Cyberrisiken, Deckungen, Services und Schadenfälle

Thomas Greub, Senior Underwriter AXA

Webinar VSV, 21.02.2024

Agenda

60 Min.

1. Cyberrisiken	Weshalb kann jedes Unternehmen betroffen sein? Weshalb kann jeder externe Vermögens-verwalter betroffen sein? Umfragen, Statistiken
2. Welche Versicherungsdeckungen gibt es?	
3. Services	
4. Schaden	Schadenbeispiel
5. Fragen und Diskussion	


1
Cyberrisiken

1.1 Weshalb kann jedes Unternehmen betroffen sein?

Unternehmensziel: Informationssicherheit

Cyber-Sicherheit ist als unternehmensweites Risikomanagement zu verstehen
Jedes relevante Problem der IT-Sicherheit ist theoretisch gelöst und trotzdem ein Disaster!

Geistiges Eigentum
Wettbewerbsvorsprung

Datenschutz
Kundenvertrauen

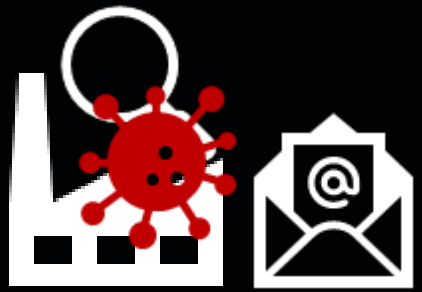
Rechtssicherheit
Haftung der Geschäftsführung

