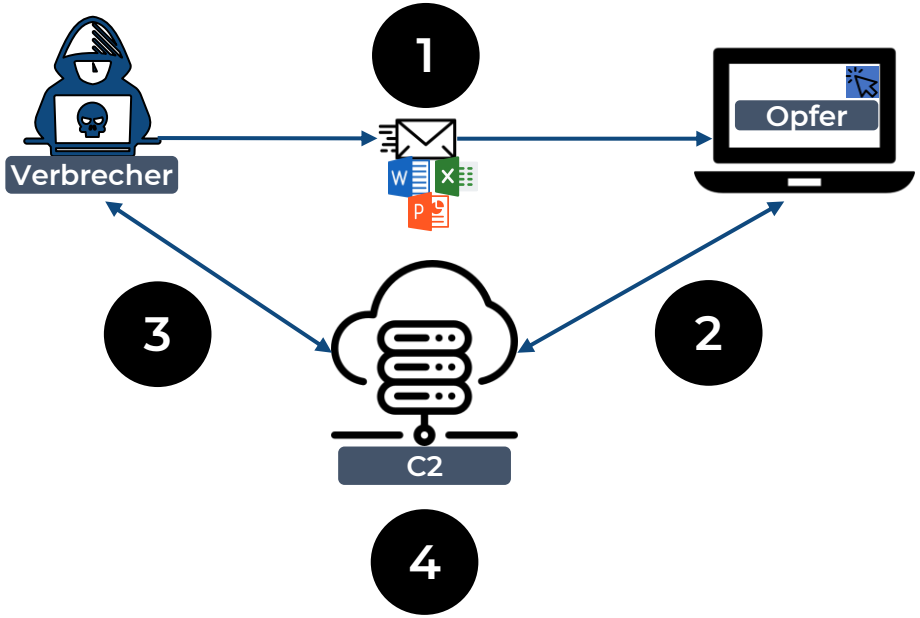
Vereinfacht dargestellt haben Cyberangriffe vier Phasen :



# Cybersicherheit
## Wie funktionieren Cyberangriffe?

### Emotet Installation

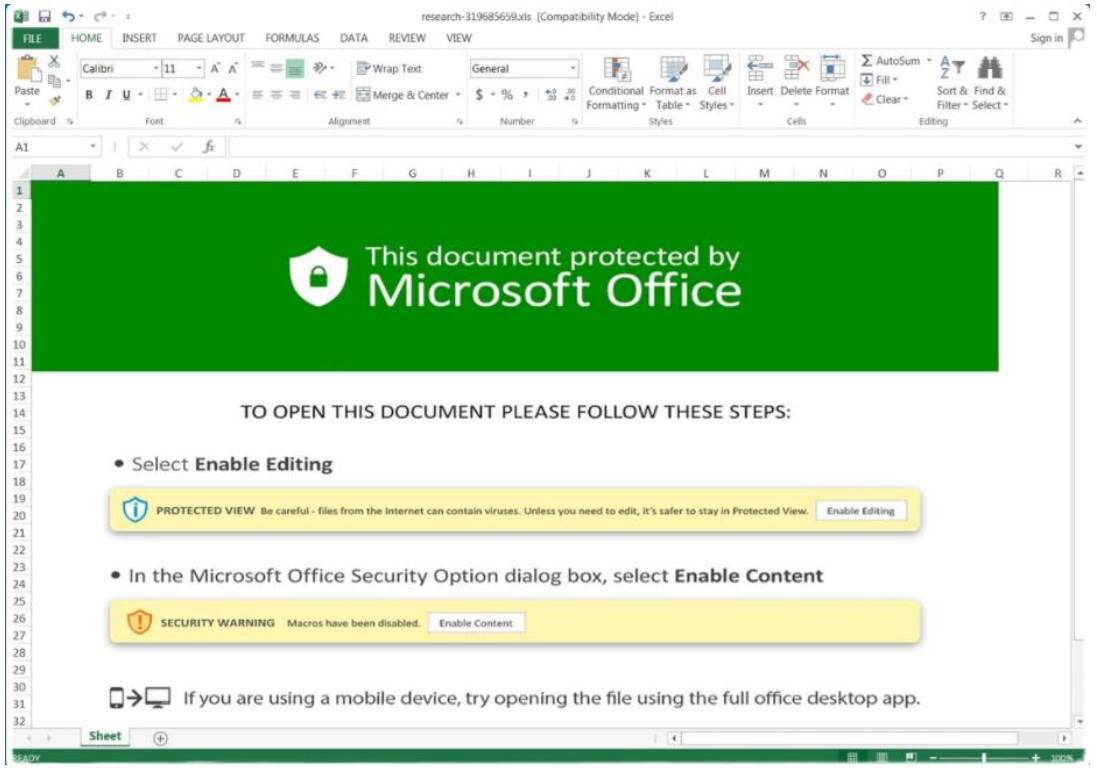
1. Verbrecher sendet dem Opfer eine E-Mail
2. Das Opfer öffnet die E-Mail und das angehängte Dokument
3. Die Schadsoftware wird heruntergeladen und ausgeführt und baut eine C2 ein
4. Verbrecher hat vollständigen Zugriff auf das/die kompromittierte(n) System(e) und kann Daten herunterladen und weitere Malware hochladen, usw.



