

# CYBERRISIKEN UND SCHWEIZER KMU

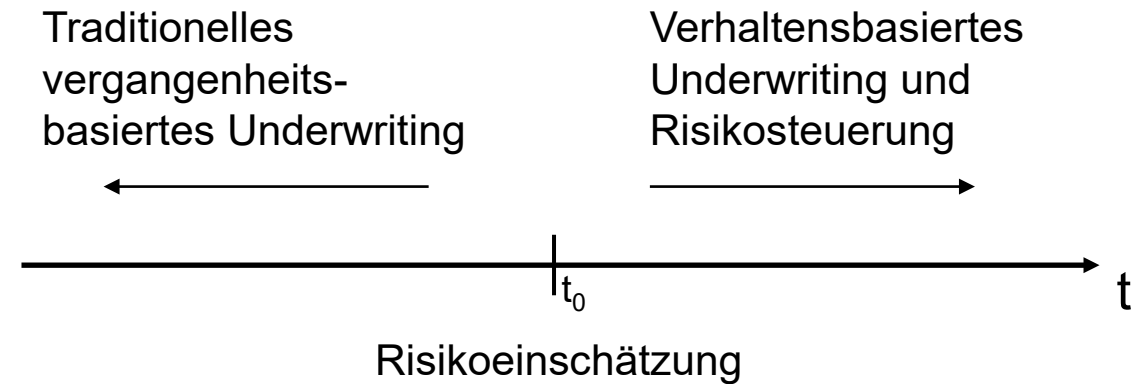
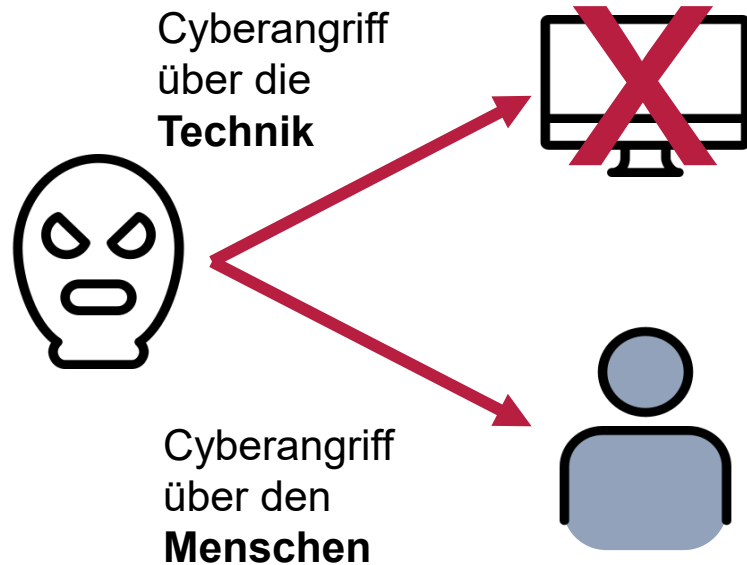
qx-Club

27. April 2021

Dr. Carlo Pugnetti, ZHAW  
Carlos Casián, Allianz Suisse



# 01 PROBLEMSTELLUNG



Je dynamischer der Markt / Technologieumfeld ist, desto wichtiger ist das Verhalten der Versicherten.

# 02 METHODIK

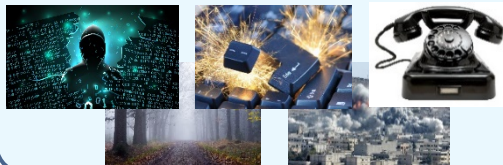
Tiefen-Metaphern-Interviews benutzen Bilder, um emotionale und unterbewusste Antriebskräfte für Verhaltensweisen und Entscheidungen zu identifizieren und an die Oberfläche zu bringen. Sie generieren keine statistisch relevanten Ergebnisse, erlauben jedoch ein tieferes Verständnis.

1

Interviewpartner werden vorgängig gebeten, Bilder im Internet zu suchen, die ihre Gefühle zur einer bestimmten Frage widerspiegeln,

**"Wie fühlen Sie sich, wenn Sie über Cyberangriffe hören?"**

Bitte suchen Sie 3-5 Bilder, die Ihre Gefühle widerspiegeln.



2

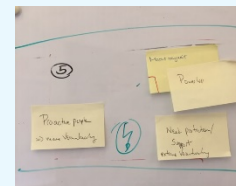
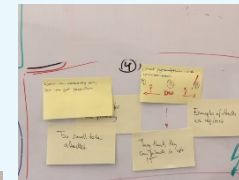
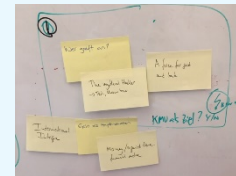
Bilder werden mit den Interviewpartner besprochen, um den Grund für die Auswahl zu verstehen und um Verbindungen zu übergeordneten Themen / Ideen zu erkennen.

17 Interviews wurden im September 2020 durch das Forschungsteam bei den ausgewählten Unternehmen durchgeführt.



3

Ergebnisse der Interviews werden durch das Forschungsteam zusammengetragen, um wiederkehrende und zentrale Themen zu erkennen, und daraus Empfehlungen abzuleiten.



★

Acht Themen als Ergebnis.