Schaden verhüten
Kosten reduzieren

Lieferfähigkeit
Verfügbarkeit der Waren

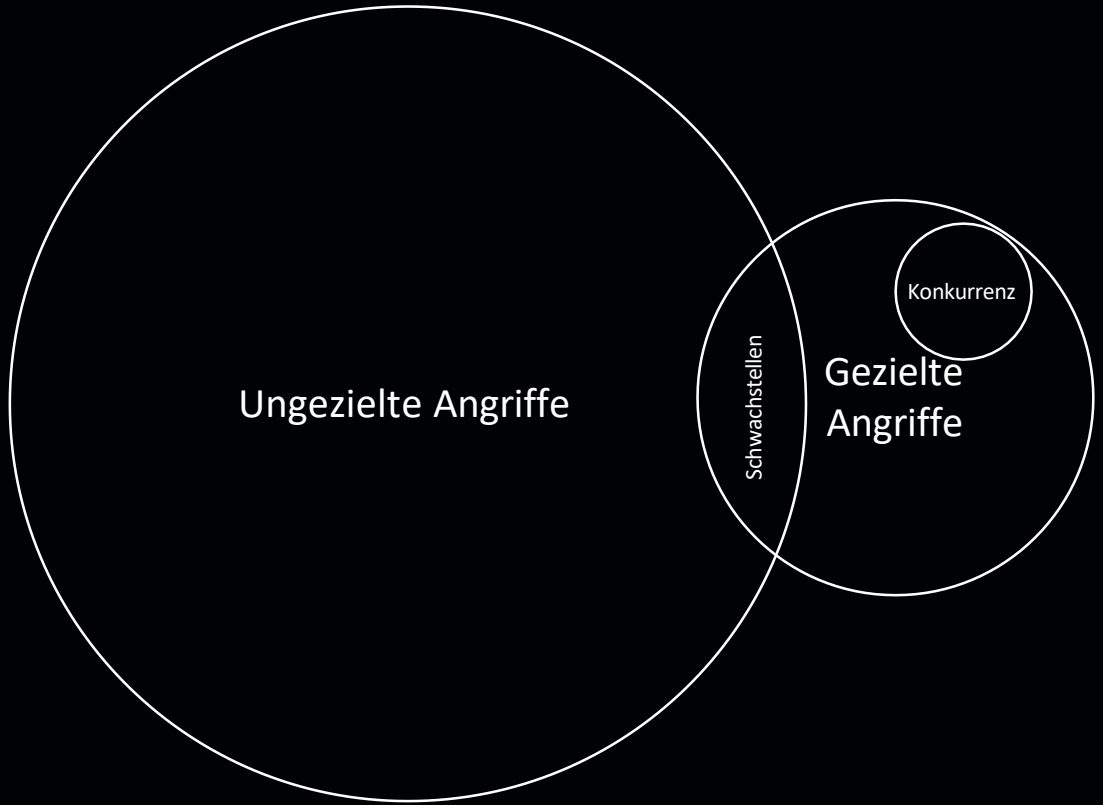
Festlegung
Risikoziele

Gezielte Angriffe

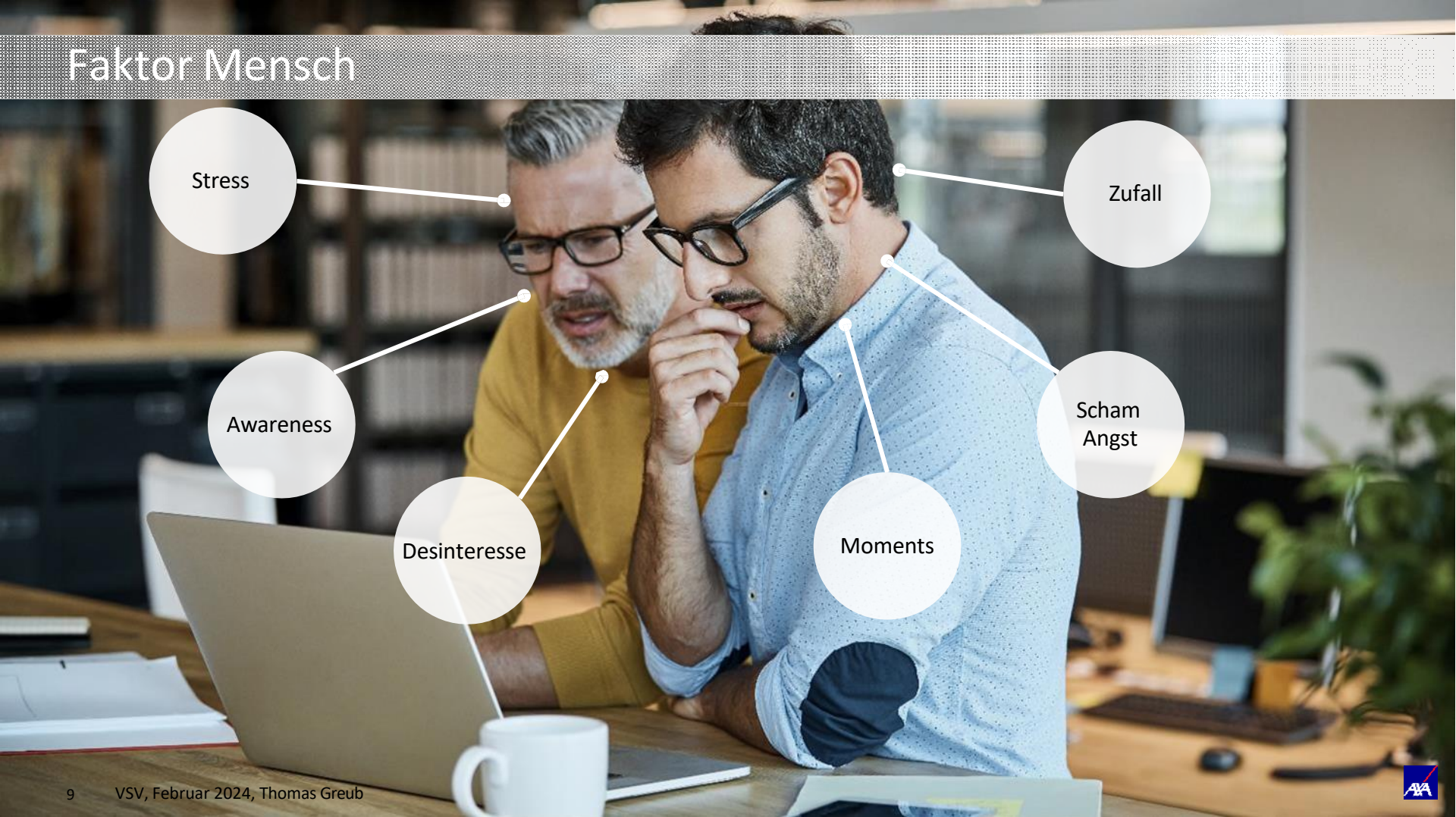


Ungezielte Angriffe

Ungezielte Angriffe



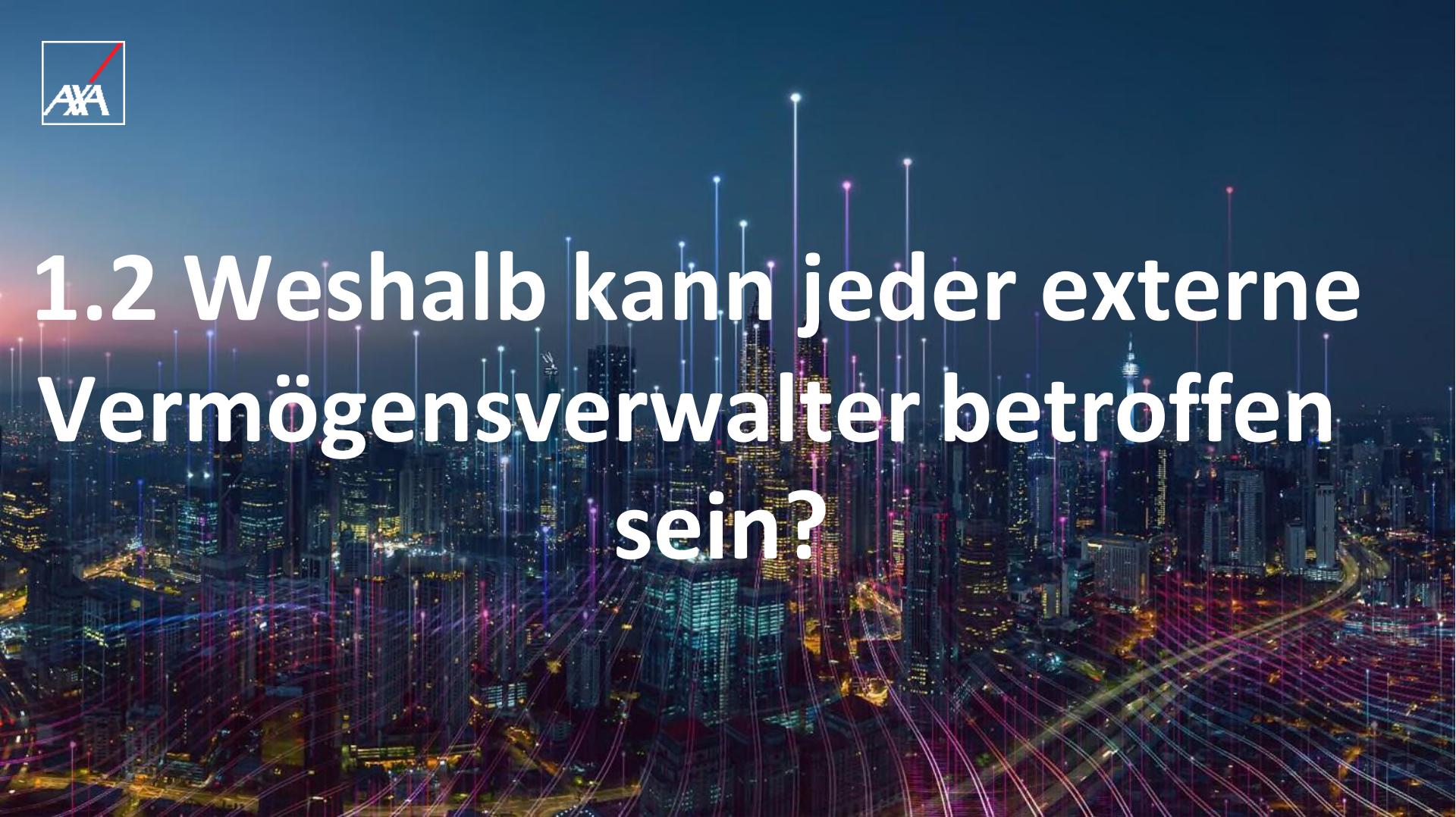
Faktor Mensch



Empfehlungen des BACS (ehemals NCSC)

Vom 29. Januar 2024 (Anti-Phishing Bericht 2023, teilweise gekürzt)

- **Meldung an das BACS:** Melden Sie verdächtige E-Mails oder Webseiten dem BACS auf antiphishing.ch.
- **Seien Sie skeptisch:** Keine Bank und kein Kreditkarteninstitut wird Sie jemals per Email oder SMS auffordern, Passwörter zu ändern oder Kreditkartendaten zu verifizieren.
- **Multi-Faktor-Authentifizierung (MFA):** Aktivieren Sie auf Ihren Online-Konten wie beispielsweise E-Mail oder Social Media wenn immer möglich eine Multi-Faktor-Authentifizierung (MFA).
- **Mehrfachverwendung von Passwörtern:** Verwenden Sie niemals dasselbe Passwort für mehrere Online-Konten. Verwenden Sie einen Passwort-Manager für die Verwaltung Ihrer Zugangsdaten.
- **Kreditkartenabrechnung:** Prüfen Sie regelmässig Ihre Kreditkartenabrechnung auf Unstimmigkeiten und wenden Sie sich bei unbekannten Transaktionen sofort an Ihren Kreditkartenanbieter.
- **Verwendung von Favoriten:** Verwenden Sie für den regelmässigen Zugriff auf Online-Konten wie beispielsweise E-Banking, Social Media oder E-Mail die Favoriten («Bookmarks»)-Funktion Ihres Web-Browsers.
- **Spoofing:** Bedenken Sie, dass Absender von E-Mails und SMS aber auch Rufnummern von eingehenden Telefonanrufen einfach zu fälschen sind. Verlangen Sie im Zweifelsfalle, dass Sie den Anrufenden zurückrufen können.