# Wie funktionieren Cyberangriffe

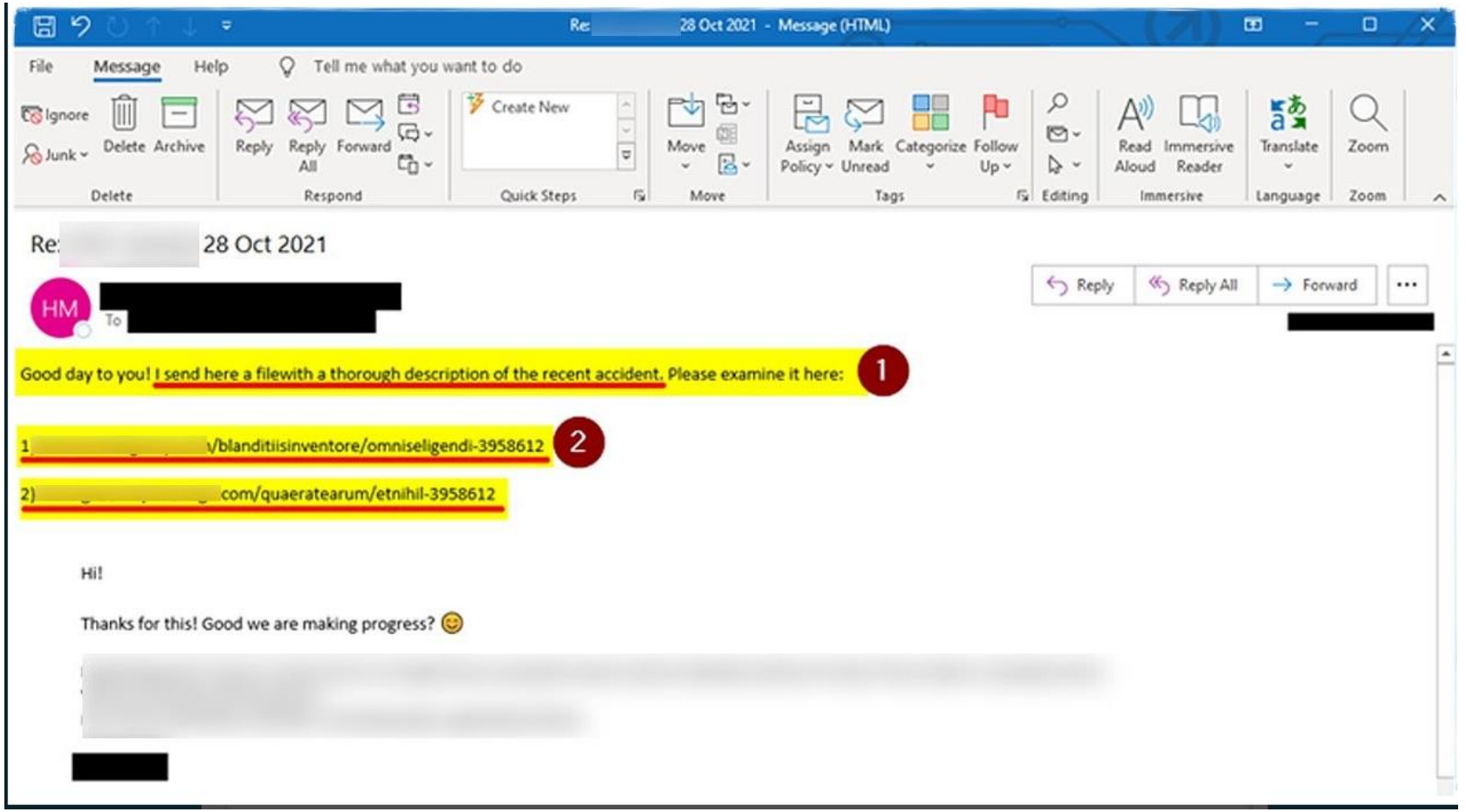
## Beispiel-E-Mail aus einem aktuellen Fall IKEA