1. Internationale Politik und organisiertes Verbrechen
2. Der Hacker-Mythos
3. Sich hilflos fühlen
4. Sich anfällig fühlen
5. Katastrophale Folgen
6. Das betrifft mich nicht
7. Proaktiv und engagiert
8. Zusätzliche Einblicke



# 03 ERGEBNISSE

**INTERNATIONALE POLITIK  
UND ORGANISIERTES  
VERBRECHEN**

SCHATTENMANN



**SICH HILFLOS FÜHLEN**

LAUTER FRAGEN



**DER HACKER-MYTHOS**

TOP ARBEITSPLATZ



**SICH ANFÄLLIG FÜHLEN**

ÜBERWACHUNG



# 03 ERGEBNISSE

## KATASTROPHALE FOLGEN

MODERNES EINBRECHEN  
UND EINDRINGEN



## DAS BETRIFFT MICH NICHT

PERSÖNLICHE  
UNTERSTÜTZUNG



## PROAKTIV UND ENGAGIERT

PLANUNG





# 04 EMPFEHLUNGEN

**VORBEREITEN**



**MITARBEITENDE  
BEFÄHIGEN**



**BEWUSSTSEIN  
SCHÄRFEN**



**WIEDERHERSTELLUNGS-  
MODUS ÜBEN**



# 05 STUDIE



Links zur Studie:

[Deutsch](#)

[Französisch](#)

[Italienisch](#)

[Englisch](#)

**FRAGEN?**

**HERZLICHEN DANK!**





**BACKUP**

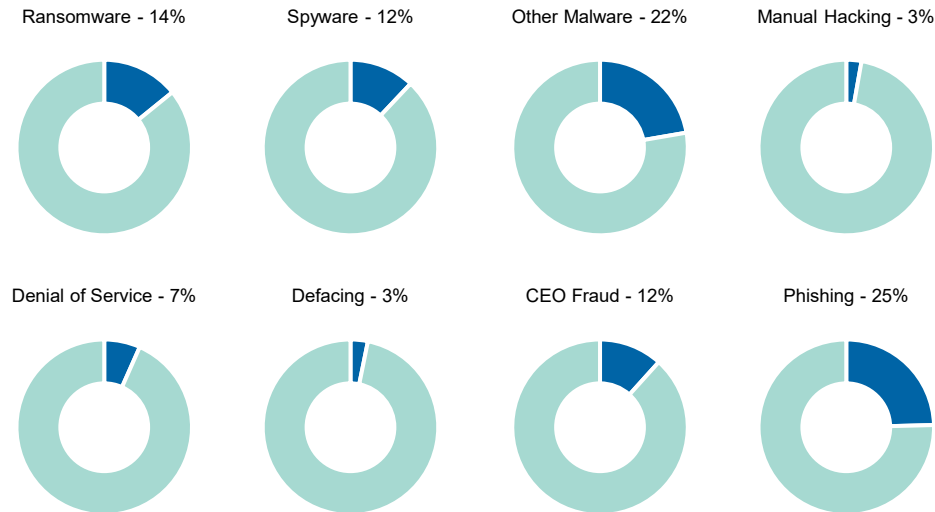


# STUDIENÜBERSICHT

## AKTUELLE LAGE

- Trotz wiederholter Bemühungen, Mitarbeitende über die Gefahr von Phishing-Angriffen zu informieren und zu schulen, fällt eine bedeutende Minderheit Cyberkriminellen zum Opfer.
- Aktuelle Studien zeigen, dass bereits jedes vierte Schweizer KMU zum Opfer eines Cyberangriffs wurde.
- Insbesondere Ransomware-Angriffe haben gemäss dem Nationalen Zentrum für Cybersicherheit (NCSC) zugenommen – gleichzeitig auch die Lösegeldforderungen
- Kürzlich durchgeführte Studien haben Cyberangriffe auf KMU in Nachbarländern genauer untersucht (siehe Tabelle).

## GESCHÄTZTE JÄHRLICHE RATE DER CYBERANGRIFFE AUF KMU IN DEUTSCHLAND 2018/2019, UNTERGLIEDERT NACH KATEGORIEN



Source: Dreissigacker et al. (2020)

## BEISPIELE VON PROMINENTEN CYBERANGRIFFEN IN DER SCHWEIZ

- Offix AG, 2019
- Swisswindows, 2019
- Meier Tobler, 2019
- Stadler Rail, 2020

## FORSCHUNGSZIEL

Unsere Forschung zielt darauf ab, soziale und kognitive Dynamiken zu untersuchen, die die Verwundbarkeit gegenüber Cyberangriffen erleichtern, um Empfehlungen für KMU zu entwickeln.

## METHODIK

Tiefen-Metaphern-Technik nach Zaltman: Interviews mit 17 Freiwilligen in drei ausgewählten KMU der Fertigungs- und Wärmebranche. Breiter Querschnitt von Mitarbeiterprofilen, einschliesslich Management, Verwaltungspersonal, Werkstatt und Außendienstmitarbeitern.

## FORSCHUNGSTEAM

- Dr. Carlo Pugnetti, Dozent am Institut für Risk & Insurance an der ZHAW
- Carlos Casián, Sach / Cyber Risk Underwriter bei Allianz Suisse