1.2 Weshalb kann jeder externe Vermögensverwalter betroffen sein?

Externe Vermögensverwalter und Cyber-Sicherheit

- IT & Cybersicherheit
  - → wird von der überwiegenden Mehrzahl der externen Vermögensverwalter in der Schweiz als sehr wichtig und mit Handlungsbedarf innert 12 Monaten bis in den nächsten drei Jahren beurteilt
  - → wird am meisten externen Dienstleistern anvertraut (ca. 60%)
    - – Status Quo der Digitalisierung und internen Organisation der externen Vermögensverwalter, Studie von Tatiana Agnesens, Luzern, Januar 2024
- Cybercrime in der Vermögensverwaltung
  - → Externe Vermögensverwalter haben oft direkten Zugriff auf das Vermögen der Klienten. Kriminelle versuchen dies auszunutzen
  - → Ein falscher Klick und schon kann eine Schadsoftware installiert werden, die Zugriff auf das E-Banking geben kann
  - → Kriminelle geben sich als Mitglied der GL aus und bringen einen Mitarbeiter dazu, eine nicht geschäftsmässig begründete Zahlung oder Auftrag vorzunehmen (CEO-Fraud)
  - → Mitarbeitende sind nicht genügend geschult im Erkennen von Phishing (gefälschte Internetinhalte)
    - – Beitrag Newsletter VSV von Andreas Corradini (AXA), Dezember 2022

Externer Vermögensverwalter in der Presse

- «Bekannter Schweizer Vermögensverwalter gehackt – Daten im Darknet geleakt» (Schlagzeile vom 07.02.2023 bei Watson)
  - Kriminelle konnten in die Server der Finaport AG eindringen und grössere Datenmengen stehlen. Es ist von 1,2 Terabyte die Rede.
  - Unternehmen bestätigte, dass von den Servern gestohlene Daten im Darknet veröffentlicht wurden
  - Finaport benachrichtigte innert 24h die Behörden
  - Es waren von allen betroffenen Daten Backups vorhanden
  - Attacken werde es weiter geben. Die Quantität und Qualität sowie Komplexität nehme zu.
  - Die Meldepflicht der Beaufsichtigten gegenüber der FINMA sei ein wichtiges Instrument zur Erkennung von Cybervorfällen
  - Finaport kam gemäss Presse nicht ungeschoren davon. Weitere Informationen liegen öffentlich nicht vor.

1.3 Umfragen, Statistiken

AXA Cyber Studie und Polizeiliche Kriminalstatistik

15% der Unternehmen waren 2021 Opfer eines Angriffes

14% der kleineren KMU

29% der grossen KMU

Jedes

10.

Unternehmen wurde wiederholt angegriffen

33’345

Straftaten im Bereich der digitalen Kriminalität 2022

+10%

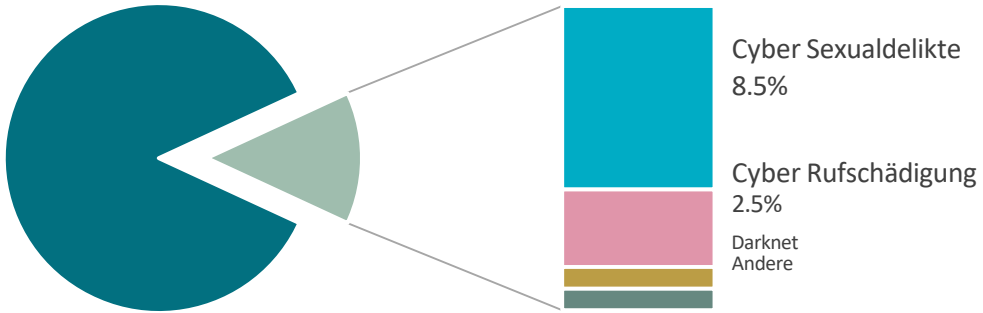
Steigerung von 2021 auf 2022

Quellen: AXA CH Studie, August 2022, Polizeiliche Kriminalstatistik 2022, 2023

Cyberkriminalität (digitale Kriminalität)

2022 wurden 33’345 Straftaten mit einer digitalen Komponente registriert
(+ 10% gegenüber 2021) – die Aufklärungsquote liegt bei 34.3%

Bereiche der digitalen Kriminalität



Cyber-Wirtschaftskriminalität 89.0% oder 29’677 Straftaten (z.B. Missbrauch von Zahlungssystemen, CEO- Fraud, digitaler Betrug)

Quelle: Polizeiliche Kriminalstatistik, Jahresbericht 2022, Neuenburg 2023

Cyberkriminalität (digitale Kriminalität)

Was waren 2022 die häufigsten Straftaten der Cyber-Wirtschaftskriminalität?

- Phishing: 2’236
- Hacking: Gewaltsames Eindringen in ein Datenverarbeitungssystem 246
- Hacking: Eindringen in ein Datenverarbeitungssystem mit fremden Zugangsdaten 796
- Malware –Ransomware 307
- Malware –E-Banking Trojaner 49
- Malware –Spyware 15
- Malware –Rogueware/Scareware 45

Quelle: Polizeiliche Kriminalstatistik, Jahresbericht 2022, Neuenburg 2023

KPMG-Studie e-Crime 2022

Begünstigende Faktoren

Nichterkennen erster Anzeichen: 84%
- 2019: 85%
- 2017: 80%
- 2015: 76%

Mangelnde Sicherheitskultur: 86%
- 2019: 86%
- 2017: 84%
- 2015: 77%

Unachtsamkeit: 95%
- 2019: 90%
- 2017: 89%
- 2015: 88%

Unzureichend geschultes Personal: 81%
- 2019: 83%
- 2017: 76%
- 2015: 60%

Zunehmende Komplexität eingesetzter Technologien: 78%
- 2019: 83%
- 2017: 81%
- 2015: 82%

Ungenügende Sicherheit der IT-Systeme: 61%
- 2019: 76%
- 2017: 68%
- 2015: 57%

“Das Risiko gibt es – aber mein Unternehmen betrifft es nicht”

Gefährlicher Irrglaube

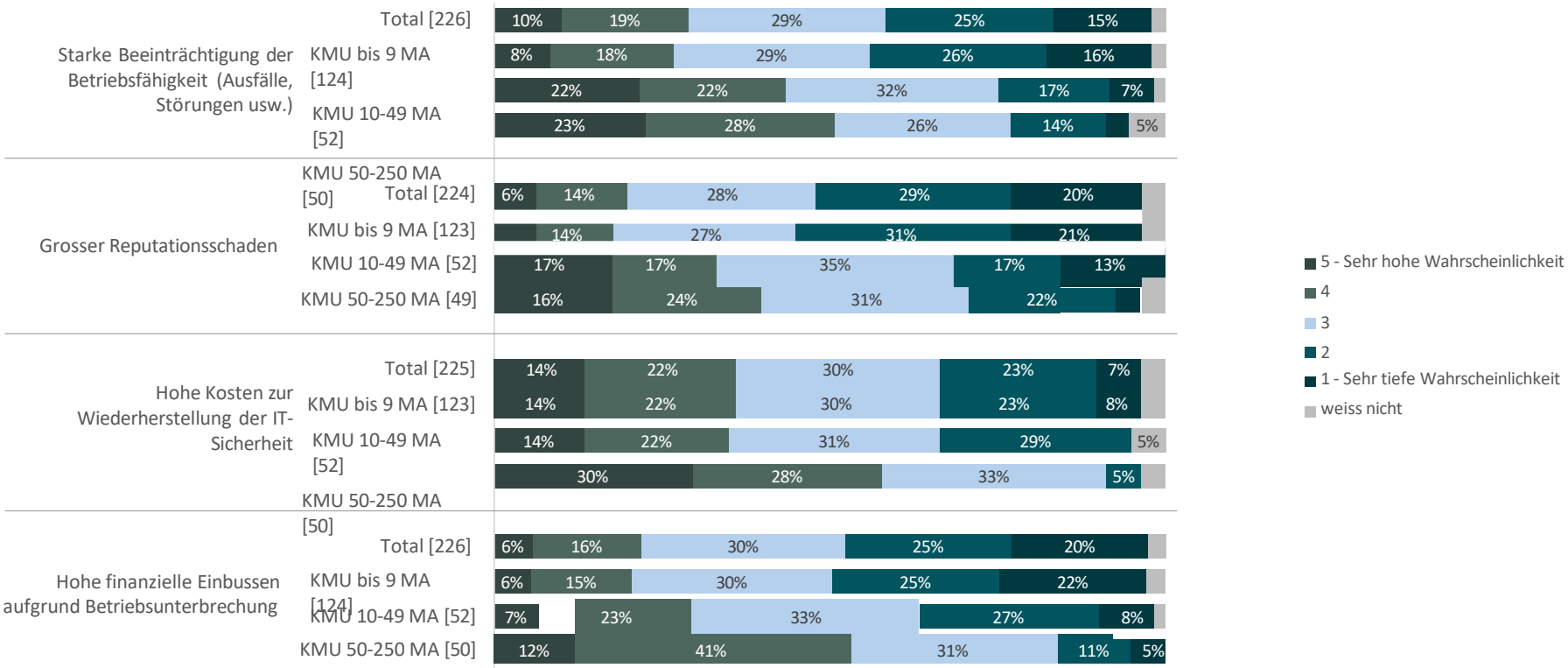
Von den Befragten, die nur ein geringes Risiko für das eigene Unternehmen sehen, sagen…