Internal emails published by Bleeping Computer reveal that leading furniture retailer IKEA is battling an ongoing campaign of phishing attacks, fueled by internal and vendor accounts that have already been compromised.



# Wie funktionieren Cyberangriffe

## Beispiel-E-Mail aus einem aktuellen Fall IKEA



# Wie funktionieren Cyberangriffe

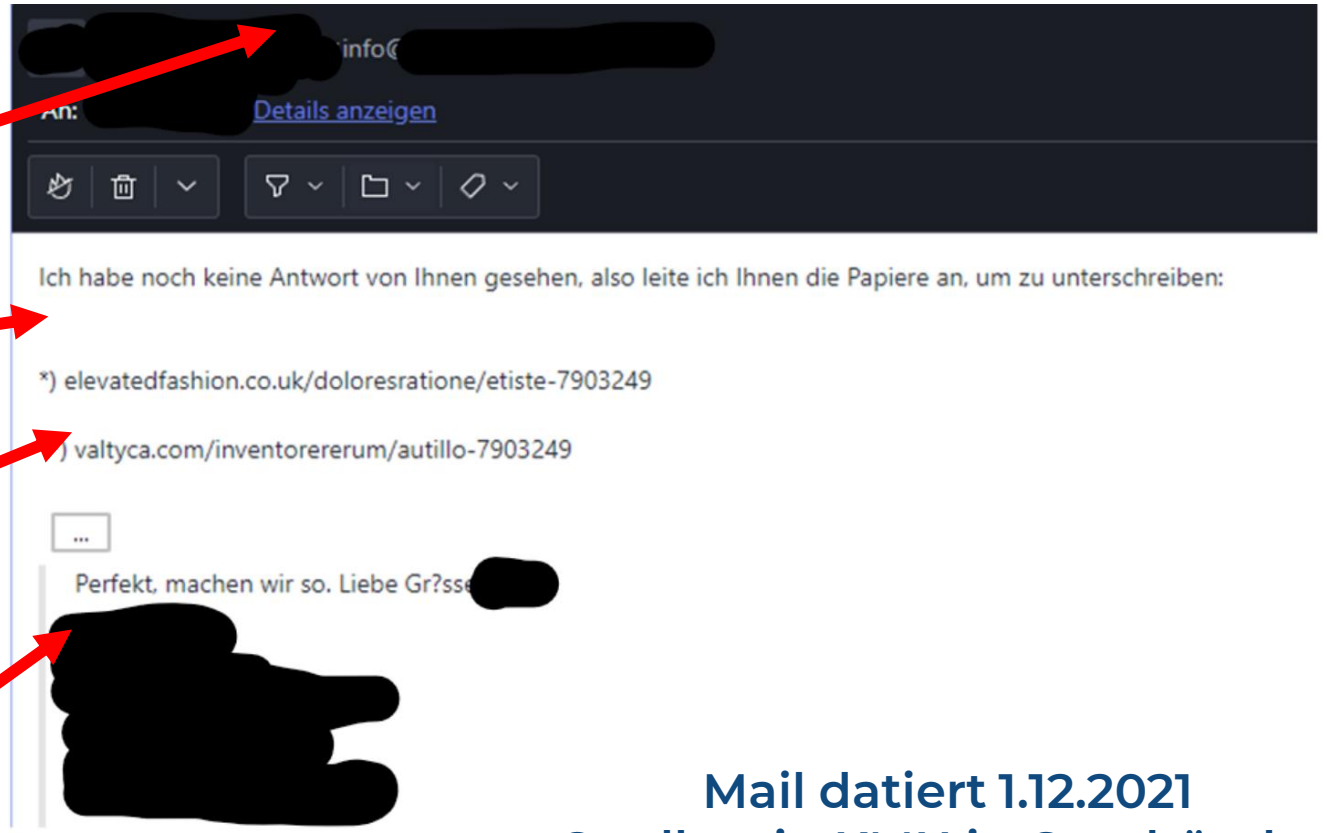
## Beispiel-E-Mail aus einem aktuellen Fall