60%	81%	58%	70%
mein Unternehmen ist zu klein	unsere Computersysteme sind umfassend geschützt	wir waren noch nie Opfer einer Cyberattacke	unsere Daten sind nicht interessant

Quelle: Cybersecurity for SMES, Challenges and Recommendations, ENISA, Juni 2021

AXA Cyber Studie

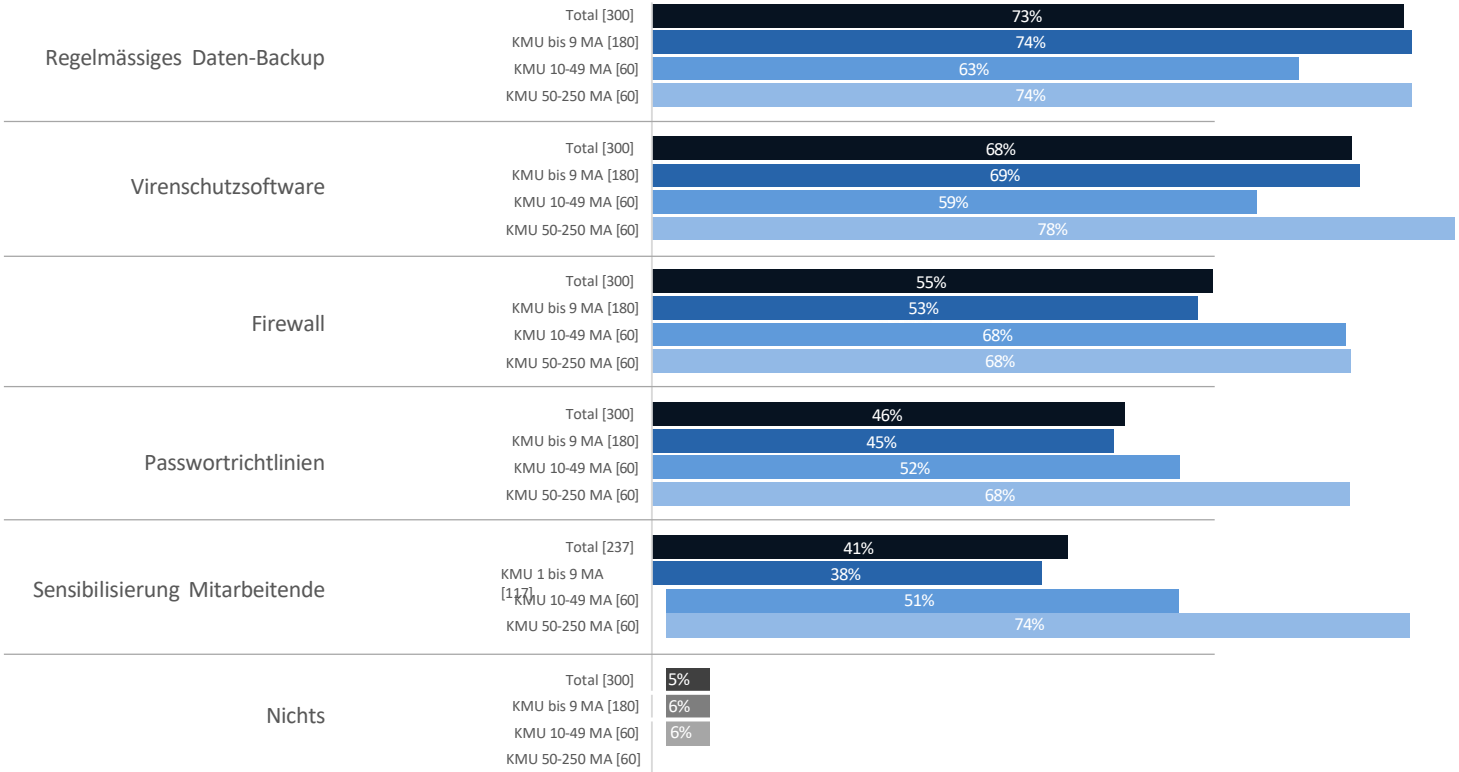
Mit welchen Folgen werden gerechnet?



Quelle: AXA CH Studie, August 2022

AXA Cyber Studie

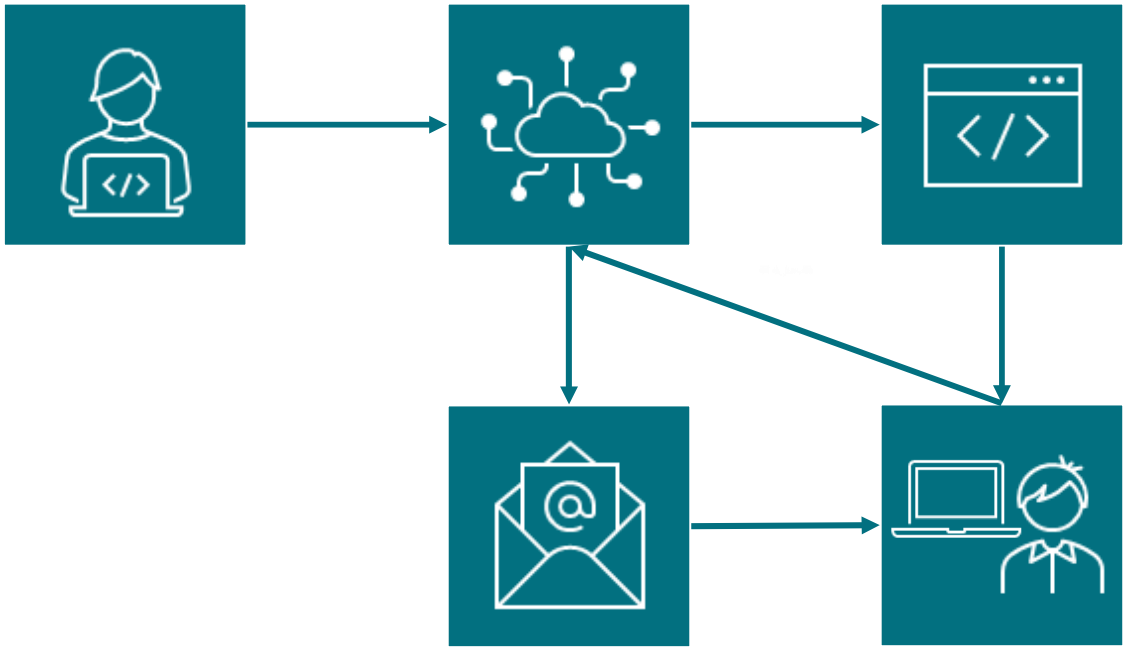
Ergriffene Massnahmen der Unternehmen



Quelle: AXA CH Studie, August 2022


2
Welche Versicherungsdeckungen gibt es?

Grundlagen - Cyberereignis



«…ein vorsätzlicher, schädigender Angriff…»

«…auf das *IT-System* des *Versicherungs-nehmers* oder auf *Cloud-Computing-Systeme*…»

AVB E2-E4

Grundlagen - Deckungen

Cyber-Eigenschaden-Ereignis	Cyber-Haftpflicht-Ereignis	Krisenmanagement	Zusatzdeckungen
			 Online Banking  Telefon-hacking  Social Engineering  Lösegeld-forderung
• Wiederherstellungskosten • Betriebsunterbruch • Datenschutzverletzung	• Entschädigung berechtigter Ansprüche • Abwehr unberechtigter Ansprüche	• Sofortmassnahmen • Krisenberatung • Krisenkommunikation	
AVB B1	AVB B2	AVB B3	AVB B4-B6

Grundlagen - Zusatzdeckungen

Manipulation E – Banking, des Webshops, oder des Warenversandes	Telefon-Hacking	Social Engineering	Lösegeldforderung
			
• Nicht autorisierte Zahlungen vom E-Banking • Diebstahl von Drittgeldern • Manipulation bei der Auslieferung von Waren • Für Eigenschäden und Haft	• Nutzung der Telefonanlage durch Dritte nach einem Cyber-Eigenschaden-Ereignis	• Betrug • Persönliche Kontakt-aufnahme vom Betrüger • Ausnützung Gutgläubigkeit etc.	• Inkl. Verhandlungskosten
AVB B4	AVB B5	AVB B6	AVB C1.12

Backup

- mind. alle 7 Tage (offline)
- Recoverytest empfohlen (nicht in AVB gefordert)

Sicherheitssysteme

- Antivirus
- Firewall, etc.

Updates

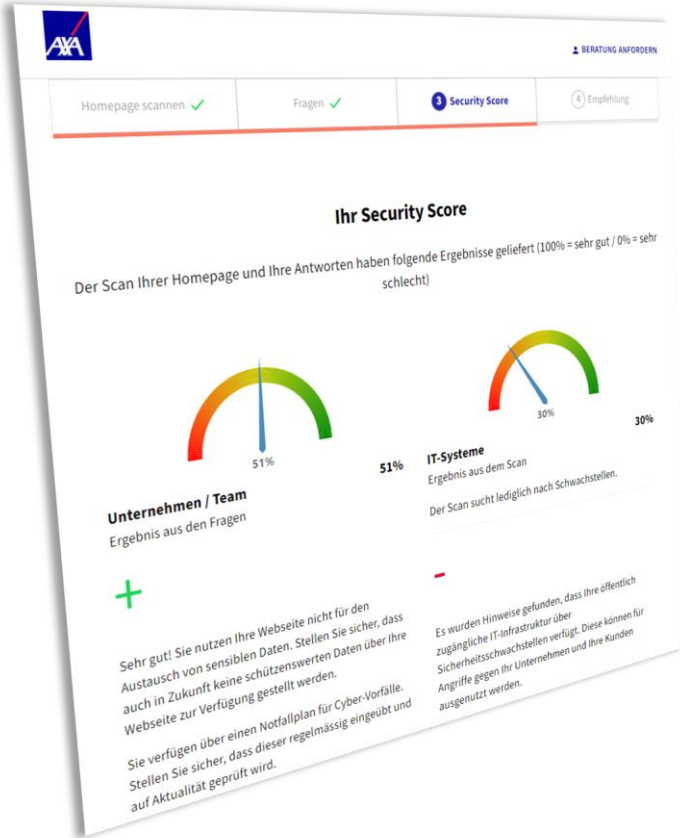
- Betriebs-, Sicherheits- und sonstige Systeme
- Zeitnah

«…gebotenen Massnahmen zum Schutz der versicherten *Daten* gegen die versicherten Gefahren….»

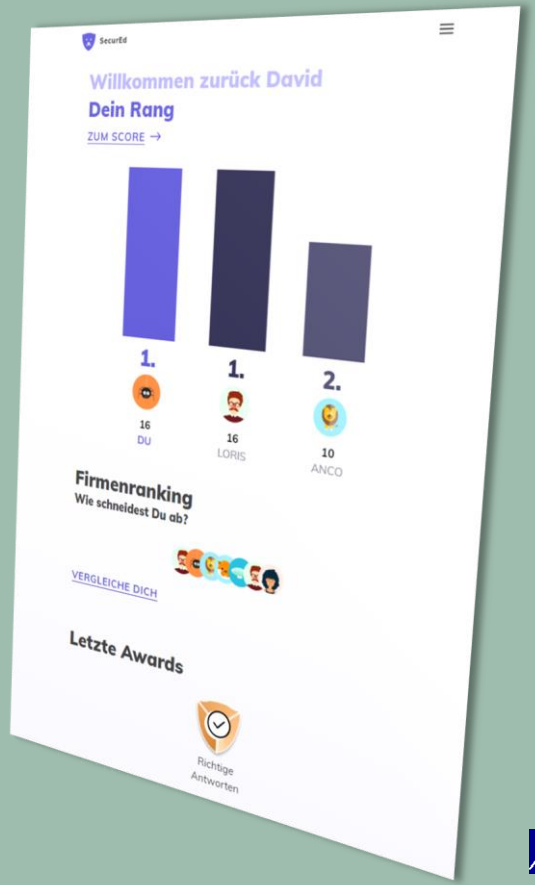
AVB A11


3
Services

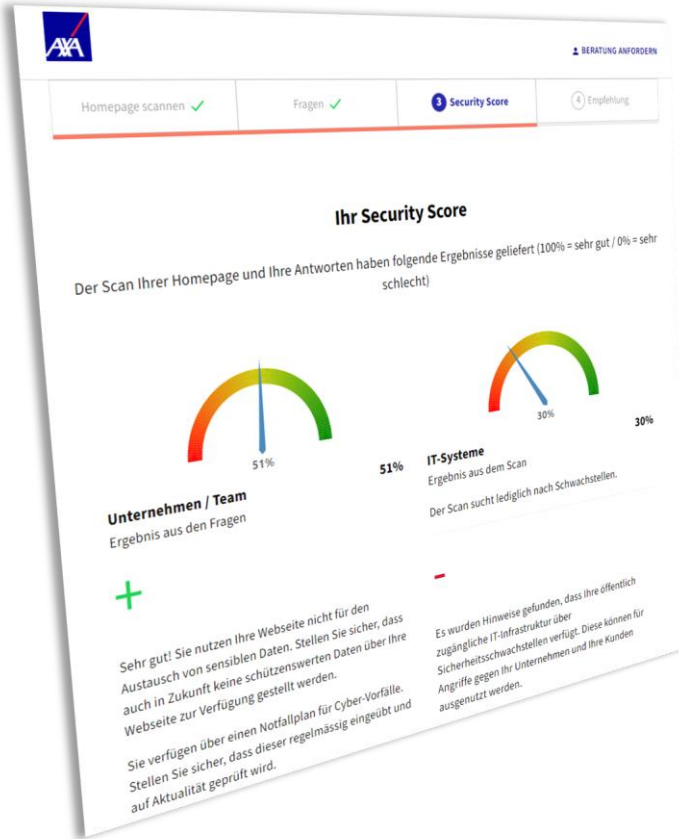
Cyber Check & Schutz



Cyber Präventionsservice



Cyber Check & Schutz



cyber-check.axa.ch

- ✓ Kurzer Selbsttest für KMU zu Cyberthemen
- ✓ Schaffung von Awareness
- ✓ Scan der Homepage via Vulnerability Test