Die E-Mail stammt von einem bekannten Absender. Kein Spoofing

Der Text ist in der Sprache der Original-E-Mail

Diese Links verweisen auf den bösartigen Inhalt (Malware)

Die E-Mail ist eine Antwort auf eine bestehende E-Mail-Konversation

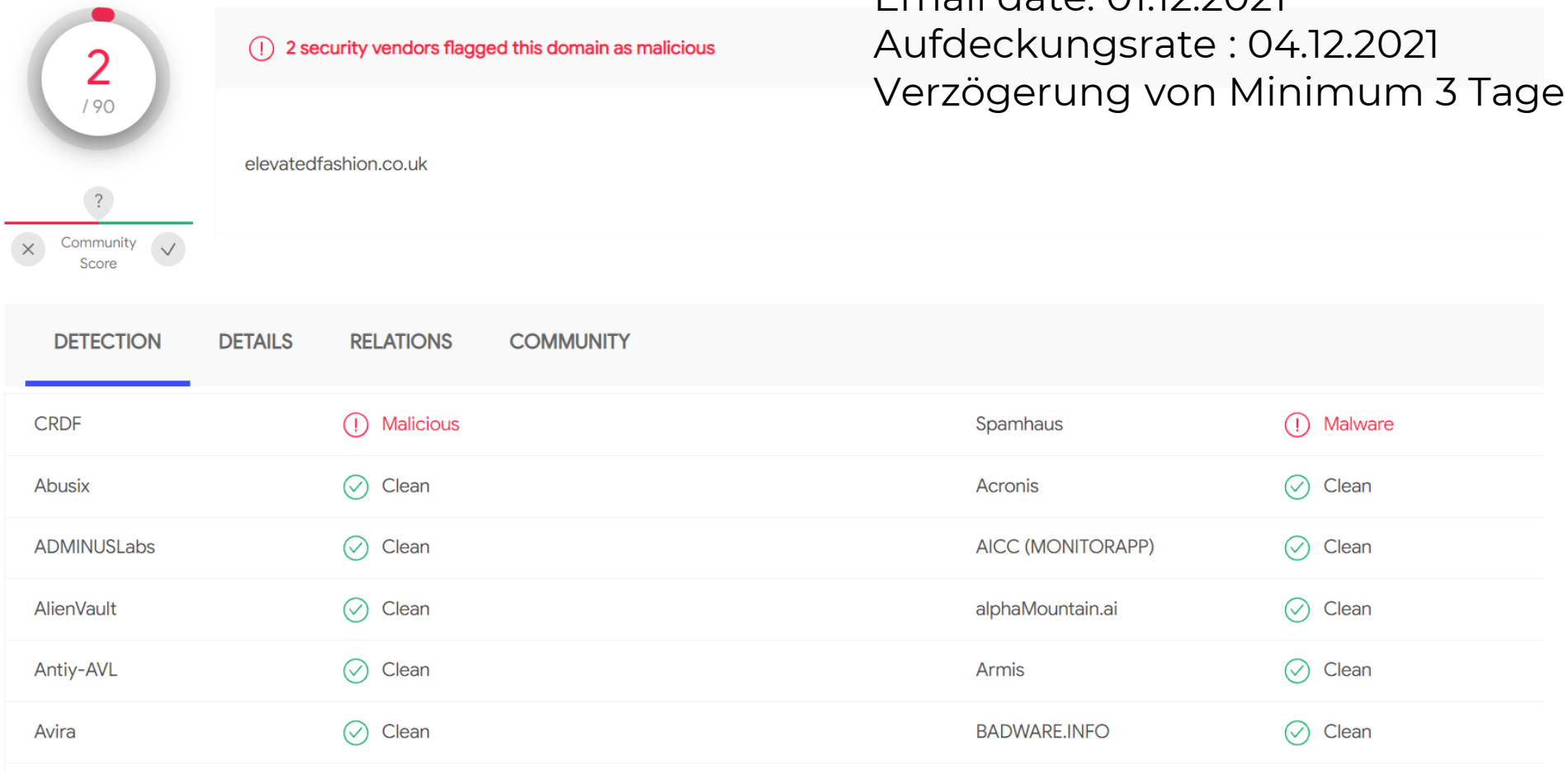