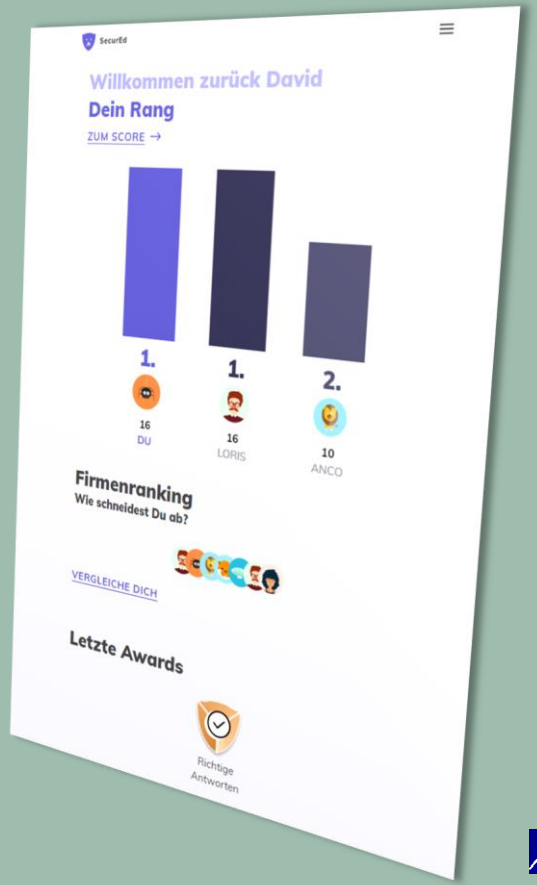
- ✓ **Es sind auch Offerten durch den Kunden möglich**

Cyber Präventionsservice

www.scrd.ch

- ✓ Schulungsplattform für Mitarbeiter
- ✓ Gamification für mehr Motivation
- ✓ Cyber Blog mit aktuellen Sicherheitslücken
- ✓ Vulnerability Scan – Aussenansicht der IT-Infrastruktur

- ✓ **Gratis – für jeden Cyberkunden der AXA**
- ✓ Registration unter www.axa.ch/cps



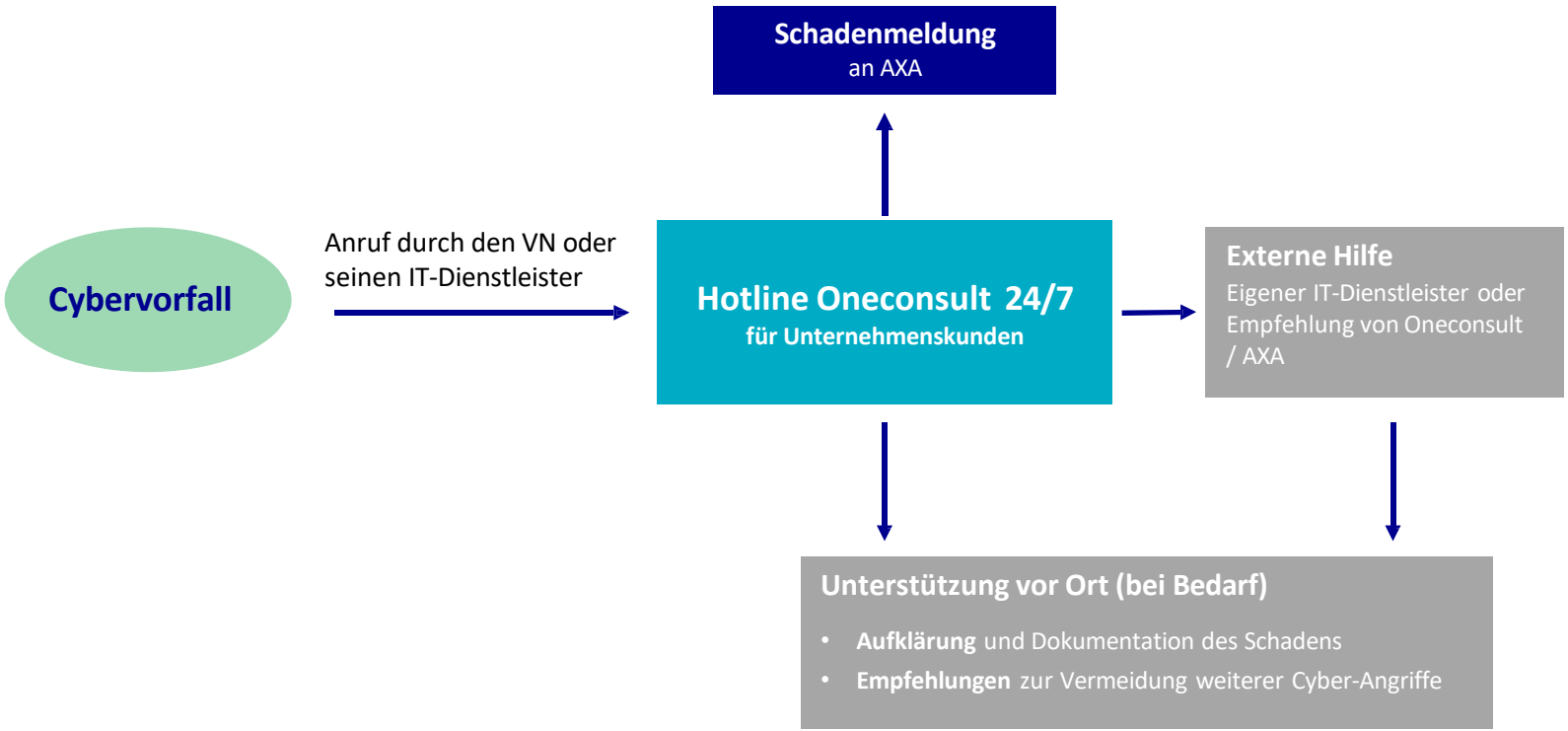

4
Schaden

Die drei Linien der Verteidigung

Cyber-Versicherung ist die 3. Linie der Verteidigung

Der Schadenmeldeprozess

Verhalten im Schadenfall bei Unternehmenskunden



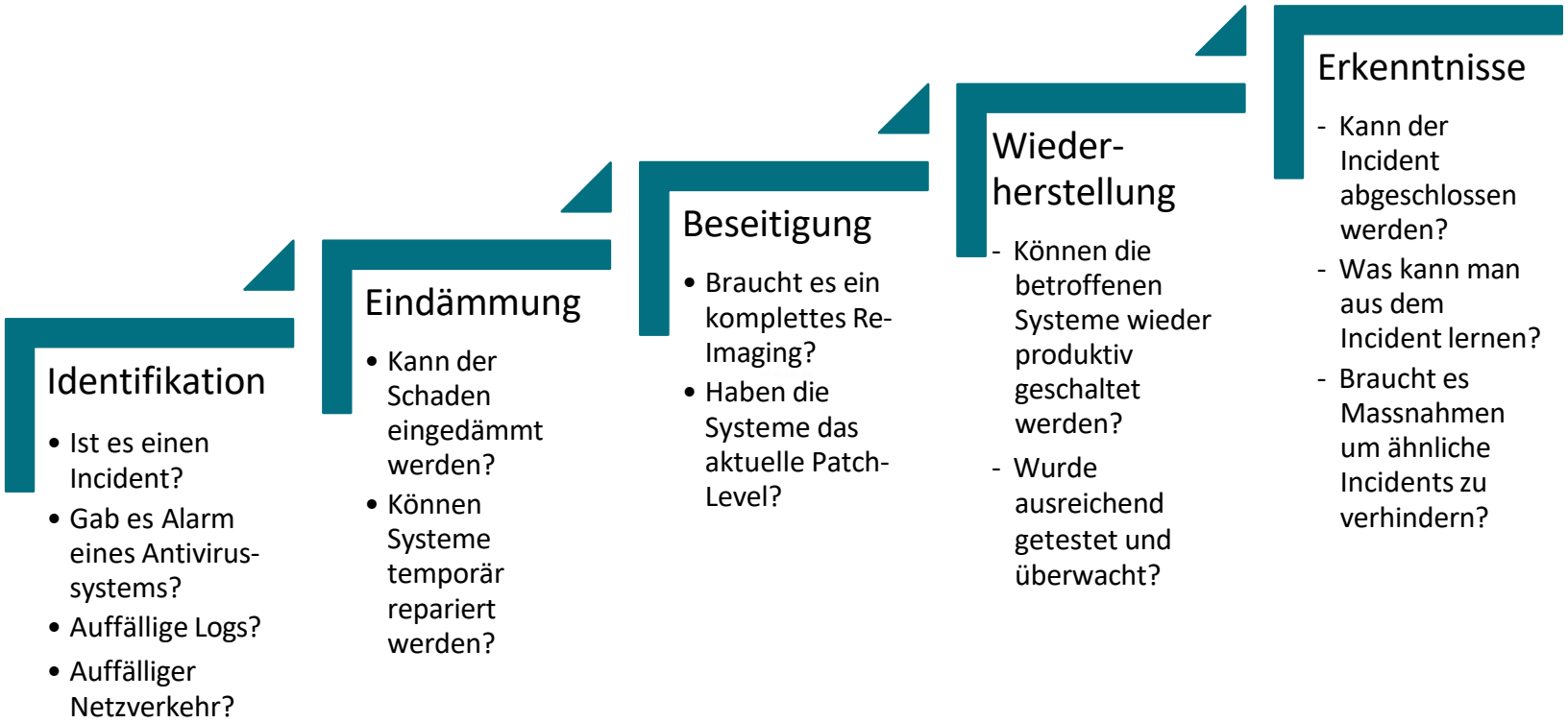
Soforthilfe im Cyber- Schadenfall

durch Oneconsult AG

- Experteneinschätzung zur geschilderten Lage
- Empfehlung von Sofortmassnahmen zur Schadensbegrenzung
- Empfehlung von Sofortmassnahmen zur Ursachenermittlung
- ersten Bewertung der bisherigen Massnahmen

- Hinsichtlich der Kosten für die Soforthilfe fällt weder ein Selbstbehalt an, noch werden die Kosten an der Versicherungssumme angerechnet.
- Dies gilt auch wenn es sich erweisen sollte, dass es sich nicht um einen nicht gedeckten Schadenfall handelt.
- Die Soforthilfe ist auf CHF 5’000 begrenzt. In dieser Zeit sollte Oneconsult abschätzen können, ob ein versichertes Ereignis vorliegt.

Phasen der Incident Response



Schadenbeispiel Müller und Meier

Intro Schadenbeispiel Müller & Meier

Müller & Meier
Vermögensverwaltung

- Externer Vermögensverwalter
- 5 Mitarbeiter mit Arbeitsplatz
- CHF 780’000 Umsatz
- Cyberversicherung Grunddeckung wurde kürzliche abgeschlossen

Schadenbeispiel Müller und Meier

Phase 1 BEC (Business Email Compromise)

Von: Nicole [redacted]
Gesendet: Dienstag, 31. Mai 2022 09:26
An: Gaetano [redacted]
Cc: Buchhaltung [redacted]
Betreff: Aw: Guten Morgen, fällige Rechnung

Hallo Gaetano,

Kannst du heute eine internationale Bankueberweisung machen? Sag mir bescheid, dann kann ich dir die Bankdaten und die Rechnung senden.

Mit Freundliche Grüße

Nicole [redacted]
Geschäftsführerin
[redacted]

Hallo Nicole

Ja, kann ich. Schick mir die Rechnung und Bankkoordinaten

Freundliche Grüsse

Gaetano [redacted]
Buchhaltung / Personal
[redacted]

Von: Nicole [redacted]
Gesendet: Donnerstag, 2. Juni 2022 08:18
An: Buchhaltung [redacted]
Betreff: Re: AW: AW: Guten Morgen, fällige Rechnung

Hallo Gaetano,

Senden Sie mir eine Zahlungsbestätigung.

Mit Freundliche Grüße

Nicole [redacted]
Geschäftsführerin
[redacted]

Schadenbeispiel Müller und Meier

Phase 1 BEC

- Durch eine gefälschte E-Mail wurde die Buchhaltung angehalten eine internationale Zahlung vorzunehmen

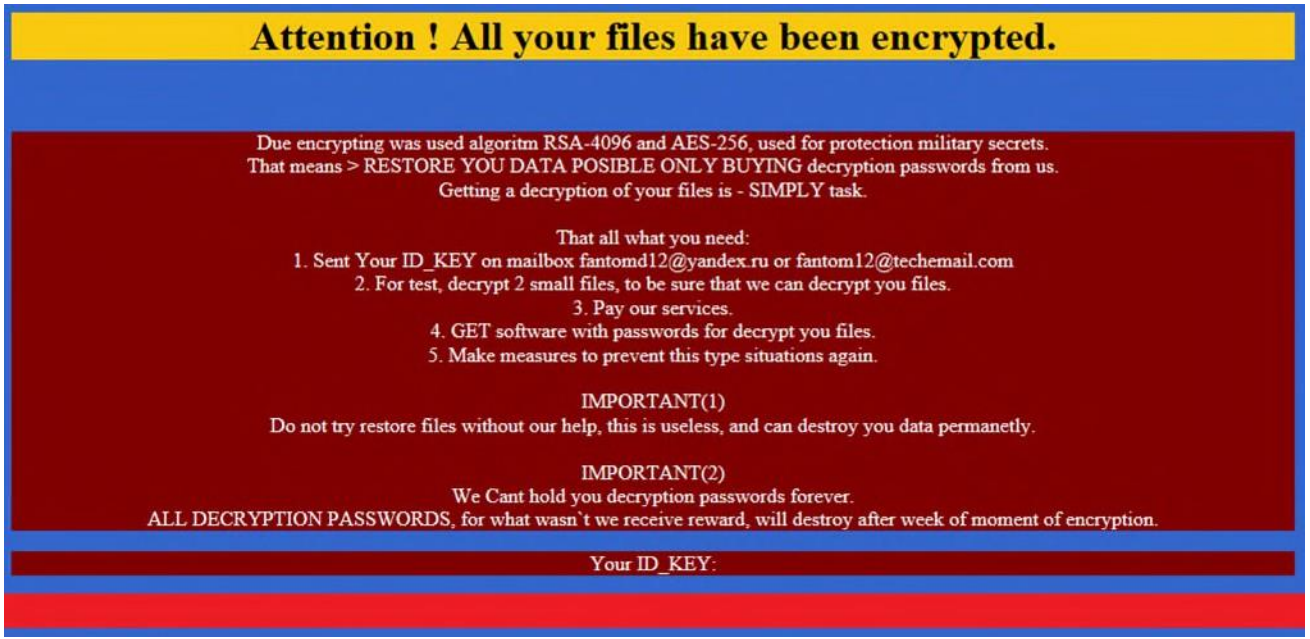
- Zahlung von 25’000 Euro an Täterschaft
- Zudem wurde eine Schadsoftware installiert und später aktiviert