**Mail datiert 1.12.2021**
**Quelle: ein KMU in Graubünden**

CETRATUS

# Wie funktionieren Cyberangriffe
## Antivirus?

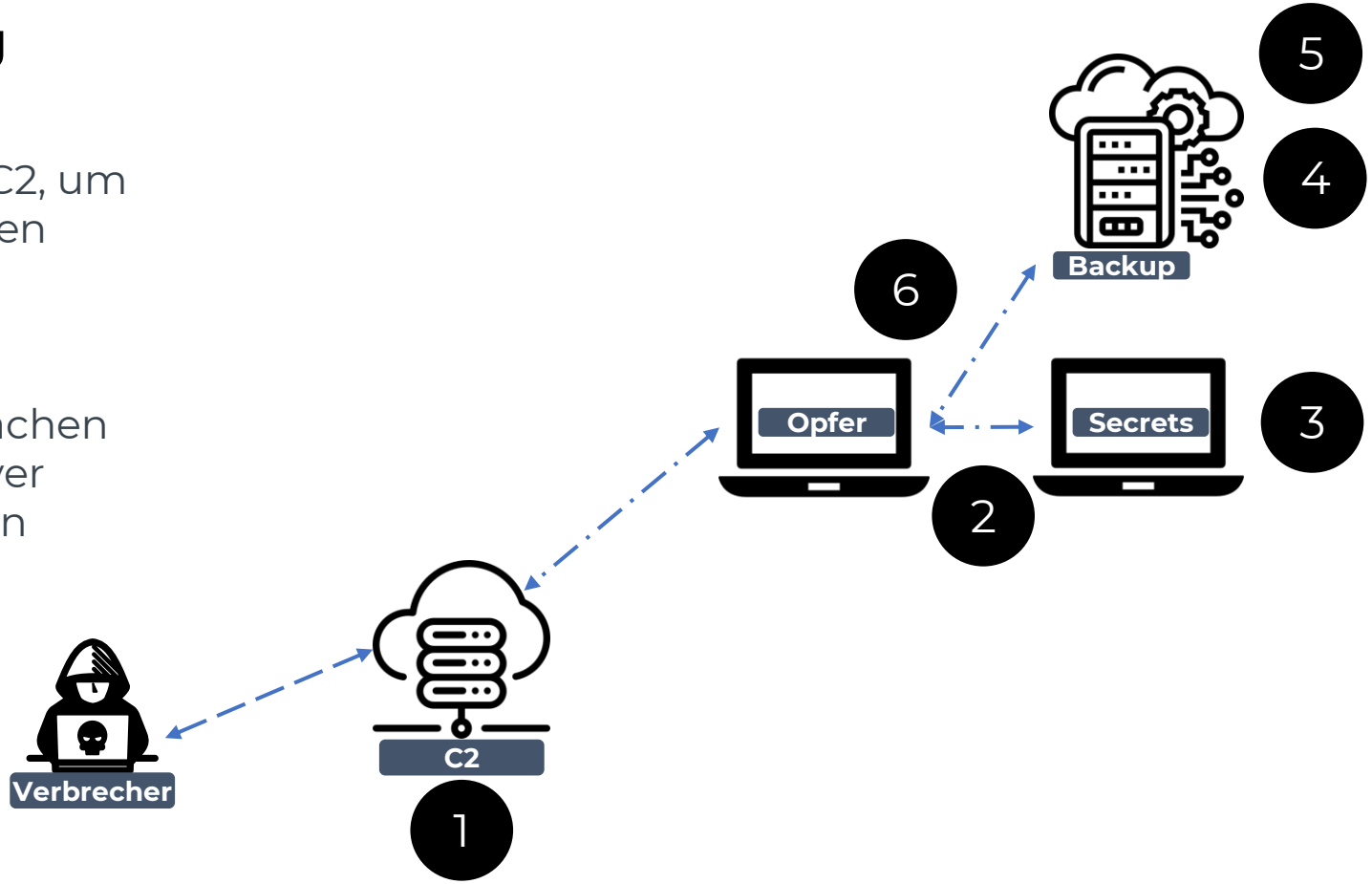
Email date: 01.12.2021
Aufdeckungsrate : 04.12.2021
Verzögerung von Minimum 3 Tagen.



# Cybersicherheit
## Wie funktionieren Cyberangriffe?

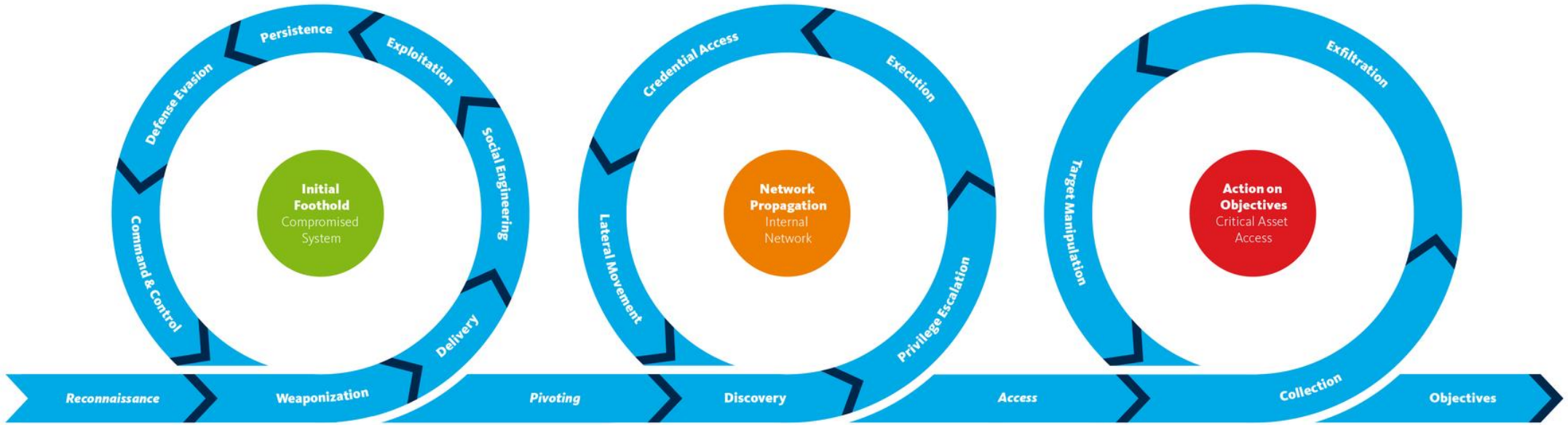
### Ransomware Verbreitung

1. Verbrecher verwendet den C2, um die Ransomware hochzuladen
2. Seitliche Bewegung
3. Geheime Daten finden und hochladen via C2
4. Backup-Server ausfindig machen
5. Vernichten von Backup Server Dateien und Konfigurationen
6. Lösegeldangriffe auf übrige Systeme durchführen



# Cybersicherheit
## Wie funktionieren Cyberangriffe?

Unified killchain



# Bedrohungslage

## Cyber Angriffe KMU

Studie zur Cybersicherheit in KMUs 2021

### Jedes dritte KMU wird Opfer eines erfolgreichen Cyberangriffs

Fr 19.11.2021 - 11:42 Uhr
von Nadja Baumgartner und cka

CYBERKRIMINALITÄT

### Cyber-Angriffe auf Firmen nehmen in der Schweiz stark zu

Lesezeit: 1 Minute

Teilen Merken Drucken Kommentare

Die Internetkriminalität hat im vergangenen Jahr hierzulande nochmals deutlich zugenommen.

**Veröffentlicht** am 11.01.2022 - 07:37 Uhr

aut einer Untersuchung von Check Point Research (CPR) nahmen Cyber- 65 Prozent zu. Die CPR- netzwerke deutlich mehr en Bereichen

KRIMINALITÄT

### KMU als Zielscheibe: Zahl der Cyberangriffe steigt stark an

Unternehmen werden immer häufiger Opfer von Cyberkriminellen. Neue Zahlen zeigen nun: Alleine im ersten Halbjahr hat sich die Zahl der Angriffe fast verdoppelt.

Menü Suchen HANDELSZEITUNG Abo

Home > Unternehmen > Die Schweiz im Cyberkrieg: Firmen müssen dringend handeln

Abo IT

### Die Schweiz im Cyberkrieg: Firmen müssen dringend handeln

Viele Schweizer Firmen sind im Internet exponiert und machen sich Sorgen um ihre Daten. Aber sie unternehmen zu wenig dagegen. Was sie tun müssen.