- Deckung für Falschzahlung wurde abgelehnt, da Social Engineering nicht abgeschlossen wurde

Schadenbeispiel Müller und Meier

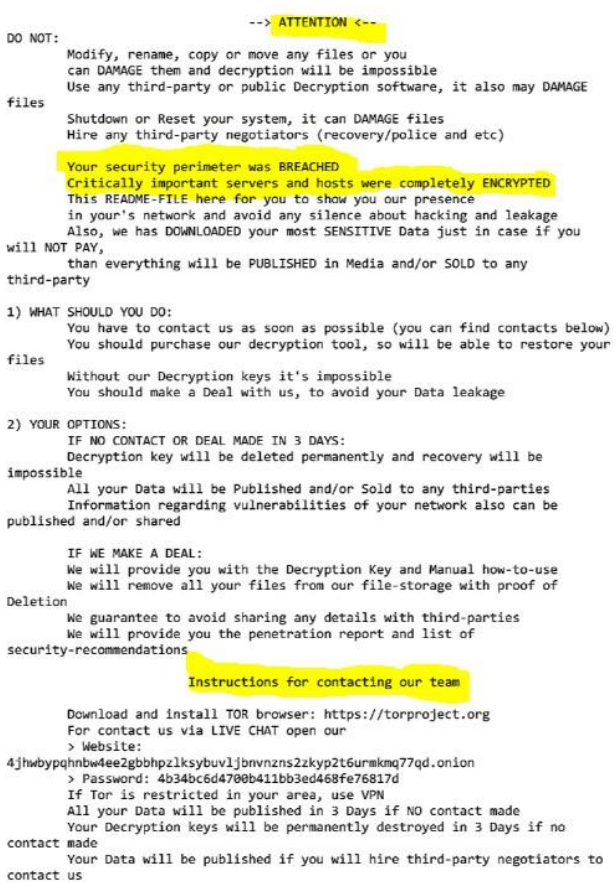
Phase 2 Ransomeware

Als Herr Tobler von Müller und Meier am Montagmorgen als erster den Computer starten will, erscheint folgende Mitteilung auf dem Bildschirm:



Schadenbeispiel Müller & Meier

Phase 2 Ransomware



```
                    --> ATTENTION <--
DO NOT:
        Modify, rename, copy or move any files or you
        can DAMAGE them and decryption will be impossible
        Use any third-party or public Decryption software, it also may DAMAGE
files
        Shutdown or Reset your system, it can DAMAGE files
        Hire any third-party negotiators (recovery/police and etc)

        Your security perimeter was BREACHED
        Critically important servers and hosts were completely ENCRYPTED
        This README-FILE here for you to show you our presence
        in your's network and avoid any silence about hacking and leakage
        Also, we has DOWNLOADED your most SENSITIVE Data just in case if you
will NOT PAY,
        than everything will be PUBLISHED in Media and/or SOLD to any
third-party

1) WHAT SHOULD YOU DO:
        You have to contact us as soon as possible (you can find contacts below)
        You should purchase our decryption tool, so will be able to restore your
files
        Without our Decryption keys it's impossible
        You should make a Deal with us, to avoid your Data leakage

2) YOUR OPTIONS:
        IF NO CONTACT OR DEAL MADE IN 3 DAYS:
        Decryption key will be deleted permanently and recovery will be
impossible
        All your Data will be Published and/or Sold to any third-parties
        Information regarding vulnerabilities of your network also can be
published and/or shared

        IF WE MAKE A DEAL:
        We will provide you with the Decryption Key and Manual how-to-use
        We will remove all your files from our file-storage with proof of
Deletion
        We guarantee to avoid sharing any details with third-parties
        We will provide you the penetration report and list of
security-recommendations

                    Instructions for contacting our team

        Download and install TOR browser: https://torproject.org
        For contact us via LIVE CHAT open our
        > Website:
4jhwbypqhnbw4ee2gbbhpzlksybuvljbnvnzns2zkyp2t6urmkmq77qd.onion
        > Password: 4b34bc6d4700b411bb3ed468fe76817d
        If Tor is restricted in your area, use VPN
        All your Data will be published in 3 Days if NO contact made
        Your Decryption keys will be permanently destroyed in 3 Days if no
contact made
        Your Data will be published if you will hire third-party negotiators to
contact us
```

Schadenbeispiel Müller & Meier

Phase 2 Ransomware

- Infektion eines einzelnen Clients durch Click auf einen Link
- Malware wurde nicht bemerkt

- Verschlüsselung der Server
- Clients ebenfalls grösstenteils verschlüsselt
- Lösegeldforderung in Form von Bitcoins

✓ Regelmässige Datensicherungen vorhanden
✗ Lokales Backup nicht brauchbar
✓ Offsite-Backup war intakt

Fazit: Schadenbeispiel Müller & Meier

Entschädigung	
Analyse Schaden, Systemüberprüfung	CHF 1’440.00
Wiederherstellung der Systeme	CHF 7’560.00
Div. Nachbesserung nach Wiederherstellung	CHF 2’880.00
Externe Kosten	
OneConsult Soforthilfe	CHF 600.00
Totale Entschädigung	**CHF 12’480.00**

Kommentare aus der IT:

- **Manchmal fühlt man sich als IT-ler wie ein Schafhirte. Allerdings sind die Schafe betrunken. Und brennen! Und klicken überall drauf! (Quelle: Henrik@Celilander)**

- **Motivation = Anreiz / Kosten (Quelle: Linus Neumann)**


5
Fragen und Diskussion

Vorteile AXA

Weshalb ist AXA der richtige Partner für Cyberversicherungen und Services

Die IT des KMU oder dessen IT-DL haben im Verdachtsfall einen **spezialisierten Ansprechpartner 24/7 zur Verfügung**

Der **Präventionsservice** ist **kostenlos** für Kunden mit einer Cyberpolice

Die **Soforthilfe** erfolgt für den Kunden **kostenlos**, auch ohne gedecktes Ereignis

Krisenmanagement durch ein geprüftes und bewährtes **Expertennetzwerk** (inkl. Deckung für PR-Kosten)

Mitglieder des VSV erhalten einen **Rabatt von 10%** auf die Cyberversicherung

Link zum Online-Rechner ➔ VSV Cyber-Angebot

Für weitere Fragen und Bemerkungen bitte E-Mail an unsere BOX

AXA Versicherungen AG

Fachbereich Cyberversicherungen

Unternehmenskunden

cyber.security@axa.ch

Exklusive Angebote für VSV Mitgliedsunternehmen | AXA

Vielen Dank für Ihre Aufmerksamkeit!