Von **Bernhard Fischer**
am 19.01.2022 - 11:28 Uhr

nsbesondere KMU

Unternehmen und insbesondere KMU sehen sich mit einer Zunahme von Cyberattacken konfrontiert. Sie sind nicht gut genug vorbereitet oder sind sich der Gefahren nicht bewusst.

Jüngstes Beispiel dafür sind signifikante Sicherheitsmängel beim nationalen Organspenderegister Swisstransplant, die es einem erlauben würden, beliebige Personen zum Organspender zu machen. Und es sei dort zudem möglich, alle Dateien auf dem Anwendungsserver auszulesen und herunterzuladen, wie das Schweizer Radio und Fernsehen (SRF) berichtet.

CETRATUS

# Also, sind sie ein ziel?

Wir unterstützen sie proaktiv und reaktiv
im Aufbau, im Betrieb und in Krisen

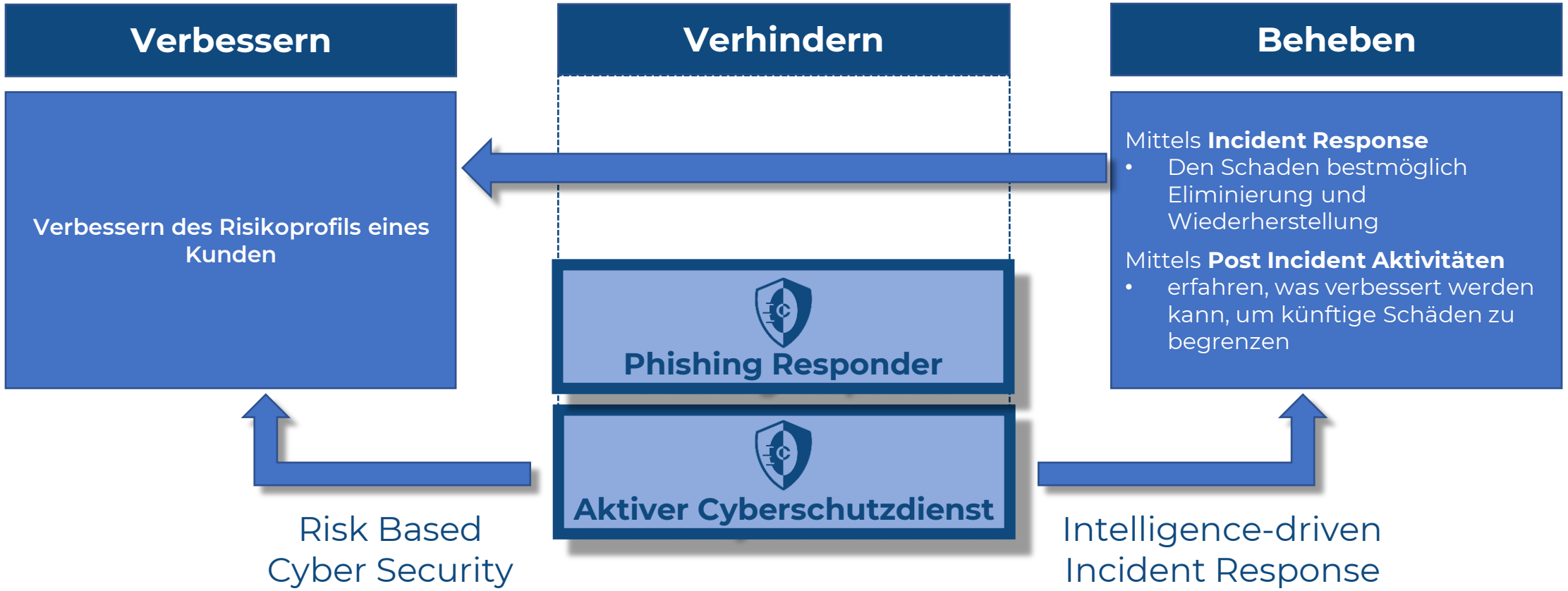
CETRATUS

Verbessern – Verhindern - Beheben



CETRATUS

# Risk Based Cyber Security



Cetratus AG
Hochwachtstrasse 10
CH-6312 Steinhausen
Tel. +41 41 520 520 1
welcome@cetratus.ch
www.cetratus.ch